I. ОСНОВНІ ПОНЯТТЯ ТЕОРІЇ БУЛЕВИХ ФУНКЦІЙ

1. Булеві вектори

1.1. Основні означення

Нехай $\mathbb{Z}_2 = \{0,1\}$. Елементи множини $\mathbb{Z}_2$ називаються булевими константами.

Логічні операції над булевими змінними множини $\mathbb{Z}_2$: заперечення, кон'юнкція, диз'юнкція, імплікація, еквівалентність та додавання за модулем 2 $(\oplus)$.

$0 \oplus 0 = 0,\ \ 0 \oplus 1 = 1,\ 1 \oplus 0 = 1,\ 1 \oplus 1 = 0.$

Вектор (упорядкований набір) вигляду $\tilde{x} = (x_1, x_2, \ldots, x_n),\ x_i \in \mathbb{Z}_2$ називається *n-вимірним булевим вектором*. Множина усіх *n*-вимірних булевих векторів позначається $\mathbb{Z}_2^n$. Тобто, $\mathbb{Z}_2^n = \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2}_{n \text{ множників}}$.

Кожному булевому вектору $\tilde{x} = (x_1, x_2, \ldots, x_n)$ ставиться у відповідність його номер $N(\tilde{x})$, який визначається наступним чином

$$N(\tilde{x}) = x_1 \cdot 2^{n-1} + x_2 \cdot 2^{n-2} + \ldots + x_{n-1} \cdot 2 + x_n.$$

Легко бачити, що для номера *n*-вимірного булевого вектора виконуються нерівності

$$0 \le N(\tilde{x}) < 2^n.$$

Приклад 1. Нехай $\tilde{x} = (0,1,0,1,1,0,1) \in \mathbb{Z}_2^7$. Тоді

$$N(\tilde{x}) = 0 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 = 32 + 8 + 4 + 1 = 45.$$

Приклад 2. Вказати вектор $\tilde{x} \in \mathbb{Z}_2^9$, номер якого рівний 117.

$$117 = 64 + 53 = 64 + 32 + 21 = 64 + 32 + 16 + 5 = 64 + 32 + 16 + 4 + 1 = 2^6 + 2^5 + 2^4 + 2^2 + 2^0.$$

Тому $\tilde{x} = (0,0,1,1,1,0,1,0,1)$.

Теорема 1. Кількість *n*-вимірних булевих векторів рівна 2^n.

Доведення. Скористаємося комбінаторним правилом множення, згідно до якого $|A \times B| = |A| \cdot |B|$, де $|A|$ — потужність множини *A*. Отримаємо

$$|\mathbb{Z}_2^n| = |\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2| = |\mathbb{Z}_2| \cdot |\mathbb{Z}_2| \cdot \ldots \cdot |\mathbb{Z}_2| = 2 \cdot 2 \cdot \ldots \cdot 2 = 2^n.$$

Мірою "близькості" між *n*-вимірними булевими векторами $\tilde{x} = (x_1, \ldots, x_n)$ та $\tilde{y} = (y_1, \ldots, y_n)$ є *відстань Хеммінга* $d(\tilde{x}, \tilde{y})$, яка визначається наступним чином:

$$d(\tilde{x},\tilde{y})=\sum_{i=1}^{n}|x_i-y_i|.$$

Приклад 3. Обчислити відстань Хеммінга між векторами $\tilde{x}=(0,1,0,1,1,0,1)$ та $\tilde{y}=(1,1,0,0,1,0,0)$.

$d(\tilde{x},\tilde{y})=1+0+0+1+0+0+1=3.$

Відстань Хеммінга між двома векторами чисельно рівна кількості координат, у яких відрізняються ці вектори. Якщо $d(\tilde{x},\tilde{y})=1$, то вектори $\tilde{x}$ та $\tilde{y}$ називаються *сусідніми*.

Властивості відстані Хеммінга:

$d(\tilde{x},\tilde{y})\geq 0,\quad d(\tilde{x},\tilde{y})=0\Leftrightarrow\tilde{x}=\tilde{y};$

$d(\tilde{x},\tilde{y})=d(\tilde{y},\tilde{x});$

для довільних $\tilde{x},\tilde{y},\tilde{z}\in\mathbb{Z}_2^n$ $d(\tilde{x},\tilde{y})\leq d(\tilde{x},\tilde{z})+d(\tilde{z},\tilde{y})$ (нерівність трикутника).

Величина $\|\tilde{x}\|=\sum_{i=1}^{n}x_i$ називається *нормою Хеммінга* булевого вектора $\tilde{x}$. Норма Хеммінга булевого вектора рівна кількості одиничних компонент вектора.

1.2. Операції над булевими векторами

Над булевими векторами можна виконувати *логічні операції*, застосовуючи їх до відповідних компонент цих векторів. Тобто, якщо $\tilde{x}=(x_1,\ldots,x_n)$, $\tilde{y}=(y_1,\ldots,y_n)$, то

$$\bar{\tilde{x}}=(\overline{x_1},\ldots,\overline{x_n});$$

$$\tilde{x}\wedge\tilde{y}=(x_1\wedge y_1,\ldots,x_n\wedge y_n);$$

$$\tilde{x}\vee\tilde{y}=(x_1\vee y_1,\ldots,x_n\vee y_n);$$

$$\tilde{x}\oplus\tilde{y}=(x_1\oplus y_1,\ldots,x_n\oplus y_n).$$

Приклад 4. Нехай $\tilde{x}=(1,0,1,1,0,0,1)$ та $\tilde{y}=(0,1,0,1,0,1,1)$. Тоді

$\bar{\tilde{x}}=(0,1,0,0,1,1,0)$, $\tilde{x}\wedge\tilde{y}=(0,0,0,1,0,0,1)$, $\tilde{x}\vee\tilde{y}=(1,1,1,1,0,1,1)$, $\tilde{x}\oplus\tilde{y}=(1,1,1,0,0,1,0)$.

Також до булевих векторів можна застосовувати *операції зсуву*. Виокремлюють *логічний* та *циклічний* зсув.

Результатом застосування операції логічного зсуву вектора $\tilde{x}=(x_1,\ldots,x_k,x_{k+1},\ldots,x_n)$ на k позицій вліво є вектор $\tilde{x}<<k=(x_{k+1},\ldots,x_n,0,\ldots,0)$.

Результатом застосування операції логічного зсуву вектора $\tilde{x}=(x_1,\ldots,x_{n-k},x_{n-k+1},\ldots,x_n)$ на k позицій вправо є вектор $\tilde{x}>>k=(0,\ldots,0,x_1,\ldots,x_{n-k})$.

Результатом застосування операції циклічного зсуву вектора $\tilde{x}=(x_1,\ldots,x_k,x_{k+1},\ldots,x_n)$ на k позицій вліво є вектор $\tilde{x}<<<k=(x_{k+1},\ldots,x_n,x_1,\ldots,x_k)$.

Результатом застосування операції циклічного зсуву вектора $\tilde{x}=(x_1,\ldots,x_{n-k},x_{n-k+1},\ldots,x_n)$ на k позицій вправо є вектор $\tilde{x}>>>k=(x_{n-k+1},\ldots,x_n,x_1,\ldots,x_{n-k})$.

Приклад 5. Нехай $\tilde{x}=(1,0,1,1,0,0,1)$. Тоді

$\tilde{x}<<2=(1,1,0,0,1,0,0)$, $\tilde{x}>>2=(0,0,1,1,0,0,1)$,

$\tilde{x}<<<2=(1,1,0,0,1,1,0)$, $\tilde{x}>>>2=(0,1,1,0,1,1,0)$.

Приклад 6. Знайти $(\tilde{x}<<<5)\oplus(\overline{\tilde{y}}>>\|\tilde{x}\|)$, де $\tilde{y}\in\mathbb{Z}_2^8$, $N(\tilde{y})=111$, $\tilde{x}=(1,0,1,0,0,1,0,0)$.

Задача 1. Записати $d(\tilde{x},\tilde{y})$ за допомогою операцій над булевими векторами та норми Хеммінга.

Задача 2. Визначити властивості бінарного відношення сусідства на множині n-місних булевих векторів та знайти його транзитивне замикання.

2. Булеві функції

2.1. Булеві функції. Основні означення

Функції вигляду $f:\mathbb{Z}_2^n \to \mathbb{Z}_2$ називаються *n*-місними *булевими функціями* (функціями двозначної логіки). Тобто, аргументами булевих функцій є *n*-вимірні булеві вектори, а значеннями — 0 або 1. Позначимо через P_2 множину усіх булевих функцій.

Оскільки область значень булевої функції (БФ) скінченна, то її можна задавати за допомогою таблиць значень. Для того, щоб задати *n*-місну БФ, достатньо вказати її на значення на кожному з 2^n булевих наборів (векторів). Якщо домовитися, що набори впорядковані у порядку зростання їх номерів, то кожна *n*-місна БФ $f(x_1,\ldots,x_n)$ однозначно задається вектором $\tilde{f} = (f_0, f_1, \ldots . f_{2^n-1})$, де f_k — значення функції *f* на наборі, номер якого рівний *k*.

Теорема 2. Кількість різних *n*-місних булевих функцій рівна 2^{2^n}.

Доведення. Кількість *n*-місних БФ співпадає із кількістю усіх можливих 2^n-вимірних булевих векторів вигляду $\tilde{f} = (f_0, f_1, \ldots . f_{2^n-1})$. За теоремою попереднього параграфу ця кількість рівна 2^{2^n}.

Номером булевої функції $f(x_1,\ldots,x_n)$ називається номер $N(\tilde{f})$, де $\tilde{f}$ — вектор значень функції *f*.

Приклад 7. Вказати таблицю значень БФ $f(x_1, x_2, x_3)$, якщо $N(\tilde{f}) = 43$.

$43 = 32 + 11 = 32 + 8 + 3 = 32 + 8 + 2 + 1 = 2^5 + 2^3 + 2^1 + 2^0$.

Тому $\tilde{f} = (0,0,1,0,1,0,1,1)$. Тоді таблиця значень БФ має наступний вигляд.

x_1	x_2	x_3	f
0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	1

Змінна x_k називається *суттєвої змінною* функції $f(x_1,\ldots,x_n)$, якщо існує такий набір $(\alpha_1,\ldots,\alpha_k,\ldots,\alpha_n) \in \mathbb{Z}_2^n$, що $f(\alpha_1,\ldots,\alpha_k,\ldots,\alpha_n) \neq f(\alpha_1,\ldots,\bar{\alpha}_k,\ldots,\alpha_n)$. У протилежному випадку змінна x_k називається *фіктивною*.

Якщо $g(x_1,\ldots,x_{k-1},x_{k+1},\ldots,x_n) = f(x_1,\ldots,x_{k-1},0,x_{k+1},\ldots,x_n)$ і x_k — фіктивна змінна функції $f(x_1,\ldots,x_{k-1},x_k,x_{k+1},\ldots,x_n)$, то кажуть, що функцію $g(x_1,\ldots,x_{k-1},x_{k+1},\ldots,x_n)$ отримано із функції $f(x_1,\ldots,x_{k-1},x_k,x_{k+1},\ldots,x_n)$ шляхом *видалення фіктивної змінної* x_k (функцію f отримано із g шляхом *введення фіктивної змінної*).

БФ функції f_1 та f_2 будемо вважати рівними, якщо одну із них можна отримати із іншої за допомогою видалення чи введення фіктивних змінних.

Приклад 8. Вказати суттєві змінні БФ $f(x_1, x_2, x_3)$, якщо $\tilde{f} = (1,1,1,1,0,1,0,1)$. Видалити фіктивні змінні.

Запишемо таблицю значень БФ *f*.

x_1	x_2	x_3	f
0	0	0	1
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Змінна x_1 є суттєвою, оскільки $f(0,0,0)=1$, а $f(1,0,0)=0$.

Змінна x_2 є фіктивною, оскільки $f(0,0,0)=f(0,1,0)=1$, $f(0,0,1)=f(0,1,1)=1$, $f(1,0,0)=f(1,1,0)=0$ та $f(1,0,1)=f(1,1,1)=1$.

Змінна x_3 є суттєвою, оскільки $f(1,0,0)=0$, а $f(1,0,1)=1$.

Перейдемо до видалення фіктивної змінної x_2. Для цього у таблиці значень функції f закреслимо стовпчик, який відповідає змінній x_2 та ті рядки, які відповідають наборам, у яких $x_2=1$. У результаті отримаємо $g(x_1,x_3)=f(x_1,x_2,x_3)$.

x_1	x_3	g
0	0	1
0	1	1
1	0	0
1	1	1

2.2. Елементарні булеві функції

Розглянемо *n*-місні БФ у випадку $n\in\{0,1,2\}$.

Якщо $n=0$, то отримуємо 0-місні БФ, які не залежать від жодної змінної, тобто є булевими константами 0 або 1.

Якщо $n=1$, то за теоремою 2 маємо $2^{2^1}=4$ різних одномісних БФ, які наведені у наступній таблиці

x	f_0	f_1	f_2	f_3
0	0	0	1	1
1	0	1	0	1

Індекс функції у таблиці співпадає із номером вектора її значень. Легко переконатися, що $f_0=0$, $f_3=1$ (у цих функціях змінна x є фіктивною), $f_1=x$, $f_2=\overline{x}$.

Якщо $n=2$, то за теоремою 2 маємо $2^{2^2}=16$ різних двомісних БФ, які наведені у наступній таблиці

x	y	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Проведемо аналіз отриманих двомісних БФ.

Розглянемо функції 0, 1 та 2 змінних (операції).

$f_0 = 0,\ f_{15} = 1.$

$f_3 = x,\ f_{12} = \overline{x},\ f_5 = y,\ f_{10} = \overline{y}.$

$f_1(x,y) = x \wedge y,\ f_7(x,y) = x \vee y,$

$f_{13}(x,y) = x \Rightarrow y,\ f_{11}(x,y) = y \Rightarrow x,$

$f_9(x,y) = x \Leftrightarrow y,\ f_6(x,y) = x \oplus y.$

Функція $f_{14}(x,y) = \overline{x \wedge y}$ називається *функцією Шеффера* (штрих Шеффера) і позначається $x \mid y$.

Функція $f_8(x,y) = \overline{x \vee y}$ називається *функцією Пірса* (стрілка Пірса) і позначається $x \downarrow y$.

Розглянуті двомісні БФ (усі функції із попередньої таблиці крім f_2 та f_4) називаються *елементарними булевими функціями* (*операціями двозначної логіки*).

2.3. Реалізація булевих функцій формулами

Суперпозиція булевих функцій — підстановка замість аргументів однієї БФ інших БФ. За допомогою суперпозиції можна отримати нові функції, використовуючи елементарні функції.

Нехай F — деяка підмножина функцій із P_2. Тоді

1) кожна функція $f \in F$ є *формулою над множиною F*;

2) якщо $f(x_1,\ldots,x_n) \in F$, $A_1,\ldots,A_n$ — вирази, які є або формулами над F, або символами змінних, тоді вираз $f(A_1,\ldots,A_n)$ — є *формулою над множиною F*.

Приклад 9. Нехай F — множина елементарних функцій. Тоді наступні вирази будуть формулами над F:

$$(x_1 \wedge x_2) \oplus (x_3 \Rightarrow \overline{x}_1);$$

$$\overline{(x_1 \downarrow x_3) \Leftrightarrow \overline{x_2 \mid x_1}}.$$

Кожній формулі φ, побудованій за допомогою застосування скінченної кількості правил вигляду a) – b), можна поставити відповідність булеву функцію f_φ, яку задає ця формула.

Приклад 10. Вказати номер булевої функції $f(x_1, x_2, x_3)$, яка задається формулою

$$(\overline{x}_3 \mid x_1) \oplus \overline{x_3 \Rightarrow (x_1 \downarrow x_2)}.$$

x_1	x_2	x_3	$\overline{x}_3$	$\overline{x}_3 \mid x_1$	$x_1 \downarrow x_2$	$x_3 \Rightarrow (x_1 \downarrow x_2)$	$\overline{x_3 \Rightarrow (x_1 \downarrow x_2)}$	$f(x_1, x_2, x_3)$
0	0	0	1	1	1	1	0	1
0	0	1	0	1	1	1	0	1
0	1	0	1	1	0	1	0	1
0	1	1	0	1	0	0	1	0
1	0	0	1	0	0	1	0	0
1	0	1	0	1	0	0	1	0
1	1	0	1	0	0	1	0	0
1	1	1	0	1	0	0	1	0

Тоді $N(\tilde{f}) = 2^7 + 2^6 + 2^5 = 224.$

При записі формул застосовують той самий пріоритет логічних операцій, що й алгебрі висловлювань. Для спрощення запису будемо записувати кон'юнкцію $x \wedge y$ у вигляді xy. Крім того будемо вважати, що пріоритет операції додавання за модулем 2 нижчий за пріоритет кон'юнкції.

Дві формули φ та ψ назвемо *рівносильними* (*еквівалентними*), якщо відповідні їм булеві функції f_φ та f_ψ рівні. Для формул зберігаються усі рівносильності логіки висловлювань. Крім того, операція додавання за модулем 2 має наступні властивості:

1. $x \oplus y = y \oplus x$;

2. $x \oplus (y \oplus z) = (x \oplus y) \oplus z$;

3. $x(y \oplus z) = xy \oplus xz$;

4. $x \oplus 0 = x$;

5. $x \oplus 1 = \bar{x}$;

6. $x \oplus y = \overline{x \Leftrightarrow y}$;

7. $x \oplus y = x\bar{y} \vee \bar{x}y$.

2.4. Двоїсті булеві функції

Функція $f^*(x_1,\ldots,x_n) = \overline{f(\bar{x}_1,\ldots,\bar{x}_n)}$ називається *двоїстою функцією* до БФ $f(x_1,\ldots,x_n)$.

Очевидно, що таблиця для двоїстої функції (при фіксованому порядку наборів) отримується із таблиці функції $f(x_1,\ldots,x_n)$ інвертуванням (тобто замінною 0 на 1 і навпаки) стовпця значень функції та його "перевертанням".

Приклад 11. Вказати двоїсті функції до функції $0, 1, x, \bar{x}, x \wedge y, x \vee y, x \Leftrightarrow y$.

Будемо розглядати усі функції прикладу як функції двох змінних. Тоді

x	y	0	0^*	1	1^*	x	x^*	$\overline{x}$	$\overline{x}^*$	xy	$(xy)^*$	$x \vee y$	$(x \vee y)^*$	$x \Leftrightarrow y$	$(x \Leftrightarrow y)^*$
0	0	0	1	1	0	0	0	1	1	0	0	0	0	1	0
0	1	0	1	1	0	0	0	1	1	0	1	1	0	0	1
1	0	0	1	1	0	1	1	0	0	0	1	1	0	0	1
1	1	0	1	1	0	1	1	0	0	1	1	1	1	1	0

Як видно з попередньої таблиці

a) $0^* = 1$;

b) $1^* = 0$;

c) $x^* = x$;

d) $\overline{x}^* = \overline{x}$;

e) $(xy)^* = x \vee y$;

f) $(x \vee y)^* = xy$;

g) $(x \Leftrightarrow y)^* = x \oplus y$.

Співвідношення a) – g) також можна отримати безпосередньо на основі означення операції двоїстості. Наприклад, якщо $f(x, y) = xy$, то $f^*(x, y) = \overline{f(\overline{x}, \overline{y})} = \overline{\overline{x} \wedge \overline{y}} = x \vee y$.

Теорема 3. Операція двоїстості має наступні властивості на множині P_2:

1) якщо $g = f^*$, то $f = g^*$, тобто $\left(f^*\right)^* = f$ (властивість взаємності);

2) якщо $g(x_1,\ldots,x_n) = f\left(f_1(x_1,\ldots,x_n),\ldots,f_m(x_1,\ldots,x_n)\right)$, то $g^* = f^*\left(f_1^*,\ldots,f_m^*\right)$ (функція, двоїста до суперпозиції функцій, є суперпозицією двоїстих функцій).

Доведення.

1) Нехай $g(x_1,\ldots,x_n) = \overline{f(\overline{x}_1,\ldots,\overline{x}_n)}$. Тоді $g^*(x_1,\ldots,x_n) = \overline{g(\overline{x}_1,\ldots,\overline{x}_n)} = \overline{\overline{f(\overline{\overline{x}}_1,\ldots,\overline{\overline{x}}_n)}} = f(x_1,\ldots,x_n)$.

2) $g^*(x_1,\ldots,x_n) = \overline{g(\overline{x}_1,\ldots,\overline{x}_n)} = \overline{f\left(f_1(\overline{x}_1,\ldots,\overline{x}_n),\ldots,f_m(\overline{x}_1,\ldots,\overline{x}_n)\right)} = \overline{f\left(\overline{\overline{f_1(\overline{x}_1,\ldots,\overline{x}_n)}},\ldots,\overline{\overline{f_m(\overline{x}_1,\ldots,\overline{x}_n)}}\right)} =$

$= f^*\left(\overline{f_1(\overline{x}_1,\ldots,\overline{x}_n)},\ldots,\overline{f_m(\overline{x}_1,\ldots,\overline{x}_n)}\right) = f^*\left(f_1^*(x_1,\ldots,x_n),\ldots,f_m^*(x_1,\ldots,x_n)\right)$.

Наслідком теореми 3 є *принцип двоїстості*: для того, щоб отримати двоїсту формулу до формули φ над множиною $\{0,1,\overline{x},x\wedge y,x\vee y\}$, треба у формулі φ всюди замінити

0 на 1, 1 на 0, $\wedge$ на $\vee$, $\vee$ на $\wedge$.

Приклад 12. Вказати формулу, двоїсту до формули $\left(\overline{x}\vee 0\vee\overline{x\wedge y}\right)\wedge\left(\overline{y\wedge 1}\vee x\vee\overline{z}\right)$.

$$\left(\left(\bar{x}\vee 0\vee\overline{x\wedge y}\right)\wedge\left(\overline{y\wedge 1}\vee x\vee\bar{z}\right)\right)^{*}=\left(\bar{x}\wedge 1\wedge\overline{x\vee y}\right)\vee\left(\overline{y\vee 0}\wedge x\wedge\bar{z}\right)$$

Приклад 13. Вказати двоїсту до функції $f\left(x,y,z\right)=\left(\bar{x}\vee z\right)\oplus\bar{y}x$.

$$f^{*}\left(x,y,z\right)=\left(\left(\bar{x}\vee z\right)\oplus\bar{y}x\right)^{*}=\left(\bar{x}\vee z\right)^{*}\Leftrightarrow\left(\bar{y}x\right)^{*}=\left(\bar{x}\right)^{*}z^{*}\Leftrightarrow\left(\bar{y}\right)^{*}\vee x^{*}=\bar{x}z\Leftrightarrow\bar{y}\vee x.$$

Якщо для БФ $f\left(x_1,\ldots,x_n\right)$ виконується умова $f^{*}\left(x_1,\ldots,x_n\right)=f\left(x_1,\ldots,x_n\right)$, то функція $f\left(x_1,\ldots,x_n\right)$ називається *самодвоїстою*.

Приклад 14. Довести, що БФ $x\oplus y\oplus z$ є самодвоїстою.

$$\left(x\oplus y\oplus z\right)^{*}=\left(x\oplus y\right)^{*}\Leftrightarrow z^{*}=\left(x^{*}\Leftrightarrow y^{*}\right)\Leftrightarrow z=\left(x\Leftrightarrow y\right)\Leftrightarrow z=\overline{x\Leftrightarrow y}\oplus z=x\oplus y\oplus z.$$

3. Спеціальні форми подання булевих функцій

Постає питання, чи можна записати довільну булеву функцію у вигляді формули?

3.1. Розклад булевих функцій за змінними

Нехай $\sigma\in\mathbb{Z}_2$. Уведемо позначення

$$x^{\sigma} = \begin{cases} x, & \text{якщо } \sigma = 1, \\ \overline{x}, & \text{якщо } \sigma = 0. \end{cases}$$

Легко переконатися, що

1) $x^{\sigma} = x\sigma \vee \overline{x}\overline{\sigma}$;

2) $x^{\sigma} = 1$ тоді і тільки тоді, коли $x = \sigma$.

Теорема 4 (про розклад булевої функції за однією змінною). Для довільної булевої функції $f(x_1, \ldots, x_n)$ справджується співвідношення

$$f(x_1, \ldots, x_{n-1}, x_n) = \overline{x}_n \wedge f(x_1, \ldots, x_{n-1}, 0) \vee x_n \wedge f(x_1, \ldots, x_n, 1). \qquad (1)$$

Доведення. Розглянемо довільний булевий вектор $(\alpha_1, \ldots, \alpha_{n-1}, \alpha_n)$ і покажемо, що для нього ліва та права частини (1) приймають однакові значення.

Якщо $\alpha_n = 0$, то ліва частина (1) рівна $f(\alpha_1, \ldots, \alpha_{n-1}, 0)$, а права —

$$\overline{0} \wedge f(\alpha_1, \ldots, \alpha_{n-1}, 0) \vee \overline{1} \wedge f(\alpha_1, \ldots, \alpha_{n-1}, 1) = f(\alpha_1, \ldots, \alpha_{n-1}, 0).$$

Якщо $\alpha_n = 1$, то ліва частина (1) рівна $f(\alpha_1, \ldots, \alpha_{n-1}, 1)$, а права —

$$\overline{1} \wedge f(\alpha_1, \ldots, \alpha_{n-1}, 0) \vee \overline{0} \wedge f(\alpha_1, \ldots, \alpha_{n-1}, 1) = f(\alpha_1, \ldots, \alpha_{n-1}, 1).$$

В обох випадках (1) справджується. Теорему доведено.

Шляхом багаторазового застосування теореми 4 можна отримати *теорему про розклад БФ за змінними*.

Теорема 5. Для довільної булевої функції $f(x_1,\ldots,x_n)$ і довільного $k\ (1\le k\le n)$ справджується співвідношення

$$f(x_1,\ldots,x_n)=\bigvee_{(\sigma_1,\ldots,\sigma_k)\in\mathbb{Z}_2^k} x_1^{\sigma_1}\wedge\ldots\wedge x_k^{\sigma_k}\wedge f(\sigma_1,\ldots,\sigma_k,x_{k+1},\ldots,x_n), \qquad (2)$$

де диз'юнкція береться по усім двійковим наборам довжини *k*.

Приклад 15. Розкласти БФ $f(x,y,z)=x\downarrow((\bar{y}\Rightarrow x)\oplus z)$ за змінними

а) *y*;

б) *x* та *z*.

а) Запишемо розклад за змінною *y*:

$$f(x,y,z)=\bar{y}\,f(x,0,z)\vee y\,f(x,1,z).$$

$$f(x,0,z)=x\downarrow((\bar{0}\Rightarrow x)\oplus z)=x\downarrow((1\Rightarrow x)\oplus z)=x\downarrow((\bar{1}\vee x)\oplus z)=\overline{x\vee(x\oplus z)}=$$

$$= \overline{x} \wedge \overline{x \oplus z} = \overline{x}\left(x \Leftrightarrow z\right) = \overline{x}\left(\overline{x}\,\overline{z} \vee xz\right) = \overline{x}\,\overline{x}\,\overline{z} \vee \overline{x}\,xz = \overline{x}\,\overline{z} \vee 0 = \overline{x}\,\overline{z}\,.$$

$$f\left(x,0,z\right) = x \downarrow \left(\left(\overline{1} \Rightarrow x\right) \oplus z\right) = x \downarrow \left(\left(0 \Rightarrow x\right) \oplus z\right) = x \downarrow \left(1 \oplus z\right) = x \downarrow \overline{z} = \overline{x \vee \overline{z}} = \overline{x}\,z\,.$$

Тому $f\left(x,y,z\right) = \overline{y}\,\overline{x}\,\overline{z} \vee y\,\overline{x}\,z = \overline{x}\left(\overline{y}\,\overline{z} \vee y\,z\right).$

б) Проведемо розклад за змінними *x* та *z*:

$$f\left(x,y,z\right) = \overline{x}\,\overline{z}\; f\left(0,y,0\right) \vee \overline{x}\,z\; f\left(0,y,1\right) \vee x\overline{z}\; f\left(1,y,0\right) \vee x\,z\; f\left(1,y,1\right).$$

$$f\left(0,y,0\right) = 0 \downarrow \left(\left(\overline{y} \Rightarrow 0\right) \oplus 0\right) = 0 \downarrow \left(y \oplus 0\right) = 0 \downarrow y = \overline{0 \vee y} = \overline{y}\,.$$

$$f\left(0,y,1\right) = 0 \downarrow \left(\left(\overline{y} \Rightarrow 0\right) \oplus 1\right) = 0 \downarrow \left(y \oplus 1\right) = 0 \downarrow \overline{y} = \overline{0 \vee \overline{y}} = y\,.$$

$$f\left(1,y,0\right) = 1 \downarrow \left(\left(\overline{y} \Rightarrow 1\right) \oplus 0\right) = 1 \downarrow \left(1 \oplus 0\right) = 1 \downarrow 1 = 0\,.$$

$$f\left(1,y,1\right) = 1 \downarrow \left(\left(\overline{y} \Rightarrow 1\right) \oplus 1\right) = 1 \downarrow \left(y \oplus 1\right) = 1 \downarrow \overline{y} = \overline{1 \vee \overline{y}} = \overline{1} = 0.$$

Тому

$$f\left(x,y,z\right) = \overline{x}\,\overline{z}\,\overline{y} \vee \overline{x}\,z\,y \vee x\overline{z}\,0 \vee x\,z\,0 = \overline{x}\,\overline{y}\,\overline{z} \vee \overline{x}\,y\,z\,.$$

Нехай $T\left(f\right) = \left\{\left(x_1,\ldots,x_n\right) \middle|\, f\left(x_1,\ldots,x_n\right) = 1\right\}$. Застосовуючи (2) у випадку $k = n$, отримуємо *теорему про розклад БФ за усіма змінними*.

Теорема 6. Для довільної булевої функції $f(x_1,\ldots,x_n)$, такої, що $f \neq 0$, справджується співвідношення

$$f(x_1,\ldots,x_n) = \bigvee_{(\sigma_1,\ldots,\sigma_n)\in T(f)} x_1^{\sigma_1} \wedge \ldots \wedge x_n^{\sigma_n}.$$

Теореми 4–6 є теоремами про "диз'юнктивний розклад". Має місце теорема про "кон'юнктивний розклад".

Теорема 7. Для довільної булевої функції $f(x_1,\ldots,x_n)$ і довільного $k\,(1\le k\le n)$ справджується співвідношення

$$f(x_1,\ldots,x_n) = \bigwedge_{(\sigma_1,\ldots,\sigma_k)\in \mathbb{Z}_2^k} \left(x_1^{\bar{\sigma}_1} \vee \ldots \vee x_k^{\bar{\sigma}_k} \vee f(\sigma_1,\ldots,\sigma_k,x_{k+1},\ldots,x_n)\right), \qquad (3)$$

де кон'юнкція береться по усім двійковим наборам довжини *k*.

Доведення випливає із теореми 5 та принципу двоїстості.

Приклад 16. Провести "кон'юнктивний розклад" БФ $f(x,y,z) = x \downarrow ((\bar{y} \Rightarrow x) \oplus z)$ за змінними *x* та *z*.

За формулою (3) маємо

$$f(x,y,z)=\big(x\vee z\vee f(0,y,0)\big)\big(x\vee\overline{z}\vee f(0,y,1)\big)\big(\overline{x}\vee z\vee f(1,y,0)\big)\big(\overline{x}\vee\overline{z}\vee f(1,y,1)\big).$$

Тому

$$f(x,y,z)=\big(x\vee z\vee\overline{y}\big)\big(x\vee\overline{z}\vee y\big)\big(\overline{x}\vee z\vee 0\big)\big(\overline{x}\vee\overline{z}\vee 0\big)=\big(x\vee z\vee\overline{y}\big)\big(x\vee\overline{z}\vee y\big)\big(\overline{x}\vee z\big)\big(\overline{x}\vee\overline{z}\big).$$

3.2. Нормальні форми булевих функцій

Нехай $\{x_1,\ldots,x_n\}$ — фіксований набір (алфавіт) змінних.

Формула $K=x_{i_1}^{\sigma_1}\wedge\ldots\wedge x_{i_r}^{\sigma_r}$, де $r\geq 1,\ 1\leq i_1<i_2<\ldots<i_r\leq n,\ \sigma_j\in\mathbb{Z}_2,\ \ j=\overline{1,r}$, називається *елементарною кон'юнкцією*, побудованою із змінних $\{x_1,\ldots,x_n\}$. Кількість змінних, які входять в елементарну кон'юнкцію, називається її *рангом*.

Формула $D=x_{i_1}^{\sigma_1}\vee\ldots\vee x_{i_r}^{\sigma_r}$, де $r\geq 1,\ 1\leq i_1<i_2<\ldots<i_r\leq n,\ \sigma_j\in\mathbb{Z}_2,\ \ j=\overline{1,r}$, називається *елементарною диз'юнкцією рангу* r, побудованою із змінних $\{x_1,\ldots,x_n\}$.

Приклад 17. Формула $x_1\overline{x}_4x_5$ — елементарна кон'юнкція рангу 3. Формула $\overline{x}_2\vee\overline{x}_3\vee x_5\vee\overline{x}_6$ — елементарна диз'юнкція рангу 4. Формули $x_1x_2\overline{x}_1x_3$ та $x_1\overline{x}_3\vee\overline{x}_4$ не є ні елементарними кон'юнкціями, ні елементарними диз'юнкціями.

Теорема 8. Із змінних $\{x_1,\ldots,x_n\}$ можна побудувати 3^n-1 різних елементарних кон'юнкцій (диз'юнкцій).

Доведення. Для кожної із змінних x_i $\left(i=\overline{1,n}\right)$ можливим є один із трьох випадків щодо її входження у елементарну кон'юнкцію *K*:

a) змінна взагалі не входить у кон'юнкцію;

b) змінна входить у кон'юнкцію із запереченням;

c) змінна входить у кон'юнкцію без заперечення.

Тому за комбінаторним правилом множення існує 3^n способів вибору змінних $\{x_1,\ldots,x_n\}$ у елементарні кон'юнкції. Відкинувши той спосіб, при якому жодна із змінних не входить у кон'юнкцію, отримаємо твердження теореми про число елементарних кон'юнкцій. Твердження про кількість елементарних диз'юнкцій можна отримати із використанням принципу двоїстості.

Задача 3. Підрахувати кількість різних елементарних диз'юнкцій рангу *r*, які можна побудувати із *n* змінних.

Вираз $K_1\vee\ldots\vee K_s$, де K_i — елементарна кон'юнкція, $K_i\neq K_j$ при $i\neq j$, $i,j=\overline{1,s}$, називається *диз'юнктивною нормальною формою* (ДНФ), побудованою із змінних $\{x_1,\ldots,x_n\}$.

Вираз $D_1 \wedge \ldots \wedge D_s$, де D_i — елементарна диз'юнкція, $D_i \neq D_j$ при $i \neq j$, $i, j = \overline{1,s}$, називається *кон'юнктивною нормальною формою* (КНФ), побудованою із змінних $\{x_1, \ldots, x_n\}$.

Приклад 18. Формула $\bar{x}_1 x_3 x_4 \vee x_2 \bar{x}_4 \vee x_1 \bar{x}_2 x_3 \bar{x}_4$ — ДНФ, побудована із змінних x_1, x_2, x_3, x_4, формула $(x_2 \vee \bar{x}_3)(x_1 \vee x_2 \vee \bar{x}_4)(x_1 \vee x_2 \vee \bar{x}_3 \vee x_4)$ — КНФ, побудована із тих самих змінних. Формула $x_2 \bar{x}_4 \vee x_1 \bar{x}_2 x_3 \bar{x}_4 \vee \bar{x}_4 x_2$ не є ДНФ (у неї входять дві однакові елементарні кон'юнкції).

Теорема 9. Із змінних $\{x_1, \ldots, x_n\}$ можна побудувати $2^{3^n-1}-1$ різних ДНФ (КНФ).

Доведення. Кожна з 3^n-1 елементарних кон'юнкцій може входити або не входити у ДНФ. Тому існує 2^{3^n-1} різних способів вибору кон'юнкцій. Відкинувши той спосіб, при якому жодна кон'юнкція не вибрана, отримаємо твердження теореми.

Теорема 10. Для кожної відмінної від 0 (1) n-місної БФ $f(x_1, \ldots, x_n)$ існує рівносильна їй ДНФ (КНФ).

Алгоритм побудови ДНФ (КНФ) формули над множиною елементарних функцій

1. За допомогою рівносильних перетворень позбавитися від операцій $\oplus, \Leftrightarrow, \Rightarrow$.

2. За допомогою рівносильностей де Моргана віднести заперечення до окремих змінних.

3. Відкрити (увести) дужки то звести подібні доданки з використанням законів ідемпотентності, несуперечності, виключення третього та властивостей булевих констант.

Приклад 19. Побудувати ДНФ та КНФ БФ $\overline{(xy \oplus \bar{z}) | (\bar{z} \vee zx)} \Rightarrow (\bar{z} \downarrow \bar{x})$ методом рівносильних перетворень.

а) Будуємо ДНФ:

$$\overline{(xy \oplus \bar{z}) | (\bar{z} \vee zx)} \Rightarrow (\bar{z} \downarrow \bar{x}) = ((xy \oplus \bar{z}) | (\bar{z} \vee zx)) \vee (\overline{\bar{z} \vee \bar{x}}) = (((xyz \vee \overline{xy}\,\bar{z}) | (\bar{z} \vee x)) \vee zx =$$

$$= (((xyz \vee (\bar{x} \vee \bar{y})\bar{z}) | (\bar{z} \vee x)) \vee zx = \overline{(xyz \vee (\bar{x} \vee \bar{y})\bar{z}) \wedge (\bar{z} \vee x)} \vee zx = \overline{xyz \vee (\bar{x} \vee \bar{y})\bar{z}} \vee \overline{\bar{z} \vee x} \vee zx =$$

$$= \overline{xyz} \wedge \overline{(\bar{x} \vee \bar{y})\bar{z}} \vee z\bar{x} \vee zx = (\bar{x} \vee \bar{y} \vee \bar{z}) \wedge (xy \vee z) \vee z(\bar{x} \vee x) = (\bar{x} \vee \bar{y} \vee \bar{z})xy \vee (\bar{x} \vee \bar{y} \vee \bar{z})z \vee z =$$

$$= \bar{x}xy \vee \bar{y}xy \vee \bar{z}xy \vee z = \bar{z}xy \vee z = xy \vee z.$$

б) Будуємо КНФ:

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

Приклад 20. Побудувати КНФ функції $x\bar{z} \vee \bar{x}z \vee x\bar{y}z$.

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

3.3. Досконалі нормальні форми

Елементарна кон'юнкція (диз'юнкція), побудована із змінних $x_1,\ldots,x_n$, називається *повною*, якщо її ранг рівний n.

Повна елементарна кон'юнкція $x_1^{\sigma_1}\wedge\ldots\wedge x_n^{\sigma_n}\ \left(\sigma_i\in\mathbb{Z}_2,\ i=\overline{1,n}\right)$ приймає значення 1 тоді і тільки тоді, коли $x_1=\sigma_1,\ldots,x_n=\sigma_n$.

Досконалою диз'юнктивною нормальною формою (ДДНФ), побудованою із змінних $x_1,\ldots,x_n$, називається диз'юнкція деякого числа різних між собою повних елементарних кон'юнкцій, побудованих із цих змінних.

Досконалою кон'юнктивною нормальною формою (ДКНФ), побудованою із змінних $x_1,\ldots,x_n$, називається кон'юнкція деякого числа різних між собою повних елементарних диз'юнкцій, побудованих із цих змінних.

Приклад 21. $xy\bar{z}\vee\bar{x}yz\vee x\bar{y}z$ — ДДНФ, побудована із змінних $\{x,y,z\}$, $(\bar{x}\vee y\vee\bar{z})(x\vee\bar{y}\vee z)$ — ДКНФ, побудована із тих самих змінних.

Теорема 11. Із змінних $\{x_1,\ldots,x_n\}$ можна побудувати $2^{2^n}-1$ різних ДДНФ (ДКНФ).

Доведення самостійно.

Теорема 12. Для кожної відмінної від 0 (1) *n*-місної БФ $f(x_1,\ldots,x_n)$ існує єдина рівносильна їй ДДНФ (ДКНФ).

Доведення. Нехай $f \neq 0$. Скористаємося теоремою 6 про розклад БФ за усіма змінними:

$$f(x_1,\ldots,x_n) = \bigvee_{(\sigma_1,\ldots,\sigma_n)\in T(f)} x_1^{\sigma_1} \wedge \ldots \wedge x_n^{\sigma_n}.$$

Права частина рівності містить диз'юнкцію повних елементарних кон'юнкцій, тобто ДДНФ. Тому для кожної БФ, відмінної від 0, існує принаймні одна ДДНФ. Єдиність ДДНФ для кожної БФ випливає з того, що згідно з теоремою 2 та теоремою 11 кількість *n*-місних БФ рівна кількості різних ДДНФ, які можна побудувати із *n* змінних.

Наслідок. Довільну БФ можна записати у вигляді формули над системою функцій $\{\neg, \wedge, \vee\}$.

Розглянемо два методи побудови ДДНФ (ДКНФ).

1) Метод рівносильних перетворень:

а) За допомогою рівносильних перетворень будується ДНФ (КНФ) БФ, заданої формулою.

б) Проводиться *поповнення* неповних елементарних кон'юнкцій (диз'юнкцій) за допомогою формул:

I) $K = K \wedge 1 = K \wedge \left(x \vee \bar{x}\right) = Kx \vee K\bar{x}$.

II) $D = D \vee 0 = D \vee x\bar{x} = \left(D \vee x\right)\left(D \vee \bar{x}\right)$.

в) Записується диз'юнкція *різних* елементарних кон'юнкцій, отриманих на попередньому етапі (кон'юнкція елементарних диз'юнкцію), яка і шуканою ДДНФ (ДКНФ).

2) Табличний метод:

а) Будується таблиця значень БФ.

б) Відмічаються набори $\left(\alpha_1,\ldots,\alpha_n\right)$, на яких функція приймає значення 1 (0).

в) Кожному такому набору ставиться у відповідність *повна* елементарна кон'юнкція $x_1^{\alpha_1}\ldots x_n^{\alpha_n}$ (елементарна диз'юнкція $x_1^{\bar{\alpha}_1} \vee \ldots \vee x_n^{\bar{\alpha}_n}$).

г) Записується диз'юнкція елементарних кон'юнкцій, отриманих на попередньому етапі (кон'юнкція елементарних диз'юнкцію), яка і є шуканою ДДНФ (ДКНФ).

Приклад 22. Побудувати ДДНФ та ДКНФ булевої функції $f\left(x,y,z\right) = \overline{\left(xy \oplus \bar{z}\right) \mid \left(\bar{z} \vee zx\right)} \Rightarrow \left(\bar{z} \downarrow \bar{x}\right)$ (функції прикладу 19) з використанням табличного методу та методу рівносильних перетворень.

1) Використаємо табличний метод.

Побудуємо таблицю значень функції $f(x,y,z)$.

x	y	z	xy	$\overline{z}$	$xy \oplus \overline{z}$	zx	$\overline{z} \vee zx$	$(xy \oplus \overline{z}) \mid (\overline{z} \vee zx)$	$\overline{(xy \oplus \overline{z}) \mid (\overline{z} \vee zx)}$	$\overline{x}$	$\overline{z} \downarrow \overline{x}$	$f(x,y,z)$
0	0	0	0	1	1	0	1	0	1	1	0	0
0	0	1	0	0	0	0	0	1	0	1	0	1
0	1	0	0	1	1	0	1	0	1	1	0	0
0	1	1	0	0	0	0	0	1	0	1	0	1
1	0	0	0	1	1	0	1	0	1	0	0	0
1	0	1	0	0	0	1	1	1	0	0	1	1
1	1	0	1	1	0	0	1	1	0	0	0	1
1	1	1	1	0	1	1	1	0	1	0	1	1

Для побудови ДДНФ відмічаємо 2-й, 4-й, 6-й, 7-й та 8-ий набори.

Записуємо відповідні повні елементарні кон’юнкції:

$$x^0y^0z^1 = \overline{x}\,\overline{y}\,z,\ \ x^0y^1z^1 = \overline{x}\,y\,z,\ \ x^1y^0z^1 = x\overline{y}z,\ \ x^1y^1z^0 = xy\overline{z},\ x^1y^1z^1 = xyz.$$

Записуємо ДДНФ:

$$\overline{x}\,\overline{y}\,z \vee \overline{x}\,y\,z \vee x\overline{y}z \vee xy\overline{z} \vee xyz.$$

Для побудови ДКНФ відмічаємо 1-й, 3-й та 5-й набори та записуємо відповідні елементарні диз'юнкції:

$$x^{\bar{0}} \vee y^{\bar{0}} \vee z^{\bar{0}} = x^1 \vee y^1 \vee z^1 = x \vee y \vee z,\ x^{\bar{0}} \vee y^{\bar{1}} \vee z^{\bar{0}} = x^1 \vee y^0 \vee z^1 = x \vee \bar{y} \vee z,\ x^{\bar{1}} \vee y^{\bar{0}} \vee z^{\bar{0}} = \bar{x} \vee y \vee z.$$

Записуємо ДКНФ:

$$(x \vee y \vee z)(x \vee \bar{y} \vee z)(\bar{x} \vee y \vee z).$$

2) Після спрощень отримаємо запис функції за допомогою ДНФ $f(x,y,z) = xy \vee z$ (див. приклад 19).

Проведемо поповнення елементарних кон'юнкцій:

$$xy = xy \wedge 1 = xy(z \vee \bar{z}) = xyz \vee xy\bar{z}.$$

$$z = (x \vee \bar{x})z = xz \vee \bar{x}z = x(y \vee \bar{y})z \vee \bar{x}(y \vee \bar{y})z = xyz \vee x\bar{y}z \vee \bar{x}yz \vee \bar{x}\,\bar{y}\,z.$$

Записуємо ДДНФ:

$$xyz \vee xy\bar{z} \vee x\bar{y}z \vee \bar{x}yz \vee \bar{x}\,\bar{y}\,z.$$

Для знаходження ДКНФ скористаємося КНФ $(x \vee z)(y \vee z)$ функції $f(x,y,z)$.

Проведемо поповнення елементарних диз'юнкцій:

$$x \vee z = x \vee z \vee 0 = x \vee z \vee y\bar{y} = (x \vee y \vee z)(x \vee \bar{y} \vee z).$$

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

Записуємо ДКНФ:

$$(x \vee y \vee z)(x \vee \bar{y} \vee z)(\bar{x} \vee y \vee z).$$

3.4. Поліноми Жегалкіна

Поліномом (многочленом) Жегалкіна називається вираз вигляду

$$\tilde{K}_0 \oplus \tilde{K}_1 \oplus \ldots \oplus \tilde{K}_m,$$

де $\tilde{K}_0 \in \mathbb{Z}_2$, $\tilde{K}_i$ — різні елементарні кон'юнкції, які не містять заперечення змінних, $i = \overline{1,m}$.

Степенем полінома Жегалкіна називається максимальний із рангів елементарних кон'юнкцій, які входять у поліном.

Приклад 23. $1 \oplus y \oplus xz \oplus xyz$ — поліном Жегалкіна 3-го степеня.

Алгоритм побудови полінома Жегалкіна БФ $f(x_1,\ldots,x_n)$.

1. Побудувати ДДНФ $K_1 \vee \ldots \vee K_s$ функції f, де K_i — повні елементарні кон'юнкції, побудовані із змінних $\{x_1, \ldots, x_n\}$.

2. Замінити формулу $K_1 \vee \ldots \vee K_s$ рівносильною їй формулою $K_1 \oplus \ldots \oplus K_s$.

3. Для кожної змінної x_i виконати заміну $\bar{x}_i$ на $x_i \oplus 1$, $i = \overline{1,n}$.

4. Розкрити дужки та звести подібні доданки з використанням рівносильності $x \oplus x = 0$.

Обґрунтування алгоритму. Пояснення потребує лише другий крок алгоритму, оскільки для довільних БФ $f, g \in P_2$ $f \vee g \neq f \oplus g$. Покажемо, що для довільних різних повних елементарних кон'юнкцій K_1, K_2 та довільного $\tilde{\alpha} = (\alpha_1, \ldots . \alpha_n) \in \mathbb{Z}_2^n$ $K_1(\tilde{\alpha}) \vee K_2(\tilde{\alpha}) = K_1(\tilde{\alpha}) \oplus K_2(\tilde{\alpha})$.

Оскільки кожна повна елементарна кон'юнкція приймає значення 1 лише на одному наборі, то неможливим є одночасне виконання рівностей $K_1(\tilde{\alpha}) = 1$, $K_2(\tilde{\alpha}) = 1$.

Якщо $K_1(\tilde{\alpha}) = K_2(\tilde{\alpha}) = 0$, то $K_1(\tilde{\alpha}) \vee K_2(\tilde{\alpha}) = 0 \vee 0 = 0 \oplus 0 = K_1(\tilde{\alpha}) \oplus K_2(\tilde{\alpha})$.

Якщо $K_1(\tilde{\alpha}) = 1$ та $K_2(\tilde{\alpha}) = 0$, то $K_1(\tilde{\alpha}) \vee K_2(\tilde{\alpha}) = 1 \vee 0 = 1 \oplus 0 = K_1(\tilde{\alpha}) \oplus K_2(\tilde{\alpha})$.

Випадок $K_1(\tilde{\alpha}) = 0$, $K_2(\tilde{\alpha}) = 1$ аналізується аналогічно.

Теорема 13. Для кожної БФ $f(x_1,\ldots,x_n)\in P_2$ існує єдиний рівносильний їй поліном Жегалкіна.

Доведення. Існування полінома Жегалкіна для довільної БФ випливає з можливості застосування вищенаведеного алгоритму до довільної БФ, відмінної від нуля (якщо $f\equiv 0$, то 0 — поліном Жегалкіна функції *f*). Єдиність випливає із того, що кількість різних поліномів Жегалкіна, які можна побудувати із *n* змінних, рівна 2^{2^n}, і це число співпадає із кількістю різних *n*-місних БФ.

Приклад 24. Побудувати поліном Жегалкіна БФ $f(x,y,z)=\overline{(xy\oplus\bar{z})\,|\,(\bar{z}\vee zx)}\Rightarrow(\bar{z}\downarrow\bar{x})$.

Запишемо ДДНФ $f(x,y,z)=\bar{x}\,\bar{y}\,z\vee\bar{x}\,y\,z\vee x\bar{y}z\vee xy\bar{z}\vee xyz$

Замінимо "$\oplus$" на "$\vee$": $f(x,y,z)=\bar{x}\,\bar{y}\,z\oplus\bar{x}\,y\,z\oplus x\bar{y}z\oplus xy\bar{z}\oplus xyz$.

Замінимо $\bar{x}$ на $x\oplus 1$: $f(x,y,z)=(x\oplus 1)(y\oplus 1)z\oplus(x\oplus 1)y\,z\oplus x(y\oplus 1)z\oplus xy(z\oplus 1)\oplus xyz$.

Виконуємо спрощення

$$f(x,y,z)=(x\oplus 1)\big((y\oplus 1)z\oplus y\,z\big)\oplus x(y\oplus 1)z\oplus xy(z\oplus 1\oplus z)=$$

$$=(x\oplus 1)(yz\oplus z\oplus y\,z)\oplus x(y\oplus 1)z\oplus xy=(x\oplus 1)z\oplus xyz\oplus xz\oplus xy=xz\oplus z\oplus xyz\oplus xz\oplus xy=$$

$$=xyz\oplus xy\oplus z.$$

4. Застосування булевих функцій в теорії контактних та логічних схем

4.1. Контактні схеми

Під *мережею* будемо розуміти деякий скінченний набір *вершин*, між деякими парами з яких встановлені *зв'язки*.

Будемо вважати, що у множині вершин мережі виділено спеціальні вершини, які називаються *полюсами*.

Під *контактною схемою* будемо розуміти мережу із двома полюсами (джерелом та стоком), ребра якої називаються *контактами* і помічені змінними $x_1,\ldots,x_n$ або їх запереченнями.

Якщо контакт помічений змінною без заперечення, то він називається *замикальним,* у протилежному випадку — *відмикальним*. Приклади контактних схем наведено на рис. 1.

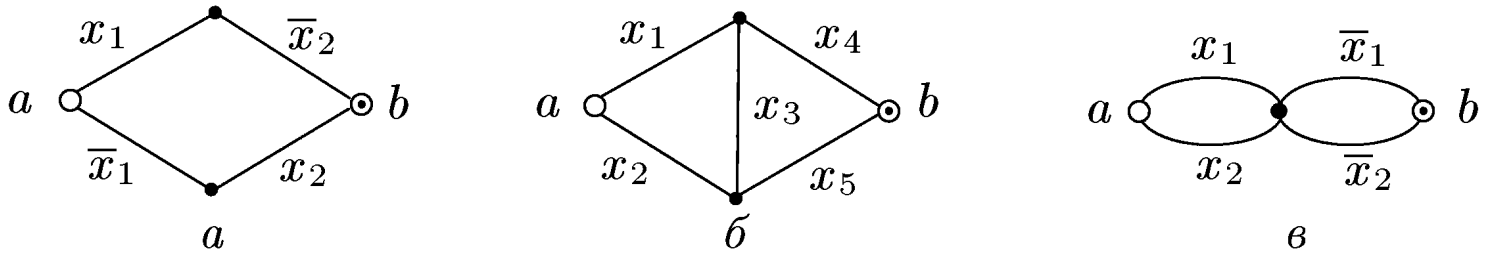


Рис. 1. Контактні схеми

Функція $f(\tilde{x}) = \bigvee\limits_{[a,b]} K_{[a,b]}$, де диз'юнкція береться по усім простим шляхам (які не містять кратні вершини) від входу *a* до виходу *b*, називається *функцією провідності контактної схеми*.

Приклад 25. Вказати функції провідності схем, наведених на рис. 1.

а) $f(\tilde{x}) = x_1\overline{x}_2 \vee \overline{x}_1 x_2$;

б) $f(\tilde{x}) = x_1x_4 \vee x_1x_3x_5 \vee x_2x_5 \vee x_2x_3x_4$;

в) $f(\tilde{x}) = x_1\overline{x}_1 \vee x_1\overline{x}_2 \vee x_2\overline{x}_1 \vee x_2\overline{x}_2 = x_1\overline{x}_2 \vee \overline{x}_1x_2$.

Часто при зображенні контактних схем використовуються провідники та ключі-перемикачі, які ставляться у відповідність кожній змінній. При цьому послідовне з'єднання провідників відповідає кон'юнкції (рис. 2), а паралельне з'єднання — диз'юнкції (рис. 3).

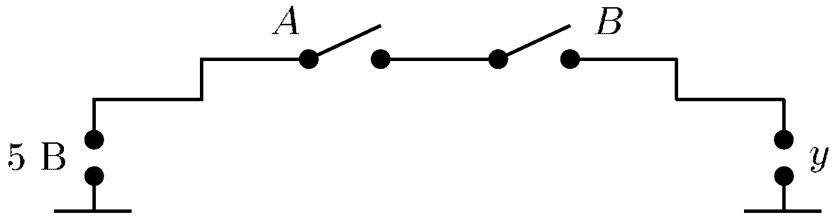


Рис. 2. Послідовні ключі

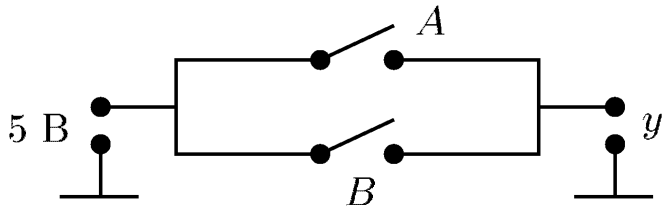


Рис. 3. Паралельні ключі

Для фізичної реалізації заперечення використовується реле з розмикальним контактом, схема якого наведена на рис. 4.

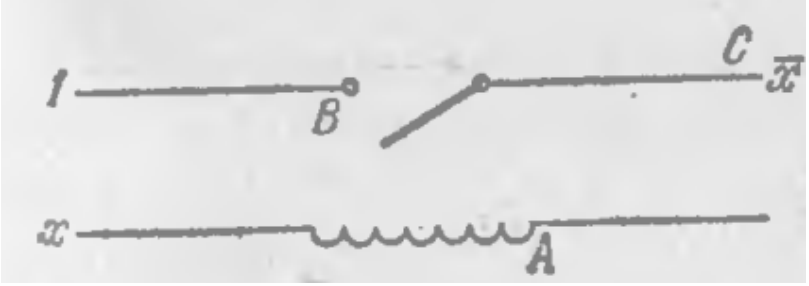


Рис. 4. Реле з розмикальним контактом

Якщо по обвитці A струм не проходить $(x=0)$, то пружина відтягує контакт B уверх і ланцюг замикається. Якщо $(x=1)$, то контакт B притягується і на виході C струму нема.

Складністю контактної схеми називається кількість контактів схеми. Так, наприклад, контактні схеми, зображені на рис. 1*а* та рис. 1*в*, мають складність 4, а контактна схема з рис. 1*б* має складність 5.

Приклад 26. Для функції $x_1\bar{x}_3 \vee x_2x_3 \vee \bar{x}_1x_2\bar{x}_3$ побудувати контактну схему, яка реалізує цю функцію та має мінімальну складність (3).

Спростимо функцію провідності схеми.

$$x_1\bar{x}_3 \vee x_2x_3 \vee \bar{x}_1x_2\bar{x}_3 = \left(x_1 \vee \bar{x}_1x_2\right)\bar{x}_3 \vee x_2x_3 = \left(x_1 \vee x_2\right)\bar{x}_3 \vee x_2x_3 = x_1\bar{x}_3 \vee x_2\bar{x}_3 \vee x_2x_3 = x_1\bar{x}_3 \vee x_2\left(\bar{x}_3 \vee x_3\right) = x_1\bar{x}_3 \vee x_2.$$

Отримана формула суттєво залежить від трьох змінних. Тому складність відповідної цій функції контактної схеми не може бути меншою за 3. Контактна схема складності 3 зображена на рис. 5.

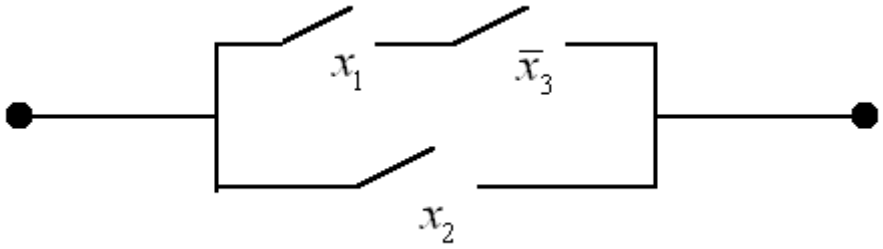


Рис. 5. Контактна схема

Приклад 27. Побудувати якомога простішу контактну схему, функція провідності якої залежить від трьох змінних і має номер 220.

$$220 = 128 + 92 = 128 + 64 + 28 = 128 + 64 + 16 + 12 = 128 + 64 + 16 + 8 + 4 = 2^7 + 2^6 + 2^4 + 2^3 + 2^2.$$

Звідси отримуємо вектор значень функції $\tilde{f} = (1,1,0,1,1,1,0,0)$, на основі якого будуємо таблицю значень функції $f(x_1, x_2, x_3)$.

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	1
1	1	0	0
1	1	1	0

Запишемо ДКНФ функції $f(x_1, x_2, x_3)$:

$$f(x_1, x_2, x_3) = (x_1 \vee \overline{x}_2 \vee x_3)(\overline{x}_1 \vee \overline{x}_2 \vee x_3)(\overline{x}_1 \vee \overline{x}_2 \vee \overline{x}_3).$$

Проведемо спрощення:

$$(x_1 \vee \overline{x}_2 \vee x_3)(\overline{x}_1 \vee \overline{x}_2 \vee x_3)(\overline{x}_1 \vee \overline{x}_2 \vee \overline{x}_3) = (x_1 \vee \overline{x}_2 \vee x_3)(\overline{x}_1 \vee \overline{x}_2) =$$

$$= \overline{x}_2 \vee (x_1 \vee x_3)\overline{x}_1 = \overline{x}_2 \vee \overline{x}_1 x_3.$$

Зобразимо відповідну контактну схему:

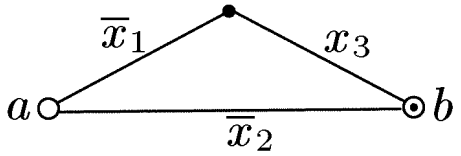


Рис. 6. Контактна схема до прикладу 27

Приклад 28. Комітет складається із чотирьох учасників. Рішення виноситься більшістю голосів. У випадку рівності голосів рішення приймається, якщо голова комітету "голосує за". Побудувати контактну схему так, щоб при голосуванні кожний натискав би на кнопку і у випадку прийняття рішення загоралася би сигнальна лампа.

Поставимо у відповідність кожному члену комісії булеву змінну x_i таким чином, щоб $x_i = 1$ тоді і тільки тоді, якщо *i*-ий член комітету "голосує за", $i = 1,2,3,4$ (голові комітету відповідає змінна x_1). Розглянемо БФ $f(x_1, x_2, x_3, x_4)$, яка приймає значення 1 тоді і тільки тоді, коли комітет приймає рішення. Легко бачити, що $f(x_1, x_2, x_3, x_4) = x_1(x_2 \vee x_3 \vee x_4) \vee \bar{x}_1 x_2 x_3 x_4$. Схема наведена на рис. 7.

Рис. 7.

4.2. Схеми із логічних елементів

Логічні схеми у комп'ютерах та інших електронних пристроях оперують з наборами вхідних та вихідних даних, що складаються з нулів та одиниць. Булеві функції використовуються для *аналізу* та *синтезу* логічних схем.

Логічний елемент — пристрій, який реалізовує деяку булеву функцію. Його входи відповідають булевим змінним, а виходи — значенню функції. Найбільш вживані логічні елементи наведені на рис. 8.

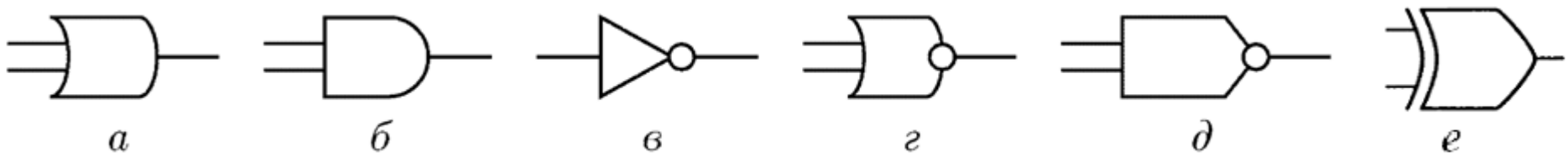


Рис. 8. Зображення логічних елементів в стандарті ISO *а*) диз'юнктор; *б*) кон'юнктор; *в*) інвертор; *г*) стрілка Пірса; *д*) штрих Шефера; *е*) суматор за модулем 2

Логічна схема будується з логічних елементів і зображає суперпозицію цих елементів. *Складністю логічної схеми* називається кількість логічних елементів, які входять у схему.

За наслідком до теореми 12 будь-яку булеву функцію можна записати у вигляді формули над системою $\{\neg, \wedge, \vee\}$. Тому довільну булеву функцію можна реалізувати схемою з інверторів, кон'юнкторів та диз'юнкторів.

Оскільки

$$\overline{x} = x \downarrow x,\ xy = \overline{x} \downarrow \overline{y} = \left(x \downarrow x\right) \downarrow \left(y \downarrow y\right), x \vee y = \overline{x \downarrow y} = \left(x \downarrow y\right) \downarrow \left(x \downarrow y\right),$$

то будь-яку БФ можна реалізувати за допомогою схеми, яка містить лише елементи, які реалізовують стрілку Пірса.

Приклад 29. Побудувати схему, яка реалізує функцію $f\left(x, y, z\right) = \left(x \vee y\right) z$.

Відповідна схема складності 2 зображена на рис. 9.

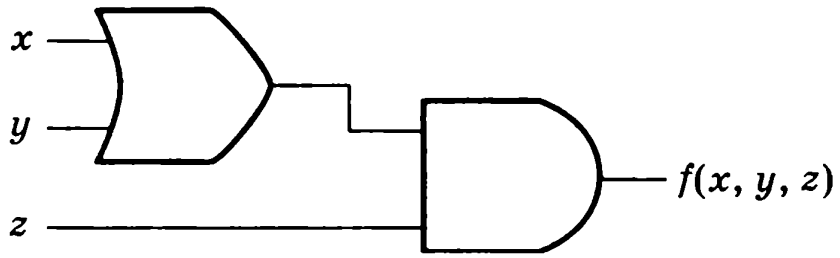


Рис. 9. Логічна схема для функції $f\left(x, y, z\right) = \left(x \vee y\right) z$

Приклад 30. Реалізувати функцію $f(x,y,z)=\overline{(xy\oplus\overline{z})\,|\,(\overline{z}\vee zx)}\Rightarrow(\overline{z}\downarrow\overline{x})$ (функція прикладу 24) за допомогою логічної схеми із кон'юнкторів та суматорів за модулем 2.

У теорії логічних схем розглядаються дві основні задачі: аналіз та синтез.

Задача 4. Підрахувати кількість *n*-місних БФ, які можна реалізувати схемами, побудованими із кон'юкторів та суматорів за модулем 2.

Аналіз логічної схеми полягає у побудові булевої функції, яку реалізує даний логічний пристрій (схема). За даною логічною схемою можна побудувати формулу, що відповідає шуканій функції або вказати значення функції для всіх наборів вхідних даних.

Приклад 31. Проаналізувати логічну схему, наведену на рис. 10.

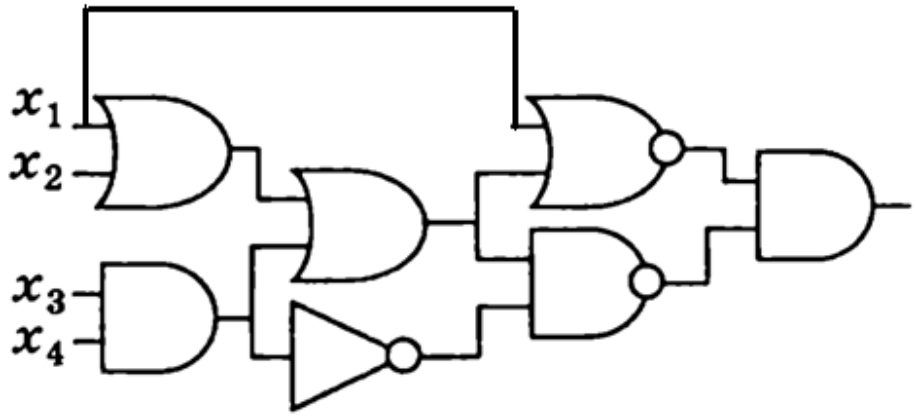


Рис. 10. Логічна схема

Запишемо формулу для функції $f(x_1, x_2, x_3, x_4)$, яку реалізує логічна схема:

$$f(x_1, x_2, x_3, x_4) = \left((x_1 \vee x_2 \vee x_3 x_4) \downarrow x_1\right) \wedge \left((x_1 \vee x_2 \vee x_3 x_4) \mid \overline{x_3 x_4}\right).$$

Задача синтезу схеми полягає у побудові логічної схеми, яка реалізує дану булеву функцію. Функція може бути задана таблицею або за допомогою формули. Використовуючи правила побудови ДДНФ та ДКНФ, можна отримати формулу над множиною $\{\neg, \wedge, \vee\}$, а потім реалізувати операції формули за допомогою відповідних логічних елементів.

Вартість логічної схеми залежить від її складності. Тому часто поряд з двома вищенаведеними задачами розглядають *задачу спрощення логічної схеми*.

Приклад 32. Спростити логічну схему із прикладу 31.

Спростимо формулу для БФ, яка реалізується схемою складності 7, наведеною на рис. 10:

$$\overline{x_1 \vee x_2 \vee x_3 x_4} \wedge \overline{(x_1 \vee x_2)\, \overline{x_3 x_4}} = \overline{x_1 \vee x_2}\; \overline{x_3 x_4} \left(\overline{x_1 \vee x_2} \vee x_3 x_4\right) = \overline{x_1 \vee x_2}\; \overline{x_3 x_4}\; \overline{x_1 \vee x_2} \vee \overline{x_1 \vee x_2}\; \overline{x_3 x_4} x_3 x_4 = \overline{x_1 \vee x_2}\; \overline{x_3 x_4} =$$
$$= \overline{x_1 \vee x_2 \vee x_3 x_4} = (x_1 \vee x_2) \downarrow (x_3 x_4).$$

Реалізуємо отриману формулу схемою. Схема, наведена на рис. 11, має складність 3.

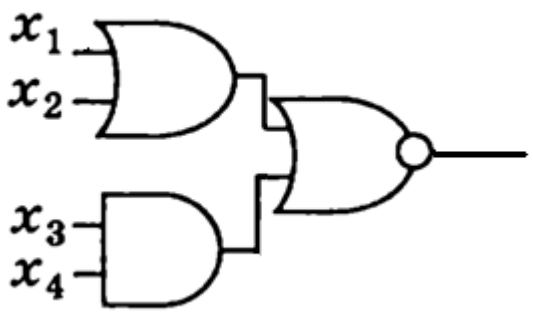


Рис. 11. Схема після спрощення

Приклад 33. Побудувати логічну схему для знаходження суми двох її бітових входів.

ІІ. АЛГЕБРАЇЧНІ СТРУКТУРИ

1. Універсальні алгебри

1.1. Основні поняття теорії алгебраїчних систем

Нехай задано деяку множину A. Функція ω вигляду $\omega: A^n \to A$ називається *n-арною операцією* на множині A (n-місною операцією).

Якщо $n=1$, то операція називається унарною, якщо $n=2$ — бінарною, якщо $n=3$ — тернарною.

Наприклад, операція заперечення — унарна операція на множині булевих функцій, симетрична різниця — бінарна операція на множині усіх підмножин деякої універсальної множини U, $\max\{x,y,z\}$ — тернарна операція на множині дійсних чисел.

Нехай $\Omega=\{\omega_1,\ldots,\omega_m\}$ — деяка множина операцій на множині A, арності яких рівні n_i $\left(i=\overline{1,n}\right)$. Пара $\langle A;\Omega\rangle$ називається *універсальною алгеброю*. При цьому множина A називається *носієм алгебри*, множина Ω — *сигнатурою алгебри*, а вектор $(n_1,\ldots,n_m)$ — *типом алгебри*.

Для алгебри $\langle A;\Omega\rangle$ також використовується позначення $\langle A;\omega_1,\ldots,\omega_m\rangle$.

Приклад 1. Розглянемо наступні алгебри:

1) $\langle \mathbb{N}; + \rangle$ — алгебра натуральних чисел із операцією додавання. Тип цієї алгебри — (2).

2) $\langle \mathbb{Z}; +, \cdot \rangle$ — алгебра цілих чисел із операціями додавання та множення. Алгебра має тип (2, 2);

3) $\langle 2^A; \cup, \cap, \overline{\ } \rangle$ — алгебра підмножин множини A типу (2, 2, 1)

4) $\langle A^+; + \rangle$ — алгебра слів у алфавіті A із операцією *конкатенації* "+",

де *слово* — непорожній ланцюжок символів алфавіту A,

конкатенація слів $w_1 = a_1 \ldots a_m$ та $w_2 = b_1 \ldots b_m$ визначається так:

$$w_1 + w_2 \stackrel{\text{def}}{=} a_1 \ldots a_m b_1 \ldots b_n .$$

5) $\langle \mathbb{R}[X]; +, \cdot \rangle$ — алгебра поліномів (многочленів) від однієї змінної з дійсними коефіцієнтами, де многочлен n-го степеня — це вираз вигляду $a_n x^n + \ldots + a_1 x + a_0$, $\left(a_i \in \mathbb{R}, i = \overline{0,n} \right)$.

6) $\langle P_2; \wedge, \vee, \neg \rangle$ — алгебра булевих функцій.

1.2. Замикання множин. Підалгебри

Нехай $\langle A; \Omega \rangle$ — універсальна алгебра. *Замиканням множини* $B \subseteq A$ відносно підмножини Σ сигнатури Ω називається множина $[B]_\Sigma$, яка складається з усіх елементів множини B та усіх тих елементів, які можна отримати, виконуючи операції (суперпозиції операцій) із Σ над аргументами із B.

Властивості операції замикання (у формулах множина операцій Σ опускається):

1. $B \subseteq [B]$.
2. $[[B]] = [B]$.
3. $B \subseteq C \Rightarrow [B] \subseteq [C]$.
4. $[B] \cup [C] \subseteq [B \cup C]$.
5. $[B \cap C] \subseteq [B] \cap [C]$.

Приклад 2.

1) У алгебрі $\langle \mathbb{N}; + \rangle$

a. $[1]_+ = [\{1\}]_+ = \mathbb{N}$;

b. $[2]_+ = 2\mathbb{N}$ — множина парних натуральних чисел.

2) У алгебрі $\langle \mathbb{Z}; +, * \rangle$

a. $[-1]_{+} = -\mathbb{N}$;

b. $[-1]_{*} = \{-1, 1\}$;

c. $[-1]_{\{+,*\}} = \mathbb{Z}$.

Якщо виконується умова $[B]_{\Sigma} = B$, то множина B називається *замкненою* відносно множини операцій Σ.

Якщо множина B замкнена відносно сигнатури алгебри Ω, то $\langle B; \Omega \rangle$ називається *підалгеброю* алгебри $\langle A; \Omega \rangle$.

Приклад 3.

1) $\langle 3\mathbb{N}; + \rangle$ — підалгебра натуральних чисел, кратних 3, у алгебрі $\langle \mathbb{N}; + \rangle$.

2) Множині усіх слів парної довжини B відповідає підалгебра $\langle B; + \rangle$ у алгебрі $\langle A^{+}; + \rangle$ (алгебрі слів у алфавіті A).

3) Множині многочленів без вільного члена B відповідає підалгебра $\langle B;+,\cdot\rangle$ у алгебрі многочленів з дійсними коефіцієнтами $\langle \mathbb{R}[X];+,\cdot\rangle$.

4) Нехай заданий деякий набір змінних $V=\{x_1,x_2,\ldots\}$ та деяка сигнатура $\Phi=\{\varphi_1,\ldots,\varphi_m\}$, яка містить функціональні символи, типу $(n_1,\ldots,n_m)$. Визначимо множину *термів* T індуктивно:

a. $V\subseteq T$ (усі змінні — терми);

b. якщо $t_1,\ldots,t_{n_i}\in T$ і $\varphi_i\in\Phi$, то $\varphi_i(t_1,\ldots,t_{n_i})\in T$.

Алгебра $\langle T;\Phi\rangle$ називається *вільною алгеброю термів*.

Якщо $V=\{x\}$, $\Phi=\{+,\cdot\}$, то у цьому випадку вільна алгебра термів $\langle T;\Phi\rangle$ — це множина усіх виразів, які можна побудувати із змінної x із застосуванням операцій додавання та множення.

Множина $B\subseteq A$ називається *системою твірних* алгебри $\langle A;\Omega\rangle$, якщо $[B]_\Omega=A$.

Алгебра $\langle A;\Omega\rangle$, яка має скінченну систему твірних, називається *скінченно-породженою*.

Приклад 4. Усі алгебри із прикладу 2 є скінченно-породженими.

Алгебра $\langle \mathbb{Z}[X];+,\cdot\rangle$ є скінченно-породженою, оскільки $[\{-1,x\}]_{\{+,\cdot\}}=\mathbb{Z}[X]$.

Алгебра $\langle \mathbb{Z}[X];+\rangle$ не є скінченно-породженою.

2. Алгебри з однією бінарною операцією

2.1. Групоїди. Півгрупи. Моноїди.

Алгебра типу (2) називається *групоїдом*.

Якщо носій групоїда скінченний, то операцію групоїда можна задати за допомогою *таблиці Келі*, яка містить результат застосування операції для усіх пар елементів групоїду.

Приклад 5. Навести таблицю Келі групоїда $\langle \mathbb{Z}_4;\oplus_4\rangle$, де $\mathbb{Z}_4=\{0,1,2,3\}$, $a\oplus_4 b=(a+b)\bmod 4$ (додавання за модулем 4).

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Таблиця Келі має наступний вигляд.

Бінарна операція $*$ називається *комутативною* на множині *A*, якщо

$$\text{для довільних } a,b\in A\ a*b=b*a.$$

Таблиця Келі комутативного групоїда є симетричною відносно головної діагоналі.

Бінарна операція $*$ називається *асоціативною* на множині *A*, якщо

$$\text{для довільних } a,b,c\in A\ (a*b)*c=a*(b*c).$$

Приклад 6.

1) Операція $\oplus_4$ є комутативною та асоціативною на множині $\mathbb{Z}_4$.

2) Операція $a * b = -a - b$ є комутативною та неасоціативною на множині цілих чисел.

3) Операція множення матриць є некомутативною та асоціативною на множині квадратних матриць $n \times n \left(n \geq 2\right)$.

4) Операція $a * b = a^b$ не є ні комутативною, ні асоціативною на множині цілих чисел.

Асоціативний групоїд називається *півгрупою*.

Приклади півгруп:

1) $\left\langle A^+; + \right\rangle$ — множина слів у алфавіті A, на які визначено операцію конкатенації;

2) $\left\langle \mathbb{N}; + \right\rangle$.

У півгрупі $\left\langle A; * \right\rangle$ вводиться поняття *степеня* елемента: $a^n \overset{\text{def}}{=} \underbrace{a * a * \ldots * a}_{n \text{ множників}}$.

Елемент $e \in A$ називається *нейтральним (одиничним) елементом* півгрупи $\left\langle A; * \right\rangle$, якщо $\forall a \in A \; a * e = e * a = a$. Наприклад,

0 є нейтральним елементом півгрупи $\left\langle \mathbb{Z}; + \right\rangle$;

1 — нейтральний елемент півгрупи $\langle \mathbb{N}; \cdot \rangle$;

у півгрупах $\langle A^+; + \rangle$ та $\langle \mathbb{N}; + \rangle$ немає нейтральних елементів.

Теорема 1. Півгрупа не може містити більше одного нейтрального елемента.

Доведення. Припустимо протилежне. Нехай e_1 та e_2 — два різні нейтральні елементи. Тоді за властивістю нейтрального елемента $e_1 = e_1 * e_2 = e_2$, тобто $e_1 = e_2$. Отримане протиріччя доводить теорему.

Півгрупа з нейтральним елементом називається *моноїдом*. Приклади моноїдів:

1) $\langle A^*; + \rangle$, де A^* множина слів у алфавіті A разом із порожнім словом e;

2) $\langle \mathbb{R}; \cdot \rangle$.

Нехай $\langle A; * \rangle$ — моноїд, $a \in A$. Якщо існує такий елемент $b \in A$, що $a * b = b * a = e$, де e — нейтральний елемент, то елемент a називається *оборотним*, а елемент b — *оберненим* до елемента a. Обернений до елемента a позначається a^{-1}.

Наприклад,

у моноїді $\langle A^*; + \rangle$ оборотним є лише елемент e;

у моноїді $\langle \mathbb{R};\cdot \rangle$ усі елементи крім 0 є оборотними $\left(\forall x \in \mathbb{R} \setminus \{0\}\ x^{-1} = \frac{1}{x} \right)$;

у моноїді $\langle \mathbb{Z};\cdot \rangle$ оборотними є -1 та 1;

у моноїді $\langle \mathbb{Z};+ \rangle$ усі елементи є оборотними $\left(\forall x \in \mathbb{Z}\ x^{-1} = -x \right)$.

Теорема 2. Кожний оборотний елемент моноїда має єдиний обернений елемент.

Доведення. Припустимо протилежне. Нехай b та c — два різні елементи, які є оберненими до a. Тоді

$$b = b * e = b * (a * c) = (b * a) * c = e * c = c.$$

Отримане протиріччя доводить теорему.

2.2. Групи

Моноїд, усі елементи якого оборотні, називається *групою*.

Якщо групова операція комутативна, то група називається *абелевою* (комутативною групою). Слід зауважити, групу можна розглядати як алгебру типу (2, 1), вважаючи, що другою операцією є унарна операція знаходження оберненого елемента, або навіть як алгебру типу (2, 1, 0) за умови, що 0-арна операція повертає нейтральний елемент групи (константу).

Приклади груп:

1) $\langle \mathbb{Z}; + \rangle$ — абелева група цілих чисел (0 — нейтральний елемент, $-x$ — елемент, обернений до x);

2) $\langle \mathbb{Z}_m; \oplus_m \rangle$ — абелева група класів лишків за модулем m ($m \in \mathbb{N}$, $m \geq 2$, $\mathbb{Z}_m = \{0,1,\ldots,m-1\}$, $x \oplus_m y = (x+y) \bmod m$, 0 — нейтральний елемент, $x^{-1} = m - x$ — елемент, обернений до x);

3) $\langle \mathbb{R}^*; \cdot \rangle$ — мультиплікативна група поля дійсних чисел ($\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, 1 — нейтральний елемент);

4) $\langle 2^A; \Delta \rangle$ — булеан множини A є групою відносно операції симетричної різниці множин ($\varnothing$ — нейтральний елемент, $x^{-1} = x$, оскільки $x \Delta x = \varnothing$);

5) $\langle \mathrm{GL}_n(\mathbb{R});\cdot\rangle$ — некомутативна група усіх невироджених $n\times n$-матриць з дійсними коефіцієнтами (E — нейтральний елемент);

Теорема 3. У довільній групі $\langle A;*\rangle$:

1) $(a*b)^{-1}=b^{-1}*a^{-1}$;

2) $a*x=a*y\Rightarrow x=y$;

3) рівняння $a*x=b$ має єдиний розв'язок $x=a^{-1}*b$;

4) $\left(a^{-1}\right)^{-1}=a$.

Якщо група скінченна, то кількість її елементів називається *порядком групи*. Так, наприклад, групи $\langle\mathbb{Z};+\rangle$, $\langle\mathbb{R}^*;\cdot\rangle$ та $\langle \mathrm{GL}_n(\mathbb{R});\cdot\rangle$ — нескінченні групи, група $\langle\mathbb{Z}_m;\oplus_m\rangle$ — скінченна група порядку m. Група $\langle 2^A;\Delta\rangle$ скінченна тоді тільки тоді, коли скінченною є множина A. Якщо $|A|=n$, то порядок групи $\langle 2^A;\Delta\rangle$ рівний 2^n.

Якщо для елемента a існує таке натуральне число n, що $a^1 \neq e, \ldots, a^{n-1} \neq e, a^n = e$, то тоді вважають, що елемент a має *скінченний порядок* n. У протилежному випадку a є елементом *нескінченного порядку*. Якщо a — елемент порядку n, то $a^{-1} = a^{n-1}$, оскільки $a * a^{n-1} = a^{n-1} * a = a^n = e$.

Наприклад,

у $\langle \mathbb{Z}; + \rangle$ усі елементи крім 0 мають нескінченний порядок;

у $\langle \mathbb{Z}_m; \oplus_m \rangle$ усі елементи мають скінченний порядок, який не перевищує m;

у $\langle \mathbb{R}^*; \cdot \rangle$ 1 має порядок 1, (-1) — порядок 2, усі інші елементи мають нескінченний порядок;

у $\langle 2^A; \Delta \rangle$ усі елементи крім $\varnothing$ 2-го порядку.

Задача 1. Для групи $\mathrm{GL}_2(\mathbb{R})$ довести, що

1) якщо $|\det A| \neq 1$, то елемент A не може мати скінченний порядок;

2) в групі існують елементи усіх можливих скінченних порядків.

Поширимо поняття степеня на від'ємні показники. Будемо вважати, що $a^{-n} = \left(a^{-1}\right)^n$, $n \in \mathbb{N}$.

Якщо $\exists a \in A$, такий що $\forall b \in A \ \ \exists k \in \mathbb{Z}$, таке, що $b = a^k$, то група $\langle A; * \rangle$ називається *циклічною* із *твірним елементом* a. У циклічній групі кожний елемент є деяким степенем твірного елемента.

Наприклад,

$\langle \mathbb{Z}; + \rangle$ — циклічна група із твірним елементом 1 (або -1);

$\langle \mathbb{Z}_m; \oplus_m \rangle$ — циклічна група, твірним елементом якої є довільне натуральне $k < m$, взаємно просте з числом m;

групи $\langle \mathbb{R}^*; \cdot \rangle$ та $\langle \mathrm{GL}_n(\mathbb{R}); \cdot \rangle$ не є циклічними.

2.3. Група перестановок

Перестановкою, визначеною на множині $\{1,\ldots,n\}$, називається довільне взаємно однозначне відображення цієї множини на саму себе. Позначимо через S_n множину усіх перестановок на множині $\{1,\ldots,n\}$.

Перестановки часто записують у вигляді

$$\begin{pmatrix} 1 & \ldots & n \\ \pi(1) & \ldots & \pi(n) \end{pmatrix},$$

записуючи під кожним елементом i значення перестановки π на цьому елементі $\left(i=\overline{1,n}\right)$.

Наприклад, циклічному зсуву 6 аргументів на 2 позицію вліво відповідає перестановка

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}.$$

На множині перестановок S_n розглядають операцію множення перестановок: *добутком* перестановок π та σ називається перестановка $\sigma \circ \pi$, яка отримується після того, як спочатку застосовується перестановка π, а потім до результату застосовується перестановка σ:

$$(\sigma \circ \pi)(x) = \sigma(\pi(x)).$$

Наприклад, для перестановок

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

маємо

$$\sigma \circ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{matrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 3 & 2 & 1 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 3 & 2 \end{matrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

У той самий час

$$\pi \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{matrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 & 4 \end{matrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

Таким чином $\sigma \circ \pi \neq \pi \circ \sigma$.

Операція множення перестановок має наступні властивості:

1) *асоціативність*, тобто $(\pi \circ \sigma) \circ \tau = \pi \circ (\sigma \circ \tau)$.

Ця властивість випливає з того, що

$$\forall x \in \{1,\ldots,n\} \ ((\pi \circ \sigma) \circ \tau)(x) = \pi(\sigma(\tau(x))) = (\pi \circ (\sigma \circ \tau))(x);$$

2) у множині S_n існує *нейтральний елемент* $e = \begin{pmatrix} 1 & \ldots & n \\ 1 & \ldots & n \end{pmatrix}$, який задовольняє умову $e \circ \pi = \pi \circ e$

для усіх $\pi \in S_n$. Перестановка e називається одиничною або тотожною перестановкою;

3) для кожної перестановки π існує обернена до неї перестановка π^{-1}, для якої $\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = e$.

Перестановка π^{-1}, для якої виконується умова

$$\pi^{-1}(b) = a \ \text{ тоді і тільки тоді, коли } \ \pi(a) = b,$$

є оберненою до перестановки π.

Отже, множина перестановок S_n утворює групу відносно операції множення перестановок. Ця група називається *симетричною групою* n-го степеня. Порядок групи S_n рівний $n!$.

Пару (i, j) назвемо *інверсією* відносно перестановки $\pi \in S_n$, якщо $i < j$, але $\pi(i) > \pi(j)$.

Перестановка $\pi \in S_n$ називається *парною*, якщо парною є кількість усіх інверсій відносно π. У протилежному випадку перестановка π називається непарною. Визначимо *функцію парності (знаку) перестановки* sgn наступним чином:

$$\operatorname{sgn}\pi = \begin{cases} 1, & \text{якщо } \pi \text{ — парна,} \\ -1, & \text{якщо } \pi \text{ — непарна.} \end{cases}$$

Функція sgn є *мультиплікативною*, тобто $\operatorname{sgn}(\pi \circ \sigma) = \operatorname{sgn}(\pi) \circ \operatorname{sgn}(\sigma)$.

Приклад 7. Вказати $\sigma = \rho^{-1} \circ \pi$ та визначити її парність, якщо

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix},\ \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 5 & 2 & 3 \end{pmatrix}.$$

Розв'язання. $\rho^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$. Тому

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{pmatrix}.$$

Вісім пар $(1,2),(1,3),(1,4),(1,5),(2,5),(3,4),(3,5),(4,5)$ утворюють інверсію відносно σ. Отже $\operatorname{sgn}\sigma = 1$.

Якщо для перестановки $\pi \in S_n$ виконуються умови

$$\pi(i_1)=i_2,\ \pi(i_2)=i_3,\ldots,\ \pi(i_{l-1})=i_l,\ \pi(i_l)=i_1,\ \pi(j)=j,\ j\notin\{1,\ldots,n\}$$

де $\{i_1,\ldots,i_l\}\subseteq\{1,\ldots,n\}$, $i_j\neq i_k$ при $j\neq k$, то перестановка π називається *циклом* довжини l і позначається $(i_1\ i_2\ldots i_l)$. Цикл довжини 2 називається *транспозицією*. Довільна транспозиція є непарною перестановкою.

Властивості циклів:

1) якщо $\pi=(i_1\ i_2\ldots i_l)$, то $\pi^{-1}=(i_l\ldots i_2\ i_1)$;

2) якщо $\pi=(i_1\ i_2\ldots i_l)$, то порядок π у групі S_n рівний l.

Два цикли $(i_1\ i_2\ldots i_l)$ та $(j_1\ j_2\ldots j_m)$ називаються *незалежними*, якщо вони не містять спільних елементів. Якщо цикли $(i_1\ i_2\ldots i_l)$ та $(j_1\ j_2\ldots j_m)$ незалежні, то $(i_1\ i_2\ldots i_l)\circ(j_1\ j_2\ldots j_m)=(j_1\ j_2\ldots j_m)\circ$ $\circ(i_1\ i_2\ldots i_l)$.

Теорема 4. Для елементів симетричної групи справджуються твердження:

1) кожна перестановка $\pi\neq e$ у S_n може бути записана у вигляді добутку незалежних циклів довжини ≥ 2;

2) якщо $\pi = \pi_1 \circ \ldots \circ \pi_r$ — запис перестановки π у вигляді добутку циклів $\pi_1, \ldots, \pi_r$, довжини яких рівні $l_1, \ldots, l_r$, то

   a. $\operatorname{sgn} \pi = (-1)^{l_1 + \ldots l_r - r}$;

   b. порядок перестановки π рівний $\text{НСК}(l_1, \ldots, l_r)$.

Наприклад, перестановки із прикладу 7 можна записати у вигляді

$$\pi = (1\,3\,2) \circ (4\,5),\ \rho = (1\,4\,2) \circ (3\,5),\ \sigma = (1\,5) \circ (3\,4).$$

Тому $\operatorname{sgn} \pi = (-1)^{3+2-2} = -1,\ \operatorname{sgn} \rho = (-1)^{3+2} = -1, \operatorname{sgn} \sigma = (-1)^{2+2-2} = 1.$

Оскільки $\text{НСК}(2,3) = 6, \text{НСК}(2,2) = 2$, то перестановки π та ρ мають порядок 6, а перестановка σ — порядок 2.

Наслідок. Кожна перестановка $\pi \in S_n$ може бути записана у вигляді

a) добутку транспозицій;

b) добутку транспозицій вигляду $(1\,i), 1 < i \le n$.

Доведення. Пункт a) випливає з теореми 4 та того, що $(i_1\ i_2 \dots i_{l-1}\ i_l) = (i_1\ i_l) \circ (i_1\ i_{l-1}) \circ \dots \circ (i_1\ i_2)$. Пункт b) випливає з a) та того, $(i\ \ j) = (1\,i) \circ (1\ j) \circ (1\,i)$.

Приклад 8. Записати перестановку

$$\pi = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 3\,5\,4\,1\,7\,8\,6\,2 \end{pmatrix}$$

у вигляді добутку транспозицій та визначити її порядок та парність.

Розв'язання. Запишемо π у вигляді $\pi = (1\,3\,4) \circ (2\,5\,7\,6\,8)$. Тому $\operatorname{sgn}\pi = (-1)^{3+5-2} = 1$, порядок π рівний $\text{НСК}(3,5) = 15$, $\pi = (1\,4) \circ (1\,3) \circ (2\,8) \circ (2\,6) \circ (2\,7) \circ (2\,5)$.

2.4. Підгрупи

Нехай $G=\langle A;*\rangle$ — група. Якщо множина $B\subseteq A$ є замкненою відносно операцій множення та знаходження оберненого елемента, то алгебра $H=\langle B;*\rangle$ називається *підгрупою* групи G. Якщо $B\neq A$ і $B\neq\{e\}$, то підгрупа H називається *власною підгрупою* групи G.

Приклади:

1) група парних чисел $\langle 2\mathbb{Z};+\rangle$ є підгрупою групи цілих чисел $\langle\mathbb{Z};+\rangle$;

2) група цілих степенів двійки H є підгрупою групи $G=\langle\mathbb{R}^*;\cdot\rangle$;

3) група матриць $\langle \mathrm{SL}_n(\mathbb{R});\cdot\rangle$, визначник яких рівний 1, є підгрупою групи $\langle \mathrm{GL}_n(\mathbb{R});\cdot\rangle$. Це випливає з того, що якщо $\det A=1,\ \det B=1$, то $\det(A\cdot B)=\det A\cdot\det B=1\cdot 1=1,\ \det A^{-1}=\dfrac{1}{\det A}=\dfrac{1}{1}=1.$

Ця група називається *спеціальною лінійною групою степеня n над* $\mathbb{R}$;

4) множина $A_n=\{\pi\in S_n\,|\,\operatorname{sgn}\pi=1\}$ усіх парних перестановок є підгрупою групи S_n.

Це випливає з того, що якщо $\pi,\rho\in A_n$, то $\operatorname{sgn}(\pi\circ\rho)=\operatorname{sgn}\pi\cdot\operatorname{sgn}\rho=1\cdot 1=1,\ \operatorname{sgn}\pi^{-1}=\dfrac{1}{\operatorname{sgn}\pi}=1$, а отже $\pi\circ\rho\in A_n$ та $\pi^{-1}\in A_n$.

Група A_n називається *знакозмінною групою степеня n*. Можна показати, що $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$.

Теорема 5. $H = \langle B; * \rangle \ (B \subseteq A)$ буде підгрупою групи $G = \langle A; * \rangle$ тоді і тільки тоді, коли для довільних $a, b \in B \ a^{-1} * b \in B$.

Теорема 6 (теорема Лагранжа). Порядок підгрупи скінченної групи є дільником порядку групи.

Наслідок 1. Порядок довільного елемента скінченної групи є дільником порядку групи.

Наслідок 2. Усі групи простого порядку циклічні.

3. Алгебри з двома бінарними операціями

3.1. Кільця

Алгебра $\langle R;+,\cdot\rangle$ типу (2, 2) називається *кільцем*, якщо

1) алгебра $\langle R;+\rangle$ є абелевою групою;

2) алгебра $\langle R;\cdot\rangle$ є півгрупою;

3) операція "множення" є дистрибутивною відносно операції "додавання":

а) $a\cdot(b+c)=a\cdot b+a\cdot c$;

б) $(b+c)\cdot a=b\cdot a+c\cdot a$.

Якщо операцію множення є комутативною, то кільце називається *комутативним*. Якщо $\langle R;\cdot\rangle$ є моноїдом, то кільце називається *кільцем з одиницею*.

Приклад 9.

1) $\langle \mathbb{Z}_m;\oplus_m,\odot_m\rangle$ — кільце класів лишків за модулем m. Це кільце є комутативним кільцем з одиницею 1.

2) $\langle 2\mathbb{Z};+,\cdot\rangle$ — кільце парних чисел. Це кільце є комутативним кільцем без одиниці.

3) $\langle M_n(\mathbb{Z});+,\cdot\rangle$ — кільце квадратних $n\times n$-матриць з цілими коефіцієнтами. Це кільце є некомутативним кільцем з одиницею E.

4) $\langle \mathbb{R}[X];+,\cdot\rangle$ — кільце многочленів від однієї змінної з дійсними коефіцієнтами. Це кільце є комутативним кільцем з одиницею 1.

5) Кільце функцій вигляду $f: R\to R$, визначених на кільці R, із значеннями у кільці R. При цьому $(f+g)(x)=f(x)+g(x)$, $(-f)(x)=-f(x)$, $0(x)=0$, $e(x)=x$.

Задача 2. Довести, що у довільному кільці $\langle R;+,\cdot\rangle$ $\forall a\in R$ $a\cdot 0=0\cdot a=0$.

Задача 3. Чи є комутативним кільце функцій із прикладу 9 п. 5.

Надалі для скорочення запису кільце $\langle R;+,\cdot\rangle$ буде ототожнюватися із його носієм R.

Нехай R — кільце з одиницею. Позначимо через $U(R)$ множину усіх елементів кільця R, які мають обернений елемент відносно операції множення. Тоді $\langle U(R);\cdot\rangle$ — група, яка називається *групою оборотних елементів кільця R*.

Наприклад,

1) для кільця цілих чисел $\mathbb{Z}$: $U(\mathbb{Z})=\{-1,1\}$;

2) для кільця дійсних чисел $\mathbb{R}$: $U(\mathbb{R}) = \mathbb{R}^*$;

3) для кільця класів лишків $\mathbb{Z}_m$: $U(\mathbb{Z}_m)$ — множина усіх чисел від 1 до $m-1$, які є взаємно простими із числом m. Зокрема, $U(\mathbb{Z}_9) = \{1,2,4,5,7,8\}$.

4) для кільця многочленів $\mathbb{R}[X]$: $U(\mathbb{R}[X]) = \mathbb{R}^*$;

Якщо для ненульового елемента $a \in R$ існує такий елемент $b \in R$, що $b \neq 0$ і $a \cdot b = 0$, то a називається (лівим) *дільником нуля*.

Комутативне кільце з одиницею, яке не містить дільників нуля, називається *цілісним*.

Наприклад,

1) кільце цілих чисел — цілісне;

2) кільце $\mathbb{Z}_m$ є цілісним тоді і тільки тоді, коли число m — просте. Зокрема, кільце $\mathbb{Z}_{15}$ не є цілісним, оскільки 3 та 5 — дільники нуля;

3) кільце $M_n(\mathbb{Z})$ також не є цілісним у випадку $n > 1$. Зокрема

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

Критерій цілісності. Комутативне кільце з одиницею цілісне тоді і тільки тоді, коли справджується закон скорочення:

$$\text{для довільних } a,b,c \in R\ (a \neq 0)\ \ a \cdot b = a \cdot c \Rightarrow b = c.$$

Елемент $a \in R$ називається *дільником* елемента $b \in R$ (b ділиться на a), якщо існує таке $c \in R$, що $a \cdot c = b$. Цей факт позначається як $a \mid b$ (або $b \vdots a$).

Властивості *відношення подільності*:

1) рефлексивність $(a \mid a)$;

2) транзитивність $(a \mid b,\ b \mid c \Rightarrow a \mid c)$;

3) якщо $a \mid b$ та $a \mid c$, то $a \mid (b \pm c)$;

4) якщо $a \mid b$ та $c \in R\ (c \neq 0)$, то $a \mid (b \cdot c)$;

5) якщо $a \mid b_1$, $a \mid b_2$ та $c_1, c_2 \in R$, то $a \mid (b_1 \cdot c_1 + b_2 \cdot c_2)$

Симетричність місця не має.

Згідно визначення довільний оборотний елемент кільця є дільником усіх інших елементів, відмінних від нуля.

Елемент $a \in R$ називається *простим* елементом кільця *R*, якщо його не можна записати у вигляді добутку двох необоротних елементів цього кільця. Простий многочлен називається ще *незвідним многочленом*.

Наприклад,

x^2+1 є простим елементом кільця многочленів $\mathbb{R}[X]$, x^3+1 — ні, оскільки $x^3+1=$ $=(x+1)(x^2-x+1)$.

x^2-2 — простий елемент кільця $\mathbb{Q}[X]$.

У кільці $\mathbb{R}[X]$ $x^2-2=\left(x-\sqrt{2}\right)\left(x+\sqrt{2}\right)$. Тому у $\mathbb{R}[X]$ многочлен x^2-2 вже не є незвідним.

Нехай *R* — цілісне кільце.

Елемент $c \in R$ називається *найбільшим спільним дільником* (НСД) елементів *a* та *b*, якщо $c \mid a$, $c \mid b$ та *c* ділиться на будь-який інший спільний дільник елементів *a* та *b*.

Наприклад, у кільці цілих чисел НСД 24 та 18 будуть числа ± 6.

У загальному випадку НСД визначається неоднозначно: якщо *c* — НСД елементів *a* та *b*, *d* — довільний оборотний елемент кільця *R*, то $c \cdot d$ також буде дільником (і навіть НСД) елементів *a* та *b*. Це випливає з того, що якщо $a=c \cdot s, b=c \cdot t$, то $a=(c \cdot d) \cdot \left(d^{-1} \cdot s\right)$, $b=(c \cdot d) \cdot \left(d^{-1} \cdot t\right)$. І навпаки, якщо

c_1 та c_2 — два різні НСД елементів a та b, то обов'язково знайдеться такий $d \in U(R)$, що $c_2 = c_1 \cdot d$. Тобто, НСД визначається з точністю до оборотного елемента кільця.

Позначимо через $\text{НСД}(a,b)$ НСД a та b. НСД має наступні властивості[1]:

1) $\text{НСД}(a,0) = a$;

2) $\text{НСД}(t \cdot a, t \cdot b) = t \cdot \text{НСД}(a,b)$;

3) $\text{НСД}\big(a, \text{НСД}(b,c)\big) = \text{НСД}\big(\text{НСД}(a,b), c\big)$.

Елемент $c \in R$ називається *найменшим спільним кратним* (НСК) елементів a та b, якщо $a \mid c$, $b \mid c$ та c є дільником будь-якого іншого спільного кратного a та b.

Має місце співвідношення:

$$\text{Якщо } a \cdot b = \text{НСД}(a,b) \cdot c, \text{ то } c = \text{НСК}(a,b).$$

Елементи a та b називаються *взаємно простими елементами* кільця R, якщо вони не мають необоротних спільних дільників $\big(\text{НСД}(a,b) = 1\big)$.

---

[1] Наступні рівності потрібно розуміти з точністю до оборотних множників.

Наприклад, у кільці $\mathbb{R}[X]$ многочлени x^2-3x+2 та x^3+8 є взаємно простими, оскільки незвідними дільниками першого многочлена є двочлени $x-1$ та $x-2$ і $x^3+8=(x+2)(x^2-2x+4)$ — розклад другого многочлена на незвідні дільники.

3.2. Евклідові кільця

Цілісне кільце R називається *евклідовим*, якщо можна вказати таку функцію $\delta : R \setminus \{0\} \to \{0\} \cup \mathbb{N}$, що

1) Для довільного $a \in R$ і довільного $b \neq 0$ $\delta(a \cdot b) \geq \delta(a)$

2) Для довільного $a \in R$ і довільного $b \neq 0$ існують такі $q, r \in R$, що

$$a = qb + r, \text{ де } \delta(r) < \delta(b) \text{ або } r = 0.$$

Попереднє співвідношення є аналогом ділення цілих чисел з остачею.

Прикладами евклідових кілець є

а) кільце цілих чисел $\mathbb{Z}$, для якого $\delta(a) = |a|$;

б) кільце многочленів $\mathbb{R}[X]$, для якого $\delta(f) = \deg f$ — степінь многочлена f.

У евклідових кільцях існує спосіб знаходження НСД, який називається алгоритмом послідовного ділення або *алгоритмом Евкліда*. Нехай задані відмінні від нуля $a, b \in R$. Провівши достатню кількість ділень з остачею, отримаємо:

$$a = q_1 b + r_1, \ (\delta(r_1) < \delta(b)),$$

$$b = q_2 r_1 + r_2, \ (\delta(r_2) < \delta(r_1)),$$

$$
\begin{aligned}
&r_1 = q_3 r_2 + r_3,\ \left(\delta(r_3) < \delta(r_2)\right),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&r_{k-2} = q_k r_{k-1} + r_k,\ \left(\delta(r_k) < \delta(r_{k-1})\right),\\
&r_{k-1} = q_{k+1} r_k,\ r_{k+1} = 0.
\end{aligned}
\qquad (1)
$$

Процес скінченний, оскільки строго спадний ланцюжок цілих невід'ємних чисел $\delta(b) > \delta(r_1) > > \delta(r_2) > \ldots$ повинен рано чи пізно обірватися, а це може відбутися лише за рахунок рівності нулю якоїсь остачі від ділення.

Покажемо, що остання відмінна від нуля остача r_k є НСД елементів *a* та *b*. З останньої рівності в (1) випливає, що $r_k \mid r_{k-1}$. Рухаючись по (1) знизу догори і використовуючи властивість 5) відношення подільності, отримаємо $r_k \mid r_{k-2}, \ldots, r_k \mid r_1,\ r_k \mid b,\ r_k \mid a$. Отже, r_k — спільний дільник елементів *a* та *b*. Нехай тепер *c* — довільний спільний дільник *a* та *b*. З першої рівності випливає, що $r_1 = a - q_1 b$, а, отже, $c \mid r_1$. З другої рівності тоді випливає, що $c \mid r_2$ і т.д. Остаточно отримаємо, $c \mid r_k$. Отже $\text{НСД}(a,b) = r_k$.

Приклад 10. Знайти

1) НСД(210, 56), НСК(210, 56);

2) НСД$\left(x^2-2x-3, 2x^3+5x^2+4x+1\right)$.

Остачу r_1 можна записати у вигляді лінійної комбінації елементів a та b: $r_1 = a - q_1 b$. Остача r_2 — у вигляді лінійної комбінації b та r_2, а, отже, у вигляді лінійної комбінації a та b. Рухаючись по (1) з зверху вниз, отримаємо, що усі r_i $(i = 1, \ldots, k)$ є лінійними комбінаціями a та b. Отримані результати можна підсумувати у вигляді наступного твердження.

Теорема 7. У евклідовому кільці R довільні два елементи a та b мають НСД та НСК. За допомогою алгоритму Евкліда можна знайти такі $u, v \in R$, що НСД$(a,b) = au + bv$.

3.3. Поля

Полем називається комутативне кільце з одиницею, у якому кожний відмінний від нуля елемент має обернений елемент.

Група $F^* = U(F) = F \setminus \{0\}$ називається *мультиплікативною групою* поля F.

Приклади полів:

1) Числові поля $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

2) $\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} \,\middle|\, a, b \in \mathbb{Q}\right\}$.

Якщо $a_1+b_1\sqrt{2}\in\mathbb{Q}\left(\sqrt{2}\right)$, $a_2+b_2\sqrt{2}\in\mathbb{Q}\left(\sqrt{2}\right)$, то

$$\left(a_1+b_1\sqrt{2}\right)+\left(a_2+b_2\sqrt{2}\right)=\left(a_1+a_2\right)+\left(b_1+b_2\right)\sqrt{2}\in\mathbb{Q}\left(\sqrt{2}\right);$$

$$\left(a_1+b_1\sqrt{2}\right)\cdot\left(a_2+b_2\sqrt{2}\right)=a_1a_2+a_1b_2\sqrt{2}+a_2b_1\sqrt{2}+2b_1b_2=\left(a_1a_2+2b_1b_2\right)+\left(a_1b_2+a_2b_1\right)\sqrt{2}\in\mathbb{Q}\left(\sqrt{2}\right);$$

$$\left(a_1+b_1\sqrt{2}\right)^{-1}=\frac{1}{a_1+b_1\sqrt{2}}=\frac{a_1-b_1\sqrt{2}}{\left(a_1+b_1\sqrt{2}\right)\left(a_1-b_1\sqrt{2}\right)}=\frac{a_1-b_1\sqrt{2}}{a_1^2-2b_1^2}=\frac{a_1}{a_1^2-2b_1^2}-\frac{b_1}{a_1^2-2b_1^2}\sqrt{2}\in\mathbb{Q}\left(\sqrt{2}\right).$$

3) $\mathbb{Z}_p$ — поле класів лишків за модулем простого числа p.

Якщо p — просте число, $0<a<p$, то $\text{НСД}(a,p)=1$. За теоремою 7 знайдуться такі цілі числа u та v, що $au+bp=1$. Тоді $au'\equiv 1\left(\text{mod}\,p\right)$, де $u'\in\mathbb{Z}_p$, $u'\equiv u\left(\text{mod}\,p\right)$. Отже, $a^{-1}=u'$.

Якщо для довільного $n\in\mathbb{N}$ і довільного $a\in F$, $a\neq 0$ $n\cdot a=\underbrace{a+a+\ldots+a}_{n\text{ доданків}}\neq 0$, то кажуть, що поле F має *характеристику* 0 $\left(\text{char}\,F=0\right)$. У протилежному випадку характеристикою поля вважається таке найменше $n\in\mathbb{N}$, що для всіх $a\in F$ $n\cdot a=0\left(\text{char}\,F=n\right)$.

Теорема 8. Для довільного поля F:

1) або $\text{char}\,F=0$, або $\text{char}\,F=p$, де p — просте число;

2) довільна підгрупа G мультиплікативної групи поля F^* є циклічною.

Розширення поля

Підполем F_1 поля F називається підмножина F, яка сама є полем відносно тих самих операцій. У цьому випадку поле F називається *розширенням поля* F_1.

Наприклад, поле $\mathbb{Q}$ — підполе поля $\mathbb{R}$, а поле $\mathbb{C}$ — розширення поля $\mathbb{R}$.

Нехай $P_n(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$ — незвідний многочлен степені n над полем F $(a_i \in F,\ i = 1,\ldots,n)$, $R = \left\{ b_0 + b_1 x + \ldots + b_{n-1}x^{n-1} \,\middle|\, b_i \in F,\ i = 0,\ldots,n-1 \right\}$ — множина многочленів, на якій задані операції додавання та множення за модулем $P_n(x)$. Тоді R — розширення поля F, отримане шляхом приєднання одного кореня многочлена $P_n(x)$ (йому відповідає елемент x поля R)).

Приклади розширень:

1) Поле $\mathbb{Q}\left(\sqrt{2}\right)$ отримане із поля $\mathbb{Q}$ шляхом приєднання елемента $\sqrt{2}$ — кореня многочлена $x^2 - 2$.

2) Поле $\mathbb{C}$ отримане із поля $\mathbb{R}$ шляхом приєднання уявної одиниці i — кореня многочлена $x^2 + 1$.

Приклад 11. Навести приклад поля із 8 елементів.

Розв'язання. Розглянемо поле $\mathbb{Z}_2$. Многочлен $P_3(x)=x^3+x+1$ є незвідним (це випливає з того, що довільний звідний многочлен 3-ї степені має лінійний дільник вигляду $(x-a)$, де a — корінь многочлена, а $P_3(0)=0^3+0+1=1\neq 0$, $P_3(1)=1^3+1+1=1\neq 0$). Тоді

$R=\{0,1,x,x+1,x^2,x^2+1,x^2+x,x^2+x+1\}$ — поле із 8 елементів, яке є розширенням поля $\mathbb{Z}_2$.

Розглянемо степені елемента $a=x$:

$a^2=x^2\in R$,

$a^3=x^3\notin R$, але $x^3\equiv x+1\,(\mathrm{mod}\,P_3)\Rightarrow a^3=x+1$,

$a^4=a^3\cdot a=(x+1)x=x^2+x\in R$,

$a^5=a^4\cdot a=(x^2+x)\cdot x=x^3+x^2\equiv x^2+x+1\,(\mathrm{mod}\,P_3)\Rightarrow a^5=x^2+x+1$,

$a^6=a^5\cdot a=(x^2+x+1)\cdot x=x^3+x^2+x\equiv x^2+1\,(\mathrm{mod}\,P_3)\Rightarrow a^6=x^2+1$,

$a^7=a^6\cdot a=(x^2+1)\cdot x=x^3+x\equiv 1\,(\mathrm{mod}\,P_3)\Rightarrow a^7=1$.

Елемент a має порядок 7, $a^{-1}=a^6$ і a є твірним елементом мультиплікативної групи поля R.

Після знаходження твірного елемента мультиплікативної групи легко виконувати операції у полі R. Наприклад,

$$\left(x^2+x\right)\cdot\left(x^2+1\right)=a^4\cdot a^6=a^{10}=a^{7+3}=a^3=x+1,$$

$$\left(x^2+x\right):\left(x^2+1\right)=a^4:a^6=a^{-2}=\left(a^{-1}\right)^2=\left(a^6\right)^2=a^{12}=a^{7+5}=a^5=x^2+x+1.$$

Теорема 9. Нехай F — скінченне поле. Тоді існує таке просте число p і $n\in\mathbb{N}$, що $\operatorname{char}F=p$, $\left|F\right|=p^n$ і поле F є розширенням поля $\mathbb{Z}_p$. І навпаки, для довільного простого числа p і довільного $n\in\mathbb{N}$ існує p^n-елементне розширення поля $\mathbb{Z}_p$.

Скінченне поле із p^n елементів називається полем Галуа і позначається $GF\left(p^n\right)$.

Задача 4. Вказати таблиці множення та ділення поля $GF(9)$.

4. Елементи теорії чисел

4.1. Розв'язування лінійних порівнянь за модулем *m*

Розглянемо у кільці $\mathbb{Z}_m$ лінійне рівняння $ax=b$, яке є рівносильним рівнянню $ax\equiv b\pmod m$, $x\in\mathbb{Z}_m$. Нехай $d=\text{НСД}(a,m)$. Можливими є такі випадки:

1) $d=1$. Тоді $a\in U\left(\mathbb{Z}_m\right)$, а тому рівняння має єдиний розв'язок $x=a^{-1}b$.

2) Число d не є дільником b. Тоді рівняння немає розв'язку, оскільки

$$ax \equiv b \pmod{m} \Leftrightarrow \exists t\ (ax - b) = mt \Leftrightarrow b = ax - mt,$$

а тому b має ділитися на будь-який спільний дільник a та m.

3) Число d є дільником b. Нехай $a = a_1 d,\ b = b_1 d,\ m = m_1 d$. Початкове рівняння буде мати d розв'язків $x_k = x_0 + m_1 \cdot k\ (k = 0, \ldots, d-1)$, де $x_0 = a_1^{-1} b_1$ — розв'язок рівняння $a_1 x = b_1$ у кільці $\mathbb{Z}_{m_1}$ (єдиний, оскільки НСД$(a_1, m_1) = 1$).

Приклад 12. Розв'язати рівняння $40x = 16$ у кільці $\mathbb{Z}_{68}$.

Розв'язання. $d = \text{НСД}(40, 68) = 4$. Оскільки $4 \mid 16$, то рівняння має 4 розв'язки.

Обчислимо $a_1 = 40 : 4 = 10,\ b_1 = 16 : 4 = 4,\ m_1 = 68 : 4 = 17$ та розглянемо рівняння $10x = 4$ у кільці $\mathbb{Z}_{17}$.

Оскільки $10 \cdot (-5) + 17 \cdot 3 = 1$, то $10 \cdot (-5) \equiv 1 \pmod{17}$.

Оскільки $-5 \equiv 12 \pmod{17}$, то у $\mathbb{Z}_{17}$ $10^{-1} = 12$.

Тому $x_0 = 12 \cdot 4 = 48 \equiv 14 \pmod{17},\ x_1 = 14 + 17 = 31,\ x_2 = 14 + 17 \cdot 2 = 48,\ x_3 = 14 + 3 \cdot 17 = 65.$

Відповідь: $\{14, 31, 48, 65\}$.

4.2. Китайська теорема про лишки

Розглянемо систему

$$x \equiv b_1 \pmod{m_1},\ x \equiv b_2 \pmod{m_2},\ldots,x \equiv b_k \pmod{m_k}, \tag{1}$$

де числа $m_1, m_2, \ldots, m_k$ попарно взаємно прості.

Тоді довільний розв'язок x системи (1) задовольняє умову

$$x \equiv x_0 \pmod{m_1 m_2 \ldots m_k},$$

де

$$x_0 = M_1 M_1' b_1 + \ldots M_2 M_2' b_2 + \ldots + M_k M_k' b_k$$

і числа M_i, M_i' визначаються так:

$$M_i = m_1 \ldots m_{i-1} m_{i+1} \ldots m_k,\ \ M_i M_i' \equiv 1 \pmod{m_i}.$$

Приклад 13. Знайти розв'язок системи

$$\begin{cases} x = 3 \pmod{15}, \\ x = 2 \pmod{11}, \\ x = 5 \pmod{14}. \end{cases}$$

Розв'язання. $M_1 = 11 \cdot 14 = 154,\ M_2 = 15 \cdot 14 = 210,\ M_3 = 15 \cdot 11 = 165,\ m_1 \cdot m_2 \cdot m_3 = 15 \cdot 11 \cdot 14 = 2310.$

$154M_1' \equiv 1 \pmod{15} \Leftrightarrow 4M_1' \equiv 1 \pmod{15}$. Оскільки $4 \cdot 4 + 15 \cdot (-1) = 1$, то можна покласти $M_1' = 4$.

$210M_2' \equiv 1 \pmod{11} \Leftrightarrow M_2' \equiv 1 \pmod{11}$. Тому можна покласти $M_2' = 1$.

$165M_3' \equiv 1 \pmod{14} \Leftrightarrow 11M_3' \equiv 1 \pmod{14}$. Оскільки $11 \cdot (-5) + 14 \cdot 4 = 1$, то $M_3' \equiv (-5) \equiv 9 \pmod{14}$.

Отже $x_0 = 154 \cdot 4 \cdot 3 + 210 \cdot 1 \cdot 2 + 165 \cdot 9 \cdot 5 = 9693 \equiv 453 \pmod{2310}$.

4.3. Функція Ейлера

Нехай n — задане натуральне число. Позначимо через $\varphi(n)$ кількість чисел від 1 до $n-1$, взаємно простих із числом n. Функція $\varphi(n)$ називається *функцією Ейлера*.

Властивості функції Ейлера:

1) якщо p — просте число, то $\varphi(p) = p - 1$;

2) якщо числа m та n взаємно прості, то $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$;

3) якщо $n = p_1^{k_1} \dots p_r^{k_r}$ — розклад числа n у добуток степенів простих множників, то

$$\varphi(n) = p_1^{k_1 - 1}(p_1 - 1) \dots p_r^{k_r - 1}(p_r - 1) = n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right).$$

4) $\sum_{d|n}\varphi(d)=n$, де сума обчислюється по усіх дільникам числа n.

Приклад 14. Обчислити $\varphi(240)$.

Розв'язання. $240=3\cdot 80=3\cdot 5\cdot 16=3\cdot 5\cdot 2^4$. Тому $\varphi(240)=(3-1)\cdot(5-1)\cdot 2^3(2-1)=64$.

Теорема 10 (теорема Ейлера). Нехай a — натуральне число, взаємно просте із числом n. Тоді $a^{\varphi(n)}\equiv 1\pmod n$.

Доведення. З визначення функції випливає, що $\varphi(n)=\left|U(\mathbb{Z}_n)\right|$ — порядок групи оборотних елементів кільця $\mathbb{Z}_n$. Нехай k — порядок елемента a у групі $U(\mathbb{Z}_n)$. Оскільки порядок кожного елемента підгрупи є дільником порядку групи, то $\varphi(n)=k\cdot l$, де l — деяке натуральне число. Тоді $a^{\varphi(n)}=\left(a^k\right)^l\equiv 1^l\equiv 1\pmod n$.

Наслідок (мала теорема Ферма). Нехай p — просте число, $0<a<p$. Тоді $a^{p-1}\equiv 1\pmod p$.

ІІІ. ЕЛЕМЕНТИ ТЕОРІЇ ГРАФІВ

1. Основні поняття теорії графів

1.1. Предмет теорії графів. Основні означення.

Виникнення теорії графів пов’язано із *задачею про Кенігсберзькі мости*. Схема міста Кенігсберга наведена на рис. 12. Потрібно обійти усі чотири ділянки суші, пройшовши по кожному мосту один раз.

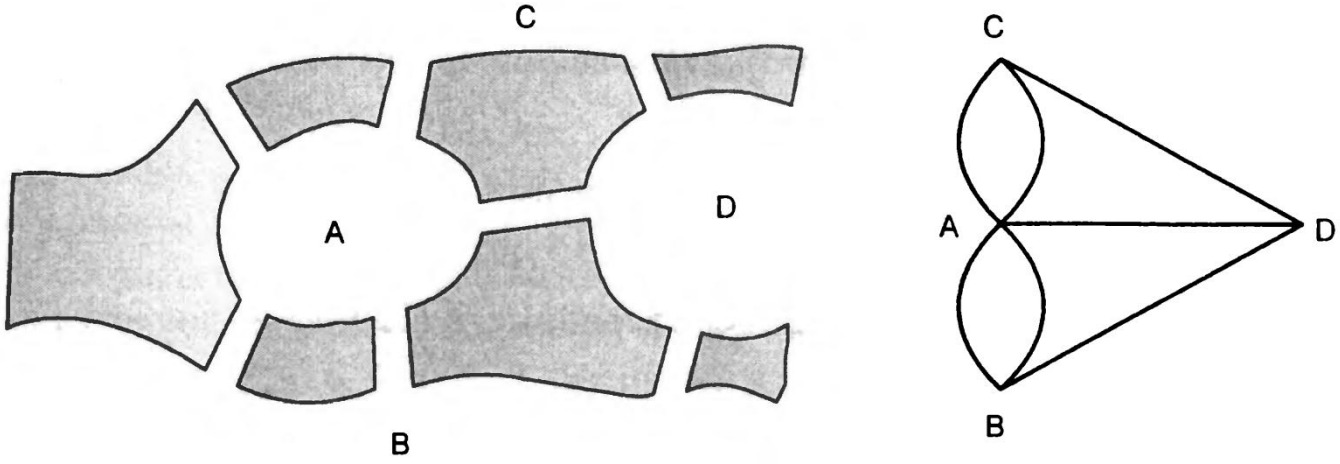


Рис. 12. Кенігсберзькі мости

Ще однією класичною задачею є *задача про три криниці*. Потрібно прокласти стежки від кожного будинку до кожної криниці таким чином, щоб стежки не перетиналися (див. рис. 13).

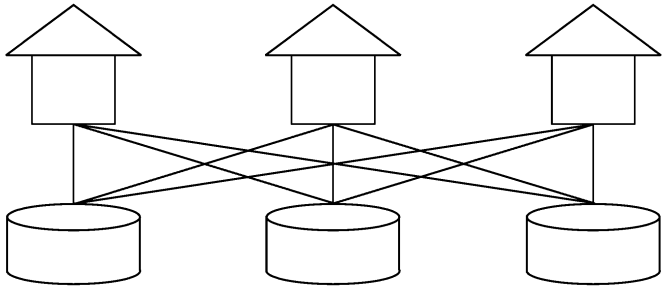


Рис. 13. Ілюстрація до задача про три криниці

Мультимножина (набір) — невпорядкована система об'єктів, *можливо із повтореннями*. При записі елементи мультимножини записуються у фігурних або трикутних дужках.

Приклад мультимножини: $\{a,b,b,c,a,a\}$.

Графом G називається пара (V,E), де *V — множина вершин* графа, *E — мультимножина ребер* графа.

Якщо множини *V* та *E* — скінченні, то граф називається *скінченним*.

Елементи мультимножини E називаються *ребрами* графа. Ребро e, яке з'єднує вершини a та b позначається $\langle a,b\rangle$ $\left(e=\langle a,b\rangle\in E,\ a,b\in V\right)$, при цьому вершини a та b називаються *суміжними* та *інцидентними* ребру e. Виокремлюють три види ребер:

ланки або невпорядковані ребра $\left(e=\{a,b\}\in\bar{E}\right)$. Набір ланок позначається $\bar{E}$;

дуги або впорядковані ребра $\left(e=(a,b)\in\vec{E}\right)$, $\vec{E}$ — набір дуг;

петлі — ребра вигляду $e=(a,a)$, початок і кінець якого співпадають.

Надалі будемо вважати, що *усі графи є скінченними* і петлі є різновидом дуг, тобто $E=\bar{E}\cup\vec{E}$. Кількість вершин графа називається його *порядком*. Приклад діаграми графа наведено на рис. 14.

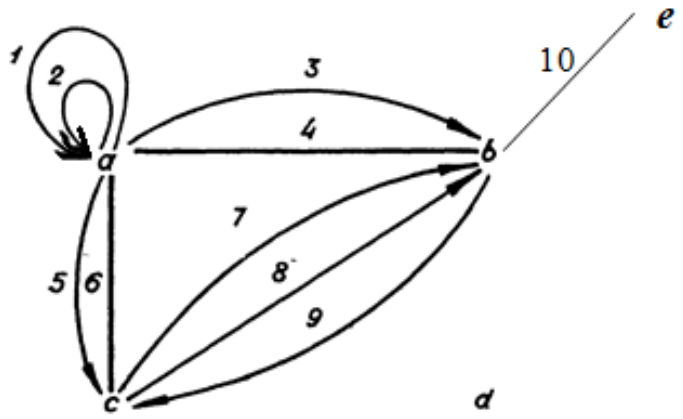


Рис. 14. Діаграма графа

Кількість ланок, інцидентних них вершині *v*, будемо позначати $\overline{\deg}(v)$.

Кількість дуг, які входять у вершину *v*, будемо позначати $\deg^+ v$.

Кількість дуг, які виходять із вершини *v*, будемо позначати $\deg^- v$.

Величина $\deg v$, яка обчислюється за формулою

$$\deg v = \overline{\deg} v + \deg^+ v + \deg^- v,$$

називається степеню вершини *v*.

Приклад. Обчислимо степінь вершини *a* графа, діаграма якого зображена на рис. 14.

$$\overline{\deg}(a) = 2,\ \deg^+(a) = 2,\ \deg^-(a) = 4,\ \deg(a) = 2+2+4 = 8.$$

Вершина *v* називається *ізольованою*, якщо $\deg(v) = 0$.

Вершина *v* називається *висячою*, якщо $\deg(v) = 1$.

Для графа, наведеного на рис. 14, вершина *d* є ізольованою, а вершина *e* — висяча.

Лема про рукостискання. Для довільного графа (V, E)

$$\sum_{v\in V}\deg(v)=2|E|;$$

$$\sum_{v\in V}\deg^{+}(v)+\sum_{v\in V}\deg^{-}(v)=2|\vec{E}|.$$

Граф $G_1=(E_1,V_1)$ називається *підграфом* графа $G=(V,E)$, якщо $V_1\subseteq V$, $E_1\subseteq E$.

Приклад. Граф, діаграма якого наведена на рис. 15, є підграфом графа з рис. 14.

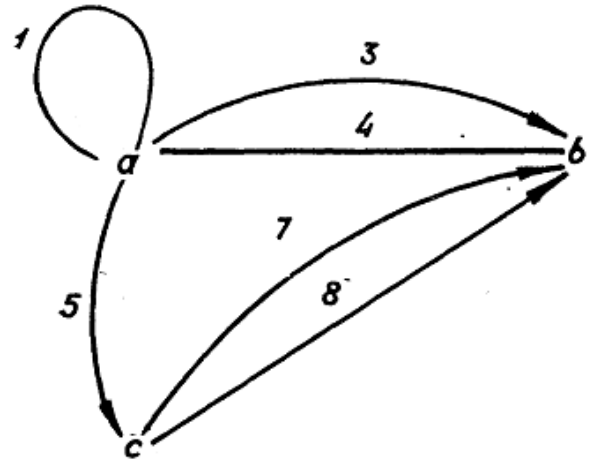


Рис. 15. Підграф графа з рис. 14.

Ізоморфізм графів — це бієкція (взаємно-однозначна відповідність) множин вершин графів, яка зберігає суміжність вершин. Тобто графи $G_1 = (V_1, E_1)$ та $G_2 = (V_2, E_2)$ *ізоморфні*, якщо бієкція $f : V_1 \to V_2$ задовольняє умову:

для довільних $a, b \in V_1 \quad \langle a, b \rangle \in E_1 \Leftrightarrow \langle f(a), f(b) \rangle \in E_2$.

Теорема 1. Ізоморфізм графів є відношенням відношення еквівалентності (на множині графів).

Приклад. Графи, діаграми яких наведені на рис. 16, є ізоморфними.

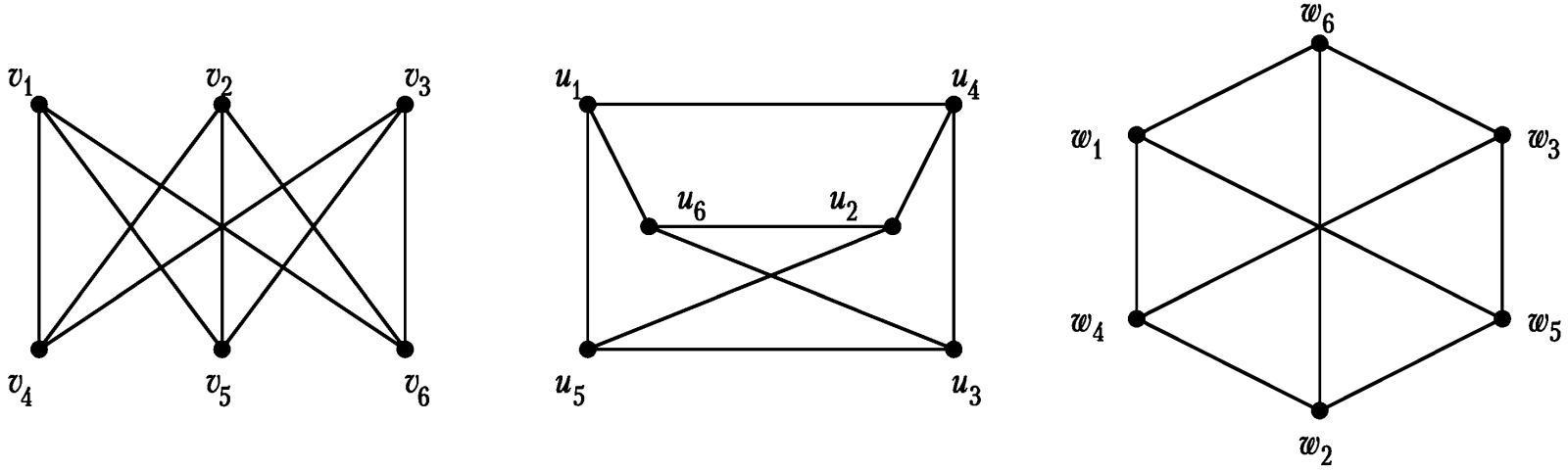


Рис. 16. Ізоморфні графи

Слід зазначити, що кількість вершин, ребер та степені вершин не визначають граф однозначно. На рис. 17 наведено діаграми двох неізоморфних графів, для яких усі відповідні параметри співпадають:

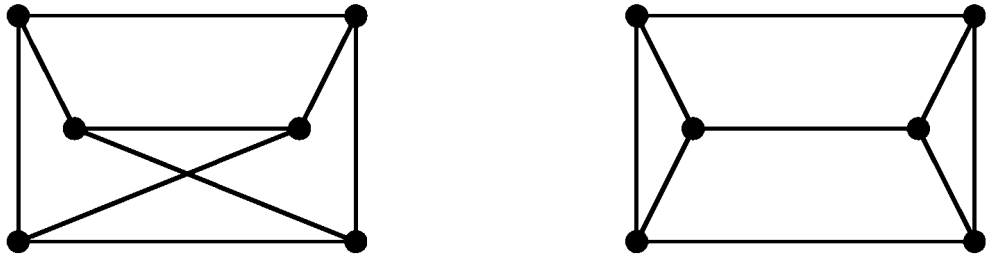


Рис. 17. Діаграми неізоморфних графів

1.2. Способи задання графів.

Основні способи задання графів:

a) перелік елементів:

Множин E та V задаються переліком їх елементів.

Приклад. Задамо переліком елементів граф, діаграма якого наведена на рис. 14:

$G=(V,E),\ V=\{a,b,c,d,e\},\ E=\{e_1=(a,a),\ e_2=(a,a),\ e_3=(a,b),\ e_4=\{a,b\},$

$e_5=(a,c),\ e_6=\{a,c\},\ e_7=(c,b),\ e_8=(c,b),\ e_9=(b,c),\ e_{10}=\{b,e\}\};$

b) графічна інтерпретація (діаграма);

c) матриця *інцидентності*.

Рядки матриці відповідають вершинам, стовпці — ребрам. Якщо вершина v_i інцидентна ребру e_j, то елемент b_{ij} матриці інцидентності B рівний:

1) –1, якщо e_j — дуга, яка виходить з вершини v_i і не є петлею;

2) 1 — у всіх інших випадках.

Якщо вершина не інцидентна ребру, то відповідний елемент матриці рівний 0.

Для графа з рис. 14 матриця інцидентності має вигляд

$$B = \begin{pmatrix} 1 & 1 & -1 & 1 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & -1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & -1 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

d) *матриця суміжності* (сусідства)

Матриця сусідства A — квадратна матриця порядку $|V|$, елементи визначаються наступним чином:

$$a_{ij} = \alpha \bar{a}_{ij} + \beta \vec{a}_{ij},$$

де $\bar{a}_{ij}$ — кількість ланок, які з'єднують вершини v_i та v_j, $\vec{a}_{ij}$ — кількість дуг, які виходять із вершини v_i і входять у вершину v_j.

Для графу з рис. 14. матриця суміжності має вигляд

$$A=\begin{pmatrix} 2\beta & \alpha+\beta & \alpha+\beta & 0 & 0 \\ \alpha & 0 & \beta & & \alpha \\ \alpha & 2\beta & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 & 0 \end{pmatrix}.$$

1.3. Основні види графів.

Виокремлюють наступні види графів:

1) порожній граф (або 0-граф) $\left(V=\varnothing\right)$;

2) *неорієнтований граф* $\left(E=\bar{E}\right)$;

3) *звичайний граф* (неорієнтований без кратних ребер);

4) *орієнтований граф* (усі ребра — дуги, тобто $E=\vec{E}$);

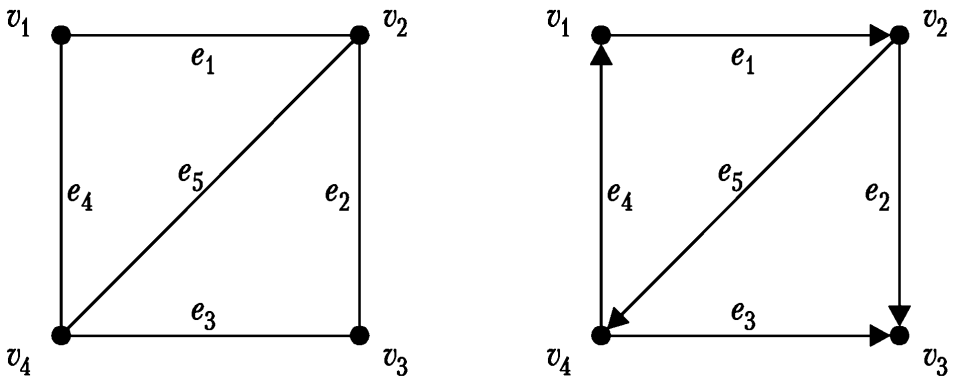


Рис. 18. Діаграми звичайного а) та орієнтованого б) графів

Неорієнтований граф $G' = (V, E')$ називається *відповідним* до орієнтованого графа $G = (V, E)$, якщо $E' = \left\{ \{a,b\} \middle| (a,b) \in E \right\}$. Граф 18 а) є відповідним до графа 18 б).

5) мультиграф (допустимими є кратні ребра);

6) псевдограф (мультиграф, для якого допускаються петлі);

7) дводольний (біхроматичний) граф — множина вершини V розбивається на дві множини V_1, V_2 $\left(V_1 \cup V_2 = V,\ V_1 \cap V_2 = \varnothing\right)$ так, що кожне ребро інцидентні одній вершині з V_1 та одній вершині з V_2;

8) граф Кеніга — звичайний дводольний граф;

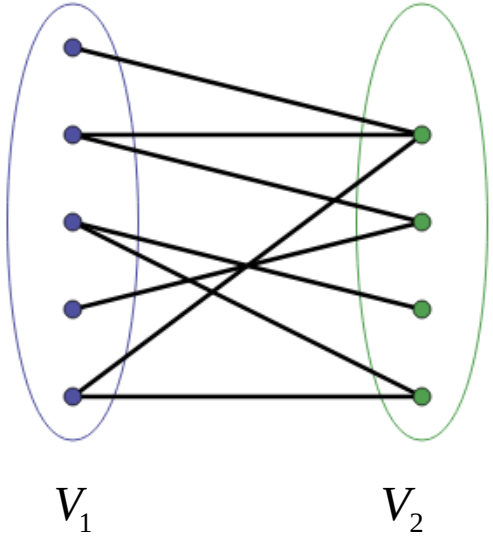


Рис. 19. Граф Кеніга

9) повний граф — граф, який містить усі ребра для графів заданого типу:

10) K_n — повний звичайний граф;

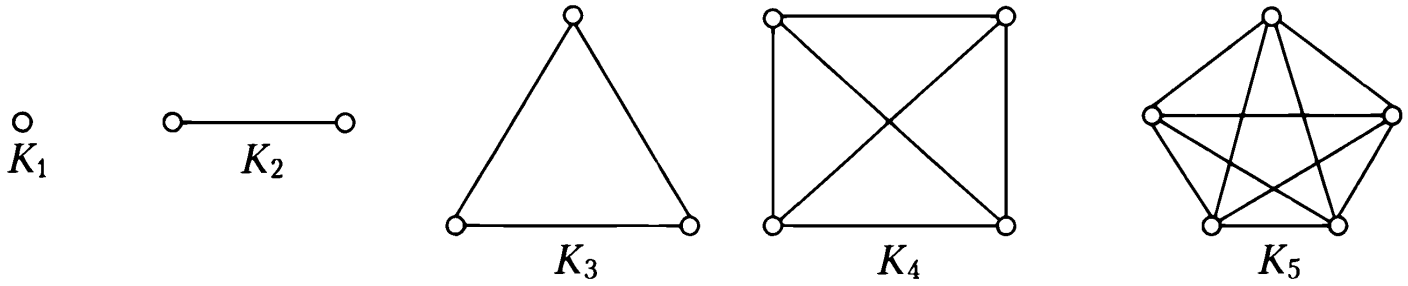


Рис. 20. Повні графи K_n для n = 1, 2, 3, 4, 5

$K_{n,m}$ — повний граф Кеніга (n та m — кількості елементів множин V_1 та V_2);

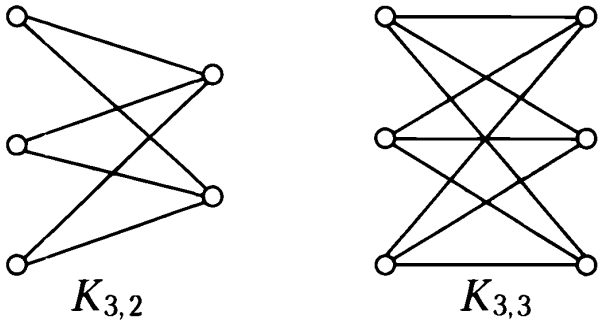


Рис. 21. Повні графи Кеніга

Граф $K_{1,m}$ називається *зірковим*.

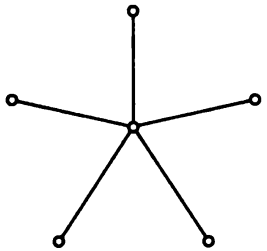
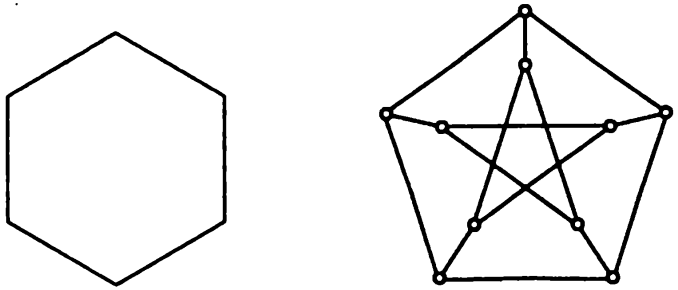


Рис. 22. Зірковий граф $K_{1,5}$

Однорідні (регулярні) графи степеня d — звичайні графи, степені усіх вершин яких рівні d ($\forall v \in V \ \deg v = d$). Зв'язний однорідний граф степені 2 називається *циклічним графом*. Циклічний граф n-го порядку позначається C_n.



а) б)

Рис. 23. Регулярні графи: а) граф C_6; б) кубічний граф Петерсена

Теорема 2. Нехай $n, d \in \mathbb{N}$ — натуральні числа, $0 \le d \le n-1$. Тоді існує регулярний граф n-го порядку степеня d.

n-вимірний куб — звичайний граф, вершинами якого є n-вимірні булеві вектори, вершини $\boldsymbol{u}$ та $\boldsymbol{v}$ суміжні тоді і тільки тоді, коли $d(\mathbf{u}, \mathbf{v}) = 1$ (відстань Хеммінга між вершинами рівна 1).

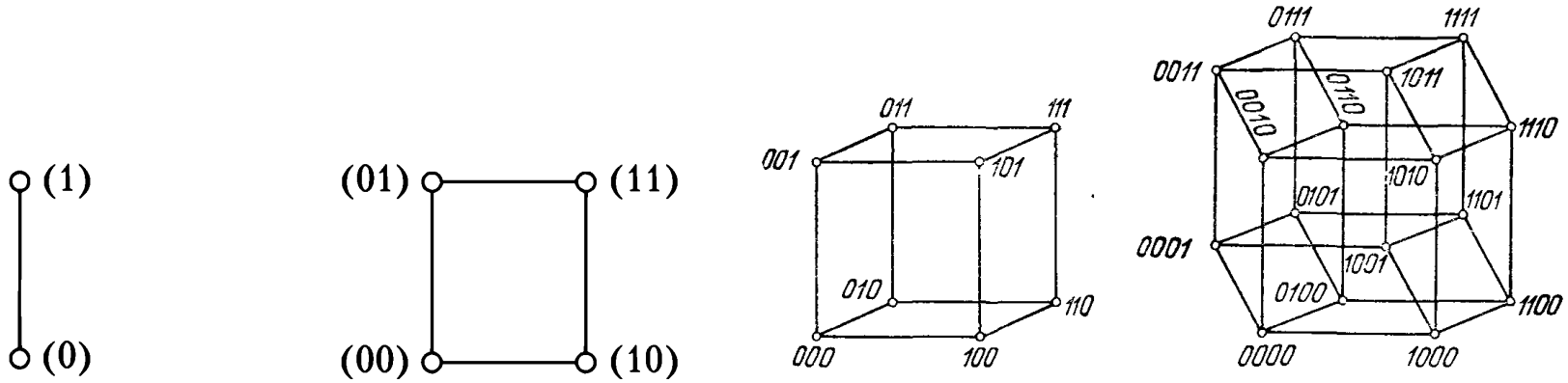


Рис. 24. n-вимірний куб

Турнір (повний орієнтований граф без петель та кратних дуг).

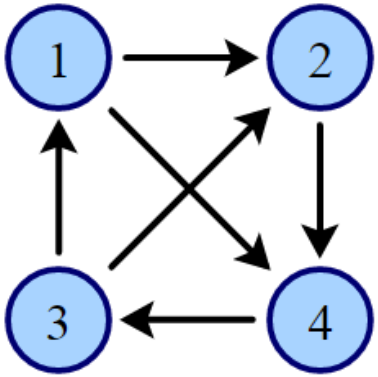


Рис. 25. Діаграма турніру

Помічені та нумеровані графи.

Якщо задана функція $f : V \to M$ та (або) $g : E \to M$, то множина M називається множиною *міток*, а граф G називається *поміченим*. Якщо функції f та g однозначні (ін'єктивні) і $M \subset \mathbb{N}$, то граф називається *(про)нумерованим*.

Прикладом нумерованого графа є граф, зображений на малюнку 25.

2. Маршрути у графі.

Нехай $G = (V, E)$ — заданий граф, $a = v_{i_0}$, $b = v_{i_m}$. Послідовність вершин та ребер

$$M(a,b) = ae_{j_1}v_{i_1}e_{j_2}\ldots v_{i_{n-1}}e_{j_n}b,$$

де e_{j_k} — ребро, інцидентне вершинам v_{i_k-1} та v_{i_k} називається *маршрутом довжини n*, який з'єднує вершини *a* та *b*. Вершини *a* та *b* називаються *кінцями маршруту*.

Якщо усі ребра маршруту є дугами $\left(e_{j_k} = \left(v_{i_k-1}, v_{i_k}\right),\ j = 1,\ldots,n\right)$, то маршрут називається *шляхом*, який з'єднує вершину *a* з вершиною *b*.

Маршрут називається *простим*, якщо вершини у ньому не повторюються (крім, можливо першої та останньої).

Якщо усі ребра у маршруті $M(a,b)$ є різними, то маршрут називається *ланцюгом*, який з'єднує вершини *a* та *b* і позначається $L(a,b)$.

Замкнений ланцюг називається *циклом*.

Орієнтований цикл називається *контуром*.

Приклади.

Теорема 3. Довільний маршрут, який з'єднує графа вершини *a* та *b* містить у собі простий ланцюг.

Теорема 4. Довільний цикл містить у собі простий цикл. Довільний цикл непарної довжини містить у собі простий цикл непарної довжини.

Теорема 5 (Кеніга). Звичайний граф дводольний тоді і тільки тоді, коли для нього не має простих циклів непарної довжини.

2.1. Метричні характеристики графів

Відстань між вершинами u та v неорієнтованого графа — це довжина найкоротшого ланцюга, який з'єднує ці вершини. Відстань позначається $d(u,v)$.

Найкоротша *геодезична* між двома вершинами — найкоротший ланцюг, який їх з'єднує.

Діаметр графа — максимальна відстань між вершинами:

$$D(G) = \max\{d(u,v) \mid u,v \in V\}.$$

Ексцентриситет $\varepsilon(v)$ вершини v — відстань до найбільш віддаленої від неї вершини:

$$\varepsilon(v) = \max\{d(v,u) \mid u \in V\}.$$

Радіус графа — мінімальний ексцентриситет:

$$R(G) = \min\{\varepsilon(v) \mid v \in V\}.$$

Центр графа — множина вершин графа, які мають мінімальний ексцентриситет:

$$C(G)=\{v \mid \varepsilon(v)=R(G)\}.$$

Приклад. Вказати ексцентриситети вершин, центр, радіус та діаметр графа, діаграма якого наведена на рис. 26.

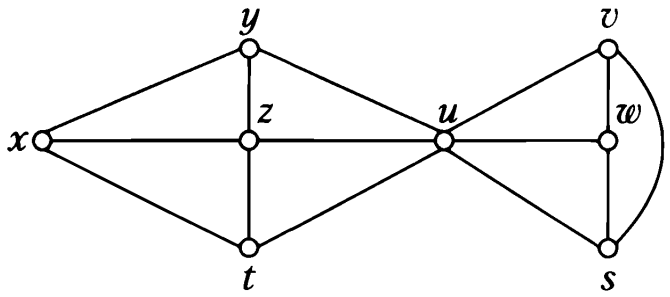


Рис. 26

$\varepsilon(x)=\varepsilon(v)=\varepsilon(w)=\varepsilon(s)=3,\ \varepsilon(y)=\varepsilon(z)=\varepsilon(t)=\varepsilon(u)=2.$

$D(G)=3,\ R(G)=2,\ C(G)=\{y,z,t,u\}.$

3. Зв’язність. Компоненти зв’язності

3.1. Відношення зв’язності у неорієнтованому графі.

Вершини $a,b \in V$ неорієнтованого графу $G=(V,E)$ називаються *зв’язними*, якщо можна побудувати ланцюг, який їх з’єднує. При цьому вершина вважається зв’язною із самою собою.

Відношення зв’язності є відношенням еквівалентності на множині вершин. *Компоненти зв’язності* графа — класи еквівалентності за відношенням зв’язності.

Кількість компонент зв’язності позначається $\kappa(G)$.

Граф G, зображений на рис. 27, має три компоненти зв’язності (G_1, G_2 та G_3).

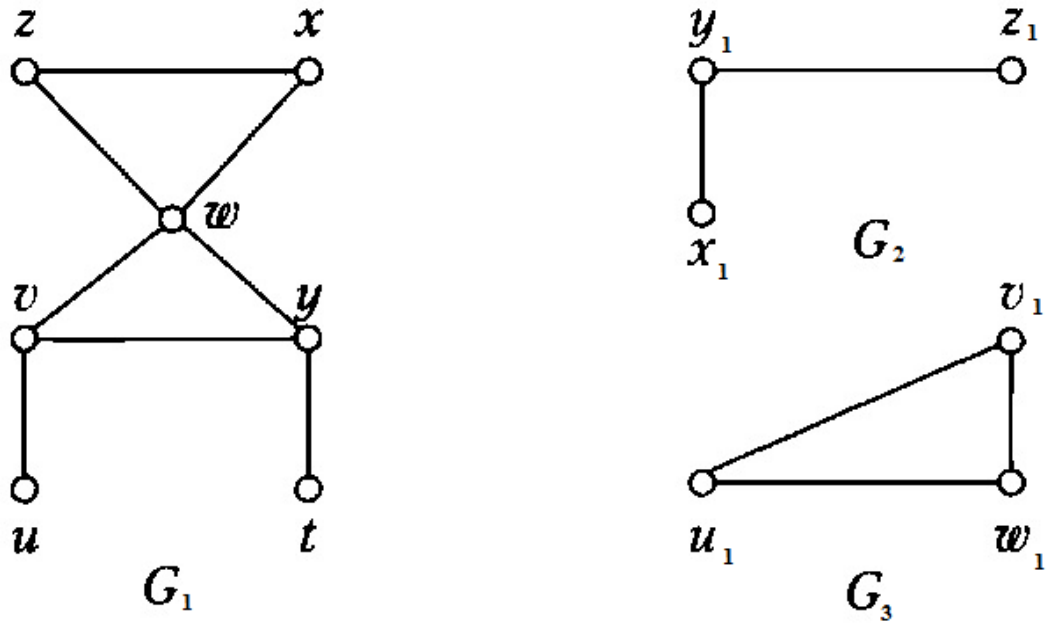


Рис. 27. Граф із трьома компонентами зв’язності

Зв’язний граф — це граф, усі вершини якого зв’язні між собою $\left(\kappa(G)=1\right)$.

3.2. Класифікація ребер та вершин неорієнтованих графів з точки зору зв’язності

Міст — ребро графа, видалення якого збільшує кількість компонент зв’язності. Усі інші ребра — *циклові*.

Точка зчеплення (шарнір) — вершина графа, видалення якої збільшує кількість компонент зв’язності.

Приклад. На рис. 28 ребро *x* — міст, усі інші ребра — циклові. Вершини *u* та *v* — мости.

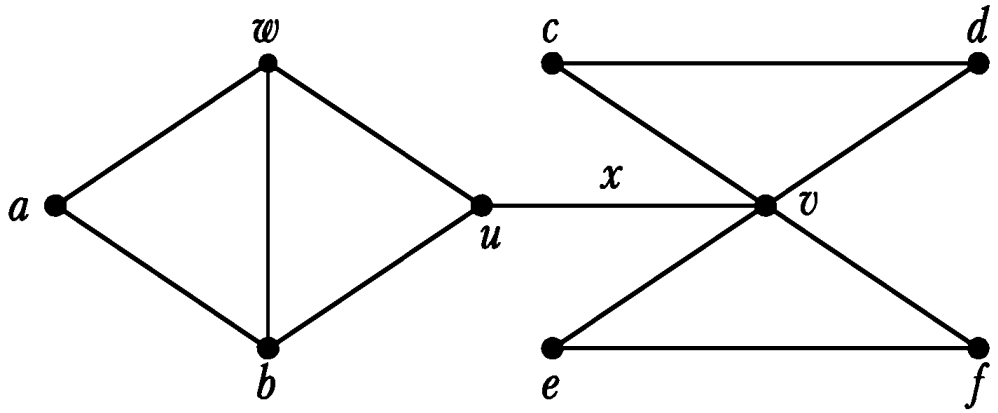


Рис. 28. Ребра та мости

Теорема 6. Кожний простий цикл містить циклове ребро.

Теорема 7. Кількість ребер звичайного графа задовольняє нерівність

$$|V|-\kappa(G)\le|E|\le\big(|V|-\kappa(G)\big)\big(|V|-\kappa(G)+1\big)/2.$$

Наслідок. Якщо $|E|>(|V|-1)(|V|-2)/2$, то граф $G=(V,E)$ — зв'язний.

3.3. Зв'язність у орієнтованих графах

Вершина b називається *досяжною* із вершини a орієнтованого графа G, якщо існує шлях, який з'єднує a з b.

Відношення досяжності не є відношенням еквівалентності.

Вершини $a,b\in V$ орієнтованого графу $G=(V,E)$ називаються *сильно зв'язними*, якщо вершина a є досяжною із b і навпаки.

Відношення сильної зв'язності є відношенням еквівалентності на множині вершин. На рис. 29 зображено *компоненти сильної зв'язності*.

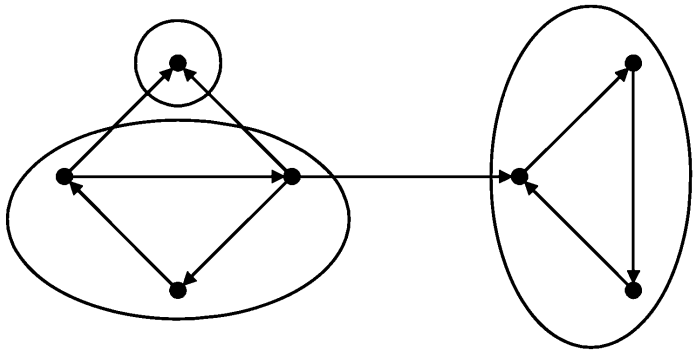


Рис. 29. Компоненти сильної зв'язності

3.4. Обхід графів

Обхід графів — систематичний перелік вершин графа. У більшості випадків вказується початкова вершина, з якої треба починати обхід.

Алгоритм обходу вершин графа

Вважаємо, що на початку усі вершини не відмічені.

Заносимо у список *L початкову вершину*.

while $L \neq \varnothing$

{

видаляємо із списку *L* першу вершину *v;*

позначаємо вершину *v* як відвідану;

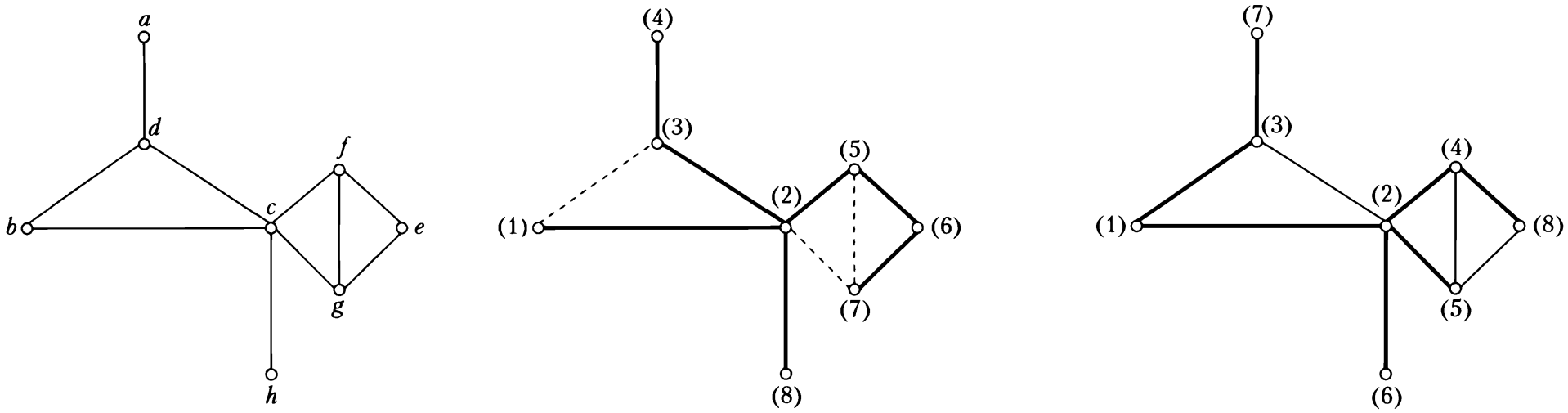
додаємо до *L* усі не відвідані вершини, у які можна потрапити із *v;*

}

Якщо у алгоритмі обходу нові вершини додаються у початок списку, то такий обхід називається *пошуком у глибину*.

Якщо у алгоритмі обходу нові вершини додаються у кінець списку, то такий обхід називається *пошуком у ширину*.

На рис. 30 продемонстровано обхід графа із застосуванням пошуку у глибину та ширину, починаючи із вершини *b*:



а б в

Рис. 30. Обхід графа у глибину (б) та ширину (в)

Приклад. Провести обхід вершин звичайного графа, діаграма якого наведена на рис. 31, починаючи із вершини *a* (попередньо позначити усі інші вершини).

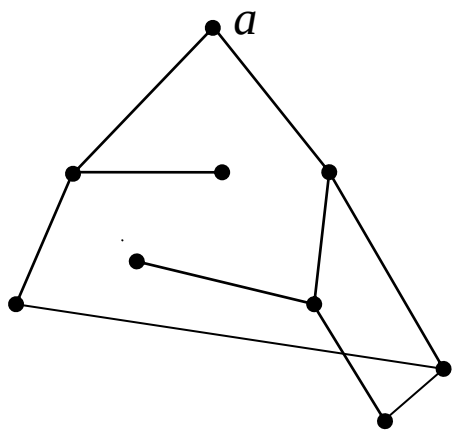


Рис. 31.

Зауваження. У наступних трьох темах усі графи (якщо це спеціально не обумовлено в умові) вважаються неорієнтованими.

4. Ейлерові та гамільтонові графи

4.1. Графи Ейлера

Граф Ейлера (ейлерів граф) — це зв'язний граф, для якого існує цикл, який містить усі ребра.

Прикладом графа Ейлера є граф G_1 на рис. 32. Графи G_2 та G_3 не є графами Ейлера.

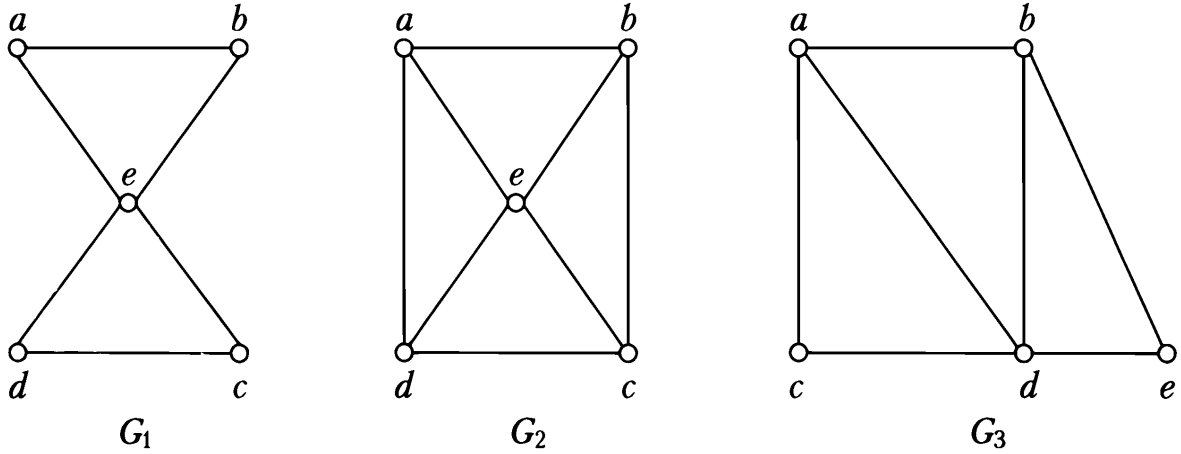


Рис. 32.

Теорема 8. Зв’язний граф є ейлеровим тоді і тільки тоді, коли степені усіх вершин є парними.

Наслідок. Зв’язний граф є ейлеровим тоді і тільки тоді, коли множину його ребер можна розбити на цикли, що не перетинаються.

Ланцюг, який містить усі ребра графа називається *ланцюгом Ейлера*. Граф, для якого існує ланцюг Ейлера називається напівейлеровим графом.

Прикладом напівейлерового графа є граф G_3.

Теорема 9. Зв’язний граф є напівейлеровим тоді і тільки тоді, коли не більше двох його вершин мають непарну степінь.

На рис. 33 зображено граф із задачі про кенігсберзькі мости. Оскільки степені усіх чотирьох вершин непарні, то він не є ні ейлеревим, ні напівейлеровим.

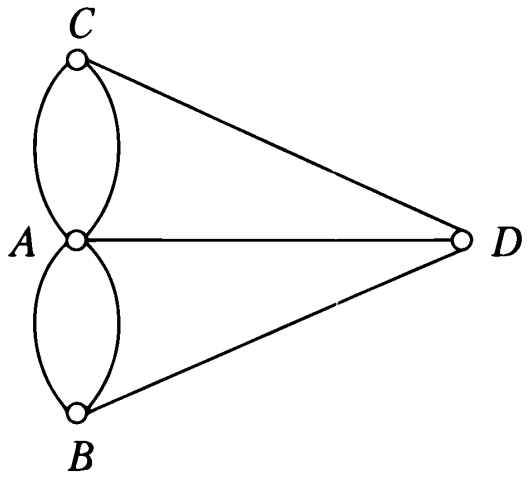


Рис. 33. Граф для задачі про кенігсберзькі мости

Алгоритм Флері знаходження ейлерового ланцюга:

1) Починаємо з вершини з непарною степеню (або з довільної вершини у випадку парності степенів усіх вершин).

2) стираємо (викреслюємо) пройдені ребра та ізольовані вершини, які виникають в процесі руху.
3) на кожному кроці вибираємо міст в якості наступного ребра тільки тоді, коли немає циклових ребер, інцидентних поточній вершині.

4.2. Гамільтонові графи.

Зв’язний граф називається *гамільтоновим*, якщо існує цикл, який проходить через кожну вершину графа рівно один раз.

Прикладом графа Гамільтона є граф, наведений на рис 34 (на діаграмі ребра циклу виділені товстішими лініями).

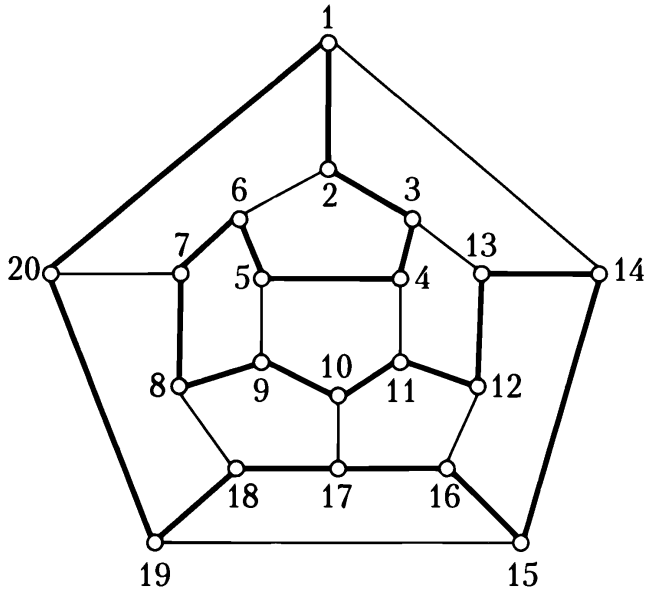


Рис. 34. Гамільтонів шлях

Теорема 10 (теорема Дірака). Якщо у графі $G=(V,E)$ з $n\geq 3$ вершинами степінь кожної вершини не менша за $n/2$, то граф G є гамільтоновим.

5. Планарні графи

Граф допускає *вкладення* (вкладається) на деякій поверхні, якщо його можна зобразити на цій поверхні так, щоб ребра графа не перетиналися.

Граф називається *планарним*, якщо його можна вкласти на площину.

На рис. 35 зображено діаграму планарного графа K_4 та його вкладення.

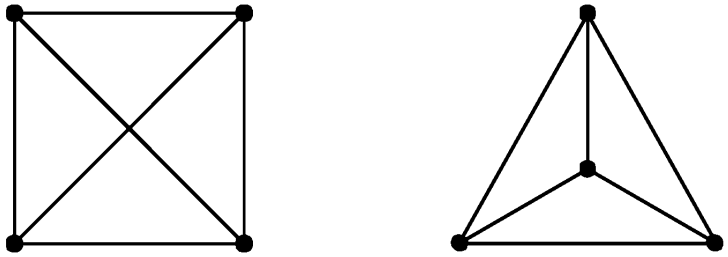


Рис. 35. Вкладення графа K_4

Теорема 11. Граф G вкладається на сфері тоді і тільки тоді, коли він є планарним.

Частина площина, обмежена ребрами планарного графа, називається *гранню*. Множина граней планарного графа позначається F. У цю множину включається також і зовнішня частина площини. Для графа, зображеного на рис. 36, $F = \{r_1, r_2, r_3, r_4\}$.

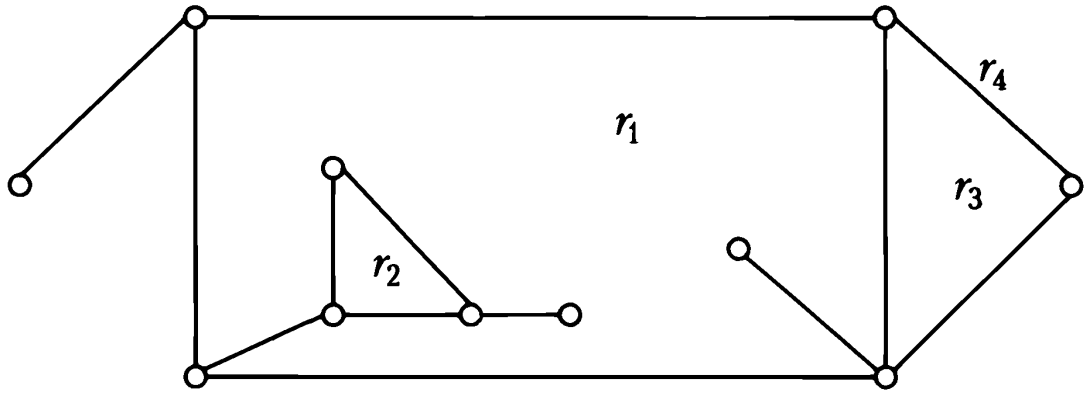


Рис 36. Грані планарного графа

Теорема 12 (формула Ейлера). Для планарного графа

$$|V|-|E|+|F|=\kappa(G)+1.$$

Наслідок 1. Для довільного випуклого многогранника

$$B + Г - P = 2,$$

де B — кількість вершин многогранника, $Г$ — кількість граней, P — кількість ребер.

Наслідок 2. У будь-якому планарному графі без кратних ребер та петель $|E|\le 3|V|-6$.

Наслідок 3. Графи K_5 та $K_{3,3}$ не є планарними.

Наслідок 4. У будь-якому планарному графі без кратних ребер та петель існує вершина, степінь якої не більша за 5.

6. Дерева

6.1. Ліс

Нехай $G=(V,E)$ — заданий неорієнтований граф. Величина

$\lambda(G)=|E|-|V|+\kappa(G)$.

Називається *цикломатичним* числом графа G.

Теорема 13. Для довільного графа G

$$\lambda(G)\geq 0 \text{ і } \lambda(G)=0 \Leftrightarrow \text{ граф } G \text{ не містить циклів.}$$

Ліс — це граф без циклів. Приклад лісу зображено на рис. 37.

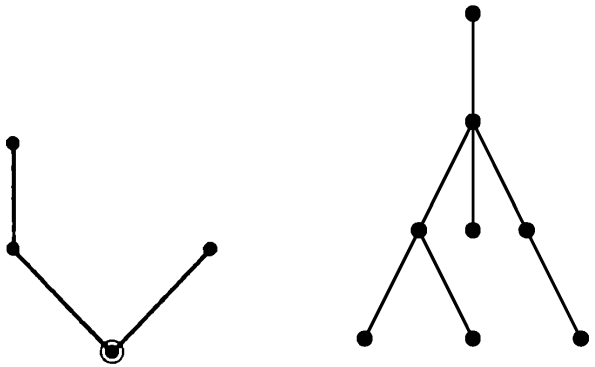


Рис 37. Ліс

Теорема 14. Наступні твердження про граф G є еквівалентними:

1) G — ліс;

2) G не містить простих циклів;

3) Всі ланцюги в G — прості;

4) $\lambda(G) = 0$.

6.2. Неорієнтовані дерева

Дерево — зв’язний граф без циклів. Приклад дерева зображено на рис. 38.

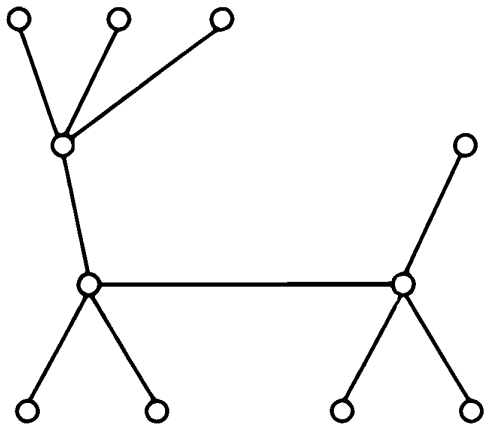


Рис. 38. Дерево

Теорема 15. Наступні твердження про граф G є еквівалентними:

1) G — дерево;

2) Будь-які дві вершини в G з'єднані рівно одним простим ланцюгом;

3) G — зв'язний граф, кожне ребро якого — міст;

4) $|V|=|E|+1$ і $\kappa(G)=1$;

5) $\lambda(G)=0$, але після добавлення довільного нового ребра $\lambda(G)=1$.

Наслідок. У нетривіальному дереві є принаймні дві висячі вершини.

6.3. Нумеровані дерева. Задання дерев за допомогою кодів Прюфера

Для компактного подання нумерованих дерев використовується *код Прюфера*, який для дерева з n вершинами містить $n-2$ числа.

При побудові коду на кожному кроці видаляється висяча вершина із найменшим номером і номер вершини, з якою вона була пов’язана, дописується у кінець коду.

Код Прюфера для дерева на рис. 39: 7, 9, 1, 7, 2, 2, 7, 1, 2, 5

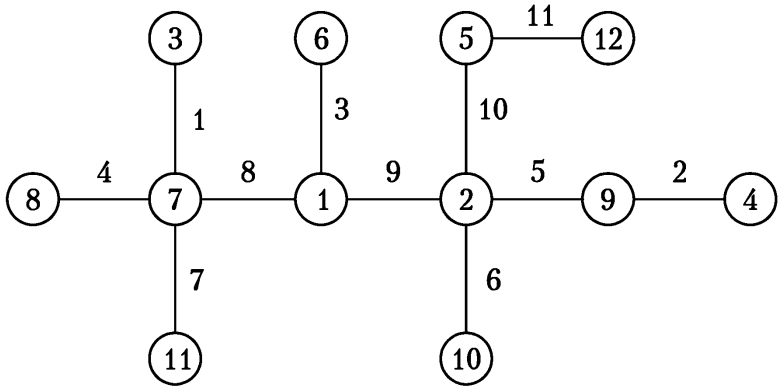


Рис. 39. Приклад побудови коду Прюфера для нумерованого дерева

При декодування на i-му $(i = 1,2,\ldots,n-2)$ кроці із списку ще невикористаних вершин вибирається (без повернення) вершина з найменшим номером, який не зустрічається у ще не обробленій частині коду Прюфера. Ця вершина з'єднується з i-ою вершиною у коді Прюфера. У кінці з'єднуються останні дві невикористані вершини.

Теорема 16 (теорема Келі). Кількість нумерованих дерев із n вершинами рівна n^{n-2}.

6.4. Кореневі дерева.

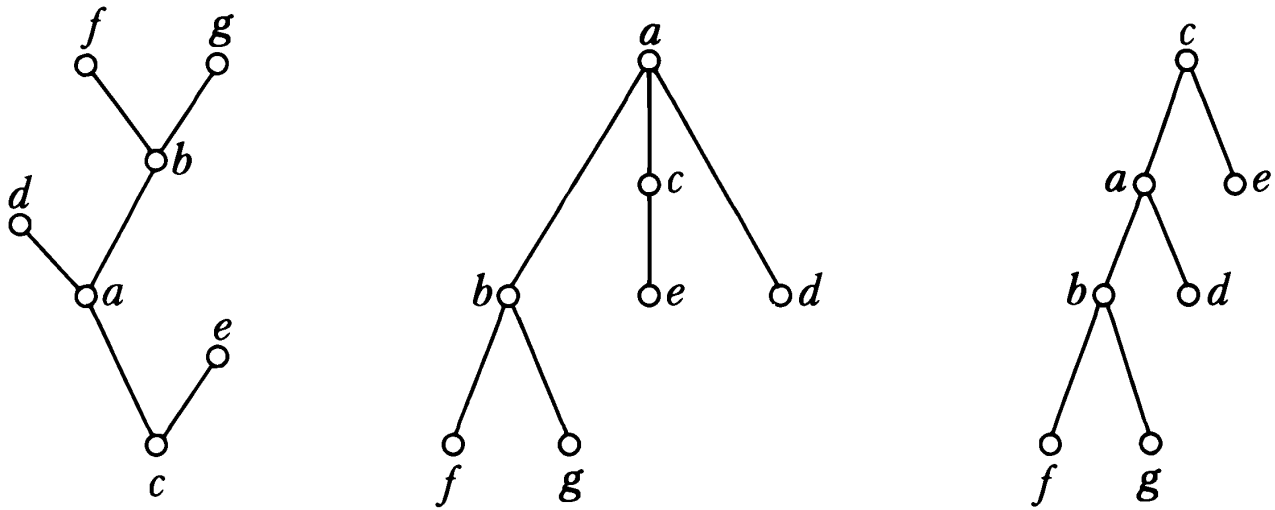
У *кореневих деревах* у множині вершин виділяється *корінь*. Орієнтація вершин кореневих дерев відбувається у напрямку від кореня. Якщо вершини v та u — суміжні і відстань від v до кореня дерева більша за відстань від u до кореня, то вершина v називається *дочірньою* вершиною для u, а вершина u — *батьківської* для v.

Теорема 17. Кожна вершина крім кореня має рівно одну батьківську вершину.

Листи — це вершини кореневого дерева, які не мають дочірніх вершин.

Множина вершин, які розташовані на однаковій відстані від кореня називається *ярусом* дерева.

Дерева б)-в) на рис. 40 — кореневі дерева з коренем a та c відповідно, які отримуються із звичайного дерева а). На рис. 40 в) a, e — вершини 1-го ярусу, b, d — 2-го, f, g — 3-го.



а) б) в)

Рис. 40. Приклад кореневих дерев з коренями *a* та *c* відповідно

6.5. Орієнтовані дерева

Означення *орієнтованого дерева*:

Існує єдина вершина *r* (корінь), для якої $\deg^+(r)=0$.

Для всіх інших вершин $v \in T \deg^+(v)=1$.

Кожна вершина досяжна із кореня.

Зауваження. При зображені орієнтованих дерев вважають, що дуги спрямовані зверху вниз. Тому на діаграмах часто не зображають стрілки.

Еквівалентне означення ордерева T з використанням піддерев.

Є єдиний елемент r — корінь.

Усі інші вершини містяться у k $(k \geq 0)$ підблоках, які називаються піддеревами.

$T = \{r, T_1, \ldots, T_k\}$.

Для *упорядкованих дерев* також вказується відносний порядок піддерев $T_1, \ldots, T_k$.

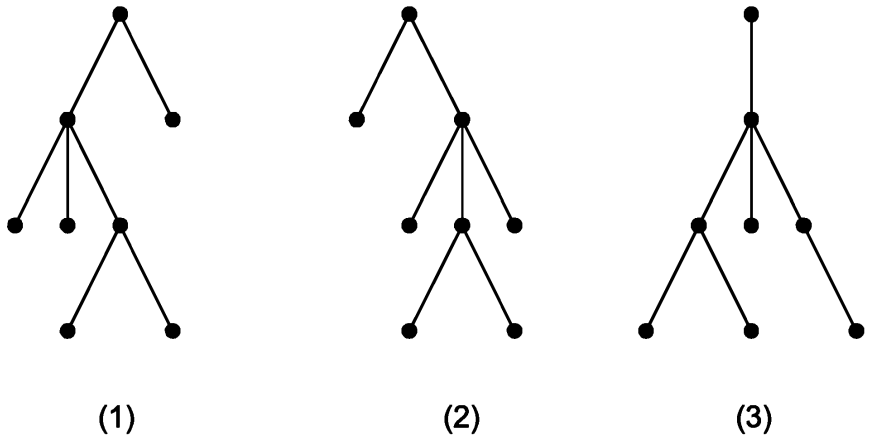


Рис. 41. Діаграми орієнтованих дерев

Наведені на рис. 41 дерева є ізоморфними як звичайні дерева та не ізоморфними, як впорядковані дерева. Як орієнтовані дерева (1) та (2) ізоморфні, але (2) та (3) та (1) та (3) не є ізоморфними.

6.6. Бінарні дерева

Означення *бінарного дерева*:

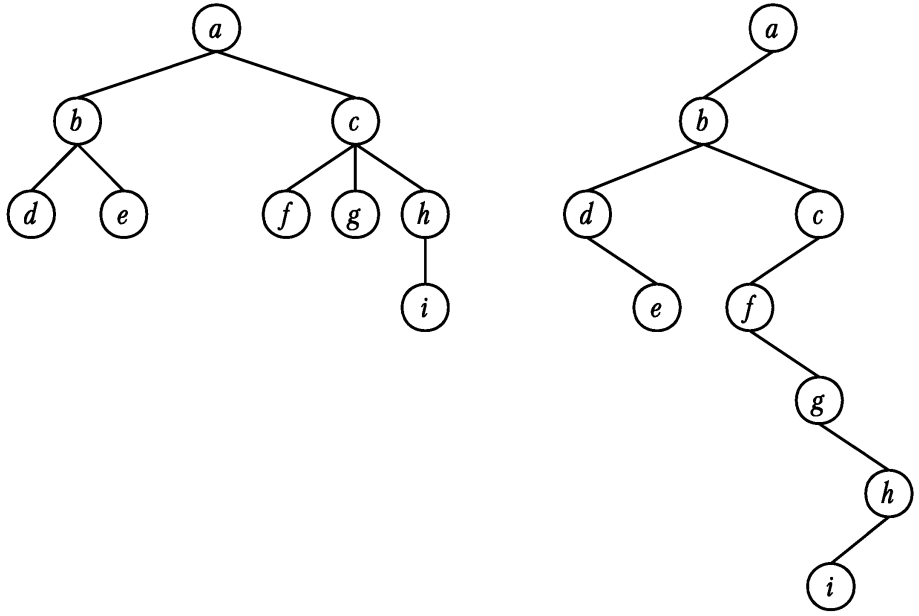
Є одна вершина — корінь дерева.

Усі інші вершини належать одному із піддерев (лівому чи правому), які не перетинаються.

За допомогою бінарних дерев можна зобразити (подати) довільне упорядковане дерево.

При переході до бінарних дерев для кожної вершини ліве ребро з’єднує її із старшим сином (у початковому дереві), праве ребро — із наступним (молодший) братом у початковому дереві.

На рис. 42 наведено упорядковане дерево а) та відповідне йому бінарне дерево б).



а) б)

Рис. 42. Зображення упорядкованого дерев а) за допомогою бінарного б)

Теорема 18. Кількість різних бінарних дерев із *n* вершинами рівна $\frac{1}{n+1}C_{2n}^{n}$.

***Обходи* бінарних дерев**:

прямий (префіксний): корінь, ліве піддерево, праве піддерево;

внутрішній (інфіксний, симетричний): ліве піддерево, корінь, праве піддерево;

кінцевий (зворотний, постфіксний): ліве піддерево, праве піддерево, корінь.

- обхід у прямому порядку: *a b d e h o c f m p q*;
- обхід у внутрішньому порядку: *d b h e o a f c p m q*;
- обхід у зворотному порядку: *d h o e b f p q m c a.*

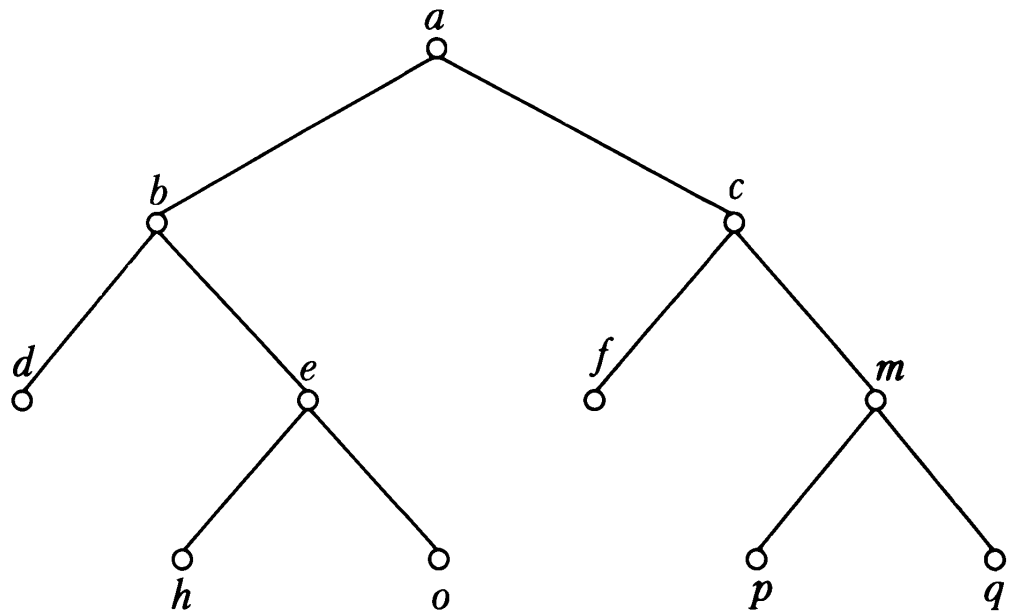


Рис. 43. Обхід бінарного дерева

Дерева арифметичних виразів (листи відповідають числам або змінним, внутрішні вершини — операціям)

Приклад. Розглянемо вираз $\left(a+\frac{b}{c}\right)*(d-e*f)$.

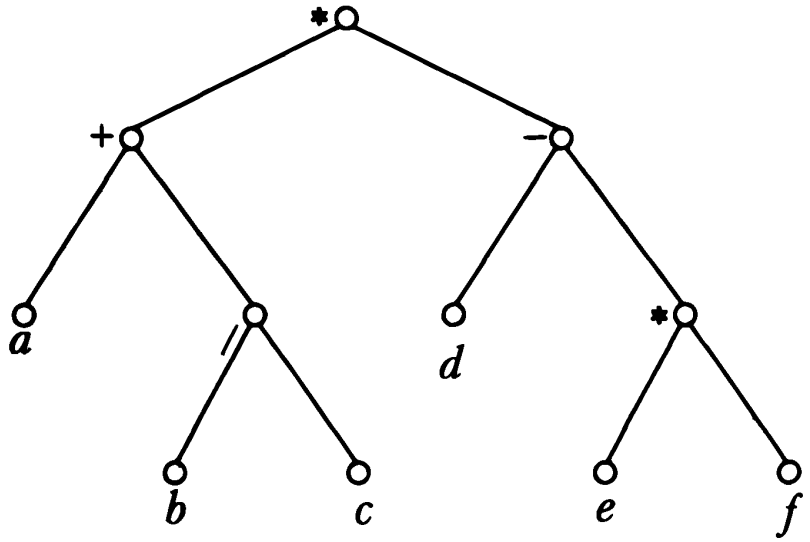


Рис. 44. Дерево арифметичного виразу

- у разі обходу в прямому порядку — *префіксний (польський) запис*

$$*+a\ /\ b\ c-d\ *\ e\ f;$$

- у разі обходу у внутрішньому порядку — *інфіксний запис* (поки що без дужок, потрібних для визначення порядку операцій)

$$a+b\ /\ c\ *\ d-e\ *\ f;$$

- у разі обходу в зворотному порядку — *постфіксний (зворотний польський) запис*

$$a\ b\ c\ /+d\ e\ f\ *-*.$$

Алгоритм Дейкстри побудови оберненої польської нотації (ОПН):

1) Поки вхідний рядок не закінчився:

Читаємо черговий символ.

Якщо символ є числом, то додаємо його у вихідний рядок.

Якщо символ є відкриваючою дужкою, то заносимо його у стек.

Якщо символ є закриваючою дужкою, то

до тих пір, поки верхнім елементом стека на буде відкриваюча дужка, виштовхуємо елементи зі стеку і вихідний рядок. При цьому відкриваюча дужка видаляється зі стеку. Якщо на верхівці стеку виявився знак

(символ) функції, то виштовхуємо його зі стеку. Якщо відкриваюча дужка незнайдена, то початковий вираз не є коректним.

Якщо символ виявився оператором o_1, то

якщо на верхівці стеку знаходиться оператор o_2, який має пріоритет ≥ за o_1, то виштовхуємо o_2 зі стеку.

заносимо o_1 у стек.

2) якщо стек непорожній, то виштовхуємо його вміст у кінець вихідного рядка.

Обчислення виразів, записаних у ОПН також засновано на використанні стека.

Алгоритм:

Обробка вхідного символу:

Якщо вхідний символ є операндом, то занести його у стек.

Якщо вхідним є символ операції, то відповідна операція виконується над потрібною кількістю операндів, які виймаються зі стеку. Результат операції заноситься у верхівку стека.

Якщо вхідний рядок оброблений не до кінця, перейти до кроку 1.

Вибрати кінцевий результат обчислень зі стеку.