Київський Університет імені Тараса Шевченка
Механіко-математичний факультет

Юрій Дрозд

Дискретна математика

Київ 2004

Зміст

Розділ 1

Комбінаторика

1. Біноміальні коефіцієнти

Означення 1.1.1. *Біноміальними коефіцієнтами* звуться функції

$$\binom{x}{n} = \frac{x(x-1)(x-2)\dots(x-n+1)}{n!},$$

де $n!$, як звичайно, позначає *факторіал* натурального числа n, тобто $n! = 1 \cdot 2 \cdot \dots \cdot n$. Зокрема, $\binom{x}{1} = x$ і $\binom{n}{n} = 1$. Ми покладемо також

$$0! = \binom{x}{0} = 1 \quad \text{для всіх } x.$$

Здебільшого нам знадобляться значення цих функцій, коли x також є натуральним числом, але значення біноміальних коефіцієнтів для нецілих x також зустрічаються досить часто. Зауважимо, що для натуральних $x \geq n$ мають місце рівністі $\binom{x}{n} = \frac{x!}{n!(x-n)!} = \binom{x}{x-n}$. Якщо ж x — натуральне число, менше за n, очевидно, $\binom{x}{n} = 0$. Важливою є також наступна властивість цих функцій.

Твердження 1.1.2. *Для довільного натурального n та для всіх x*

$$\binom{x+1}{n} = \binom{x}{n} + \binom{x}{n-1}$$

Доведення. При $n = 1$ ця формула тривіальна. Якщо $n > 1$,

$$\begin{aligned}\binom{x}{n} + \binom{x}{n-1} &= \frac{x(x-1)\dots(x-n+1)}{n!} + \frac{x(x-1)\dots(x-n+2)}{(n-1)!} = \\ &= \frac{x(x-1)\dots(x-n+2)(x-n+1+n)}{n!} = \\ &= \frac{(x+1)x\dots(x-n+2)}{n!} = \binom{x+1}{n}.\end{aligned}$$

□

Теорема 1.1.3 (Біноміальна формула). *Для довільного натурального n*

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Доведення. Якщо $n = 1$, ця формула знову тривіальна. Припустимо, що вона вірна для числа n, і перевіримо, що вона вірною і для $n+1$.

Дійсно,

$$
\begin{aligned}
(x+y)^{n+1} = (x+y)(x+y)^n = (x+y)\sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k} = \\
= \sum_{k=0}^{n}\binom{n}{k}x^{k+1}y^{n-k} + \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k+1} = \\
= \sum_{k=0}^{n}\left(\binom{n}{k-1}+\binom{n}{k}\right)x^k y^{n-k+1} = \sum_{k=0}^{n}\binom{n+1}{k}x^k y^{n+1-k}.
\end{aligned}
$$

У останньому рядку ми використали твердження 1.1.2. Отже, за принципом математичної індукції біноміальна формула є вірною для всіх n. $\square$

Наслідок 1.1.4. 1. *Якщо n і k натуральні, то й $\binom{n}{k}$ — натуральне число.*
2. $\sum_{k=0}^{n}\binom{n}{k} = 2^n$.
3. $\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$.

Доведення. 1 випливає з того, що коефіцієнти многочлена $(x+y)^n$ — натуральні числа.

2 та 3 одержуються з біноміальної формули, якщо покласти, відповідно, $x = y = 1$ та $x = 1, y = -1$. $\square$

Формула 3 з останнього наслідку показує, що суми біноміальних коефіцієнтів $\binom{n}{k}$ з парними і з непарними номерами k рівні.

З твердження 1.1.2 виводиться ще одна дуже важлива властивість біноміальних коефіцієнтів. Нехай $f(x)$ якась функція, визначена для всіх натуральних чисел. Позначимо $\Delta f(x) = f(x+1) - f(x)$. Очевидно, для довільного натурального x має місце рівність

$$f(x) = f(0) + \sum_{k=0}^{x-1}\Delta f(k).$$

Крім того, $\Delta x^n = (x+1)^n - x^n = \sum_{k=0}^{n-1}\binom{x}{k}x^k$, тому, якщо $f(x)$ — многочлен степеня n, то $\Delta f(x)$ — многочлен степеня $n-1$. Твердження 1.1.2 показує, що $\Delta\binom{x}{n} = \binom{x}{n-1}$, отже, оскільки $\binom{0}{n} = 0$, при $n \geq 1$ і натуральному x

$$\binom{x}{n} = \sum_{k=1}^{x-1}\binom{k}{n-1}.$$

Теорема 1.1.5. *Нехай $f(x)$ — довільний многочлен з комплексними коефіцієнтами степеня n, такий що $f(0), f(1), \ldots, f(n)$ — цілі числа. Тоді існують такі цілі числа $c_0, c_1, \ldots, c_n$, що*

$$f(x) = \sum_{m=0}^{n} c_m\binom{x}{m}.$$

Зауважимо, що, за наслідком 1.1.3.1, справедливе й оберене твердження: така сума приймає цілі значення при довільному натуральному (і навіть цілому) значенні x.

Доведення. Скористаємося індукцією за степенем n. Якщо $n = 0$, $f(x) = c_0\binom{x}{0}$, де $c = f(0)$. Припустимо, що твердження вірне для многочленів степеня n, і виведемо, що воно вірне і для многочленів степеня $n+1$. Дійсно, нехай многочлен $f(x)$ степеня $n+1$ приймає цілі значення при $x = 0, 1, \ldots, n+1$. Тоді $\Delta f(x)$ — многочлен степеня n, і його значення при $x = 0, 1, \ldots, n$ цілі. Отже, знайдуться цілі числа $c_1, c_2, \ldots, c_n$, такі що

$$\Delta f(x) = \sum_{m=0}^{n} c_m \binom{x}{m}.$$

Тоді, при всіх натуральних значеннях x

$$\begin{aligned} f(x) &= f(0) + \sum_{k=1}^{x-1} \sum_{m=0}^{n} c_m \binom{x}{m} = \\ &= f(0) + \sum_{m=0}^{n} c_m \sum_{k=1}^{x-1} \binom{x}{m} = f(0)\binom{x}{0} + \sum_{m=0}^{n} c_m \binom{x}{m+1}. \end{aligned}$$

Але відомо, що коли два многочлени приймають однакові значення в нескінченній кількості точок, вони збігаються. Отже остання рівність має місце як рівність многочленів. За принципом математичної індукції теорема вірна для многочленів всіх степенів. $\square$

Відзначимо ще наступну важливу властивість, яка витікає з попередніх результатів.

Теорема 1.1.6. *Нехай $f : \mathbb{N} \to \mathbb{C}$ — така функція, що $\Delta f(x)$ — многочлен степеня n. Тоді $f(x)$ — многочлен степеня $n+1$, який є лінійною комбінацією біноміальних коефіцієнтів $\binom{x}{m}$ з $m \leq n+1$.*

Доведення. За теоремою 1.1.4, $\Delta f(x) = \sum_{m=0}^{n} c_m \binom{x}{m}$ для деяких значень c_k. Тоді знов

$$\begin{aligned} f(x) &= f(0) + \sum_{k=1}^{x-1} \sum_{m=0}^{n} c_m \binom{x}{m} = \\ &= f(0) + \sum_{m=0}^{n} c_m \sum_{k=1}^{x-1} \binom{x}{m} = f(0) + \sum_{m=0}^{n} c_m \binom{x}{m+1}. \end{aligned}$$

Залишається згадати, що $\binom{x}{m}$ — многочлен степеня m. $\square$

2. Алгебра множин

Нагадаємо деякі поняття з теорії множин.

Означення 1.2.1. Нехай дано набір множин M_i $(i \in I)$.

1. *Об'єднанням* множин M_i зветься множина $\bigcup_{i \in I} M_i$, така що $x \in \bigcup_{i \in I} M_i$ тоді й лише тоді, коли $x \in M_i$ для деякого (принаймні одного) індекса i. Якщо множина індексів I порожня, вважають, що об'єднання $\bigcup_{i \in I} M_i$ — також порожня множина.

2. *Перетином* множин M_i зветься множина $M = \bigcap_{i\in I} M_i$, така що $x \in \bigcap_{i\in I} M_i$ тоді й лише тоді, коли $x \in M_i$ для всіх індексів $i \in I$.

   Якщо ми розглядаємо лише такі множини, які є підмножинами деякої фіксованої множини U («універсуму»), вважають, що коли множина індексів I порожня, перетин $\bigcap_{i\in I} M_i$ є весь універсум U.
3. *Різницею* множин M і N зветься множина $M \setminus N$, така що $x \in M \setminus N$ тоді й лише тоді, коли $x \in M$, але $x \notin N$. Якщо ми розглядаємо лише такі множини, які є підмножинами деякої фіксованої множини U («універсуму»), то різницю $U \setminus M$ звуть *доповненням* до M і позначають $\complement M$.
4. *Декартовим добутком* множин M_i зветься множина $\prod_{i\in I} M_i$, елементами якої є функції $p : I \to \bigcup_{i\in I} M_i$, такі що $p(i) \in M_i$ для кожного $i \in I$. Зокрема, якщо принаймні одна з множин M_i порожня, добуток $\prod_{i\in I} M_i$ також порожній.

   Якщо множина індексів I скінченна: $I = \{\, i_1, i_2, \dots, i_n \,\}$, елементи декартова добутку звичайно записують у вигляді впорядкованих наборів $p = (x_1, x_2, \dots, x_n)$, де $x_k = p(i_k) \in M_{i_k}$.

Нагадаємо також деякі властивості цих операцій.

Твердження 1.2.2. 1. *Закони дистрибутивності:*

$$M \cup \big(\bigcap_{i\in I} N_i\big) = \bigcap_{i\in I} \big(M \cup N_i\big);$$

$$M \cap \big(\bigcup_{i\in I} N_i\big) = \bigcup_{i\in I} \big(M \cap N_i\big).$$

2. *Правила де Моргана:*

$$M \setminus \big(\bigcap_{i\in I} N_i\big) = \bigcup_{i\in I} \big(M \setminus N_i\big);$$

$$M \setminus \big(\bigcup_{i\in I} N_i\big) = \bigcap_{i\in I} \big(M \setminus N_i\big).$$

   Зокрема,

$$\complement\big(\bigcap_{i\in I} N_i\big) = \bigcup_{i\in I} \big(\complement N_i\big);$$

$$\complement\big(\bigcap_{i\in I} N_i\big) = \bigcup_{i\in I} \big(\complement N_i\big).$$

3. *Закони добутку:*

$$M \times \big(\bigcup_{i\in I} N_i\big) = \bigcup_{i\in I} \big(M \times N_i\big);$$

$$M \times \big(\bigcap_{i\in I} N_i\big) = \bigcap_{i\in I} \big(M \times N_i\big);$$

$$M \times \big(N \setminus L\big) = \big(M \times N\big) \setminus \big(M \times L\big).$$

Доведення. Всі ці правила доводяться простою перевіркою, тому ми обмежимось лише одним з них, наприклад, другим правилом де Моргана. Треба перевірити два включення:

(i) $$M \setminus \big(\bigcup_{i\in I} N_i\big) \subseteq \bigcap_{i\in I} \big(M \setminus N_i\big)$$

та

(ii) $$M \setminus \big(\bigcup_{i\in I} N_i\big) \supseteq \bigcap_{i\in I} \big(M \setminus N_i\big).$$

Перевірка (i). Якщо елемент x належить лівій частині, він належить M, але не належить об'єднанню $\bigcup_{i\in I} N_i$, тобто не належить жодній з множин N_i. Тому він належить кожній з множин $M \setminus N_i$, тобто належить їхньому перетину. Отже ліва частина міститься в правій.

Перевірка (ii). Якщо елемент x належить правій частині, він належить кожній з множин $M \setminus N_i$, тобто він належить M, але не належить жодній з множин N_i. Тому він не належить до об'єднання $\bigcup_{i\in I} N_i$, а тому належить до різниці $M \setminus \big(\bigcup_{i\in I} N_i\big)$. Отже, й права частина міститься в лівій. □

Якщо задано відображення $f : M \to M'$, то для кожної підмножини $N \subseteq M$ визначений її образ $f(N) = \{\, f(x) \mid x \in N \,\}$, а для кожної підмножини $N' \subseteq M'$ — її прообраз $f^{-1}(N') = \{\, x \in M \mid f(x) \in N' \,\}$. Мають місце наступні властивості.

Твердження 1.2.3. 1. *Для будь-яких підмножин $N_i \subseteq M$*

$$f\big(\bigcup_{i\in I} N_i\big) = \bigcup_{i\in I} f(N_i);$$
$$f\big(\bigcap_{i\in I} N_i\big) \subseteq \bigcap_{i\in I} f(N_i);$$
$$f\big(N_1 \setminus N_2\big) \supseteq f(N_1) \setminus f(N_2),$$

причому нерівності у другому й третьому рядках можуть бути строгими, якщо відображення f не є ін'єктивним.

2. *Для будь-яких підмножин $N_i' \subseteq M'$*

$$f^{-1}\big(\bigcup_{i\in I} N_i'\big) = \bigcup_{i\in I} f^{-1}(N_i');$$
$$f^{-1}\big(\bigcap_{i\in I} N_i'\big) = \bigcap_{i\in I} f^{-1}(N_i');$$
$$f^{-1}\big(N_1' \setminus N_2'\big) = f^{-1}(N_1') \setminus f^{-1}(N_2').$$

Нагадаємо, що відображення f зветься *ін'єктивним*, якщо воно переводить різні елементи в різні, і *сюр'єктивним*, якщо кожен елемент з M' є образом якогось елемента з M. Відображення, яке одночасно є ін'єктивним і сюр'єктивним, зветься *бієктивним*, або *взаємно однозначним*.

Доведення твердження 1.2.3 залишається читачеві як вправа.

3. Формула включення і вилучення

Ми позначаємо через $\#(M)$ кількість елементів у множині M.

Твердження 1.3.1. *Нехай $M_1, M_2, \dots, M_n$ — деякі скінченні множини. Тоді*

(3.1)
$$\#\Big(\bigcup_{i=1}^{n} M_i\Big) = \sum_{i=1}^{n} \#(M_i) - \sum_{i<j} \#(M_i \cap M_j) + \sum_{i<j<k} \#(M_i \cap M_j \cap M_k) - $$
$$- \dots + (-1)^{m-1} \sum_{i_1<i_2<\dots<i_m} \#\Big(\bigcap_{s=1}^{m} M_{i_s}\Big) + \dots + (-1)^{n-1} \#\Big(\bigcap_{i=1}^{n} M_i\Big).$$

Формула (3.1) зветься *формулою включення та вилучення.*

Доведення. Скористаймося індукцією за n. Первіримо спочатку формулу (3.1), коли $n = 2$. Тоді вона має вигляд

$$\#(M \cup N) = \#(M) + \#(N) - \#(M \cap N). \tag{3.2}$$

Нехай $M \cap N = \{ a_1, a_2, \dots, a_r \}$, $M \setminus N = \{ b_1, b_2, \dots, b_s \}$ і $N \setminus M = \{ c_1, c_2, \dots, c_t \}$. Тоді, очевидно,

$$M \cup N = \{ a_1, a_2, \dots, a_r, b_1, b_2, \dots, b_s, c_1, c_2, \dots, c_t \},$$

тобто

$$\#(M \cup N) = r + s + t = (r + s) + (r + t) - r = \#(M) + \#(N) - \#(M \cap N),$$

що й треба було довести.

Припустимо, що формула (3.1) є вірною для n множин, і розглянемо набір з $n+1$ множини $M_1, M_2, \dots, M_{n+1}$. Позначимо $M = \bigcup_{i=1}^{n} M_i$, $N = M_{n+1}$. За індуктивним припущенням, кількість елементів у множині M визначається за формулою (3.1). Крім того, за твердженням 1.2.2.1,

$$M \cap N = \bigcup_{i=1}^{n} (M_i \cap N),$$

звідки, знов-таки за індуктивним припущенням,

$$\#(M \cap N) = \sum_{i=1}^{n} \#(N_i) - \sum_{i<j} \#(N_i \cap N_j) + \sum_{i<j<k} \#(N_i \cap N_j \cap N_k) - $$
$$- \dots + (-1)^{m-1} \sum_{i_1<i_2<\dots<i_m} \#\Big(\bigcap_{s=1}^{m} N_{i_s}\Big) + \dots + (-1)^{n-1} \#\Big(\bigcap_{i=1}^{n} N_i\Big),$$

де $N_i = M_i \cap M_{n+1}$. Зауважимо також, що

$$\bigcap_{i_1<i_2<\dots<i_m} N_i = \Big(\bigcap_{i_1<i_2<\dots<i_m} M_i\Big) \cap M_{n+1}.$$

Для підрахунку кількості елементів у об'єднанні $\bigcup_{i=1}^{n+1} M_i = M \cup N$ використаємо вже доведену формулу (3.2):

$$\#\big(\bigcup_{i=1}^{n+1} M_i\big) = \#(M) + \#(N) - \#(M \cap N) =$$

$$\sum_{i=1}^{n} \#(M_i) - \sum_{i<j\le n} \#(M_i \cap M_j) + \sum_{i<j<k\le n} \#(M_i \cap M_j \cap M_k) -$$

$$- \cdots + (-1)^{m-1} \sum_{i_1<i_2<\cdots<i_m\le n} \#\big(\bigcap_{s=1}^{m} M_{i_s}\big) + \cdots + (-1)^{n-1}\#\big(\bigcap_{i=1}^{n} M_i\big) +$$

$$+ \#(M_{n+1}) - \sum_{i=1}^{n} \#(M_i \cap M_{n+1}) + \sum_{i<j<n+1} \#(M_i \cap M_j \cap M_{n+1}) - \cdots +$$

$$+ (-1)^m \sum_{i_1<i_2<\cdots<i_m<n+1} \#\big(\big(\bigcap_{s=1}^{m} M_{i_s}\big) \cap M_{n+1}\big) + \cdots + (-1)^n \#\big(\bigcap_{i=1}^{n+1} M_i\big),$$

що лише порядком доданків відрізняється від формули (3.1) для набору $M_1, M_2, \ldots, M_{n+1}$. За принципом математичної індукції, твердження повінстю доведене. □

Якщо множини $M_1, M_2, \ldots, M_n$ попарно не перетинаються, об'єднання $\bigcup_{i=1}^{n}$ зветься *незв'язним об'єднанням* і позначається $\bigsqcup_{i=1}^{n} M_i$. Формула (3.1) перетворюється тоді на очевидну рівність

$$\#\big(\bigsqcup_{i=1}^{n} M_i\big) = \sum_{i=1}^{n} \#(M_i), \tag{3.3}$$

яка зветься *формулою розбиття*, оскільки множина $M = \bigsqcup_{i=1}^{n} M_i$ розбита на n частин, які не перетинаються.

Частковим випадком формули розбиття є наступна *формула шарів*.

Твердження 1.3.2. *Якщо задано відображення $f : M \to N$ скінченних множин, то*

$$\#(M) = \sum_{x\in N} \#\big(f^{-1}(x)\big).$$

Доведення. Дійсно, $M = \bigsqcup_{x\in N} f^{-1}(x)$, отже залишається використати формулу розбиття. □

Незважаючи на свою очевидність, формула розбиття, зокрема, формула шарів, є дуже корисною при багатьох комбінаторних обчисленнях. Зокрема, з неї одразу одержується наступна *формула добутку*.

Твердження 1.3.3. $\#\big(\prod_{i=1}^{n} M_i\big) = \prod_{i=1}^{n} \#(M_i)$.

Доведення. Скористаємося індукцією за n. База індукції, $n = 1$, тривіальна. Припустимо, що формула добутку вірна для n співмножників, і розглянемо проекцію добутку $P = \prod_{i=1}^{n+1} M_i$ на M_{n+1}, тобто відображення $p : P \to M_{n+1}$, яке переводить $(x_1, x_2, \ldots, x_{n+1})$ у x_{n+1}. Очевидно, для кожного $x \in M_{n+1}$ шар $p^{-1}(x)$ ототожнюється з $\prod_{i=1}^{n} M_i$, отже містить $\prod_{i=1}^{n} \#(M_i)$ елементів. Таким чином, усього P містить $\left(\prod_{i=1}^{n} \#(M_i)\right) \cdot \#(M_{n+1})$, що й треба було довести. $\square$

Якщо всі M_i у добутку — це та сама множина M, елементи цього добутку ототожнюються з відображеннями $N \to M$, де N — множина з n елементів.

Наслідок 1.3.4. *Якщо $\#(M) = m$, а $\#(N) = n$, існує m^n відображень $M \to N$.*

4. Сполучення, розміщення, перестановки

Скористаємося одержаними результатами для розв'язання деяких комбінаторних задач. Перш за все, підрахуємо кількість C_n^m підмножин, які мають m елементів у множині з n елементів. Такі підмножини інколи (за старою традицією) звуться *сполученнями*, або *комбінаціями* з n елементів по m.

Твердження 1.4.1. $C_n^m = \dbinom{n}{m}$.

Доведення. Скористаємося індукцією за n. Якщо $n = 1$, єдиний можливий випадок — це $m = 1$, і $C_1^1 = 1 = \binom{1}{1}$. Припустимо, що формула вірна для підмножин довільної множини з n елементів. Розглянемо множину M, яка має $n+1$ елемент. Фіксуємо один з елементів a і покладемо $N = M \setminus \{ a \}$. Усі підмножини $A \subseteq M$, які містсть m елементів, розіб'ємо на ті, що містять a, й ті, що його не містять. Останні — це підмножини N; за індуктивним припущенням їх є $\binom{n}{m}$. Перші ж мають вигляд $B \cup \{ a \}$, де $B \subseteq N$ — підмножина з $m-1$ елемента; за індуктивним припущенням їх є $\binom{n}{m-1}$. Отже,

$$C_{n+1}^m = \binom{n}{m} + \binom{n}{m-1} = \binom{n+1}{m}.$$

За принципом математичної індукції, твердження вірне для всіх n. $\square$

Наслідок 1.4.2. *Загальна кількість підмножин множини, яка має n елементів, дорівнює 2^n.*

Доведення. Дійсно, ця кількість дорівнює

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

$\square$

Нехай тепер задано дві множини, M і N, причому $\#(M) = m$, $\#(N) = n$. Визначимо, скільки існує *ін'єктивних відображень* $M \to N$. Знов-таки за старою традицією, такі відображення звуть *розміщеннями* з n елементів по m, а їхню кількість позначають A_n^m.

Твердження 1.4.3. $A_n^m = n(n-1)(n-2)\dots(n-m+1)$.

Доведення. Знов-таки використаємо індукцію, цього разу за m. Очевидно, $A_n^1 = n$, тобто при $m = 1$ вказана формула вірна. Припустимо, що вона вірна для m елементів, розглянемо множину M з $m+1$

елемента і фіксуємо один з них a. Для кожного елемента $x \in N$ ін'єктивні відображення $f : M \to N$, такі що $f(a) = x$, можна ототожнити з ін'єктивними відображеннями $M \setminus \{a\} \to N \setminus \{x\}$. За індуктивним припущенням їх є $A_{n-1}^{m-1} = (n-1)(n-2)\dots(n-m+1)$. Отже, всього індуктивних відображень $M \to N$ є $n \cdot A_{n-1}^{m-1} = n(n-1)(n-2)\dots(n-m+1)$, що й треба було довести. □

Якщо $M = N$ (скінченна множина!), ін'єктивні відображення $M \to N$ є обов'язково бієктивними; вони звуться *перестановками* множини M, або перестановками з n елементів.

Наслідок 1.4.4. *Кількість перестановок з n елементів дорівнює $n!$.*

Підрахуємо тепер, скільки існує *сюр'єктивних* відображень $N \to M$, де $\#(M) = m$, $\#(N) = n$. Позначимо їхнє число через D_n^m. Ці числа пов'язані з *розбиттями* множини N на m непорожніх частин. Дійсно, кожна сюр'єкція $N \to M$ визначає таке розбиття. Уся різниця полягає в тому, що ті відображення, які відрізняються на перестановку множини M, задать ті самі розбиття. Кількість розбиттів множини N на m частин позначають S_n^m і звуть *числом Стірлінга другого роду*. Сюр'єктивні відображення $N \to M$ можна ототожнити з розподілами n елементів по m скриньках за умови, що жодна скринька не залишається порожньою. Якщо ж вважати, що всі скриньки однакові й ми не можемо їх розрізнити між собою, то такі розподіли ототожнюються з розбиттями N на m частин, тобто їхня кількість виражається числом Стірлінга.

Твердження 1.4.5. 1. $D_n^m = \sum_{k=0}^{m-1} (-1)^k \binom{m}{k} (m-k)^n$.

2. $S_n^m = \frac{1}{m!} \sum_{k=0}^{m-1} (-1)^k \binom{m}{k} (m-k)^n$.

Доведення. Звичайно, $D_n^m = m^n - D^*$, де D^* — кількість відображень $N \to M$, які не є сюр'єктивними. Позначимо через $F(x_1, x_2, \dots, x_k)$ множину тих відображень, образи яких які не містять жоден з елементів $x_1, x_2, \dots, x_k$. Очевидно, кількість таких відображень дорівнює $(m-k)^n$, а при фіксованому k множина $\{x_1, x_2, \dots, x_k\}$ може бути вибрана $C_m^k = \binom{m}{k}$ способами. Крім того, $F(x_1, x_2, \dots, x_k) = \bigcap_{i=1}^k F(x_i)$. Тому, за формулою включення і вилучення,

$$D^* = \#\Big(\bigcup_{x \in N} F(x)\Big) = \binom{m}{1}(m-1)^n - \binom{m}{2}(m-2)^n + \dots +$$
$$+ (-1)^{k-1}\binom{m}{k}(m-k)^n + \dots + (-1)^{m-1}\binom{m}{m-1},$$

звідки випливає необхідна формула для D_n^m. Оскільки з вищесказаного випливає, що $S_n^m = D_n^m / m!$, ми одержуємо також і формулу для S_n^m. □

Часто при комбінаторних обчисленнях доводиться застосовувати процедуру «залежного вибору». Вона полягає в наступній задачі:

Задача 1.4.6. *Треба вибрати деякі n об'єктів $a_1, a_2, \dots, a_n$ (елементів, підмножин, чи чогось іншого). Відомо, що:*

- *перший з них a_1 можна обрати m_1 способами;*
- *при фіксованому першому другий a_2 можна обрати m_2 способами;*
- *при фіксованих перших двох третій a_3 можна обрати m_3 способами, і т.д.,*
- *нарешті, при фіксованих перших $n-1$ останній a_n можна обрати m_n способами.*

Твердження 1.4.7. *Задача 1.4.6 має $m_1 m_2 \dots m_n$ різних розв'язків.*

Доведення. Доведення легко отримати індукцією за кількістю «кроків вибору» n. База індукції, $n = 1$, тривіальна. Припустимо, що твердження вірне для n кроків вибору, і доведемо, що тоді воно вірне й для $n+1$ кроку. Дійсно, розглянемо множину всіх можливих виборів $M = \{ (a_1, a_2, \dots, a_{n+1}) \}$ з $n+1$ об'єкту та множину $N = \{ (a_1, a_2, \dots, a_n) \}$ всіх можливих виборів з n об'єктів, і визначимо відображення $\phi : M \to N$, яке кожному вибору $(a_1, a_2, \dots, a_{n+1}) \in M$ ставить у відповідність вибір $(a_1, a_2, \dots, a_n) \in N$. За умовою, при фіксованих $a_1, a_2, \dots, a_n$ останній елемент a_{n+1} можна обрати m_{n+1} способами. Це означає, що для кожного елемента $x \in N$ прообраз $\phi^{-1}(x)$ містить m_{n+1} елементів. Але, за індуктивним припущенням, $\#(N) = m_1 m_2 \dots m_n$. Тому, за формулою шарів (твердження 1.3.2), маємо, що $\#(M) = \#(N) m_{n+1} = m_1 m_2 \dots m_{n+1}$, що й треба було довести. □

Зауважимо, що частковим випадком задачі 1.4.6 є задача про ін'єктивні відображення, а твердження 1.4.3 є частковим випадком твердження 1.4.7.

5. Твірні функції

У багатох задачах комбінатоики дуже зручними є так звані *твірні функції*. Насправді, у більшості випадків нас цікавлять не стільки самі функції, скільки відповідні степеневі ряди; більш того, найчастіше не виникає навіть питання про збіжність цих рядів. Тому ми розглянемо чистл алгебричне поняття *формального степеневого ряду*.

Означення 1.5.1. 1. *Формальним степеневим рядом* зветься вираз

$$f(t) = \sum_{n=0}^{\infty} a_n t^n = a_0 + a_1 t + a_2 t^2 + \dots + a_n t^n + \dots, \tag{5.1}$$

де a_n — довільні комплексні числа.
Фактично, такий ряд можна ототожнити з функцією $a : \mathbb{N}^0 = \mathbb{N} \cup \{ 0 \} \to \mathbb{C}$, яка ставить у відповідність числу n число a_n. Втім, запис (5.1) є більш виразним, особливо, коли йдеться про дії з такими рядами, і надалі ми завжди будемо ним користуватися. Ми також будемо часто казати просто «*ряд*» (замість «формальний степеневий ряд»), оскільки інші ряди у нас не зустрічатимуться.

2. *Сумою* двох рядів, $f = \sum_{n=0}^{\infty} a_n t^n$ та $g = \sum_{n=0}^{\infty} b_n t^n$ зветься ряд $f + g = \sum_{n=0}^{\infty} (a_n + b_n) t^n$.
3. *Добутком* двох рядів, $f = \sum_{n=0}^{\infty} a_n t^n$ та $g = \sum_{n=0}^{\infty} b_n t^n$ зветься ряд $fg = \sum_{n=0}^{\infty} (a * b)_n t^n$, де коефіцієнти $(a * b)_n$ визначаються формулою

$$(a * b)_n = \sum_{k=0}^{n} a_k b_{n-k} = a_0 b_n + a_1 b_{n-1} + \dots + a_{n-1} b_1 + a_n b_0. \tag{5.2}$$

   Функція $a * b : \mathbb{N}^0 \to \mathbb{C}$, значення якої задаються правилом (5.2), зветься *згорткою*, або *композицією*, функцій a та b.
4. *Порядком* $\operatorname{ord} f$ ряду $f(t) = \sum_{n=0}^{\infty} a_n t^n$ зветься $\min\{\, n \mid a_n \neq 0 \,\}$. Якщо всі $a_n = 0$ (тоді пишуть $f = 0$), вважаємо, що $\operatorname{ord} f = \infty$.

Легко переконатися, що відносно цих операцій множина $\mathbb{C}[[t]]$ всіх формальних степеневих рядів утворює комутативне кільце. Воно містить кільце многочленів $\mathbb{C}[t]$, якщо кожен многочлен розглядати як степеневий ряд, в якому *майже всі* коефіцієнти (тобто, всі, крім скінченної кількості) дорівнюють 0. Ми залишаємо перевірку всіх необхідних властивостей читачеві (це зовсім проста вправа). Корисною властивістю цього кільця є наступна. Зауважимо, що ми не ставимо питання про збіжність ряду (5.1), а тому й про його значення при заданому значенні змінної t. Втім, завжди має сенс значення $f(0)$: це є просто *вільний член* a_0.

Твердження 1.5.2. *Ряд* $f(t) = \sum_{n=1}^{\infty} a_n t^n$ *є обертовним у кільці* $\mathbb{C}[[t]]$ *тоді й лише тоді, коли* $\operatorname{ord} f = 0$, *тобто* $a_0 \neq 0$.

Доведення. Легко бачити, що $\operatorname{ord}(fg) = \operatorname{ord} f + \operatorname{ord} g$. Оскільки $\operatorname{ord} 1 = 0$, звідси випливає необхідність даної умови. Припустимо, що $a_0 \neq 0$ і побудуємо обернений елемент f^{-1}, такий що $ff^{-1} = 1$. Ми будуватимемо коефіцієнти b_n ряду f^{-1} *рекурсивно*, тобто для знаходження кожного наступного вважатимемо, що всі попередні вже знайдені. Нам потрібно, щоб $a_0 b_0 = 1$, а для всіх номерів $n > 0$ справжнювалася рівність

$$a_0 b_n + a_1 b_{n-1} + \dots + a_{n-1} b_1 + a_n b_0 = 0.$$

Для цього покладемо

$$\begin{aligned} b_0 &= a_0^{-1}, \\ b_1 &= -a_0^{-1} a_1 b_0, \\ b_2 &= -a_0^{-1} (a_1 b_1 + a_2 b_0), \end{aligned}$$

і взагалі,

$$b_n = -\, a_0^{-1} (a_1 b_{n-1} + a_2 b_{n-2} + \dots + a_n b_0).$$

Оскільки $a_0 \neq 0$, ці формули дійсно визначають коефіцієнти оберненого ряда f^{-1}. □

Приклад 1.5.3. 1. Легко бачити, що

$$(1 - t)^{-1} = 1 + t + t^2 + t^3 + \dots + t^n + \dots$$

(«формула суми геометричної прогресії»).

2. Перевіримо, що

$$(1-t)^{-m} = \sum_{n=0}^{\infty}(-1)^n\binom{-m}{n}t^n = \sum_{n=0}^{\infty}\binom{m+n-1}{n}t^n.$$

Нагадаємо, що $(1-t)^m = \sum_{n=0}^{m}(-1)^n\binom{m}{n}t^n$, зокрема, вільний член дорівнює 1. При $n=0$ маємо $(-1)^0\binom{m-1}{0}=1$, що й треба. Залишається довести, що для кожного $n>0$ має місце рівність

$$\sum_{k=0}^{n}\binom{m}{k}\binom{-m}{n-k} = 0.$$

Але з формули додаваення (вправа 1(b) із завдання 1) випливає, що

$$\sum_{k=0}^{n}\binom{m}{k}\binom{-m}{n-k} = \binom{0}{n} = 0 \text{ при } n>0,$$

що й треба було довести.

З цих двох прикладів, зокрема, випливає, що

$$\Big(\sum_{n=0}^{\infty}t^n\Big)^m = \sum_{n=0}^{\infty}\binom{m+n-1}{n}t^n. \tag{5.3}$$

Степеневий ряд $\sum_{n=1}^{\infty}a_nt^n$ звичайно зветься *твірною функцією*, або *твірним рядом* для послідовності $\mathbf{a}=(a_n)$, або, що те саме, функції $\mathbf{a}:\mathbb{N}\to\mathbb{C}$. Ми позначатимемо його $F_{\mathbf{a}}$. У комбінаториці нас найбільше цікавитимуть, звичайно, функції, які набувають цілочисельних значень («*цілозначні функції*»), але досить часто у проміжних обчисленнях виникають і функції, які не обов'язково є цілозначними. Формальні перетворення з рядами у багатьох випадках дозволяють порівняно легко обчислити твірні ряди для функцій, які виникають у комбінаториці.

Розглянемо, наприклад, таку задачу.

Задача 1.5.4. *Знайти кількість K_n розв'язків рівняння*

$$\phi_1(x_1)+\phi_2(x_2)+\dots+\phi_k(x_k)=n,$$

де $\phi_1,\phi_2,\dots,\phi_k$ — відомі функції $\mathbb{N}^0\to\mathbb{N}^0$, кожна з яких приймає кожне значення лише скінченну кількість разів.

Твердження 1.5.5. *Позначимо $K_n^m = \#\{\,c\mid\phi_m(c)=n\,\}$ і нехай $F_m = \sum_{n=0}^{\infty}K_n^mt^n$ — твірний ряд функції K^m. Тоді добуток $F=F_1F_2\dots F_k$ є твірним рядом функції K з задачі 1.5.4, тобто $F=\sum_{n=1}^{\infty}K_nt^n$.*

Доведення. Дійсно, згідно з означенням добутку рядів, коефіцієнт біля t^n у ряді F дорівнює сумі

$$\sum_{n_1+n_2+\dots+n_k=n}K_{n_1}^1K_{n_2}^2\dots K_{n_k}^k.$$

Останній добуток — це кількість таких наборів $x_1,x_2,\dots,x_k$, що $\phi_i(x_i)=n_i$. Отже, сума всіх цих добутків — це загальна кількість таких наборів $x_1,x_2,\dots,x_k$, що $\sum_{i=1}^{k}\phi_i(x_i)=n$, тобто K_n. $\square$

Приклад 1.5.6. 1. Підрахуємо кількість розв'язків рівняння $x_1 + x_2 + \cdots + x_k = n$ у цілих невід'ємних числах. У цьому випадку всі функції ϕ_i — тотожні: $\phi_i(x) = x$. Тому $K_n^m = 1$ і $F_m = \sum_{n=0}^{\infty} t^n = (1-t)^{-1}$. Тому $F = (1-t)^{-k}$ і, згідно з прикладом 1.5.3.2, шукана кількість дорівнює

$$\binom{k+n-1}{n}, \text{ або, що те саме, } \binom{n+k-1}{k-1}.$$

До речі, ця кількість, очевидно, дорівнює кількості одночленів степеня n від k змінних (x_i — це показних степеня при i-й змінній).

2. Нехай тепер $C_m(k,n)$ позначає кількість розв'язків рівняння того ж самого рівняння $\sum_{i=1}^{k} x_i = n$, але за умови, що $0 \leq x_i \leq m$ для всіх номерів i. Це знову варіант задачі 1.5.4, в якому тепер

$$\phi_i(x) = \begin{cases} 1 & \text{якщо } x \leq m, \\ 0 & \text{якщо } x > m. \end{cases}$$

Тому

$$F_i = 1 + t + t^2 + \cdots + t^m = \frac{1-t^{m+1}}{1-t} \quad \text{для всіх } i$$

і

$$F = \left(\frac{1-t^{m+1}}{1-t}\right)^k = (1-t^{m+1})^k (1-t)^{-k} =$$
$$= \sum_{j=0}^{k} (-1)^j \binom{k}{j} t^{j(m+1)} \sum_{l=0}^{\infty} \binom{l+k-1}{k-1} t^l =$$
$$= \sum_{n=0}^{\infty} \left(\sum_{j=0}^{k} (-1)^j \binom{k}{j} \binom{n-j(m+1)+k-1}{k-1} \right) t^n,$$

звідки

$$C_m(k,n) = \sum_{j=0}^{[n/(m+1)]} (-1)^j \binom{k}{j} \binom{n-j(m+1)+k-1}{k-1},$$

де, як звичайно, $[a]$ позначає *цілу частину* числа a, тобто найбільше ціле число, яке не перебільшує a.

3. (Вправа.) Переконайтеся, що останню формулу можна переписати як

$$C_m(k,n) = k \sum_{j=0}^{[n/(m+1)]} \frac{(-1)^j}{n-j(m+1)} \binom{n-j(m+1)+k}{j,\ k-j}$$

Зазначимо ще одни важливий наслідок методу твірних функцій.

Наслідок 1.5.7. *Нехай c_n — така послідовність, що $c_0 \neq 0$. Тоді існує єдина послідовність c'_n, така що*

$$\sum_{k=0}^{n} c'_k c_{n-k} = \begin{cases} 0, & \text{якщо } n \neq 0, \\ 1 & \text{якщо } n = 0. \end{cases} \tag{5.4}$$

Якщо пслідовноісті A_n та B_n пов'язані співвідношенням $B_n = \sum_{k=0}^{n} c_k A_{n-k}$ для всіх n, то також $A_n = \sum_{k=0}^{n} c'_k B_{n-k}$ для всіх n.

Доведення. Перше твердження випливає з твердження 1.5.2, оскільки воно рівносильне тотожності $\sum_{k=0}^{\infty} c'_k t^k \cdot \sum_{m=0}^{\infty} c_m t^m = 1$. Після цього друге твердження очевидне, оскільки перше співвідношення переписується як $\sum_{n=0}^{\infty} B_n t^n = \sum_{k=0}^{\infty} c_k t^k \cdot \sum_{m=0}^{\infty} A_m t^m$, а друге — як $\sum_{n=0}^{\infty} A_n t^n = \sum_{k=0}^{\infty} c'_k t^k \cdot \sum_{m=0}^{\infty} B_m t^m$. □

Послідовність c'_n, визначену правилом (5.4), будемо звати *двоїстою* до послідовності c_n.

Приклад 1.5.8.

1. Згідно з прикладом 1.5.3(2), двоїстою до послідовності $c_n = \binom{m}{n}$ є послідовність $c'_n = \binom{m+n-1}{n}$. Тому з рівностей
$$B_n = \sum_{k=0}^{n} \binom{m}{k} A_{n-k} \quad \text{для всіх } n$$
випливає, що також
$$A_n = \sum_{k=0}^{n} \binom{m+k-1}{k} B_{n-k} \quad \text{для всіх } n.$$
2. З задачі 2 завдання 3 випливає, що коли $B_n = \sum_{k=0}^{n} A_{n-k}/k!$ для всіх n, то також $A_n = \sum_{k=0}^{n} (-1)^k B_{n-k}/k!$ для всіх n.

У багатьох випадках зручнішим є дещо інший степеневий ряд, пов'язаний з послідовністю $\mathbf{a} = (a_n)$, а саме, ряд
$$\widetilde{F}_{\mathbf{a}}(t) = \sum_{n=0}^{\infty} \frac{a_n}{n!} t^n.$$
Цей ряд зветься *експоненційною твірною* послідовності $\mathbf{a}$. Якщо $\widetilde{F}_{\mathbf{b}}(t) = \sum_{n=0}^{\infty} b_n/n!$ — експоненційна твірна послідовності (b_n), то їхній добуток
$$\begin{aligned}\widetilde{F}_{\mathbf{a}}(t)\widetilde{F}_{\mathbf{b}}(t) &= \sum_{n=0}^{\infty} t^n \sum_{k=0}^{n} \frac{a_k}{k!} \cdot \frac{b_{n-k}}{(n-k)!} = \\ &= \sum_{n=0}^{\infty} t^n \frac{a_k b_{n-k}}{n!} \cdot \frac{n!}{k!(n-k)!} = \\ &= \sum_{n=0}^{\infty} \frac{t^n}{n!} \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}\end{aligned}$$
є експоненціною твірною послідовності $\mathbf{c} = \mathbf{a} \star \mathbf{b}$, де $c_n = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}$. Цю послідовність звуть *біноміальною композицією* послідовностей $\mathbf{a}$ та $\mathbf{b}$. Отже, ми довели таке твердження.

Твердження 1.5.9. *Якщо $\widetilde{F}_{\mathbf{a}}$ та $\widetilde{F}_{\mathbf{b}}$ — експоненційні твірні послідовностей $\mathbf{a}$ та $\mathbf{b}$, то їхній добуток є експоненційною твірною біноміальної композиції цих послідовностей.*

Наслідок 1.5.10. *Нехай $\widetilde{F}_{\mathbf{c}}$ — експоненційна твірна послідовності (c_n), в якій $c_0 \neq 0$, $(\widetilde{F}(t))^{-1} = \sum_{n=0}^{\infty} c'_n t^n$ (такий ряд існує за твердженням 1.5.2). Тоді з рівностей*

$$B_n = \sum_{k=0}^{n} \binom{n}{k} c_k A_{n-k} \quad \text{для всіх } n$$

випливає, що також

$$A_n = \sum_{k=0}^{n} \binom{n}{k} c'_k B_{n-k} \quad \text{для всіх } n.$$

Наприклад, з рівностей

$$B_n = \sum_{k=0}^{n} \binom{n}{k} A_k \quad \text{для всіх } n$$

випливає, що також

$$A_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} B_k \quad \text{для всіх } n$$

Доведення. Перше твердження очевидно випливає з твердження 1.5.9. Після цього друге є безпосереднім наслідком формули $(\exp t)^{-1} = \exp(-t)$ (див. завдання 3, задача 2) та того, що $\binom{n}{k} = \binom{n}{n-k}$. □

6. Рекурентні послідовності

Техніку твірних рядів зручно застосовувати до так званих *рекурентних послідовностей*. У загальному випадку, так зветься довільна послідовність a_n, в якій задані перші m членів $a_0, a_1, \ldots, a_{m-1}$, а наступні (тобто при $n \geq m$) визначаються правилом

$$a_{n+m} = R(a_n, a_{n+1}, \ldots, a_{n+m-1}),$$

де $R(x_1, x_2, \ldots, x_m)$ — деяка відома функція. Ми розглянемо найпростіший випадок, коли остання залежність має вигляд

$$a_{n+m} = c_1 a_n + c_2 a_{n+1} + \cdots + c_m a_{n+m-1}, \tag{6.1}$$

де $c_1, c_2, \ldots, c_m$ — задані константи. За допомогою твірних функцій можна порівняно легко обчислити всі члени такої послідовності.

Теорема 1.6.1. *Нехай рекурентна послідовність $\mathbf{a} = (a_n)$ визначена правилом* (6.1) *і заданими значеннями $a_0, a_1, \ldots, a_{m-1}$,* $F_{\mathbf{a}}(t) =$

$\sum_{n=0}^\infty a_n t^n$ — твірна функція цієї послідовності. Позначимо

$$
\begin{aligned}
\widetilde f(t) &= \sum_{k=0}^{m-1} c_{k+1} t^{m-k},\\
f(t) &= 1 - \widetilde f(t),\\
g_k(t) &= \sum_{n=0}^{k-1} a_n t^n \quad (0 \le k < m),\\
g(t) &= g_0(t) - \sum_{k=1}^{m-1} c_{k+1} t^{m-k} g_k(t).
\end{aligned}
$$

Тоді $F_{\mathbf a}(t) = g(t)/f(t)$. (Зауважимо, що, оскільки вільний член $f(t)$ дорівнює 1, остання частка існує в кільці формальних степеневих рядів.)

Доведення. Зауважимо, що

$$
\begin{aligned}
\sum_{n=m}^\infty a_n t^n &= \sum_{n=0}^\infty a_{n+m} t^{n+m} = \sum_{n=0}^\infty \Big(\sum_{k=0}^{m-1} c_{k+1} a_{n+k}\Big) t^{n+m} =\\
&= \sum_{k=0}^{m-1} c_{k+1} t^{m-k} \sum_{n=0}^\infty a_{n+k} t^{n+k} =\\
&= \sum_{k=0}^{m-1} c_{k+1} t^{m-k} \Big(\sum_{n=0}^\infty a_n t^n - \sum_{n=0}^{k-1} a_n t^n\Big) =\\
&= \sum_{k=0}^{m-1} c_{k+1} t^{m-k} F_{\mathbf a}(t) - \sum_{k=1}^{m-1} c_{k+1} t^{m-k} g_k(t).
\end{aligned}
$$

Отже,

$$
\begin{aligned}
F_{\mathbf a}(t) = \sum_{n=0}^\infty a_n t^n &= a_0 + a_1 t + \dots + a_{m-1} t^{m-1} + \sum_{n=m}^\infty a_n t^n =\\
&= g_0(t) + \widetilde f(t) F_{\mathbf a}(t) - \sum_{k=0}^{m-1} c_{k+1} t^{m-k} g_k(t) =\\
&= g(t) + \widetilde f(t) F_{\mathbf a}(t),
\end{aligned}
$$

звідки й випливає потрібна формула. □

Звернемо увагу на те, що дріб $g(t)/f(t)$ порівняно неважко перетворити на степеневий ряд. Для цього достатньо розкласти його на *найпростіші дроби*, тобто на дроби вигляду $A_{ij}/(t-\lambda_i)^j$, де $\lambda_1, \lambda_2, \dots, \lambda_r$ — корені многочлена $f(t)$, а j не перебільшує кратності кореня λ_i. Після цього можна скористатися наведеними вище формулами для рядів $(1-t)^{-j}$. Найпростіший випадок, звичайно, одержимо, якщо всі корені многочлена $f(t)$ прості, тобто $f(t) = C\prod_{i=1}^m (t-\lambda_i)$, де всі числа $\lambda_1, \lambda_2, \dots, \lambda_m$ різні. Тоді

$$
\frac{g(t)}{f(t)} = \sum_{i=1}^m \frac{A_i}{t-\lambda_i}.
$$

Числа A_i легко обчислити з рівності многочленів

$$g(t) = \sum_{i=1}^{m} A_i \frac{f(t)}{t - \lambda_i} = \sum_{i=1}^{m} A_i C \prod_{j \neq i} (t - \lambda_j).$$

Підставивши в неї $t = \lambda_i$, одержимо

$$A_i = \frac{g(\lambda_i)}{C \prod_{j \neq i} (\lambda_i - \lambda_j)} = \frac{g(\lambda_i)}{f'(\lambda_i)},$$

оскільки $f'(t) = C \sum_{i=1}^{m} \prod_{j \neq i} (t - \lambda_j)$. Але

$$\frac{1}{t - \lambda} = -\frac{1}{\lambda} \cdot \frac{1}{1 - \frac{t}{\lambda}} = -\frac{1}{\lambda} \sum_{n=0}^{\infty} \frac{t^n}{\lambda^n}.$$

Звідси одержимо наступний результат про значення a_n, які є коефіцієнтами степеневого ряду $g(t)/f(t)$.

Наслідок 1.6.2. *Якщо многочлен $f(t)$ з теореми 1.6.1 має лише прості корені $\lambda_1, \lambda_2, \dots, \lambda_m$, то*

$$a_n = \sum_{i=1}^{m} \frac{B_i}{\lambda_i^{n+1}}, \quad \text{де} \quad B_i = -\frac{g(\lambda_i)}{\lambda_i f'(\lambda_i)}. \tag{6.2}$$

Тому значення a_n, які є коефіцієнтами степеневого ряду $f(t)/g(t)$ можна обчислити

Приклад 1.6.3 (Числа Фібоначчі). *Числа Фібоначчі* Φ_n визначаються рекурентним співвідношенням $\Phi_{n+2} = \Phi_n + \Phi_{n+1}$, за умов $a_0 = 0$, $a_1 = 1$. Отже, в цьому випадку $\widetilde{f}(t) = t^2 + t$, $g_0(t) = t$, $g_1(t) = 0$, тобто $f(t) = 1 - t - t^2$, $g(t) = t$. Корені $f(t)$ дорівнюють $\lambda_{\pm} = (-1 \pm \sqrt{5})/2$, причому $\lambda_+ \lambda_- = -1$ і $f'(\lambda_{\pm}) = \mp\sqrt{5}$. Звідси

$$\Phi_n = \frac{1}{\sqrt{5}} \Big(-\frac{1}{\lambda_+^n} + \frac{1}{\lambda_-^n} \Big) = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right).$$

Цю дещо несподівану на перший погляд формулу для чисел Фібоначчі вперше одержав Даніел Бернуллі в 1728 році.

7. Ряди Діріхле

Розглянемо ще один варіант техніки твірних функцій, який має особливо великі застосування в теорії чисел. Він пов'язаний з так званими *рядами Діріхле.*

Означення 1.7.1. 1. (Формальним) рядом Діріхле, або *L-рядом* послідовності $\mathbf{a} = (a_n)$ зветься вираз

$$L_{\mathbf{a}}(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Тут знов-таки s — деякий формальний символ, і нас не цікавитиме питання про збіжність таких рядів.

2. Сума і добуток рядів Діріхле $L_{\mathbf{a}}(s)$ та $L_{\mathbf{b}}(s)$ звуться, відповідно, ряди

$$L_{\mathbf{a}}(s)+L_{\mathbf{b}}(s)=\sum_{n=1}^{\infty}\frac{a_n+b_n}{n^s},$$
$$L_{\mathbf{a}}(s)L_{\mathbf{b}}(s)=\sum_{n=1}^{\infty}\frac{c_n}{n^s},\quad \text{де}\quad c_n=\sum_{d|n}a_d b_{n/d}.$$

Послідовність $\mathbf{c}=(c_n)$ з формули добутку зветься *мультиплікативною згорткою*, або *мультиплікативною композицією* послідовностей $\mathbf{a}$ та $\mathbf{b}$ і позначається $\mathbf{a}\circ\mathbf{b}$.

Ряд Діріхле $\zeta(s)=\sum_{n=1}^{\infty}n^{-s}$ зветься *гармонічним рядом*, або *дзета-функцією*.

Знов-таки неважко переконатися, що відносно цих дій множина рядів Діріхле утворює комутативне кільце, причому має місце результат, аналогічний твердженню 1.5.2.

Твердження 1.7.2. *У кільці рядів Діріхле ряд $L_{\mathbf{a}}(s)$ має обернений тоді й лише тоді, коли* $a_1\neq 0$.

Обчислимо ряд Діріхле, обернений до гармонічного ряду $\zeta(s)$.

Твердження 1.7.3. *Оберненим до гармонічного ряду є ряд*

$$\mathrm{M}(s)=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s},$$

де $\mu(n)$ — так звана функція Мебіуса*, яка визначається правилами:*
- $\mu(1)=1$,
- $\mu(n)=(-1)^m$, якщо $n=p_1p_2\dots p_m$, де $p_1,p_2,\dots,p_m$ — попарно різні первинні числа,
- $\mu(n)=0$ інакше (тобто, якщо n ділиться на квадрат якогось первинного числа).

Доведення. Треба перевірити, що $\mathrm{M}(s)\zeta(s)=1$, тобто для кожного $n>1$ має місце рівність $\sum_{d|n}\mu(d)=0$. Нехай $n=p_1^{k_1}p_2^{k_2}\dots p_m^{k_m}$, де $p_1,p_2,\dots,p_m$ — попарно різні первинні числа. Кожен дільник d числа n має вигляд $p_1^{l_1}p_2^{l_2}\dots p_m^{l_m}$, де $0\le l_i\le k_i$. Якщо якийсь показник $l_i>1$, $\mu(d)=0$, інакше $\mu(d)=(-1)^r$, де r — кількість ненульових показників. При фіксованому значенні r існує $\binom{m}{r}$ варіантів для вибору r ненульових показників серед m можливих. Отже,

$$\sum_{d|n}\mu(d)=\sum_{r=0}^{m}(-1)^r\binom{m}{r}=0,$$

що й треба було довести. □

Звідси одержуємо такий наслідок.

Наслідок 1.7.4 (Мебіусова формула обертання). *Нехай α,β — дві функції натурального аргумету. Якщо $\beta(n)=\sum_{d|n}\alpha(d)$ для кожного n, то також $\alpha(n)=\sum_{d|n}b(d)\mu(n/d)$ для кожного n.*

Доведення. Перша формула показує, що $L_\beta(s) = L_\alpha(s)\zeta(s)$. Доможивши на $\mathrm{M}(s)$, одержимо $L_\alpha(s) = L_\beta(s)\mathrm{M}(s)$, що рівносильно другій формулі. $\square$

Інколи формули з останнього наслідку зручніше переписати в рівносильному вигляді

$$\beta(n) = \sum_{d|n} \alpha\Big(\frac{n}{d}\Big) \quad \text{і} \quad \alpha(n) = \sum_{d|n} \mu(d)\beta\Big(\frac{n}{d}\Big).$$

Приклад 1.7.5 (Функція Ойлера). *Функція Ойлера* $\varphi(n)$ визначається як кількість натуральних чисел $a < n$, які *співпервинні* з n (тобто не мають з n спільних множників, крім 1). Зокрема, $\varphi(1) = 1$, $\varphi(p) = p-1$ і $\varphi(p^m) = p^m - p^{m-1}$, якщо p — первинне число. Легко переконатися, що $\sum_{d|n} \varphi(n/d) = n$. Це випливає з того, що, коли $n = cd$, $\varphi(c)$ збігається з кількістю чисел $a < n$, таких що найбільший спільний дільник (a, n) дорівнює d. Дійсно, кожне таке число має вигляд $a = bd$, де $(b, c) = 1$, і навпаки, якщо $a = bc$, $(b, c) = 1$, то $(a, n) = d$. Якщо d пробігає всі дільники n, вичерпуються як раз всі можливості для найбільшого спільного дільника (a, n). За Мебіусовою формулою обертання, маємо звідси

$$\varphi(n) = \sum_{d|n} \mu(d)\,\frac{n}{d} = \sum_{d|n} d\,\mu\Big(\frac{n}{d}\Big).$$

Функція α натурального аргументу зветься *мультиплікативною*, якщо для довільних співпервинних чисел m, n має місце рівність $f(mn) = f(m)f(n)$. Такою є, наприклад, функція Мебіуса. Такі функції мають наступну важливу властивість.

Твердження 1.7.6. *Якщо функції α та β мультиплікативні, то їхня мультиплікативна згортка $\alpha\circ\beta$ також мультиплікативна. Зокрема, функції α та β з наслідку 1.7.4 є мультиплікативними одночасно.*

Доведення. Очевидно, кожен дільник d добутку співпервинних чисел mn однозначно розкладається в добуток bc, де $b|m$, $c|n$, причому також $(b, c) = 1$. Тому

$$\begin{aligned}(\alpha \circ \beta)(mn) &= \sum_{d|mn} \alpha(d)\beta(mn/d) = \sum_{b|m}\sum_{c|n} \alpha(bc)\beta(mn/bc) = \\ &= \sum_{b|m}\sum_{c|n} \alpha(b)\alpha(c)\beta(m/b)\beta(n/c) = \\ &= \sum_{b|m} \alpha(b)\beta(m/b) \cdot \sum_{c|n} \alpha(c)\beta(n/c) = \\ &= (\alpha \circ \beta)(m) \cdot (\alpha \circ \beta)(n).\end{aligned}$$

$\square$

Для функції Ойлера одержимо такий наслідок.

Наслідок 1.7.7 (Формула Ойлера). *Якщо $n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$, то*

$$\varphi(n) = \prod_{i=1}^{m} \big(p_i^{k_i} - p_i^{k_i-1}\big) = n \prod_{i=1}^{m} \Big(1 - \frac{1}{p_i}\Big).$$

Розділ 2

Елементи математичної логіки

1. Булеві функції та логічні сполучники

Логічним висловлюванням зветься деяке твердження, яке може бути *вірним* або *хибним*. Такому твердженню A приписується *логічне*, або *булеве значення*, а саме:

$$\operatorname{val} A = \begin{cases} \mathbf{1} & \text{якщо } A \text{ вірне,} \\ \mathbf{0} & \text{якщо } A \text{ хибне.} \end{cases}$$

Розділ математики, який вивчає логічні висловлювання, відноситься до *математичної логіки*. Зараз ми лише познайомимось з деяким його елементарним фрагментом. Зауважимо, що математична логіка здебільшого не цікавиться, *чому* те чи інше висловлювання є вірним чи хибним. Це — задача інших, «конкретних» наук. Наприклад, розглянемо наступні висловлювання:

А. $2 \times 2 = 4$.
Б. Лондон — столиця України.
В. Росія — батьківщина слонів.
Г. Київ було засновано в V сторіччі по р.Х.
Д. Ім'я другої за списком дівчини цієї групи — Наталя.

З арифметки відомо, що висловлювання A вірне, з географії — що висловлювання B хибне, з зоології — що висловлювання C хибне (хоч як би це не дратувало деяких «патріотів»). Відносно висловлювання D думки фахіців–істориків розходяться, а значення висловлювання E взагалі залежить від того, про яку саме групу йдеться. Але, повторюємо, вирішувати все це — не справа математичної логіки.

Натомість математична логіка вивчає, як з одних висловлювань можна конструювати інші («складені») в такий спосіб, щоб значення нового висловлювання повністю визначалося значеннями висловлювань, з яких воно утворене. Для цього використовуються *логічні сполучники*.

ОЗНАЧЕННЯ 2.1.1. *n-місним логічним сполучником* зветься операція C, яка за довільним набором висловлювань $A_1, A_2, \dots, A_n$ утворює нове висловлювання $C = \mathsf{C}(A_1, A_2, \dots, A_n)$, причому логічне значення висловлювання C повністю визначається логічними значеннями висловлювань $A_1, A_2, \dots, A_n$.

Якщо нас, як це ведеться в математичній логіці, не цікавить *зміст* розглядуваних висловлювань, то, очевидно, сполучник C повністю визначається функцією від n змінних $\mathsf{c}(a_1, a_2, \dots, a_n)$, де всі a_i належать множині булевих значень $\mathbb{B} = \{\mathbf{0}, \mathbf{1}\}$ і цій же множині належать і значення функції c; отже $\mathsf{c} : \mathbb{B}^n \to \mathbb{B}$. Саме, ця функція визначається рівністю

$$\operatorname{val} \mathsf{C}(A_1, A_2, \dots, A_n) = \mathsf{c}(\operatorname{val} A_1, \operatorname{val} A_2, \dots, \operatorname{val} A_n) \tag{1.1}$$

для довільних висловлювань $A_1, A_2, \dots, A_n$. Функція c зветься *приєднаною функцією* сполучника C. Навпаки, за будь-якою n-функцією $\mathsf{c} : \mathbb{B}^n \to \mathbb{B}$ можна визначити такий сполучник C, щоб справжнювалася рівність (1.1). Такі функції звуться *булевими функціями*.

Насправді, реально використовується досить обмежений набір логічних сполучників. Наведемо найважливіші з них, вказавши їхні приєднані функції. Більш того, ми, за сталим звичаєм, позначатимемо ці сполучники тими самими літерами, що й відповідні функції, і називатимемо їх також однаково.

1. *Заперечення* $\neg$ — це одномісний (унарний) сполучник з приєднаною функцією

A	$\neg A$
$\mathbf{0}$	$\mathbf{1}$
$\mathbf{1}$	$\mathbf{0}$

   Висловлювання $\neg A$ передається також словами «не A».
2. *Кон'юнкція* $\wedge$ (або &) — це двомісний (бінарний) сполучник з приєднаною функцією

A	B	$A \wedge B$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{0}$	$\mathbf{1}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$

   Висловлювання $A \wedge B$ передається також словами «A і B».
3. *Диз'юнкція* $\vee$ — це двомісний (бінарний) сполучник з приєднаною функцією

A	B	$A \vee B$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{0}$	$\mathbf{1}$	$\mathbf{1}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$

   Висловлювання $A \vee B$ передається також словами «A або B».
4. *Імплікація* $\Rightarrow$ — це двомісний (бінарний) сполучник з приєднаною функцією

A	B	$A \Rightarrow B$
$\mathbf{0}$	$\mathbf{0}$	$\mathbf{1}$
$\mathbf{0}$	$\mathbf{1}$	$\mathbf{1}$
$\mathbf{1}$	$\mathbf{0}$	$\mathbf{0}$
$\mathbf{1}$	$\mathbf{1}$	$\mathbf{1}$

   Висловлювання $A \Rightarrow B$ передається також словами «Якщо A, то B».

5. *Еквіваленція* $\Leftrightarrow$ — це двомісний (бінарний) сполучник з приєднаною функцією

A	B	$A \Leftrightarrow B$
0	**0**	**1**
0	**1**	**0**
1	**0**	**0**
1	**1**	**1**

Висловлювання $A \Leftrightarrow B$ передається також словами «A тоді й лише тоді, коли B».

6. *Логічне додавання*, (*розділяюче* «або», *антиеквіваленція*) $\oplus$ — це двомісний (бінарний) сполучник з приєднаною функцією

A	B	$A \oplus B$
0	**0**	**0**
0	**1**	**1**
1	**0**	**1**
1	**1**	**0**

Висловлювання $A \oplus B$ передається також словами «або A, або B».

Як і звичайні арифметичні операції, логічні сполучники можна комбінувати, утворюючи нові висловлювання. Порядок їх застосування найчастіше визначається дужками, наприклад

$$E = (A \Leftrightarrow (\neg((\neg B) \wedge C))) \Rightarrow ((A \vee (\neg C)) \oplus (D \Rightarrow B)).$$

Знов-таки, як і в арифметиці, щоб зменшити кількість дужок та зробити складені висловлювання більш виразними, використовують домовленість про *порядок дій*:

1. Першим завжди застосовують *заперечення*.
2. Після заперечення застосовують *кон'юнкцію* та *диз'юнкцію*.
3. Потому застосовують *логічне додавання*.
4. Нарешті, останніми застосовують *імплікацію* та *еквіваленцію*.
5. Всередині кожної групи порядок дій визначається дужками.

За такої домовленості, останній приклад можна переписати скорочено так:

$$E = (A \Leftrightarrow \neg(\neg B \wedge C)) \Rightarrow A \vee \neg C \oplus (D \Rightarrow B).$$

Зрозуміло, що коли задано (логічне) значення висловлювань A, B, C, D, легко обчислити й значення утвореного з них висловлювання E, наприклад:

A	B	C	D	$\neg B$	$\neg C$	E_1	E_2	E_3	E_4	E_5	E_6	E
0	**1**	**1**	**0**	**0**	**0**	**0**	**1**	**0**	**0**	**1**	**1**	**1**
1	**1**	**0**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**1**	**0**	**0**

де позначено:

$$\begin{aligned}
E_1 &= \neg B \wedge C,\\
E_2 &= \neg(\neg B \wedge C) = \neg E_1,\\
E_3 &= A \Leftrightarrow \neg(\neg B \wedge C) = A \Leftrightarrow E_1,\\
E_4 &= A \vee \neg C,\\
E_5 &= D \Rightarrow B,\\
E_6 &= A \vee \neg C \oplus (D \Rightarrow B) = E_4 \oplus E_5.
\end{aligned}$$

Висловлювання, які не розділяються на частини, звуться *елементарними*, або *атомами*. Звісно, перелік атомів залежить від того, яку задачу ми розглядаємо. Більш того, оскільки значення елементарних висловлювань визначається позалогічними методами, у логіці атоми розглядаються здебільшого як *змінні*, які можуть набувати значень з множини $\mathbb{B}$ (*логічні*, або *булеві змінні*). Тоді складене висловлювання стає булевою функцією від цих змінних. Неважко зрозуміти, що, взагалі кажучи, різні складені висловлювання можуть визначати ту саму булеву функцію. Найпростіший приклад: вирази $A \oplus B$ та $\neg(A \Leftrightarrow B)$ задають одну й ту ж булеву функцію. Ось ще приклади таких збігів:

$$A \vee B = B \vee A, \tag{B1}$$
$$A \wedge B = B \wedge A, \tag{B2}$$
$$A \vee (B \vee C) = (A \vee B) \vee C, \tag{B3}$$
$$A \wedge (B \wedge C) = (A \wedge B) \wedge C, \tag{B4}$$
$$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C), \tag{B5}$$
$$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C), \tag{B6}$$
$$A \vee A = A, \tag{B7}$$
$$A \wedge A = A, \tag{B8}$$
$$\neg(A \vee B) = \neg A \wedge \neg B, \tag{B9}$$
$$\neg(A \wedge B) = \neg A \vee \neg B, \tag{B10}$$
$$\neg\neg A = A, \tag{B11}$$
$$A \vee \neg A = \mathbf{1}, \tag{B12}$$
$$A \wedge \neg A = \mathbf{0}. \tag{B13}$$
$$A \Rightarrow B = \neg A \vee B, \tag{B14}$$
$$A \Leftrightarrow B = (A \Rightarrow B) \wedge (B \Rightarrow A), \tag{B15}$$
$$A \vee B = A \oplus B \oplus A \wedge B, \tag{B16}$$

У рядках (B12) та (B13) через **1** та **0** позначено сталі функції, які завжди приймають значення, відповідно, **1** та **0**.

Оскільки булеві функції відіграють істотну роль у сучасній математиці й техніці, виникає питання, які набори булевих функцій є *повними*, тобто такими, через які за допомогою суперпозицій можна виразити всі інші. Цьому питанню буде присвячено наступний розділ.

2. Повні набори булевих функцій

У цьому розділі ми розглянемо декілька важливих прикладів повних наборів і дамо критерій, за яким визначається, чи даний набір є повним, чи ні.

2.1. Нормальні форми булевих функцій.

Означення 2.2.1. Нехай фіксовано деякий набір $\mathbf{A} = \{ a_1, a_2, \dots, a_n \}$ булевих змінних.

1. *Елементарною кон'юнкцією* зветься вираз вигляду $a_1' \wedge a_2' \wedge \dots a_n'$, де кожне a_i' — це або a_i, або $\neg a_i$. Наприклад, для $n = 4$,

$$a_1 \wedge \neg a_2 \wedge a_3 \wedge \neg a_4,\ \neg a_1 \wedge \neg a_2 \wedge a_3 \wedge \neg a_4,\ a_1 \wedge a_2 \wedge \neg a_3 \wedge a_4.$$

2. *Досконалою диз'юнктивною нормальною формою* (скорочено *ДДНФ*) зветься диз'юнкція елементарних кон'юнкцій, наприклад

$$(a_1 \wedge \neg a_2 \wedge a_3 \wedge \neg a_4) \vee (\neg a_1 \wedge \neg a_2 \wedge a_3 \wedge \neg a_4) \vee (a_1 \wedge a_2 \wedge \neg a_3 \wedge a_4).$$

3. *Елементарною диз'юнкцією* зветься вираз вигляду $a_1' \vee a_2' \vee \dots a_n'$, де кожне a_i' — це або a_i, або $\neg a_i$, наприклад

$$a_1 \vee a_2 \vee a_3 \vee \neg a_4,\ \neg a_1 \vee \neg a_2 \vee \neg a_3 \vee \neg a_4,\ a_1 \vee a_2 \vee \neg a_3 \vee a_4.$$

4. *Досконалою кон'юнктивною нормальною формою* (скорочено *ДКНФ*) зветься кон'юнкція елементарних диз'юнкцій, наприклад

$$(a_1 \vee a_2 \vee a_3 \vee \neg a_4) \wedge (\neg a_1 \vee \neg a_2 \vee \neg a_3 \vee \neg a_4) \wedge (a_1 \vee a_2 \vee \neg a_3 \vee a_4).$$

Зауважимо, що всі ці означення залежать від обраного набору змінних $a_1, a_2, \dots, a_n$.

Теорема 2.2.2.
1. *Для кожної булевої функції від булевих змінних $a_1, a_2, \dots, a_n$ існує еквівалентна їй* ДДНФ, *яка визначена однозначно з точністю до перестановки елементарних кон'юнкцій.*
2. *Для кожної булевої функції від булевих змінних $a_1, a_2, \dots, a_n$ існує еквівалентна їй* ДКНФ, *яка визначена однозначно з точністю до перестановки елементарних диз'юнкцій.*

Доведення. Ми доведемо тільки друге твердження (про ДКНФ), залишивши перше з них читачеві як вправу. Перш за все зробимо наступне зауваження.

Лема 2.2.3.
1. *Елементарна диз'юнкція $a_1' \vee a_2' \vee \dots a_n'$ приймає значення* $\mathbf{1}$ *при всіх значеннях змінних $a_1, a_2, \dots, a_n$, крім одного, яке визначається так:*

$$a_i = \begin{cases} \mathbf{0} & \text{якщо } a_i' = a_i, \\ \mathbf{1} & \text{якщо } a_i' = \neg a_i. \end{cases}$$

При цих значеннях змінних вона приймає значення $\mathbf{0}$.

2. *Навпаки, для будь-яких заданих значень змінних* $a_1, a_2, \dots, a_n$ *існує єдина елементарна диз'юнкція, яка приймає значення* $\mathbf{0}$ *при таких значеннях змінних, а саме* $a_1' \vee a_2' \vee \dots a_n'$*, де*

$$a_i' = \begin{cases} a_i & \text{якщо } \operatorname{val} a_i = \mathbf{0}, \\ \neg a_i & \text{якщо } \operatorname{val} a_i = \mathbf{1}. \end{cases}$$

Будемо казати, що елементарна диз'юнкція відповідає *тому набору значень змінних, при якому вона набуває значення* $\mathbf{0}$*, і навпаки.*

Доведення. Диз'юнкція приймає значення $\mathbf{0}$ тоді й лише тоді, коли всі її складові частини мають значення $\mathbf{0}$. Але вказані значення a_i — це точно ті, при яких $a_i' = \mathbf{0}$. Звідси випливають обидва твердження леми. $\square$

Повернемося до доведення теореми. Згадаємо, що кон'юнкція набуває значення $\mathbf{0}$ тоді й лише тоді, коли це значення мають всі її складові частини. Тому ДКНФ набирає значення $\mathbf{0}$ при тих і лише тих наборах значень змінних, які відповідають тим елементарним диз'юнкціям, які входять до її складу. Звідси, зокрема, випливає, що різні ДКНФ (тобто ті, до складу яких входять різні набори елементарних диз'юнкцій) задають різні функції. Нарешті, якщо f — довільна булева функція від змінних $a_1, a_2, \dots, a_n$, а $E_1, E_2, \dots, E_m$ — всі елементарні диз'юнкції, які відповідають тим наборам значень змінних $a_1, a_2, \dots, a_n$, при яких f набуває значення $\mathbf{0}$, то з леми 2.2.3 одразу випливає, що КНФ $E_1 \wedge E_2 \wedge \dots \wedge E_m$ еквівалентна функції f. $\square$

Наслідок 2.2.4. *Набори булевих функцій* $\{\neg, \wedge\}$ *та* $\{\neg, \vee\}$ *є повними.*

Доведення. З теореми 2.2.2 випливає, що повним є набір $\{\neg, \vee, \wedge\}$. Але з тотожностей (B9) та (B10) одержуємо, що $A \vee B = \neg(\neg A \wedge \neg B)$, а $A \wedge B = \neg(\neg A \vee \neg B)$. $\square$

2.2. Булеві многочлени. Інший важливий набір булевих функцій складають $\{\mathbf{0}, \mathbf{1}, \wedge, \oplus\}$ (перші дві — це булеві константи). З їхнього означення видно, що насправді функції $\wedge$ та $\oplus$ — це множення та додавання *за модулем 2*, якщо вважати $\mathbf{0}$ та $\mathbf{1}$, відповідно, класами лишків, які містять 0 та 1. Тому кон'юнкцію $\wedge$ звуть також *булевим множенням* і замість $A \wedge B$ пишуть AB. Ми будемо дотримуватись таких позначень у цьому підрозділі. Враховуючи те, що класи лишків утворюють кільце, і тотожність (B8), довільний вираз від булевих змінних $x_1, x_2, \dots, x_n$, в якому беруть участь лише функції $\wedge$, $\oplus$ та булеві константи, можна записати як многочлен вигляду

$$\sum_{1 e i_1 < i_2 < \dots < i_k \leq n} c_{i_1 i_2 \dots i_k} x_{i_1} x_{i_2} \dots x_{i_k} \qquad (c_{i_1 i_2 \dots i_k} \in \{\mathbf{0}, \mathbf{1}\})$$

(всі невідомі зустрічаються лише в першому степені). Такі многочлени ми зватимемо *булевими многочленами.*

Теорема 2.2.5. *Для кожної булевої функції* $f(x_1, x_2, \dots, x_n)$ *існує єдиний булів многочлен* $F(x_1, x_2, \dots, x_n)$*, еквівалентний функції* F*.*

Доведення. Зауважимо, що кількість булевих одночленів $x_{i_1}x_{i_2}\dots x_{i_k}$ від n змінних дорівнює кількості підмножин у множині $\{x_1, x_2, \dots, x_n\}$, тобто 2^n. Щоб задати булів многочлен, треба кожному такому одночлену поставити у відповідність $\mathbf{0}$ або $\mathbf{1}$ — відповідний коефіцієнт. Тому загальна кількість таких многочленів дорівнює 2^{2^n}, тобто загальній кількості булевих функцій. Отже, достатньо довести лише одне з двох тверджень теореми: *існування* многочлена F або його *єдиність*. Ми будемо доводити існування, користуючись індукцією за кількістю невідомих n. Якщо $n = 1$, є всього 4 булевих функції: дві констатнти, тотожня функція $f(x) = x$ та заперечення $\neg x = \mathbf{1} \oplus x$. Всі вони виражаються булевими многочленами. Припустимо, що твердження теореми вірне для функцій від n змінних, і розглянемо довільну булеву функцію $f(x_1, x_2, \dots, x_{n+1})$ від $n + 1$ змінної. Позначимо $f_0(x_1, x_2, \dots, x_n) = f(x_1, x_2, \dots, x_n, \mathbf{0})$ і $f_1(x_1, x_2, \dots, x_n) = f(x_1, x_2, \dots, x_n, \mathbf{1})$. Це вже функції від n змінних. За індуктивним припущенням, існують булеві многочлени F_0 та F_1, такі що $f_0(x_1, x_2, \dots, x_n) = F_0(x_1, x_2, \dots, x_n)$ і $f_1(x_1, x_2, \dots, x_n) = F_1(x_1, x_2, \dots, x_n)$ для довільних значень змінних $x_1, x_2, \dots, x_n$. Але легко бачити, що для довільних значень $x_1, x_2, \dots, x_{n+1}$

$$
\begin{aligned}
&f(x_1, x_2, \dots, x_{n+1}) = \\
&\quad = (\mathbf{1} \oplus x_{n+1}) f_0(x_1, x_2, \dots, x_n) \oplus x_{n+1} f_1(x_1, x_2, \dots, x_n) = \\
&\quad = (\mathbf{1} \oplus x_{n+1}) F_0(x_1, x_2, \dots, x_n) \oplus x_{n+1} F_1(x_1, x_2, \dots, x_n),
\end{aligned}
$$

а останній вираз є булевим многочленом. За принципом математичної індукції, теорему повністю доведено. □

2.3. Теорема Поста. Серед усіх булевих функцій виділяються спеціальні підкласи, які напевно не є повними. Для цього зручно ввести порядок на множині булевих значень, вважаючи, що $\mathbf{0} < \mathbf{1}$. Позначимо також, для довільного набору $\mathbf{a} = (a_1, a_2, \dots, a_n)$ булевих значень, $\neg\mathbf{a} = (\neg a_1, \neg a_2, \dots, \neg a_n)$.

Означення 2.2.6. Кажуть, що булева функція $f(x_1, x_2, \dots, x_n)$

- *зберігає нуль*, якщо $f(\mathbf{0}, \mathbf{0}, \dots, \mathbf{0}) = \mathbf{0}$;
- *зберігає одиницю*, якщо $f(\mathbf{1}, \mathbf{1}, \dots, \mathbf{1}) = \mathbf{1}$;
- *монотонна*, якщо з нерівностей $a_i \le b_i$ для всіх i випливає, що $f(a_1, a_2, \dots, a_n) \le f(b_1, b_2, \dots, b_n)$;
- *самодвоїста*, якщо $f(\neg\mathbf{a}) = \neg f(\mathbf{a})$ для довільного набору $\mathbf{a}$ булевих значень;
- *лінійна*, якщо вона еквівалентна лінійному булевому многочлену, тобто виразу вигляду

$$c_0 \oplus c_1 \wedge x_1 \oplus c_2 \wedge x_2 \oplus \dots \oplus c_n \wedge x_n,$$

  де $c_i \in \{\mathbf{0}, \mathbf{1}\}$.

Позначимо через

- $\mathfrak{F}_0$ множину всіх булевих функцій, які зберігають нуль;
- $\mathfrak{F}_1$ множину всіх булевих функцій, які зберігають одиницю;

- $\mathfrak{F}_2$ множину всіх монотонних булевих функцій;

- $\mathfrak{F}_3$ множину всіх самодвоїстих булевих функцій;

- $\mathfrak{F}_4$ множину всіх лінійних булевих функцій.

Наступне твердження очевидне, і ми залишаємо його доведення читачеві як вправу.

Твердження 2.2.7. *Якщо булева функція F одержана з деяких функцій, які всі належать класу $\mathfrak{F}_k$ ($0 \leq k \leq 4$), за допомогою суперпозицій, то вона теж належить класу $\mathfrak{F}_k$.*

З твердження 2.2.7 одразу випливає необхідність умов наступної теореми, яка характеризує повні набори булевих функцій.

Теорема 2.2.8 (Теорема Поста). *Набір $\mathfrak{M}$ булевих функцій є повним тоді й лише тоді, коли $\mathfrak{M} \not\subseteq \mathfrak{F}_k$ для кожного $0 \leq k \leq 4$; інакше кажучи, коли він містить*

- *принаймні одну функцію, яка не зберігає нуль;*
- *принаймні одну функцію, яка не зберігає одиницю;*
- *принаймні одну немонотонну функцію;*
- *принаймні одну несамодвоїсту функцію;*
- *принаймні одну нелінійну функцію.*

Доведення. Ми вже перевірили, що повний набір задовольняє цим вимогам. Навпаки, припустимо, що всі вони виконані. Позначимо $\mathfrak{N}$ множину всіх функцій, які можна отримати суперпозиціями з $\mathfrak{M}$. Виберемо для кожного $k = 0, 1, 2, 3, 4$ функцію g_k, яка належить $\mathfrak{M}$, але не належить $\mathfrak{F}_k$. Зокрема, тоді $g_0(\mathbf{0}, \mathbf{0}, \ldots, \mathbf{0}) = \mathbf{1}$. Позначимо $f_0(x) = g_0(x, x, \ldots, x)$. Якщо $g_0(\mathbf{1}, \mathbf{1}, \ldots, \mathbf{1}) = \mathbf{0}$, то $f_0 = \neg$, інакше $f_0 = \mathbf{1}$. Так само, функція $f_1(x) = g_1(x, x, \ldots, x)$ — або константа $\mathbf{0}$, або заперечення. Отже, $\mathfrak{N}$ містить обидві константи $\mathbf{0}, \mathbf{1}$, або $\mathfrak{N}$ містить заперечення.

Оскільки функція g_2 немонотонна, існують такі значення $a_1, a_2, \ldots, a_n$ та $b_1, b_2, \ldots, b_n$ її аргументів, що, для кожного номера i, коли $a_i = \mathbf{1}$, то й $b_i = \mathbf{1}$, але $g_2(a_1, a_2, \ldots, a_n) = \mathbf{1}$, $g_2(b_1, b_2, \ldots, b_n) = \mathbf{0}$. Припустимо, що $\mathfrak{N}$ містить обидві константи $\mathbf{0}, \mathbf{1}$. Розглянемо функцію $f_2(x) = g_2(y_1, y_2, \ldots, y_n)$, де

$$y_i = \begin{cases} \mathbf{0} & \text{якщо } a_i = b_i = \mathbf{0}, \\ \mathbf{1} & \text{якщо } a_i = b_i = \mathbf{1}, \\ x & \text{якщо } a_i = \mathbf{0},\ b_i = \mathbf{1}. \end{cases}$$

Тоді $f_2(\mathbf{0}) = g_2(a_1, a_2, \ldots, a_n) = \mathbf{1}$, $f_2(\mathbf{1}) = g_2(b_1, b_2, \ldots, b_n) = \mathbf{0}$, тобто $f_2 = \neg$. Отже, якщо $\mathfrak{N}$ містить обидві констатнти, вона містить і заперечення.

Оскільки функція g_3 несамодвоїста, існують такі значення $a_1, a_2, \ldots, a_n$ її змінних, що $g(a_1, a_2, \ldots, a_n) = g(\neg a_1, \neg a_2, \ldots, \neg a_n)$. Припустимо, що $\mathfrak{N}$ містить заперечення. Розглянемо функцію $f_3(x) = g_3(y_1, y_2, \ldots, y_n)$, де

$$y_i = \begin{cases} x & \text{якщо } a_i = \mathbf{1}, \\ \neg x & \text{якщо } a_i = \mathbf{0}. \end{cases}$$

Тоді

$$f_3(\mathbf{1}) = g_3(a_1, a_2, \dots, a_n) = g_3(\neg a_1, \neg a_2, \dots, \neg a_n) = f_3(\mathbf{0}),$$

тобто f_3 — константа. Тоді $\neg f_3$ — друга булева константа. Отже, якщо $\mathfrak{N}$ містить заперечення, воно містить і обидві константи. Враховуючи всі попередні розгляди, ми одержимо, що $\mathfrak{N}$ напевне містить і заперечення, і обидві булеві константи.

Розглянемо, нарешті, нелінійну функцію g_4. Її можна вважати булевим многочленом, тобто булевою сумою деяких кон'юнкцій вигляду $x_{i_1} \wedge x_{i_2} \wedge \dots \wedge x_{i_m}$ Нехай m — найменше число, таке що $m > 1$ і член $w = x_{i_1} \wedge x_{i_2} \wedge \dots \wedge x_{i_m}$ дійсно входить до булевого многочлену g_4 (воно існує, бо цей многочлен нелінійний). Розглянемо функцію $f_4(x, y) = g_4(y_1, y_2, \dots, y_n)$, де

$$y_i = \begin{cases} x & \text{якщо } i = i_1, \\ y & \text{якщо } i \in \{ i_2, \dots, i_m \}, \\ \mathbf{0} & \text{якщо } i \notin \{ i_1, i_2, \dots, i_m \}. \end{cases}$$

Після такої підстановки всі нелінійні члени, крім w, обертаються на $\mathbf{0}$. Тому f_4 — це булів многочлен вигляду

$$f_4(x, y) = c \oplus a \wedge x \oplus b \wedge y \oplus x \wedge y,$$

де a, b, c — деякі булеві константи. Зауважимо, що $\neg f_4 = \mathbf{1} \oplus f_4 = \neg c \oplus a \wedge x \oplus b \wedge y \oplus x \wedge y$. Тому можна вважати, що $c = \mathbf{0}$. Розглянемо різні випадки.

1. Якщо $a = b = \mathbf{0}$, то $f_4(x, y) = x \wedge y$.
2. Якщо $a = b = \mathbf{1}$, то $f_4(x, y) = x \oplus y \oplus x \wedge y = x \vee y$.
3. Якщо $a = \mathbf{1}$, $b = \mathbf{0}$, то $f_4(x, y) = x \oplus x \wedge y = x \wedge (\mathbf{1} \oplus y) = x \wedge \neg y$ і $f_4(x, \neg y) = x \wedge y$.
4. Так само, якщо $a = \mathbf{0}$, $b = \mathbf{1}$, то $f_4(\neg x, y) = x \wedge y$.

Отже, напевне $\mathfrak{N}$ містить кон'юнкцію або диз'юнкцію. Оскільки $\mathfrak{N}$ містить заперечення, з наслідку 2.2.4 випливає, що $\mathfrak{M}$ — повний набір. □

З теореми Поста безпосередньо випливає, що кожен повний набір $\mathfrak{M}$ булевих функцій містить підмножину $\mathfrak{M}'$, яка складається щонайбільше з 5 елементів і також є повним набором. Насправді, цю оцінку можна легко зменшити.

Наслідок 2.2.9. *Кожен повний набір $\mathfrak{M}$ булевих функцій містить підмножину $\mathfrak{M}'$, яка складається щонайбільше з 4 елементів і також є повним набором.*

Доведення. Нехай $g_0 \in \mathfrak{M}$ — функція, яка не зберігає нуль, тобто $g_0(\mathbf{0}, \dots, \mathbf{0}) = \mathbf{1}$. Якщо $g_0(\mathbf{1}, \dots, \mathbf{1}) = \mathbf{0}$, ця функція також не зберігає одиницю. Якщо ж $g_0(\mathbf{1}, \dots, \mathbf{1}) = \mathbf{1}$, вона несамодвоїста. Отже, ця функція «покриває» дві з п'яти вимог теореми Поста. Щоб задовольнити інші три умови, потрібні ще щонайбільше три функції з множини $\mathfrak{M}$. Разом з g_0 вони й утворюють повний набір $\mathfrak{M}' \subseteq \mathfrak{M}$, який складається щонайбільше з 4 елементів. □

Приклад 2.2.10. Легко переконатися, що приналежність "стандартних" булевих функцій до класів $\mathfrak{F}_i$ визначається наступною таблицею:

	$\mathfrak{F}_0$	$\mathfrak{F}_1$	$\mathfrak{F}_2$	$\mathfrak{F}_3$	$\mathfrak{F}_4$
$\mathbf{0}$	$+$	$-$	$+$	$-$	$+$
$\mathbf{1}$	$-$	$+$	$+$	$-$	$+$
$\neg$	$-$	$-$	$-$	$+$	$+$
$\vee$	$+$	$+$	$+$	$-$	$-$
$\wedge$	$+$	$+$	$+$	$-$	$-$
$\Rightarrow$	$-$	$+$	$-$	$-$	$-$
$\Leftrightarrow$	$-$	$+$	$-$	$-$	$+$
$\oplus$	$+$	$-$	$-$	$-$	$+$

За цією таблицею легко перевіряти, чи є той чи інший набір булевих функцій від двох змінних повним. Звичйно, ця таблиця містить не всі функції від двох змінних (точніше, лише половину з них), але читач легко може доповнити її.

Сформулюємо ще один важливий наслідок з теореми Поста.

Наслідок 2.2.11. *Існує рівно дві булевих функції від двох змінних $f(x, y)$, такі що набір $\{ f \}$, який складається з однієї функції f є повним. Саме, це* стрілка Пірса *(або* антикон'юнкція*)* $x \uparrow y = \neg(x \wedge y)$ *та* штрих Шеффера *(або* антидиз'юнкція*)* $x \mid y = \neg(x \vee y)$.

Доведення. Шукана функція f мусить не зберігати нуль та одиницю, звідки $f(\mathbf{0}, \mathbf{0}) = \mathbf{1}$ і $f(\mathbf{1}, \mathbf{1}) = \mathbf{0}$. Крім того, ця функція мусить бути несамодвоїстою, тому значення $f(\mathbf{0}, \mathbf{1})$ та $f(\mathbf{1}, \mathbf{0})$ мають бути однаковими. Якщо $f(\mathbf{0}, \mathbf{1}) = f(\mathbf{1}, \mathbf{0}) = \mathbf{1}$, одержимо стрілку Пірса, якщо ж $f(\mathbf{0}, \mathbf{1}) = f(\mathbf{1}, \mathbf{0}) = \mathbf{0}$, одержимо штрих Шеффера. Легко бачити, що обидві ці функції також немонотонні й нелінійні, тобто кожна з множин $\{ \uparrow \}$ та $\{ \mid \}$ є повним набором. $\square$

3. Відношення

Означення 2.3.1. *n-місним* (або *n-арним*) *відношенням* на множині M зветься підмножина $R \subseteq M^n$. Кажуть, що елементи $a_1, a_2, \dots, a_n \in M$ (у заданому порядку) *знаходяться у відношенні* R, якщо $(a_1, a_2, \dots, a_n) \in R$.

Якщо $n = 2$, замість $(a, b) \in R$ частіше пишуть aRb. Наприклад, $a < b,\ a \sim b,\ a \equiv b$, і т. ін.

Інколи відношення зручно ототожнювати з функцією $\rho : M^n \to \mathbb{B}$ від n змінних, визначеною на множині M і з *булевими значеннями* $\{ \mathbf{0}, \mathbf{1} \}$. Дійсно, за кожним відношенням $R \subseteq M^n$ можна визначити функцію $\rho : M^n \to \mathbb{B}$, поклавши

$$\rho\,(a_1, a_2, \dots, a_n) = \begin{cases} \mathbf{1}, & \text{якщо } (a_1, a_2, \dots, a_n) \in R, \\ \mathbf{0}, & \text{якщо } (a_1, a_2, \dots, a_n) \notin R. \end{cases}$$

Навпаки, кожна функція $\rho : M^n \to \mathbb{B}$ визначає відношення $R \subseteq M^n$, а саме, $(a_1, a_2, \dots, a_n) \in R$ тоді й лише тоді, коли $\rho\,(a_1, a_2, \dots, a_n) = \mathbf{1}$. Це дає взаємно однозначну відповідність між відношеннями та булевозначними функціями. Очевидно, якщо M — скінченна множина з m

елементами, всього існує 2^{m^n} n-місних відношень на цій множині. Втім, багато з них є «однаковими» в розумінні наступного означення.

ОЗНАЧЕННЯ 2.3.2. Два n-місні відношення, $R \subseteq M^n$ та $S \subseteq N^n$, звуться *ізоморфними*, якщо існує така біекція $\phi : M \to N$, що, для довільних елементів $a_1, a_2, \dots, a_n \in M$, $(a_1, a_2, \dots, a_n) \in R$ тоді й лише тоді, коли $(\phi a_1, \phi a_2, \dots, \phi a_n) \in S$. У цьому випадку пишуть $R \simeq S$ і кажуть, що ϕ є *ізоморфізмом* відношення R на відношення S.

Легко перевірити, що коли ϕ — ізоморфізм R на S, то обернена біекція ϕ^{-1} є ізоморфізмом S на R, а якщо, крім того, $\psi : N \to L$ є ізоморфізмом S на відношення $T \subseteq L^n$, то добуток $\psi\phi$ є ізоморфізмом R на T. (Перевірте ці твердження!)

Якщо $R \subseteq M^n$ — відношення на множині M, а $N \subseteq M$ — якась підмножина, можна розглянути *обмеження* $R|_N$ цього відношення на N, поклавши $R|_N = R \cap N^n$. Дуже часто замість $R|_N$ продовжують писати R (і ми також будемо так робити.

Насправді, майже ніколи не доводиться розглядати *довільні* відношення. Найчастіше мають справу зі спеціальними класами відношень (переважно, двомісних, або бінарних). Для бінарних відношень визначено операції добутку та обертання.

1. *Добутком*, або *композицією*, бінарних відношень $R \subseteq M^2$ та $S \subseteq M^2$ зветься бінарне відношення

$$RS = \left\{\, (a, b) \in M^2 \,|\, \text{існує такий } c \in M, \text{ що } (a, c) \in R \text{ і } (c, b) \in S \,\right\}.$$

2. *Оберненим* до відношення $R \subseteq M^2$ зветься відношення

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

Відношення *рівності* $a = b$ часто зветься також *діагоналлю* і позначається Δ, або Δ_M, якщо треба явно вказати множину M. Очевидно, воно відіграє роль *нейтрального елемента* відносно добутку відношень: $\Delta R = R\Delta = R$ для довільного відношення $R \subseteq M^2$.

Далі ми розглянемо найбільш важливі класи відношень.

3.1. Еквівалентності.

ОЗНАЧЕННЯ 2.3.3. *Відношенням еквівалентності* (або просто *еквівалентністю*) на множині M зветься двомісне відношення $\sim$ на цій множині, яке має наступні властивості:

1. *Рефлексивність*: $a \sim a$ для всіх $a \in M$.
2. *Симетричність*: якщо $a \sim b$, то й $b \sim a$.
3. *Транзитивність*: якщо $a \sim b$ і $b \sim c$, то й $a \sim c$.

Зауважимо, що ці властивості легко формулюються на мові дій над відношеннями:

- рефлексивність: $R \supseteq \Delta$;
- симетричність: $R^{-1} \subseteq R$ (тоді, очевидно, $R^{-1} = R$);
- транзитивність: $R^2 \subseteq R$ (звичайно, R^2 позначає RR).

Приклади відношень еквівалентності зустрічаються дуже часто. Наведемо деякі з них.

- Відношення рівності $a = b$.

- Відношення порівняння цілих чисел за заданим модулем $a \equiv b \mod m$.
- Відношення рівнопотужності підмножин заданої множини $\#(A) = \#(B)$.
- Відношення ізоморфізму n-місних відношень $R \simeq S$ на даній множині M.

Читач легко поповнить цей перелік. Очевидно, що обмеження відношення еквівалентності на довільну підмножину знов-таки є еквівалентністю.

Відношення еквівалентності тісно пов'язані з *розбиттями* множини. Для цього введемо поняття *класів еквівалентності.*

Означення і твердження 2.3.4. Нехай $\sim$ — еквівалентність на множині M. *Класом елемента a* відносно цієї еквівалентності (або, якщо відношення $\sim$ фіксоване, *класом еквівалентності* елемента a) зветься підмножина $M_a = \{\, b \in M \mid b \sim a \,\}$.

Ці класи мають такі властивості:

1. $M = \bigcup_{a\in M} M_a$; *саме,* $a \in M_a$ *для кожного* $a \in M$.
2. $b \in M_a$ *тоді й лише тоді, коли* $M_b = M_a$.
3. *Два різні класи не мають спільних елементів.*

Множину класів еквівалентності відносно $\sim$ позначають $M/\!\sim$ і звуть *фактормножиною* множини M за еквівалентністю $\sim$. *Множиною представників* відносно $\sim$ зветься довільна підмножина $\widetilde{M} \subseteq M$, яка містить точно по одному елементу з кожного класу еквівалентності.

Доведення. *1* — наслідок рефлексивності.

2: Якщо $b \in M_a$, а $c \in M_b$, то $b \sim a$ і $c \sim b$, звідки $c \sim a$, тобто $c \in M_a$. Отже, $M_b \subseteq M_a$. Але з симетричності випливає, що також $a \sim b$, тобто $a \in M_b$, а тому $M_a \subseteq M_b$.

3: Якщо $M_a \cap M_b \neq \emptyset$, візьмемо довільний елемент $c \in M_a \cap M_b$. Згідно з *2*, тоді $M_c = M_a$ і $M_c = M_b$, отже $M_a = M_b$. $\square$

Теорема 2.3.5.

1. *Кожне розбиття* $M = \bigsqcup_{i\in I} M_i$ *множини* M *на підмножини, які не мають спільних елементів, визначає еквівалентність* $\sim$ *на цій множині: вважаємо, що* $a \sim b$, *якщо знайдеться такий індекс* $i \in I$, *що* a *та* b *обидва належать підмножині* M_i.
2. *Навпаки, кожне відношення еквівалентності* $\sim$ *на множині* M *визначає розбиття цієї множини:* $M = \bigsqcup_{a\in\widetilde{M}} M_a$, *де* $\widetilde{M}$ *— деяка множина представників відносно* $\sim$.

Очевидно, ці дві операції є взаємно оберненими.

Доведення цієї теореми очевидно випливає з означення і твердження 2.3.4. Ми залишаємо його читачеві в якості дуже простої вправи.

Підрахуємо кількість усіх відношень еквівалентності на заданій множині M, яка має m елементів, або, що те саме, кількість розбиттів множини M. Це число B_m зветься *числом Белла.* При фісованому n кількість розбиттів M на n частин визначається числом Стірлінга другого роду $S^n_m = \dfrac{1}{n!}\displaystyle\sum_{k=0}^{n}(-1)^k\binom{n}{k}(n-k)^m$ (див. твердження 1.4.5; ми додали сюди нульовий член з $k = n$). Крім того, відомо, що $S_m^n = 0$, коли $n > m$ або $n = 0$. Отже,

$$\mathrm{B}_m = \sum_{n=0}^{\infty} S_m^n = \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n-k)^m. \tag{3.1}$$

Виявляється, останню формулу можна перетворити до більш красивого вигляду.

Твердження 2.3.6. $\mathrm{B}_m = \dfrac{1}{e} \displaystyle\sum_{n=0}^{\infty} \frac{n^m}{n!}$.

Доведення. Оскільки $\dfrac{1}{n!}\dbinom{n}{k} = \dfrac{1}{k!(n-k)!}$, формулу (3.1) можна переписати у вигляді

$$\mathrm{B}_m = \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{(-1)^k}{k!} \frac{(n-k)^m}{(n-k)!}.$$

Тут (k, n) пробігає всі такі пари натуральних чисел, що $n \geq k$. Тому порядок пісумовування можна змінити так:

$$\mathrm{B}_m = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \sum_{n=k}^{\infty} \frac{(n-k)^m}{(n-k)!}$$

(ми також змінили індекс підсумовування з n на l.) Поклавши в останній сумі $l = n - k$, одержимо

$$\mathrm{B}_m = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \sum_{l=0}^{\infty} \frac{l^m}{l!} = \frac{1}{e} \sum_{n=0}^{\infty} \frac{n^m}{n!},$$

оскільки $\sum_{k=0}^{\infty} (-1)^k/k! = e^{-1}$. (На останньому кроці ми також змінили індекс пісумовування з l на n.) □

Зауваження. Можна розглянути ряд Діріхле $L_{\mathbf{a}}(s)$, де $a_n = 1/n!$. Легко переконатися, що цей ряд рівномірно збігається при $s \in \mathbb{R}$ (скористайтеся, наприклад, ознакою Вайєрштрасса). Тому він визначає неперервну функцію $\beta(s)$. Твердження 2.3.6 тоді показує, що $\mathrm{B}_m = \beta(-m)$. Крім того, оскільки й ряд для e^{-1} абсолютно збіжний, це також виправдовує зроблені нами формальні перетворення нескінченних сум.

3.2. Порядки та квазіпорядки.

Означення 2.3.7.
1. *Відношенням квазіпорядку* (або просто *квазіпорядком*) на множині M зветься бінарне відношення $\preccurlyeq$ на цій множині, яке має наступні властивості:
   (а) *Рефлексивність*: $a \preccurlyeq a$ для кожного $a \in M$.
   (б) *Транзитивність*: якщо $a \preccurlyeq b$ та $b \preccurlyeq c$, то також $a \preccurlyeq c$.
   Якщо, крім того, це відношення *антисиметричне*, тобто з того, що одночасно $a \preccurlyeq b$ та $b \preccurlyeq a$ випливає, що $a = b$, воно зветься *відношенням порядку* (або просто *порядком*) на множині M.
2. Кажуть, що квазіпорядок (зокрема, порядок) $\preccurlyeq$ є *лінійним*, якщо для довільних елементів $a, b \in M$ або $a \preccurlyeq b$, або $b \preccurlyeq a$. Якщо треба

підкреслити, що деякий квазіпорядок (порядок) не обов'язково лінійний, кажуть про *частковий* квазіпорядок (порядок).

3. Якщо $\preccurlyeq$ — порядок на M, то *відповідним строгим порядком* зветься відношення $\prec$: $a \prec b$ тоді й лише тоді, коли $a \preccurlyeq b$ і $a \neq b$. (Інколи, щоб підкреслити різницю між $\prec$ та $\preccurlyeq$, останнє відношення звуть «*нестрогим порядком*».)

Очевидно, строгий порядок $\prec$ завжди є транзитивним та *асиметричним*; останнє означає, що неможливо, щоб одночасно було $a \prec b$ та $b \prec a$. Навпаки, якщо $\prec$ — транзитивне і асиметричне відношення, то відношення $\preccurlyeq$, задане правилом: $a \preccurlyeq b$ тоді й лише тоді, коли $a \prec b$ або $a = b$, є відношенням (нестрогого) порядку.

Наведемо кілька прикладів відношення порядку (та квазіпорядку).

- Звичайне відношення $\leq$ на множині дійсних чисел є лінійним порядком. Відповідний строгий порядок — це відношення $<$.
- Відношення *подільності* $a|b$ цілих чисел є (частковим) квазіпорядком (не порядком, бо, наприклад, $2|(-2)$ і $(-2)|2$). Якщо обмежитись натуральними числами, то подільнсть є відношенням (часткового) порядку.
- Відношення $\subseteq$ є відношенням порядку (знов-таки, часткового) на множині підмножин деякої множини M. Відповідний строгий порядок — це відношення $\subset$.

Знов-таки, обмеження квазіпорядку (порядку) на довільну підмножину є знов квазіпорядком (порядком). Якщо квазіпорядок є лінійним, таким є й його обмеження.

Кожне відношення еквівалентності є, зокрема, відношенням квазіпорядку. Виявляється, що відношення квазіпорядку, в деякому розумінні, є комбінацією відношень еквівалентності та порядку.

Теорема 2.3.8. *Нехай $\preccurlyeq$ — квазіпорядок на множині M. Визначимо відношення $\sim$ правилом: $a \sim b$ тоді й лише тоді, коли $a \preccurlyeq b$ та $b \preccurlyeq a$.*

1. *Відношення $\sim$ є еквівалентністю на M.* (Воно зветься *еквівалентністю, породженою квазіпорядком $\preccurlyeq$.*)
2. *Якщо $a \sim a'$ і $b \sim b'$, то $a \preccurlyeq b$ тоді й лише тоді, коли $a' \preccurlyeq b'$.*

   Зокрема, на множині $\widetilde{M}$ класів еквівалентності за відношенням $\sim$ можна визначити відношення $\preccurlyeq^*$ правилом: $A \preccurlyeq^* B$ тоді й лише тоді, коли $a \preccurlyeq b$ для деяких (тоді й для будь-яких) елементів $a \in A$, $b \in B$.
3. *Відношення $\preccurlyeq^*$ на множині $\widetilde{M}$ є порядком.*
4. *Порядок $\preccurlyeq^*$ є лінійним тоді й лише тоді, коли таким є квазіпорядок $\preccurlyeq$.*

Доведення цієї теореми полягає у безпосередній перевірці потрібних властивостей. Ми залишаємо його читачеві як нескладну вправу.

Розділ 3

Теорія графів

1. Основні поняття теорії графів

Поняття графа та пов'язані з ним широко застосовуються в сучасній теоретичній і прикладній математиці. Розрізняють *орієнтовані* та *неорієнтовані* графи. Щоб розрізняти їх, ми будемо орієнтовані графи називати *орграфами*, а неорієнтовані — просто *графами* (це стає останнім часом досить розпрвсюдженим слововживанням). Існує кілька варіантів означень графів та орграфів. Ми обрали найбільш загальні; всі інші будуть одержані з них спеціалізаціями.

Означення 3.1.1. 1. *Орієнтований граф*, або *орграф* Γ складається з двох множин: множини *вершин* $\mathrm{Ver}\,\Gamma$ та множини *стрілок* $\mathrm{Arr}\,\Gamma$, і двох відображень $\varepsilon_0 : \mathrm{Arr}\,\Gamma \to \mathrm{Ver}\,\Gamma$ та $\varepsilon_1 : \mathrm{Arr}\,\Gamma \to \mathrm{Ver}\,\Gamma$.

2. Вершини $\varepsilon_0\alpha$ і $\varepsilon_1\alpha$ звуться, відповідно, *початком* та *кінцем* стрілки α. Кажуть, що α — стрілка з вершини $\varepsilon_0\alpha$ до вершини $\varepsilon_1\alpha$. Кажуть також, що ці вершини *інцидентні стрілці* α і навпаки.
3. Якщо $\varepsilon_0\alpha = \varepsilon_1\alpha$, стрілка α зветься *петлею* (при вершині $a = \varepsilon_0\alpha$). Якщо $\varepsilon_0\alpha = \varepsilon_0\beta$ і $\varepsilon_1\alpha = \varepsilon_1\beta$, кажуть, що α та β — *кратні стрілки.*
4. Орграф, в якому немає петель та кратних стрілок, будемо звати *простим орграфом.* (Цей термін не є загальновживаним.)

Ось приклад орграфа:

(1.1)
$$\begin{tikzcd}
 & a \arrow[r, "\alpha"] \arrow[dl, bend left, "\sigma"] \arrow[ddr, "\gamma"] & b \arrow[loop right, "\beta"] \\
c \arrow[ur, bend left, "\tau"] & & \\
 & d \arrow[uu, "\theta"] & e \arrow[l, "\delta"] \arrow[uu, bend left, "\xi"] \arrow[uu, bend right, "\eta"]
\end{tikzcd}$$

Цей орграф не простий: він має петлю β та кратні стрілки ξ, η. Якщо вилучити петлю й одну з кратних стрілок, скажімо, η, одержимо простий орграф

(1.2)
$$\begin{tikzcd}
 & a \arrow[r, "\alpha"] \arrow[dl, bend left, "\sigma"] \arrow[ddr, "\gamma"] & b \\
c \arrow[ur, bend left, "\tau"] & & \\
 & d \arrow[uu, "\theta"] & e \arrow[l, "\delta"] \arrow[uu, "\xi"]
\end{tikzcd}$$

Стрілки σ, τ в ньому не кратні: хоча вони сполучають ті самі точки, але йдуть у зворотньому напрямку.

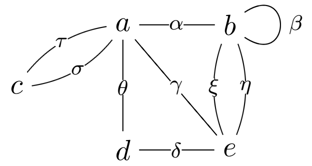
Зауважимо, що пару відображень $\varepsilon_0, \varepsilon_1$ можна замінити одним відображенням $\mathrm{Arr}\,\Gamma \to (\mathrm{Ver}\,\Gamma)^2$, яке ставить у відповідність стрілці α пару вершин $(\varepsilon_0\alpha, \varepsilon_1\alpha)$. Якщо замість пар вершин розглядати невпорядковані пари, одержимо поняття *неорієнтованого графа.*

Точніше, *невпорядкованою парою* елементів множини M зветься її підмножина $\{\, a, b \,\}$, яка містить один або два елементи (один елемент виходить, якщо $a = b$, оскільки $\{\, a, a \,\} = \{\, a \,\}$). Множину неорієнтованих пар елементів з M позначимо $\Pi(M)$.

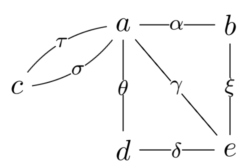
Означення 3.1.2.

1. *Неорієнтований граф* (або просто *граф*) Γ складається з двох множин: множини *вершин* $\operatorname{Ver}\Gamma$ та множини *ребер* $\operatorname{Ed}\Gamma$, і відображення $e : \operatorname{Ed}\Gamma \to \Pi(\operatorname{Ver}\Gamma)$, де $\Pi(\operatorname{Ver}\Gamma)$ — множина неорієнтованих пар вершин.
2. Вершини з пари $\varepsilon\alpha$ звуться *кінцями* ребра α. Якщо $\varepsilon\alpha = \{\, a, b \,\}$, кажуть, що α — ребро між a та b. Кажуть також, що ці вершини *інцидентні* ребру α і навпаки.
3. Якщо ребро α має один кінець a, тобто $\varepsilon\alpha = \{\, a \,\}$, кажуть, що α — петля (при вершині a). Якщо ребра α і β мають однакові кінці, тобто $\varepsilon\alpha = \varepsilon\beta$, кажуть, що α, β — кратні ребра.
4. Граф без петель і кратних ребер зветься *простим.*
5. *Повним графом* на множині M зветься неорієнтований граф зі множиною вершин M і множиною ребер $\{\, \{\, a, b \,\} \mid a, b \in M,\ a \neq b \,\}$. Ми вважаємо. що $\varepsilon\alpha = \alpha$ для кожної пари $\alpha = \{\, a, b \,\}$. Іншими словами, це — простий граф, в якому між кожними (різними) вершинами є ребро.

Звичайно, з кожного орієнтованого графа Γ можна зробити неорієнтований граф $\breve{\Gamma}$, «забуваючи орієнтацію», тобто поклавши $\operatorname{Ver}\breve{\Gamma} = \operatorname{Ver}\Gamma$, $\operatorname{Ed}\breve{\Gamma} = \operatorname{Arr}\Gamma$ і $\varepsilon\alpha = \{\, \varepsilon_0\alpha, \varepsilon_1\alpha \,\}$. Кажуть, що $\breve{\Gamma}$ — *підлеглий граф орграфа* Γ, а Γ є *орієнтацією* графа $\breve{\Gamma}$. (Зауважимо, що орієнтація визначена неоднозначно — той самий граф може мати різні орієнтації.) Ось підлеглі графи орграфів (1.1) та (1.2):



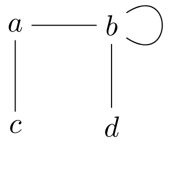
та



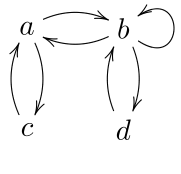
Зверніть увагу, що підлеглий граф простого орграфа (1.2) не є простим: стрілки σ, τ, які не були кратними, стали кратними ребрами.

Інколи зручно за неорієнтованим графом Γ побудувати інший орієнтований граф $\widehat{\Gamma}$, який зветься *біорієнтацією* графа Γ. Він має ті самі вершини, але кожному ребру α графа Γ з $\varepsilon\alpha = \{\, a, b \,\}$, яке не є петлею, відповідають дві стрілки α^+, α^- графа $\widehat{\Gamma}$, одна з яких — з вершини a до вершини b, а друга навпаки. Якщо α петля, їй відповідає одна стрілка — петля в тій самій точці. Ось приклад графа та його біорієнтації:

$\Gamma =$



$\widehat{\Gamma} =$



Якщо на множині M задано двомісне відношення R, за ним можна побудувати орграф $\Gamma = \Gamma(R)$, який зветься *графом відношення* R. Вершини цього графа — це елементи множини M, а стрілки знаходяться у взаємно однозначній відповідності з парами $(a, b) \in R$: кожній такій парі відповідає стрілка з початком a та кінцем b. Очевидно, цей граф не має кратних ребер, але може мати петлі.

Аналогічно, за кожним *симетричним* відношенням $S \subseteq M^2$ можна побудувати неорієнтований граф. Його вершини, знов-таки, збігаються з елементами M, причому кратних ребер немає, а ребро між вершинами a та b існує тоді й лише тоді, коли $(a, b) \in S$ (або, що те саме, $(b, a) \in S$).

Якщо відношення R *рефлексивне*, його здебільшого зображають простим орграфом, вилучивши з графа $\Gamma(R)$ всі петлі. Те саме стосується симетричних рефлексивних відношень: їх зображають простими (неорієнтованими) графами.

Скінченні графи інколи зручно задавати матрицями. Існує два варіанти такого задавання.

Означення 3.1.3. Нехай Γ — деякий орграф; $\operatorname{Ver}\Gamma = \{ v_1, v_2, \dots, v_m \}$, $\operatorname{Arr}\Gamma = \{ \alpha_1, \alpha_2, \dots, \alpha_n \}$.

1. *Матрицею суміжності* орграфа Γ зветься $m\times m$ матриця $A(\Gamma) = (a_{ij})$, де a_{ij} — кількість стрілок з початком v_j і кінцем v_i.
2. *Матрицею суміжності* $M(\Gamma)$ неорієнтованого графа Γ зветься матриця суміжності $M(\widehat{\Gamma})$ його біорієнтації.
3. *Матрицею інцидентності* орграфа Γ, який не має петель, зветься $m \times n$ матриця $I(\Gamma) = (e_{ij})$, де
$$e_{ij} = \begin{cases} 1, & \text{якщо } \varepsilon_0\alpha_j = v_i, \\ -1, & \text{якщо } \varepsilon_1\alpha_j = v_i, \\ 0 & \text{інакше.} \end{cases}$$
4. *Матрицею інцидентності* неорієнтованого графа Γ (можливо, з петлями) зветься $m \times n$ матриця $I(\Gamma) = (d_{ij})$, де
$$d_{ij} = \begin{cases} 1, & \text{якщо } v_i \in \varepsilon\alpha_j, \\ 0 & \text{інакше.} \end{cases}$$

Очевидно, і матриця суміжності, і матриця інцидентності повністю визначають граф, з точністю до назв його вершин та ребер.

Як завжди, важливими поняттями теорії графів є поняття *ізоморфізму* та *гомоморфізму*.

Означення 3.1.4. 1. *Гомоморфізмом* $\phi : \Gamma \to \Delta$ орграфа Γ в орграф Δ зветься пара відображень $\phi = (\phi_0, \phi_1)$, де $\phi_0 : \operatorname{Ver}\Gamma \to \operatorname{Ver}\Delta$, $\phi_1 : \operatorname{Arr}\Gamma \to \operatorname{Arr}\Delta$, причому $\varepsilon_0\phi_1(\alpha) = \phi_0(\varepsilon_0\alpha)$ і $\varepsilon_1\phi_1(\alpha) = \phi_0(\varepsilon_1\alpha)$ для кожної стрілки $\alpha \in \operatorname{Arr}\Gamma$. (Кажучи словами, ці відображення зберігають початки й кінці всіх стрілок.)
2. Якщо Γ і Δ — неорієнтовані графи, *гомоморфізмом* $\phi : \Gamma \to \Delta$ зветься така пара відображень $\phi = (\phi_0, \phi_1)$, $\phi_0 : \operatorname{Ver}\Gamma \to \operatorname{Ver}\Delta$, $\phi_1 : \operatorname{Ed}\Gamma \to \operatorname{Ed}\Delta$, що коли $\varepsilon\alpha = \{ a, b \}$, то $\varepsilon\phi_1(\alpha) = \{ \phi_0(a), \phi_0(b) \}$.

3. Якщо в гомоморфізмі $\phi = (\phi_0, \phi_1)$ обидва відображення ϕ_0, ϕ_1 взаємно однозначні, кажуть, що ϕ — *ізоморфізм* графа Γ на граф Δ. Якщо такий ізоморфізм існує, кажуть, що графи Γ і Δ *ізоморфні*, і пишуть $\Gamma \simeq \Delta$.

Як і в інших розділах математики, в теорії графів дуже часто не розрізняють ізоморфні графи, оскільки вони мають абсолютно однакові властивості (як графи).

Надалі, розглядаючи гомоморфізм графів ϕ, ми часто опускатимемо індекси при ϕ_0 та ϕ_1, тобто писатимемо $\phi(a)$ і для вершин, і для ребер графа Γ.

Наступне твердження цілком очевидне, і його доведення ми залишаємо читачеві.

Твердження 3.1.5. *Наступні властивості рівносильні:*

1. *Графи Γ і Δ ізоморфні.*
2. *Матрицю інцидентності $I(\Delta)$ можна одержати з матриці інцидентності $I(\Gamma)$ деякими перестановками рядків і стовпчиків.*
3. *Матрицю суміжності $A(\Delta)$ можна одержати з матриці суміжності $A(\Gamma)$* одночасною *перестановкою рядків і стовпчиків.* (*Одночасною* означає, що, коли ми переставляємо i-й рядок на j-е місце, ми мусимо також переставити i-й стовпчик на j-е місце.)

З кожного орграфа Γ можна утворити *обернений орграф* Γ°. Він має ті самі множини вершин та стрілок, але ці стрілки змінюють орієнтацію (або відображення ε_0 та ε_1 «міняються місцями»): вершина, яка була початком стрілки, стає її кінцем і навпаки. На мові матриць це означає, що $A(\Gamma^\circ) = A(\Gamma)^\top$ (транспонована матриця), а $I(\Gamma^\circ) = -I(\Gamma)$. Якщо Γ — граф відношення R, то Γ° — граф оберненого відношення R^{-1}.

Означення 3.1.6.

1. *Підграфом* орграфа Γ зветься такий орграф Γ', що $\operatorname{Ver}\Gamma' \subseteq \operatorname{Ver}\Gamma$, $\operatorname{Arr}\Gamma' \subseteq \operatorname{Arr}\Gamma$, причому початки й кінці всіх стрілок у графі Γ' — ті самі, що й у графі Γ. (Зокрема, якщо $\alpha \in \operatorname{Arr}\Gamma'$, то й $\varepsilon_i\alpha \in \operatorname{Ver}\Gamma'$ $(i = 0, 1)$.)
2. Якщо Γ — неорієнтований граф, його *підграфом* зветься такий (неорієнтований) граф Γ', що $\operatorname{Ver}\Gamma' \subseteq \operatorname{Ver}\Gamma$, $\operatorname{Ed}\Gamma' \subseteq \operatorname{Ed}\Gamma$, причому кінці всіх ребер у графі Γ' — ті самі, що й у графі Γ. (Зокрема, якщо $\alpha \in \operatorname{Ed}\Gamma'$, то $\varepsilon\alpha \subseteq \operatorname{Ver}\Gamma'$.)
3. Підграф Γ' зветься *повним*, якщо кожна стрілка (ребро) α така, що $\varepsilon\alpha \subseteq \operatorname{Ver}\Gamma'$, належить $\operatorname{Arr}\Gamma'$ (відповідно, $\operatorname{Ed}\Gamma'$). У цьому випадку ми будемо писати $\Gamma' \subseteq \Gamma$.
4. *Доповненням* підграфа $\Gamma' \subseteq \Gamma$ зветься найменший підграф $\complement\Gamma'$ з усіх таких підграфів $\Gamma'' \subseteq \Gamma$, що $\operatorname{Arr}\Gamma'' = \complement \operatorname{Arr}\Gamma$ і $\operatorname{Ver}\Gamma'' \cup \operatorname{Ver}\Gamma' = \operatorname{Ver}\Gamma$.

   Іншими словами, стрілки (ребра) графа $\complement\Gamma'$ — це ті стрілки (ребра) графа Γ, які не належать до підграфа Γ', а вершина $a \in \operatorname{Ver}\Gamma$ належить $\complement\Gamma'$ у двох випадках: якщо вона не належить Γ' або якщо вона інцидентна стрілці (ребру), яке не належить Γ'.

Ось приклади повного й неповного підграфів графа (1.1) (з однаковою множиною вершин):

$$\begin{tikzcd} a \arrow[r, "\alpha"] \arrow[dr, "\gamma"'] & b \arrow[loop right, "\beta"] \\ & e \arrow[u, "\xi"] \arrow[u, bend right, "\eta"'] \end{tikzcd} \qquad \begin{tikzcd} a \arrow[r, "\alpha"] & b \arrow[loop right, "\beta"] \\ e \arrow[ur, "\xi"] & \end{tikzcd}$$

А ось, відповідно, їхні доповнення:

$$\begin{tikzcd} & a \arrow[dl, bend left, "\tau"] & \\ c \arrow[ur, bend left, "\sigma"] & & \\ & d \arrow[uu, "\theta"] & e \arrow[l, "\delta"'] \end{tikzcd} \qquad \begin{tikzcd} & a \arrow[dl, bend left, "\tau"] \arrow[ddr, "\gamma"] & b \\ c \arrow[ur, bend left, "\sigma"] & & \\ & d \arrow[uu, "\theta"] & e \arrow[l, "\delta"'] \arrow[uu, "\eta"'] \end{tikzcd}$$

Зверніть увагу, що ці доповнення мають різні множини вершин.

Якщо Γ' і Γ'' — підграфи Γ, визначені їх *об'єднання* $\Gamma' \cup \Gamma''$ та *перетин* $\Gamma' \cap \Gamma''$: треба взяти, відповідно, об'єднання чи перетин підмножин вершин та підмножин стрілок (або ребер).

Якщо Γ' та Γ'' — такі підграфи графа Γ, що $\Gamma' \cup \Gamma'' = \Gamma$, а $\Gamma' \cap \Gamma'' = \emptyset$, кажуть, що граф Γ є *прямим* (або *незв'язним*) *об'єднанням* своїх підграфів Γ' та Γ''. (Під *порожнім* графом $\emptyset$ ми розуміємо такий, у якого множина вершин порожня. Звичайно, тоді й множина стрілок або ребер теж має бути порожньою.)

Нарешті, для орієнтованих графів визначена операція *прямого* (або *декартова*) добутку.

Означення 3.1.7. *Прямим добутком* орієнтованих графів Γ і Δ зветься граф $\Gamma \times \Delta$ зі множиною вершин $\operatorname{Ver}\Gamma \times \operatorname{Ver}\Delta$ і множиною стрілок $\operatorname{Arr}\Gamma \times \operatorname{Arr}\Delta$, в якому $\varepsilon_i(\alpha, \beta) = (\varepsilon_i\alpha, \varepsilon_i\beta)$ $(i = 0, 1)$.

Наприклад, прямим добутком графів $1 \to 2 \to 3$ та $1 \rightleftarrows 2$ є граф

$$\begin{tikzcd} (1,1) \arrow[dr] & (2,1) \arrow[dr] & (3,1) \\ (1,2) \arrow[ur] & (2,2) \arrow[ur] & (3,2)\,. \end{tikzcd}$$

Зауважимо, що коли Γ — граф відношення R, а Δ — граф відношення S, то граф $\Gamma \times \Delta$ є графом відношення $R \times S$.

Ми не будемо визначати й розглядати прямі добутки неорієнтованих графів. Пропонуємо читачеві визначити це поняття в такий спосіб, щоб, коли Γ є графом симетричного відношення R, а Δ — графом симетричного відношенні S, їхній прямий добуток був графом симетричного відношення $R \times S$.

2. Шляхи і компоненти.Числові характеристики графів

Означення 3.2.1.

A. Нехай $\mathbf{G}$ — орієнтований граф.

1. *Шляхом* у графі $\mathbf{G}$ зветься така послідовність p стрілок $\alpha_1, \alpha_2, \dots, \alpha_l$, що $\varepsilon_1\alpha_i = \varepsilon_0\alpha_{i+1}$ для кожного $i = 1, 2, \dots, l-1$. Число $l = \mathrm{L}(p)$ зветься *довжиною* цього шляху, а вершини $\varepsilon_0\alpha_i$ $(1 \le i \le)$ та $\varepsilon_1\alpha_l$ — його *вершинами*. Такий шлях часто

записують як «добуток» стрілок: $p = \alpha_l \dots \alpha_2\alpha_1$, і кажуть, що це — шлях з вершини $a = \varepsilon_0\alpha_1$ (яку звуть *початком* цього шляху) до вершини $b = \varepsilon_1\alpha_l$ (яку звуть *кінцем* цього шляху). Пишуть також $p : a \to b$.

2. Шлях $\alpha_l \dots \alpha_2\alpha_1$ зветься *циклом*, якщо його початок і кінець збігаються.
3. Якщо $p = \alpha_l \dots \alpha_2\alpha_1$ — шлях з вершини a до вершини b, а $q = \beta_k \dots \beta_2\beta_1$ — шлях з вершини b до вершини c, їхньою *композицією* (або *добутком*) зветься шлях $qp = \beta_k \dots \beta_2\beta_1\alpha_l \dots \alpha_2\alpha_1$ (з вершини a до вершини c).
4. Якщо $a = b$ або існує шлях з a до b, ми писатимемо $a \rightsquigarrow b$ і казатимемо, що вершина b *слідує за* вершиною a у графі Γ.

Б. Нехай $\mathbf{G}$ — неорієнтований граф.

1. *Шляхом* у графі $\mathbf{G}$ зветься така послідовність p ребер $\alpha_1, \alpha_2, \dots, \alpha_l$ та вершин $a_0, a_1, \dots, a_l$, що $a_i \in \varepsilon\alpha_i \cup \varepsilon\alpha_{i+1}$ для кожного $i = 1, 2, \dots, l-1$. Число $l = \mathrm{L}(p)$ зветься *довжиною* цього шляху, а вершини $a_0, a_1, \dots, a_l$ — його *вершинами*. Такий шлях часто записують як $p = a_l\alpha_l a_{l-1} \dots a_2\alpha_2 a_1\alpha_1 a_0$, і кажуть, що це — шлях з вершини $a = a_0$, яку звуть *початком* шляху p, до вершини $b = a_l$, яку звуть *кінцем* цього шляху. Пишуть також $p : a_0 \to a_l$.
2. Шлях зветься *циклом*, якщо обидва його кінці збігаються.
3. Шлях $p^\circ = a_0\alpha_1 a_1\alpha_2 a_2 \dots a_{l-1}\alpha_l a_l$ зветься *оберненим* (або *протилежним*) до шляху $p = a_l\alpha_l a_{l-1} \dots a_2\alpha_2 a_1\alpha_1 a_0$. (Якщо $p : a \to b$, то $p^\circ : b \to a$. Досить часто ці шляхи ототожнюються, але це не завжди зручно і ми цього не робитимемо.)
4. Якщо $p = a_l\alpha_l a_{l-1} \dots a_2\alpha_2 a_1\alpha_1 a_0$ — шлях з вершини $a = a_0$ до вершини $b = a_l$, а $q = b_k\beta_k b_{k-1} \dots b_2\beta_2 b_1\beta_1 b_0$ — шлях з $b = b_0$ до $c = b_k$, їхньою *композицією* (або *добутком*) зветься шлях $qp = c\beta_k b_{k-1} \dots b_1\beta_1 b\, \alpha_l a_{l-1} \dots a_1\alpha_1 a$ з вершини a до вершини c.
5. Якщо $a = b$ або існує шлях з a до b, ми писатимемо $a \leftrightsquigarrow b$ і казатимемо, що ці вершини *сполучені* у графі Γ.
6. *Дорогою* (або *маршрутом*) в орієнтованому графі зветься шлях у підлеглому неорієнтованому графі. Вершини орієнтованого графа звуться *сполученими*, якщо вони сполучені в підлеглому неорієнтованому графі.

В. Граф зветься *зв'язним*, якщо кожні дві його вершини сполучені; інакше він зветься *незв'язним*.

Маючи на увазі пункти А.4 та Б.5, зручно розглядати «порожні» шляхи. Саме, для кожної вершини a ми введемо *порожній шлях* $\emptyset_a : a \to a$ довжини 0, в якому немає жодної стрілки (ребра). Ми вважаємо також, що $\emptyset_a p = p$ і $q\emptyset_a = q$ для кожного шляху p з кінцем a та кожного шляху q з початком a. Після цього умову «$a = b$» у пунктах А.4 та Б.5 можна випустити. (Очевидно, порожній шлях завжди є циклом, але звичайно ці «тривіальні» цикли не враховуються.)

Наступне твердження цілком очевидне і його доведення ми залишаємо читачеві.

Означення і твердження 3.2.2. 1. Відношення $\leftrightsquigarrow$ є відношенням еквівалентності на множині вершин графа.

2. Повний підграф $\Gamma' \subseteq \Gamma$ зветься *зв'язною компонентою*, або просто *компонентою* графа Γ, якщо його множина вершин є класом еквівалентності відносно відношення $\leftrightsquigarrow$.
3. Кожен граф є прямим (незв'язним) об'єднанням своїх зв'язних компонент.
4. Кожна зв'язна компонента є максимальним (відносно включення) зв'язним підграфом графа Γ.
5. Відношення $\rightsquigarrow$ в орієнтованому графі є відношенням квазіпорядку.
6. Відношення $\rightsquigarrow$ є відношенням порядку тоді й лише тоді, коли в орграфі Γ немає циклів (крім порожніх).
7. Повний підграф Γ' орграфа Γ зветься його *циклічною компонентою*, якщо його множина вершин є класом еквівалентності відносно відношення еквівалентності породженого квазіпорядком $\rightsquigarrow$ (тобто відношення «$a \rightsquigarrow b$ і $b \rightsquigarrow a$»).
8. Орграф зветься *сильно зв'язним*, якщо він складається з однієї циклічної компоненти, тобто з кожної вершини цього графа існує шлях в кожну іншу вершину.

Надалі ми позначатимемо через $\nu_v(\Gamma)$ кількість вершин, через $\nu_e(\Gamma)$ — кількість стрілок (або ребер) у графі Γ, а через $\nu_c(\Gamma)$ кількість його зв'язних компонент.

Теорема 3.2.3. *Нехай Γ — простий неорієнтований граф (тобто, без петель і кратних ребер). Тоді*

$$\nu_e(\Gamma) \geq \frac{1}{2}\big(\nu_v(\Gamma) - \nu_c(\Gamma)\big)\big(\nu_v(\Gamma) - \nu_c(\Gamma) + 1\big).$$

Рівність досягається тоді й лише тоді, коли одна компонента Γ є повним графом, а а всі інші містять по одній вершині.

Доведення. Повний граф з n вершинами має $n(n-1)/2$ ребер. Звідси легко перевірити, що в описаному випадку, дійсно $\nu_e = (\nu_v - \nu_c)(\nu_v - \nu_c + 1)/2$. З іншого боку, якщо $m > 1$, то для довільного $n \geq m$ має місце очевидна нерівність

$$\frac{n(n-1)}{2} + \frac{m(m-1)}{2} < \frac{(n+1)n}{2} + \frac{(m-1)(m-2)}{2}.$$

Зробимо з графом Γ такі перетворення, які не змінюють число вершин і компонент.

1. Замінимо кожну компоненту повним графом з тією ж множиною вершин. (При цьому кількість ребер може лише збільшитись.)
2. Нехай тепер компонента Γ_1 має найбільшу кількість вершин n. Якщо якась компонента Γ_2 має $m > 1$ вершин, замінимо пару компонент Γ_1, Γ_2 повними графами, які мають, відповідно, $n+1$ та $m-1$ вершину.
3. Будемо повторювати пункт 2, доки всі компоненти, крім однієї, на міститимуть по одній вершині.

Кожна процедура вигляду 2 збільшує число ребер. Очевидно, з цього випливає твердження теореми. □

Наслідок 3.2.4. *Якщо в неорієнтованому графі без петель і кратних ребер $\nu_e > (\nu_v - 1)(\nu_v - 2)/2$, то він є звязним.*

Розглянемо довільний зв'язний неорієнтований граф Γ. *Відстанню* між вершинами a, b графа Γ (або довільної його орієнтації) зветься найменша можлива довжина шляху з вершини a до вершини b; вона позначається $d(a, b)$, або $d_\Gamma(a, b)$, якщо треба явно вказати граф Γ. Наступні властивсті очевидні:

- $d(a, a) = 0$;
- якщо $b \neq a$, то $d(a, b) > 0$;
- $d(a, b) = d(b, a)$;
- $d(a, c) \leq d(a, b) + d(b, c)$ («нерівність трикутника».

Іншими словами, функція $d(a, b)$ є *метрикою* на множині вершин графа. *Діаметром* графа Γ зветься $\sup \{\, d(a, b) \mid a, b \in \mathrm{Ver}\,\Gamma \,\}$.

Для кожної вершини $a \in \Gamma$ покладемо $r(a) = \sup \{\, d(a, b) \mid b \in \mathrm{Ver}\,\Gamma \,\}$ і визначимо *радіус* графа Γ як число $r(\Gamma) = \sup \{\, r(a) \mid a \in \mathrm{Ver}\,\Gamma \,\}$. Якщо $r(\Gamma) < \infty$ (наприклад, якщо граф скінченний), кожна вершина a, для якої $r(a) = r(\Gamma)$ зветься *центром* графа Γ. Зауважимо, що граф може мати кілька центрів. Наприклад, граф $a - b - c - d$ має центри b і c (його радіус дорівнює 2). Очевидно $d(\Gamma) \leq 2r(\Gamma)$.

Якщо відстань, радіус та діаметр вимірюють *найкоротші* шляхи, існують їхні аналоги, які вимірюють *найдовші* шляхи. Звичайно, шляхи можна «нарощувати», повторюючи ребра і вставляючи цикли. Тому ми введемо такі поняття.

Означення 3.2.5. 1. Шлях $a_l \alpha_l a_{l-1} \dots a_2 \alpha_2 a_1 \alpha_1 a_0$ зветься *простим шляхом*, якщо всі його вершини $a_0, a_1, \dots, a_l$ різні.

2. Цикл $a_l \alpha_l a_{l-1} \dots a_2 \alpha_2 a_1 \alpha_1 a_0$ зветься *простим циклом*, якщо всі його вершини $a_1, a_2, \dots, a_l$ різні. (Нагадаємо, що в циклі завжди $a_l = a_0$, тобто він ніколи не є простим шляхом).

Очевидно, у зв'язному графі між кожними двома вершинами існує простий шлях. *Розмахом* (або *протяжністю*) між вершинами a і b зветься

$$\mathrm{L}(a, b) = \sup \{\, \mathrm{L}(p) \mid p : a \to b \text{ — простий шлях} \,\}.$$

Розмахом графа Γ зветься $\mathrm{L}(\Gamma) = \sup \{\, \mathrm{L}(a, b) \mid a, b \in \mathrm{Ver}\,\Gamma \,\}$. *Глибиною* вершини a назвемо $e(a) = \sup \{\, \mathrm{L}(a, b) \mid b \in \mathrm{Ver}\,\Gamma \,\}$. Нарешті, *глибиною графа* Γ назвемо $e(\Gamma) = \sup \{\, e(a) \mid a \in \mathrm{Ver}\,\Gamma \,\}$.

Інший важливий інваріант графа пов'язаний зі *степенями вершин.*

Означення 3.2.6. **A**. Нехай Γ — неорієнтований граф.

1. Кажуть, що граф Γ *локально скінченний*, якщо кожна його вершина a інцидентна лише скінченній кількості ребер.
2. *Степінь* вершини a визначається як число $\rho(a) = k + l$, де k — загальна кількість ребер, інцидентних вершині a, а l — кількість петель при цій вершині. (Отже, кожна петля тут рахується двічі — і в k, і в l.)

3. Вершина a зветься парною (непарною), якщо таким є число $\rho(a)$.
4. *Степінь* графа Γ визначається як $\rho(\Gamma) = \sup\{\, \rho(a) \mid a \in \operatorname{Ver}\Gamma \,\}$.
5. Граф Γ зветься *однорідним степеня* ρ, якщо $\rho(a) = \rho$ для кожної його вершини ρ.

Б. Нехай Γ — орієнтований граф.

1. Кажуть, що граф Γ *локально скінченний*, якщо таким є його підлеглий неорієнтований граф.
2. *Додатній* (*від'ємний*) *степінь* вершини a визначається як число $\rho^+(a) = \#\{\, \alpha \in \operatorname{Arr}\Gamma \mid \varepsilon_0\alpha = a \,\}$ (відповідно, $\rho^-(a) = \#\{\, \alpha \in \operatorname{Arr}\Gamma \mid \varepsilon_1\alpha = a \,\}$.
3. *Додатній* та *від'ємний степені* графа Γ визначаються як $\rho^\pm(\Gamma) = \sup\{\, \rho^\pm(a) \mid a \in \operatorname{Ver}\Gamma \,\}$.

Зауважимо, що ці означення узгоджено так, що $\rho(a) = \rho^+(a) + \rho^-(a)$, де $\rho^\pm$ визначаються в орієнтованому, а ρ — у підлеглому неорієнтованому графі.

Твердження 3.2.7. 1. *У скінченному орієнтованому графі* Γ

$$\nu_e(\Gamma) = \sum_{a \in \operatorname{Ver}\Gamma} \rho^+(a) = \sum_{a \in \operatorname{Ver}\Gamma} \rho^-(a).$$

2. *У скінченному неорієнтованому графі* Γ

$$2\nu_e(\Gamma) = \sum_{a \in \operatorname{Ver}\Gamma} \rho(a).$$

Зокрема, якщо граф Γ *— однорідний степеня* ρ, *то* $2\nu_e(\Gamma) = \rho\nu_v(\Gamma)$.

Доведення очевидне. □

Наслідок 3.2.8. *У скінченному неорієнтованому графі кількість непарних вершин завжди парна.*

Відзначимо ще одне співвідношення.

Твердження 3.2.9. *Нехай* Γ *— скінченний зв'язний неорієнтований граф радіусу* r *і степеня* ρ. *Тоді*

$$\nu_v(\Gamma) \leq \frac{\rho^{r+1} - 1}{\rho - 1},$$

причому, якщо $r > 1$, *ця нерівність строга.*

Доведення. Фіксуємо якийсь центр c графа Γ і позначимо $V_m = \{\, a \in \operatorname{Ver}\Gamma \mid d(c,a) = m \,\}$, $n_m = \#(V_m)$. Тоді $\operatorname{Ver}\Gamma = \cup_{m=0}^r V_m$ — розбиття множини вершин, тобто $\nu_v = \sum_{m=0}^r n_m$. З усіх вершин множини V_m виходить щонайбільше ρn_m ребер. Але ясно, що кожна вершина множини V_{m+1} має бути інцидентна принаймні одному з цих ребер. Тому $n_{m+1} \leq \rho n_m$; більш того, якщо $m > 0$, $n_{m+1} < \rho n_m$: адже якісь з цих ребер мусять мати кінці у V_{m-1}. Оскільки $v_0 = 1$, звідси $v_m \leq \rho^m$, причому $v_m < \rho^m$ при $m > 1$. Отже

$$\nu_v \leq 1 + \rho + \rho^2 + \cdots + \rho^r = \frac{\rho^{r+1} - 1}{\rho - 1},$$

причому при $r > 1$ ця нерівність строга. □

3. Ойлерові та гамільтонові графи

У цьому підрозділі ми вважаємо всі графи неорієнтованими і зв'язними.

Означення 3.3.1. 1. Шлях $p = a_l\alpha_l a_{l-1}\dots a_2\alpha_2 a_1\alpha_1 a_0$ зветься *ойлеровим*, якщо всі ребра $\alpha_1, \alpha_2, \dots, \alpha_l$ різні. Якщо, опріч того, p є циклом, він зветься *ойлеровим циклом.*

2. *Ойлеровим числом* $\mathrm{eul}(\Gamma)$ графа Γ зветься найменше можливе число m, для якого існує m таких ойлерових шляхів у цьому графі, що кожне ребро з $\mathrm{Ed}\,\Gamma$ належить точно одному з цих шляхів. Такий набір ойлерових шляхів назвемо *ойлеровим покриттям* графа Γ.
3. Граф Γ зветься *ойлеровим*, якщо в ньому існує ойлерів цикл, який містить всі ребра цього графа. Такий цикл ми будемо звати *повним ойлеровим циклом.*

Такі графи вперше розглянув у 1736 Ойлер у зві'язку з задачею про Кенігсберзькі мости. Йому ж належить наступний красивий критерій.

Теорема 3.3.2 (Критерій Ойлера). *Зв'язний граф є ойлеровим тоді й лише тоді, коли всі його вершини парні.*

Доведення. Необхідність. Нехай $p = a_l\alpha_l a_{l-1}\dots a_2\alpha_2 a_1\alpha_1 a_0$ — повний ойлерів цикл, a — довільна вершина графа Γ і $0 \le j_1 < j_2 < \dots < j_n < l$ — усі такі (різні) номери, що $a_{j_i} = a$. Якщо $l_1 = 0$, позначимо $\alpha_0 = \alpha_l$. Тоді всі ребра $\alpha_{j_i}, \alpha_{j_i+1}$ інцидентні вершині a й інших ребер, які були б інцидентними цій вершині, немає. Якщо якесь з цих ребер є петлею, воно в цьому переліку зустрінеться двічі, так само, як при підрахунку степеня вершини a. Усі інші ребра, які інцидентні a, в цьому переліку зустрічаються по одному разу. Отже, $\rho(a) = 2n$ і вершина a парна.

Достатність. Серед усіх ойлерових шляхів у графі Γ розглянемо шлях $p = a_l\alpha_l a_{l-1}\dots a_2\alpha_2 a_1\alpha_1 a_0$ найбільшої довжини l. Тоді, зокрема, кожне ребро, яке інцидентне вершині a_0 мусить входити до цього шляху: інакше його можна подовжити. Якщо $a_0 \ne a_l$, той самий підрахунок, що й вище, показує, що коли $0 \le j_1 < j_2 < \dots < j_n < l$ — усі такі (різні) номери, що $a_{j_i} = a$, то $\rho(a) = 2n + 1$, що неможливо. Отже, p — це цикл. Але в циклі всі вершини рівноправні. Тому кожне ребро графа Γ, інцидентне якійсь із вершин $a_1, a_2, \dots, a_n$, належить до p. Оскільки граф зв'язний, у ньому не може бути інших вершин. Отже, p — повний ойлерів цикл. □

Наслідок 3.3.3. *Якщо зв'язний граф* Γ *містить непарні вершини і їх кількість дорінює* $2n$ (нагадаємо, що вона завжди парна, див. наслідок 3.2.8), *то* $\mathrm{eul}(\Gamma) = n$.

Доведення. Нехай $p_1, p_2, \dots, p_r$ — ойлерове покриття графа Γ; $p_i : a_i \to b_i$. Позначимо $a_{r+1} = a_1$. Розглянемо граф $\widetilde{\Gamma}$ з тією ж множиною вершин і множиною ребер $\mathrm{Ed}\,\Gamma \sqcup \{\,\theta_1, \theta_2, \dots, \theta_r\,\}$, де $\varepsilon(\theta_i) = \{\,a_{i+1}, b_i\,\}$. У графі $\widetilde{\Gamma}$ є ойлерів цикл: $a_1\theta_r p_r\theta_{r-1}\dots\theta_2 p_2\theta_1 p_1$. Тому всі його вершини парні. Але парність вершини a у графах Γ та $\widetilde{\Gamma}$ та сама, крім, можливо, випадку, коли $a \in \{ a_i, b_i \}$. Отже, кількість непарних вершин у графі Γ не більша за $2r$, тобто $\mathrm{eul}(\Gamma) \geq n$.

Нехай тепер $a_1, a_2, \dots, a_{2n}$ — всі непарні вершини графа Γ. Знов-таки, утворимо новий граф $\widetilde{\Gamma}$ з $\operatorname{Ver}\widetilde{\Gamma} = \operatorname{Ver}\Gamma$ і $\operatorname{Ed}\widetilde{\Gamma} = \operatorname{Ed}\Gamma \sqcup \{ \theta_1, \theta_2, \dots, \theta_n \}$, де $\varepsilon(\theta_i) = \{ a_{2i-1}, a_{2i} \}$. У графі $\widetilde{\Gamma}$ всі вершини вже парні, тому в ньому є повний ойлерів цикл p. Вилучимо з p всі ребра $\theta_1, \theta_2, \dots, \theta_n$. Залишиться, очевидно, ойлерове покриття, і воно складається щонайбільше з n шляхів. Отже, $\mathrm{eul}(\Gamma) \leq n$ і твердження доведене. □

Інша задача пов'язана з так званими гамільтоновими шляхами та циклами.

Означення 3.3.4. Простий цикл (простий шлях) зветься *гамільтоновим циклом* (*гамільтоновим шляхом*), якщо він містить всі вершини графа. Граф зветься *гамільтоновим*, якщо в ньому є гамільтонів цикл.

Зауважимо, що коли $a_l\alpha_l \dots \alpha_2 a_1 \alpha_1 a_l$ — гамільтонів цикл, то $a_l\alpha_l \dots \alpha_2 a_1$ — гамільтонів шлях. Навпаки, якщо $p = a_l\alpha_l \dots \alpha_2 a_1$ — такий гамільтонів шлях, що вершини a_1 та a_l сполучені ребром α_1, то $p = a_l\alpha_l \dots \alpha_2 a_1 \alpha_1 a_l$ — гамільтонів цикл. Якщо $l = 2$, ребра α_1 та α_2 є кратними ребрами; якщо ж $l > 2$, з усіх кратних ребер між якимись двома вершинами до гамільтонова шляху може потрапити щонайбільше одне. Отже, граф, який має принаймні 3 вершини є гамільтоновим тоді й лише тоді, коли таким є простий граф, одержаний з нього вилученням кратних ребер та петель. Тому надалі ми розглядатимемо лише прості графи.

На відміну від ойлерових графів, досі не знайдено критеріїв того, що даний граф є гамільтоновим. Ми наведемо лише деякі достатні умови гамільтоновості. Вони базуються на наступному понятті.

Означення 3.3.5. Нехай p — деякий простий шлях у графі Γ, V — множина вершин цього шляху. Кажуть, що шлях p — *циклічного типу*, якщо в графі Γ існує простий цикл з тією ж множиною вершин (іншими словами, якщо повний підграф графа Γ зі множиною вершин V є гамільтоновим).

Так буде, зокрема, якщо існує ребро, кінці якого — це початок та кінець шляху p.

Теорема 3.3.6. *Нехай Γ — простий зв'язний граф, $\mathrm{L} = \mathrm{L}(\Gamma)$ — його розмах, $p = a_l\alpha_l \dots \alpha_2 a_1 \alpha_1 a_0$ — максимальний простий шлях у цьому графі (тобто такий, що його не можна продовжити до більшого простого шляху, додаючи нові ребра на початку чи на кінці).*

1. *Якщо $\rho(a_0) + \rho(a_l) > l$, шлях p — циклічного типу.*
2. *Якщо $l = \mathrm{L}$ (тобто p — найдовший простий шлях) і p — циклічного типу, то p — гамільтонів шлях, а граф Γ гамільтонів.*
3. *Якщо $\nu_v - 1 \leq \rho(a) + \rho(b)$ для кожної пари вершин $a \neq b$, у графі Γ є гамільтонів шлях.*
4. *Якщо $\nu_v \leq \rho(a) + \rho(b)$ для кожної пари вершин $a \neq b$, граф Γ гамільтонів.*

Доведення. *1.* Позначимо $k = \rho(a_0)$, $m = \rho(a_l)$. Оскільки шлях p — максимальний, кожне ребро, одним кінцем якого є a_0 чи a_l має другим кінцем одну з вершин шляху p. Якщо є ребро a між a_0 та a_l, додавши його до p, одержимо простий цикл з тими ж вершинами. Припустимо, що такого ребра немає. Крім ребра α_1, з вершини a_0 виходить $k-1$ ребер, і у кожного з них другий кінець належить множині $\{ a_i \mid 2 \leq i \leq l-1 \}$. Нехай $M = \{ i \mid 1 \leq i \leq l-2$ і існує ребро між a_0 та $a_{i+1} \}$. З вершини a_l, крім α_l, виходить $m-1$ ребер, кінці яких належать $\{ a_i \mid 1 \leq i \leq l-2 \}$. Оскільки $(k-1)+(m-1) > l-2$ знайдеться ребро β з кінцями a_l та a_i для деякого $i \in M$. Тоді є й ребро γ з кінцями a_0 та a_{i+1}, і існує простий цикл з тією ж множиною вершин $a_0\alpha_1a_1 \dots \alpha_ia_i\beta a_l\alpha_la_{l-1} \dots \alpha_{i+2}a_{i+1}\gamma a_0$.

2. Якщо якась вершина не належить до шляху p, вона сполучена шляхом з вершинами цього шляху (адже граф зв'язний). Тому знайдеться ребро β, один кінець якого a лежить на шляху p, а друга його вершина b на цьому шляху не лежить. Нехай p' — простий цикл з тією ж множиною вершин, що й у шляху p. Очевидно, можна вважати, що p' починається з вершини a. Тоді, дописавши до нього на початку ребро β, ми побудуємо простий шлях довжини $\mathrm{L}+1$, що неможливо.

3. Ясно, що $\mathrm{L} \leq \nu_v - 1$. Розглянемо якийсь найдовший простий шлях p у графі Γ; нехай $p : a \to b$. Якщо $\mathrm{L} = \nu_v - 1$, всі ν_v вершин лежать на цьому шляху, отже, p — гамільтонів шлях. Якщо ж $\mathrm{L} < \nu_v - 1$, маємо $\rho(a) + \rho(b) > \mathrm{L}$, тому, згідно з *1*, шлях p — циклічного типу, а тоді згідно з *2*, граф Γ гамільтонів.

Так само доводиться й *4*. □

Наслідок 3.3.7 (Ознака Дірака). *Нехай Γ — простий зв'язний граф.*

1. *Якщо $\rho(a) \geq \nu_v/2$ для кожної вершини a, граф Γ гамільтонів.*
2. *Якщо $\rho(a) \geq (\nu_v - 1)/2$ для кожної вершини a, у графі Γ є гамільтонів шлях.*

4. Дерева

Означення 3.4.1. Неорієнтований зв'язний граф зветься *деревом*, якщо в ньому немає циклів (зокрема, кратних ребер та петель). Орієнтований граф зветься (орієнтованим)*деревом*, якщо таким є його підлеглий неорієнтований граф.

Очевидно, у (неорієнтованому) дереві Δ для довільних двох вершин a, b існує єдиний простий шлях $p : a \to b$. Фіксуємо одну вершину o дерева Δ, яку зватимемо *коренем* дерева, і позначимо, для кожної вершини $a \in \Delta$, $d(a) = d(o, a)$. Тоді, для кожного ребра α з кінцями a та b, $|d(a) - d(b)| = 1$. Тому дерево з фіксованим коренем ("*кореневе дерево*") має дві природні орієнтації: *відкореневу*, в якій, для кожної стрілки α, $d(\varepsilon_1\alpha) = d(\varepsilon_0\alpha) + 1$ і *докореневу*, в якій $d(\varepsilon_1\alpha) = d(\varepsilon_0\alpha) - 1$.

Кінцевою вершиною зв'язного графа зветься така його вершина a, яка інцидентна єдиному ребру (тобто $\rho(a) = 1$). Кожне скінченне дерево, в якому є хоча б дві вершини, має принаймні дві кінцеві вершини (такими будуть, наприклад, кінці найдовшого простого шляху). Якщо вилучити з дерева кінцеву вершину і єдине інцидентне їй ребро, знов залишиться дерево, в якому буде на одну вершину й на одне ребро менше. Продовжуючи цю процедуру ми врешті решт отримаємо граф, який має одну вершину й жодного ребра. Тому в дереві Δ завжди $\nu_v(\Delta) = \nu_e(\Delta) + 1$.

Означення і теорема 3.4.2. *Нехай* Γ *— скінченний зв'язний граф.* Цикловим числом *графа* Γ *зветься число* $\gamma(\Gamma) = \nu_e(\Gamma) - \nu_v(\Gamma) + 1$.

1. $\gamma(\Gamma) \geq 0$, причому $\gamma(\Gamma) = 0$ тоді й лише тоді, коли Γ — дерево.
2. $\gamma(\Gamma)$ дорівнює максимальній кількості ребер, які можна вилучити з графа Γ (не вилучаючи вершин) так, щоб залишився зв'язний граф.

Доведення. Будемо доводити обидва твердження одночасно індукцією за кількістю ребер. Якщо $\nu_e(\Gamma) = 0$, вони тривіальні. Припустимо, що вони вірні для всіх графів, які містять менше ребер, ніж Γ. Ми вже знаємо, що коли Γ — дерево, то $\gamma(\Gamma) = 0$. Розглянемо довільне ребро α. Якщо його можна вилучити, і при цьому залишиться зв'язний граф Γ', то очевидно, що це ребро належить якомусь циклу (додайте до нього довільний шлях, який сполучає його кінці в графі Γ'). Навпаки, якщо вилучити якесь ребро, яке належить циклу, залишиться зв'язний граф Γ'. За припущенням індукції, $\gamma' = \gamma(\Gamma') \geq 0$, звідки $\gamma = \gamma(\Gamma) = \gamma' + 1 > 0$. Отже, остання нерівність має місце завжди, коли Γ не є деревом. Крім того, з Γ' можна вилучити щонайбільше γ' ребер так, щоб залишився зв'язний граф. Тому з Γ можна вилучити щонайбільше γ ребер зі збереженням зв'язності. □

Розглянемо тепер питання про центри дерев. Найпростіше дерево — це *ланцюг*

$$0 - 1 - 2 - \cdots - n.$$

Діаметр такого ланцюга, очевидно, дорівнює n, а радіус $[(n+1)/2]$. Якщо n парне, він має єдиний центр $n/2$; якщо n непарне, центрів два: $(n \pm 1)/2$. Виявляється, аналогічно ведуть себе ці параметри і в довільному дереві. Зауважимо, що в дереві, очевидно, відстань $d(a,b)$ між вершинами збігається з розмахом $\mathrm{L}(a,b)$ між ними і дорівнює довжині єдиного простого шляху між a та b. Зокрема, діаметр дорівнює найбільшій довжині простого шляху.

Теорема 3.4.3. *Нехай* Δ *— дерево діаметра* d, $p = a_d\alpha_d \dots \alpha_2 a_1 \alpha_1 a_0$ *— один з його найдовших простих шляхів.*

1. *Припустимо, що число* d *парне:* $d = 2r$. *Тоді*
   (а) *Радіус графа* Δ *дорівнює* r.
   (б) *Вершина* a_r *є єдиним центром графа* Δ.
   (в) *Якщо* $q = b_d\beta_d \dots \beta_2 b_1 \beta_1 b_0$ *— інший найдовший простий шлях, то* $b_r = a_r$.
2. *Припустимо, що число* d *парне:* $d = 2r - 1$. *Тоді*
   (а) *Радіус графа* Δ *дорівнює* r.
   (б) *Граф* Δ *має два центри:* a_r *і* a_{r-1}.
   (в) *Якщо* $q = b_d\beta_d \dots \beta_2 b_1 \beta_1 b_0$ *— інший найдовший простий шлях, то* $\beta_r = \alpha_r$.

Доведення. Ми розглянемо випадок 2 ($d = 2r - 1$); випадок 1 ($d = 2r$) цілком аналогічний (навіть трохи простіший) і ми залишаємо його читачеві як вправу.

Перш за все покажемо, що $d(b, a_r) \leq r$ і $d(b, a_{r-1}) \leq r$ для кожної вершини b. Розглянемо простий шлях від a_0 до b і останню вершину a_k

шляху p, яка на ньому лежить. Нехай $l = d(a_k, b)$. Тоді $d(a_0, b) = l+k \le d$ і $d(a_d, b) = l + d - k \le d$. Якщо $k \le r - 1$, звідси $d(b, a_r) = l + r - k \le r$, $d(b, a_{r-1}) = l + r - 1 - k < r$:

$$\begin{array}{l} a_0 - \cdots - a_k - \cdots - a_{r-1} - a_r - \cdots - a_d \\ b \end{array}$$

Якщо ж $k \ge r$, то $d(b, a_{r-1}) = l + k - r + 1 \le d - r + 1 = r$, $d(b, a_r) = l + k - r < r$:

$$\begin{array}{r} a_0 - \cdots - a_{r-1} - a_r - \cdots - a_k - \cdots - a_d \\ b \end{array}$$

Отже, $r(\Gamma) \le r$. Але $d = 2r - 1 \le 2r(\Gamma)$, тому $r(\Gamma) = r$, а a_r і a_{r-1} — центри графа Δ.

Візьмемо тепер за b довільний центр Δ. Тоді $d(a_0, b) = l + k \le r$ і $d(a_d, b) = l + d - k \le r$, звідки $2l \le 2r - d = 1$, тобто $l = 0$, а тоді $d - r \le k \le r$, тобто $k = r$ або $k = r - 1$. Отже, інших центрів, крім a_r та a_{r-1} у графа Δ немає.

Зауважимо, що p — це довільний шлях найбільшої довжини. Отже, якщо q — інший такий шлях, як у пункті (в), його це стосується так само: центрами графа Δ є вершини b_r, b_{r-1} і лише вони. Тому $\varepsilon\alpha_r = \{ a_r, a_{r-1} \} = \{ b_r, b_{r-1} \} = \varepsilon\beta_r$. Оскільки кратних ребер немає, $\alpha_r = \beta_r$. $\square$

Нарешті, розглянемо задачу про *перерахування дерев* із заданою множиною вершин M.

Теорема 3.4.4. *Існує m^{m-2} різних дерев із заданою множиною вершин M, яка містить m елементів.*

Доведення. Ми вважатимемо, що $M = \{ 1, 2, \dots, m \}$. За кожним деревом Δ зі множиною вершин M побудуємо вектор $v(\Delta) \in M^{m-2}$, $v(\Delta) = (a_1, a_2, \dots, a_{m-2})$, за наступними правилами:

- Знайдемо найменший (відносно звичайної нерівності чисел) елемент $b_1 \in M$, який є кінцевою вершиною графа Δ. Розглянемо єдине ребро α_1, інцидентне b_1; позначимо a_1 його другий кінець.
- Розглянемо підграф Δ_1 графа Δ, який одержується вилученням вершини b_1 та ребра α_1.
- У графі Δ_1 знов знайдемо найменшу кінцеву вершину b_2. Розглянемо інцидентне їй ребро α_2 і позначимо a_2 його другий кінець.
- Розглдянемо підграф Δ_2, одержаний з Δ_1 вилученням вершини b_2 і ребра α_2.
- Продовжимо цю процедуру $m - 2$ рази, одержавши вектор $v(\Delta)$.

Зауважимо, що після вилучення b_{m-2} та α_{m-2} залишаться дві вершини b_{m-1}, a_{m-1}, сполучені останнім ребром α_{m-1}. Звідси очевидно, що коли Δ і Γ — різні дерева з тією ж множиною вершин, то $v(\Delta) \ne v(\Gamma)$.

Навпаки, за кожним вектором $\mathbf{a} = (a_1, a_2, \dots, a_{m-2}) \in M^{m-2}$ побудуємо таке дерево Δ, що $v(\Delta) = \mathbf{a}$, за правилами:

- Знайдемо найменший $b_1 \in M$, відмінний від усіх a_i $(1 \le i \le m - 2)$. Введемо до множини ребер ребро α_1 з кінцями a_1 та b_1.

- Знайдемо найменший $b_2 \in M$, відмінний від b_1 і від a_i з $2 \leq i \leq m-2$. Введемо ребро α_2 з кінцями a_2 та b_2.
- Знайдемо найменший $b_3 \in M$, відмінний від b_1, b_2 і від a_i з $3 \leq i \leq m-2$. Введемо ребро α_3 з кінцями b_3 та a_3.
- Повторимо цю процедуру $m-2$ рази. Після цього введемо ребро α_{m-1}, кінці якого — ті два елементи з M, які відрізняються від усіх b_i $(1 \leq i \leq m-2)$.

В результаті одержимо граф Δ без петель і кратних ребер, який має m вершин і $m-1$ ребро. Доведемо, що він зв'язний, індукцією за m. Якщо $m = 2$, це очевидно. Припустимо, що це вірно для множин з $m-1$ елементами. Розглянемо множину $M_1 = M \setminus \{ b_1 \}$ і вектор $\mathbf{a}_1 = (a_2, a_3, \dots, a_{m-2})$. Граф, побудований за цим вектором зі множиною вершин M_1, є зв'язним (за припущенням індукції). Але граф Δ відрізняється від нього лише додатковою вершиною b_1 і ребром α_1 з кінцями b_1, a_1. Оскільки $a_1 \in M_1$, граф Δ також зв'язний. За теоремою 3.4.2, він є деревом. Легко бачити, що $v(\Delta) = \mathbf{a}$.

Отже, дерева зі множиною вершин M знаходяться у взаємно однозначній відповідності з векторами $(a_1, a_2, \dots, a_{m-2}) \in M^{m-2}$. Остання множина має m^{m-2} елементи, що й доводить теорему. □

Доведемо ще одне твердження, яке стосується *нескінченних дерев* і відіграє важливу роль у багатьох питаннях.

Теорема 3.4.5. *Нехай Δ — нескінченне дерево, в якому $\rho(a) < \infty$ для кожної вершини a. Тоді в кожній вершині дерева Δ починається якийсь нескінченний простий шлях.*

Доведення. Фіксуємо вершину a. Від неї до кожної вершини графа веде деякий простий шлях. Перше ребро цього шляху інцидентне a і таких ребер — скінченна кількість. Отже, принаймні одне з них є першим ребром шляхів, які ведуть до нескіченної кількості вершин. Нехай це ребро α_1 і $\varepsilon\alpha_1 = \{ a, a_1 \}$. Тоді з вершини a_1 починається нескінченна кількість простих шляхів до вершин, відмінних від a. Знов-таки, знайдеться ребро α_2, $\varepsilon\alpha_2 = \{ a_1, a_2 \}$ $(a_2 \neq a)$, з якого починається безліч таких шляхів. Те саме стосується вершини a_2 і т.д. Продовжуючи цю процедуру, ми й одержимо нескінченний простий шлях, який пояинається у вершині a. □

5. Дводольні графи

5.1. Парування й дефіцити.

Означення 3.5.1. *Дводольним графом* зветься орієнтований граф Γ разом із таким (фіксованим) розбиттям множини його вершин $\mathrm{Ver}\,\Gamma = V_0 \sqcup V_1$, що $\varepsilon_0\alpha \in V_0$ і $\varepsilon_1\alpha \in V_1 \neq \emptyset$ для кожної його стрілки α.

Ми будемо звати множини V_0 і V_1, відповідно, *верхнім* та *нижнім поверхами* дводольного графа.

Досить часто говорять і про неорієнтовані дводольні графи, тобто такі неорієнтовані графи, які мають дводольну орієнтацію. Очевидно, якщо розбиття вершин на верхній та нижній поверхи фіксовані, ця орієнтація визначається однозначно. Тому нам здається більш природним говорити про дводольні графи як про орієнтовані.

Означення 3.5.2. Нехай Γ — дводольний граф, V_0 і V_1 — його верхній та нижній поверхи.

1. Підмножина стрілок $P \subseteq \operatorname{Arr}\Gamma$ зветься *паруванням*, якщо $\varepsilon_0\alpha \neq \varepsilon_0\beta$ і $\varepsilon_1\alpha \neq \varepsilon_1\beta$ для кожних двох стрілок $\alpha \neq \beta$ з підмножини P.
2. Якщо P — деяке парування, позначимо $E_0(P) = \{\, \varepsilon_0\alpha \mid \alpha \in P \,\}$ і $E_1(P) = \{\, \varepsilon_1\alpha \mid \alpha \in P \,\}$. Кажуть, що P — *парування між* $E_0(P)$ та $E_1(P)$, або що P — *парування для* $E_0(P)$, або для $E_1(P)$.
3. Кожне парування між V_0 та V_1 зветься *повним паруванням* (у дводольному графі Γ).

Зауважимо, що $\#(E_0(P)) = \#(E_1(P))$ для кожного парування P. Зокрема, якщо існує повне парування, обов'язково $\#(V_0) = \#(V_1)$.

Ось приклади задач, які фактично є задачами про існування парувань у дводольних графах.

1. На вечірку запрошені юнаки й дівчата. Деякі з них знайомі між собою, деякі ні. Чи можна їх розбити на пари так, щоб у кожну пару потрапили юнак і дівчина, знайомі між собою? (Ця задача має безліч варіантів.)
2. Задано кілька множин N_i (які можуть перетинатися). Чи можна вибрати з кожної з них по елементу так, щоб усі ці елементи були різними? Такий набір елементів зветься *системою різних представників* для множин N_i (Тут можна за V_0 взяти множину всіх елементів, за V_1 — множину множин N_i, і вважати, що стрілка $a \to N_i$ існує, якщо $a \in N_i$.)

Досить легко дати необхідну умову існування парування для підмножини $A \subseteq V_0$ (або V_1). Надалі ми фіксуємо деякий скінченний дводольний граф Γ з верхнім поверхом V_0 і нижнім поверхом V_1.

Означення 3.5.3. Нехай $A \subseteq V_0$.

1. Позначимо A^+ множину тих елементів $b \in V_1$, для яких існує стрілка з кінцем b і початком в A. Покладемо $\delta(A) = \#(A) - \#(A^+)$.
2. *Дефіцитом* підмножини A зветься число
$$\delta^*(A) = \max\left\{\, \delta(A') \mid A' \subseteq A \,\right\}.$$
Оскільки $\delta(\emptyset) = 0$, завжди $\delta^*(A) \geq 0$.
3. Якщо $\delta^*(A) = 0$, підмножина A зветься *бездефіцитною*.

Аналогічно визначається дефіцит підмножини $B \subseteq V_1$. (Множину елементів $a \in V_0$, для яких існує стрілка з початком a і кінцем у B, позначимо B^-.)

Нам будуть потрібні такі властивості цих понять.

Твердження 3.5.4. 1. *$\delta(A \cup B) + \delta(A \cap B) \geq \delta(A) + \delta(B)$, причому рівність досягається тоді й лише тоді, коли $(A \cap B)^+ = A^+ \cap B^+$.*

2. $\delta^*(A \cup B) + \delta^*(A \cap B) \geq \delta^*(A) + \delta^*(B)$.
3. *Якщо A' — така підмножина в A, що $\delta(A') = \delta^*(A)$, то підмножина $A'' = A \setminus A'$ бездефіцитна.*
4. *Серед підмножин $A' \subseteq A$, для яких $\delta(A') = \delta^*(A)$, є найбільша й найменша.*

Доведення. 1. Легко бачити, що $(A \cup B)^+ = A^+ \cup B^+$, а $(A \cap B)^+ \subseteq A^+ \cap B^+$. Оскільки $\#(A \cup B) + \#(A \cap B) = \#(A) + \#(B)$, звідси $\#((A \cup B)^+) + \#((A \cap B)^+) \leq \#(A) + \#(B)$. Віднявши останню нерівність від попередньої рівності, одержимо твердження 1.

2. Виберемо $A' \subseteq A$ і $B' \subseteq B$ так, що $\delta^*(A) = \delta(A')$ і $\delta^*(B) = \delta(B')$. Тоді

$$\delta^*(A \cup B) + \delta^*(A \cap B) \geq \delta(A' \cup B') + \delta(A' \cap B') \geq \\ \geq \delta(A') + \delta(B') = \delta^*(A) + \delta^*(B).$$

3 випливає з 1, оскільки $\delta(A' \cup A'') \leq \delta(A')$, а $A' \cap A'' = \emptyset$.

4. Якщо $\delta(A') = \delta(A'') = \delta^*(A)$, то, оскільки $\delta(A' \cup A'') \leq \delta^*(A)$ і $\delta(A' \cap A'') \leq \delta^*(A)$, з нерівності 1 випливає, що $\delta(A' \cup A'') = \delta(A' \cap A'') = \delta^*(A)$. Отже, найбільшою з таких підмножин є об'єднання, а найменшою — перетин всіх цих підмножин. $\square$

Очевидно, якщо парування для підмножини A існує, $\#(A^+) \geq \#(A)$. Звідси випливає необхідність у наступній теоремі.

Теорема 3.5.5. *Для того, щоб існувало парування для підмножини $A \subseteq V_0$ (або V_1), необхідно і достатньо, щоб ця підмножина була бездефіцитною.*

Доведення. Требе доводити *достатність*. Це ми зробимо індукцією за кількістю n елементів в A. Якщо $n = 1$, твердження очевидне: оскільки $\delta(A) \leq 0$, існує стрілка α з початком у єдиній вершині з A, і можна покласти $P = \{\,\alpha\,\}$. Припустимо, що для бездефіцитних підмножин, які мають n елементів твердження вірне, і нехай A — бездефіцитна підмножина з $n+1$ вершиною. Можливі два випадки.

1. *$\delta(B) < 0$ для кожної непорожньої підмножини $B \subseteq A$.*

Виберемо якусь вершину $a \in A$ і якусь вершину b, для якої існує стрілка $\alpha : a \to b$. Вилучимо з графа Γ вершини a, b і всі інцидентні їм стрілки. У графі Γ', що залишиться, розглянемо підмножину $A' = A \setminus \{\,a\,\}$. Вона має n елементів. Якщо $B \subseteq A'$ — довільна підмножина, то $\#(B) > \#(B^+)$ (у графі Γ). Але, якщо рахувати B^+ у графі Γ', вона може втратити лише один елемент b. Тому у графі Γ' $\delta(B) \leq 0$. Отже, підмножина A' у графі Γ' знов бездефіцитна. За припущенням індукції, в цьому графі існує парування P' для підмножини A'. Тоді $P = P' \cup \{\,\alpha\,\}$ — парування для підмножини A у графі Γ.

2. *Існують непорожні підмножини $B \subseteq A$, для яких $\delta(B) = 0$.*

Нехай $B \subseteq A$ — така непорожня підмножина з $\delta(B) = 0$, яка містить найменшу кількість елементів. Знову виберемо якусь вершину $a \in A$ і якусь вершину b, для якої існує стрілка $\alpha : a \to b$. Вилучимо з графа Γ вершини a, b і всі інцидентні їм стрілки. У графі Γ', що залишиться, розглянемо підмножину $A' = A \setminus \{\,a\,\}$. Вона має n елементів. Нехай

$B' \subseteq A'$ Якщо в графі Γ було $\delta(B') < 0$, то, як і у випадку 1, у графі Γ' буде $\delta(B') \leq 0$. Припустимо, що $\delta(B') = 0$ у графі Γ. З нерівності 1 твердження 3.5.4 випливає, що також $\delta(B \cap B') = 0$, причому $(B \cap B')^+ = B^+ \cap B'^+$. Оскільки $B \cap B' \subset B$, а B була найменшою за кількістю елементів, то $B \cap B' = \emptyset$, а тоді й $B^+ \cap B'^+ = \emptyset$. Зокрема, жодна стрілка з вершин підмножини B' не закінчується у вершині b, яку ми вилучили, тобто значення $\delta(B')$ однакове в графах Γ і Γ'. Отже, $\delta(B') = 0$ також у графі Γ', і знову A' — бездефіцитна підмножина в цьому графі. Тому, як і у випадку 1, у графі Γ' існує парування P' для підмножини A', а тоді $P = P' \cup \{\, \alpha \,\}$ — парування для A у графі Γ. $\square$

Наслідок 3.5.6. *Нехай $\delta = \delta^*(A)$, $D \subseteq A$ — найменша підмножина, для якої $\delta(D) = \delta$.*

1. *δ дорівнює найменшій кількості вершин, які треба вилучити з підмножини A для того, щоб для підмножини, яка залишиться, існувало парування.*
2. *Якщо $C \subseteq A$ — така підмножина, яка містить δ вершин, що для $A \setminus C$ існує парування, то $C \subseteq D$.*

Доведення. Використаємо індукцію за δ; випадок $\delta = 0$ тривіальний (тут $D = \emptyset$). Припустимо, що для підмножин з меншим дефіцитом твердження вірне. Вилучимо з A якусь вершину a і розглянемо підмножину $A' = A \setminus \{\, a \,\}$. Якщо $a \notin D$, то $D \subseteq A'$, а тому $\delta^*(A') = \delta$. Отже, вилучення вершин з поза D не змінює дефіцит. Припустимо тепер, що $a \in D$ і нехай $B \subseteq A'$. Оскільки $B \cap D \subset D$ (адже $a \notin B$), з нерівності 1 твердження 3.5.4 випливає, що $\delta(B) < \delta$. Отже, в цьому випадку $\delta^*(A') < \delta$. Розглянемо підмножину $D' = D \setminus \{\, a \,\}$. Якщо $D'^+ \subset D^+$, то $\delta(D') \geq \delta(D)$, що неможливо, оскільки підмножина D була найменшою з $\delta(D) = \delta$. Отже, $D'^+ = D^+$, а тоді $\delta(D') = \delta - 1$. Тому $\delta(A') = \delta - 1$ і найменша підмножина в A' з дефіцитом $\delta - 1$ міститься в D'. За припущенням індукції, з A' можна вилучити $\delta - 1$ вершин так, щоб залишилася бездуфіцитна підмножина, причому $\delta - 1$ — найменше число з цією властивістю, а всі ці вершини треба обов'язково брати з D' Разом з a це становить як раз δ вершин, і всі вони належать D. $\square$

Застосуємо ці результати до задачі 2, розглянутої вище. Вони переформулюються у наступному вигляді.

Наслідок 3.5.7 (Теорема Холла). *Нехай $N_1, N_2, \dots, N_n$ — деякий набір (скінченних) множин.*

1. *Для того, щоб можна було вибрати систему різних представників для множин N_i, необхідно й достатньо, щоб для довільного набору номерів $1 \leq j_1 < j_2 < \dots < j_m \leq n$ перетин $\bigcap_{i=1}^m N_{j_i}$ містив принаймні m елементів.*
2. *Для кожного набору номерів $\mathbf{J} = \{\, j_1, j_2, \dots, j_m \,\}$ як вище, покладемо $\delta(\mathbf{J}) = m - \#\bigl(\bigcap_{i=1}^m N_{j_i}\bigr)$, і нехай $\delta = \max\{\, \delta(\mathbf{J}) \,\}$. Тоді найбільша кількість підмножин з N_i, для яких існує система різних представників, дорівнює $n - \delta$.*

Теорему 3.5.5 можна доповнити наступним корисним результатом.

Теорема 3.5.8. *Нехай P і Q — деякі парування, $A = E_0(P)$, $B = E_0(Q)$. Існує таке парування $R \subseteq P \cup Q$, що $A \subseteq E_0(R)$ і $B \subseteq E_1(R)$.*

Зокрема, якщо $\#(A) < \#(B)$ ($\#(A) > \#(B)$), парування R напевне більше, ніж P (відповідно, ніж Q).

Доведення. Позначимо $A' = E_0(Q)$, $B' = E_1(P)$. Очевидно, можна вважати, що $\operatorname{Arr}\Gamma = P \cup Q$, $V_0 = A \cup A'$, $V_1 = B \cup B'$. Тоді кожна вершина v інцидентна щонайбільше двом стрілкам, причому, якщо $v \notin (A \cap A') \cup (B \cap B')$, вона інцидентна лише одній стрілці. Розглянемо максимальний (тобто непродовжуваний) простий *неорієнтований* шлях p у графі Γ: $p = v_0\alpha_1 v_1 \alpha_2 v_2 \dots \alpha_n v_n$. Оскільки цей шлях максимальний, єдиною стрілкою, яка інцидентна його ребрам і не збігається з жодною з $\alpha_1, \alpha_2, \dots, \alpha_n$, може бути лише стрілка α_0 між v_0 та v_n. Зокрема, шлях p, разом із стрілкою α_0, якщо така існує, є зв'язною компонентою графа Γ. Очевидно, у цьому шляху вершини з V_0 та V_1 чергуються: якщо $v_i \in V_0$, то $v_{i+1} \in V_1$ і навпаки. Більш того, стрілки з P і Q теж чергуються: якщо $\alpha_i \in P$, то $\alpha_{i+1} \in Q \setminus P$ і навпаки. Тому, якщо n непарне, множина стрілок з непарними номерами $R(p) = \{\, \alpha_1, \alpha_3, \dots, \alpha_n \,\}$ є паруванням між $\{\, v_0, v_2, \dots, v_{n-1} \,\}$ та $\{\, v_1, v_3, \dots, v_n \,\}$. Нехай тепер n парне. Тоді v_0 та v_n одночасно належать V_0 чи V_1, зокрема, стрілки між v_0 та v_n не існує. Припустимо, що $v_0 \in V_0$ (випадок $v_0 \in V_1$ цілком аналогічний). Якщо $v_0 \notin A$, стрілки з парними номерами $\alpha_2, \alpha_4, \dots, \alpha_n$ утворюють парування $R(p)$ між $\{\, v_1, v_3, \dots, v_{n-1} \,\}$ та $\{\, v_2, v_4, \dots, v_n \,\}$. Якщо $v_0 \in A$, стрілка α_1 обов'язково належить P (адже якась стрілка з P мусить бути інцидентною до v_0). Тоді $\alpha_n \in Q \setminus P$, а тому $v_n \notin A$, бо ця вершина не інцидентна жодній стрілці з P. У цьому випадку множина стрілок з непарними номерами $R(p) = \{\, \alpha_1, \alpha_3, \dots, \alpha_{n-1} \,\}$ є паруванням між $\{\, v_0, v_2, \dots, v_{n-2} \,\}$ та $\{\, v_1, v_3, \dots, v_{n-1} \,\}$. Об'єднавши всі парування $R(p)$, коли p пробігає всі максимальні неорієнтовані шляхи графа Γ, одержимо таке парування $R \subseteq P \cup Q$, що напевне $E_0(P) \supseteq A$ і $E_1(R) \supseteq B$. □

Наслідок 3.5.9. *Позначимо $v_i = \#(V_i)$ і $\delta_i = \delta^*(V_i)$ ($i = 0, 1$).*

1. *Повне парування у графі Γ існує тоді й лише тоді, коли $\delta_0 = \delta_1 = 0$.*
2. $v_0 - \delta_0 = v_1 - \delta_1$.
3. $\#(E_0(P)) = \#(E_1(P)) \le v_0 - \delta_0$ *для кожного парування P у графі Γ.*
4. *Існує таке парування R, що $\#(E_0(R)) = \#(E_1(R)) = v_0 - \delta_0$.*

Доведення. Твердження 3 та необхідність у твердженні 1 — безпосередні наслідки теореми 3.5.5.

За наслідком 3.5.6, існує таке парування P_0, що коли $A = E_0(P)$, то $\#(A) = v_0 - \delta_0$, і таке парування P_1, що коли $B = E_1(P_1)$, то $\#(B) = v_1 - \delta_1$. За теоремою 3.5.7, тоді існує парування R, для якого $E_0(R) \supseteq A$ і $E_1(R) \supseteq B$. Але за тією ж теоремою 3.5.6, $\#(E_0(R)) \le v_0 - \delta_0$ і $\#(E_1(R)) \le v_1 - \delta_1$. Отже, $E_0(R) = A$ і $E_1(R) = B$; зокрема, $\#(A) = \#(B)$, тобто має місце рівність 2, а паросполучення R задовольняє умовам з твердження 4. Звідси ж випливає й достатність у твердженні 1. □

5.2. Прості шляхи в орграфі. Ми застосуємо теореми про парування, щоб одержати деякі результати про покриття орієнтованих графів простими шляхами й циклами. Для цього використаємо наступну констирукцію.

Означення 3.5.10. Нехай Γ — орієнтований граф. *Дублем* графа Γ зветься дводольний граф $\Gamma^\sharp$, який визначається в наступний спосіб:

- $\operatorname{Ver}\Gamma^\sharp = \{\, v_1, v_2, \dots, v_n, v_1', v_2', \dots, v_n' \,\}$, де $\{\, v_1, v_2, \dots, v_n \,\} = \operatorname{Ver}\Gamma$, а $v_1', v_2', \dots, v_n'$ — нові символи, відмінні від усіх $a_1, a_2, \dots, a_n$.
- $\operatorname{Arr}\Gamma^\sharp = \operatorname{Arr}\Gamma$.
- Якщо $\alpha : a \to b$ у графі Γ, то $\alpha : a \to b'$ у графі $\Gamma^\sharp$.
- $V_0 = \{\, a_1, a_2, \dots, a_n \,\}$, $V_1 = \{\, a_1', a_2', \dots, a_n' \,\}$.

Зауважимо, що, оскільки $\#(V_0) = \#(V_1) = n$, також $\delta^*(V_0) = \delta^*(V_1)$. Це число назвемо *дефіцитом графа* Γ і позначимо $\delta^*(\Gamma)$.

Ось приклад графа Γ та його дубля:

$$\Gamma = \begin{tikzcd} 1 \arrow[r] \arrow[d] & 2 \arrow[r] \arrow[d] & 4 \\ 3 \arrow[r] & 5 \end{tikzcd} \qquad \Gamma^\sharp = \begin{tikzcd} 1 \arrow[dr] \arrow[drr] & 2 \arrow[drr] \arrow[drrr] & 3 \arrow[drr] & 4 & 5 \\ 1' & 2' & 3' & 4' & 5' \end{tikzcd}$$

Розглянемо деяке парування $P = \{\, \alpha_1, \alpha_2, \dots, \alpha_m \,\}$ $\alpha_i : a_i \to b_i'$ у графі $\Gamma^\sharp$. У графі Γ стрілки $\alpha_1, \alpha_2, \dots, \alpha_m$ разом з інцидентними ним вершинами утворюють підграф Γ_P, у якому з кожної точки виходить щонайбільше одна стрілка і в кожну точку входить щонайбільше одна стрілка. Якщо $p : a \to b$ — максимальний простий (орієнтований) шлях у підграфі Γ_P, то єдиною стрілкою цього підграфа між вершинами шляху p, яка сама цьому шляху не належить, може бути лише стрілка $\beta_p : b \to a$. Тому шлях p, разом зі стрілкою β_p, якщо вона існує, є компонентою графа Γ_P, і кожна з цих компонент є або простим шляхом (можливо, порожнім), або простим циклом.

Навпаки, нехай Γ' — підграф Γ, кожна компонента якого є простим шляхом або простим циклом. Тоді з кожної вершини у графі Γ' виходить щонайбільше одна стрілка, і в кожну вершини у графі Γ' входить щонайбільше одна стрілка. Тому множина всіх стрілок графа Γ' утворює парування P в графі $\Gamma^\sharp$. Розглянемо якусь вершину a підграфа Γ'. Очевидно, $a \notin E_0(P)$ тоді й лише тоді, коли вона є кінцем якогось із шляхів, який є компонентою Γ'. Так само, $a' \notin E_1(P)$ тоді й лише тоді, коли вершина a є початком такого шляху. Зокрема, кількість компонент Γ', які не є циклами, дорівнює $\#(\operatorname{Ver}\Gamma') - \#(E_0(P)) = \#(\operatorname{Ver}\Gamma') - \#(E_1(P))$.

Зауважимо, що дефіцит підмножин у V_0 чи V_1 має очевидний зміст, якщо розглядати сам граф Γ. Дійсно, якщо $A \subseteq V_0 = \operatorname{Ver}\Gamma$, то

$$A^+ = \left\{\, b' \in V_1 \,\middle|\, \text{у графі } \Gamma \text{ існує стрілка } a \to b,\ \text{де } a \in A \,\right\}.$$

Аналогічно, якщо $B' \subseteq V_1$, $B' = \{\, b' \mid b \in B \,\}$ для деякої підмножини $B \subseteq \operatorname{Ver}\Gamma$, то

$$B'^- = \{\, a \in V_0 \mid \text{у графі } \Gamma \text{ існує стрілка } a \to b,\ \text{де } b \in B \,\}.$$

Для кожної підмножини $A \operatorname{Ver}\Gamma$ позначимо

$$\begin{aligned} A^{\rightarrow} &= \{\, b \in \operatorname{Ver}\Gamma \mid \text{у графі } \Gamma \text{ існує стрілка } a \to b \,\}, \\ A^{\leftarrow} &= \{\, b \in \operatorname{Ver}\Gamma \mid \text{у графі } \Gamma \text{ існує стрілка } b \to a \,\}. \end{aligned}$$

Тоді, $\delta(A) = \#(A) - \#(A^{\rightarrow})$, якщо розглядати A як підмножину V_0, і $\delta(A') = \#(A) - \#(A^{\leftarrow})$, де $A' = \{\, a' \mid a \in A \,\} \subseteq V_1$. Зокрема,

$$\begin{aligned} \delta^*(\Gamma) &= \max\{\, \#(A) - \#(A^{\rightarrow}) \mid A \subseteq \operatorname{Ver}\Gamma \,\} = \\ &= \max\{\, \#(A) - \#(A^{\leftarrow}) \mid A \subseteq \operatorname{Ver}\Gamma \,\}. \end{aligned} \tag{5.1}$$

Ці розгляди ведуть до наступного результату.

Теорема 3.5.11. *Число $\delta^*(\Gamma)$, визначене формулою* (5.1), *є найменшим з таких чисел δ, що всі вершини графа Γ можна включити в набір δ простих шляхів і якогось числа простих циклів, які між собою не перетинаються.* (Можливо, деякі з цих δ простих шляхів порожні.)

Зокрема, всі вершини графа Γ можна включити в набір простих циклів, які між собою не перетинаються, тоді й лише тоді, коли $\delta^*(\Gamma) = 0$.

Доведення. Ми вже бачили, що коли такі шляхи й цикли існують, то в графі $\Gamma^\sharp$ є парування P, для якого $\#(E_0(P)) = m - \delta$, де $m = \#(\operatorname{Ver}\Gamma)$. За наслідком 3.5.6, $\delta \geq \delta^*(V_0) = \delta^*(\Gamma)$. Навпаки, за тим самим наслідком, у графі $\Gamma^\sharp$ існує парування P, для якого $\#(E_0(P)) = m - \delta^*(\Gamma)$. Воно й визначає, як ми бачили вище, покриття вершин графа Γ простими шляхами й циклами, які не перетинаються, причому кінці шляхів — це вершини з $V_0 \setminus E_0(P)$, кількість яких дорівнює $\delta^*(\Gamma)$. □

5.3. Теорема Ділуорта. Дещо несподівано з останньої теореми виводиться один важливий результат про впорядковані множини. З кожним (частковим) порядком $\preccurlyeq$ на деякій множині M пов'язаний простий орієнтований граф $\Gamma_\prec$ зі множиною вершин M, в якому стрілка $a \to b$ існує тоді й лише тоді, коли $a \prec b$. Оскільки відношення $\preccurlyeq$ антисиметричне, в цьому графі немає циклів. Тому, за теоремою 3.5.11, його дефіцит $\delta^*(\Gamma_\prec)$ дорівнює найменшій кількості простих шляхів, які разом містять всі вершини по одному разу. Зауважимо, що простий шлях у графі $\Gamma_\prec$ — це *ланцюг* у впорядкованій множині M, тобто такий набір елементів $a_0, a_1, \dots, a_l$, що $a_0 \prec a_1 \prec \dots \prec a_l$. Виявляється, що дефіцит також має просте означення в термінах порядку.

Означення 3.5.12. *Шириною* впорядкованої множини M з порядком $\preccurlyeq$ зветься найбільше число $\mathrm{w} = \mathrm{w}(\prec)$, для якого в M існує підмножина N, що складається з w *непорівняних* елементів (тобто $a \not\prec b$ для довільних $a, b \in N$).

Лема 3.5.13. $\delta^*(\Gamma_\prec) = \mathrm{w}(\prec)$.

Доведення. Нехай $A \subseteq M$ — якась підмножина. Зауважимо, що

$$A^{\rightarrow} = \{\, b \in M \mid a \prec b \text{ для деякого } a \in A \,\}.$$

Зокрема, $A^{\rightarrow}$ містить усі елементи підмножини A, крім *мінімальних*, тобто таких $a \in A$, що $b \not\prec a$ для кожного $b \in A$. Тому $\delta(A)$ не перебільшує кількості мінімальних елементів цієї підмножини, зокрема $\delta(A) \leq \mathrm{w}(\prec)$ (оскільки мінімальні елементи напевне непорівняні).

Нехай тепер $N \subseteq M$ складається з w непорівняних елементів, $A = \{\, a \in M \mid b \preccurlyeq a$ для деякого $b \in N \,\}$. Тоді $A^{\to} = A \setminus N$, отже, $\delta(A) = \mathrm{w}$ і $\delta^{*}(\Gamma) = \mathrm{w}(\prec)$. $\square$

Наслідок 3.5.14 (Теорема Ділуорта). *Найменша кількість ланцюгів, які містять всі елементи впорядкованої множини, дорівнює її ширині.*

Задачі

Завдання 1.

1. Доведіть, що:

(1) Якщо x — натуральне число, то $\binom{-x}{n} = (-1)^n \binom{x+n-1}{n}$.

(2) Має місце «*формула додавання*»: $\binom{x+y}{n} = \sum_{k=0}^{n} \binom{x}{k}\binom{y}{n-k}$.

2. (1) Доведіть, що функція $S_m(n) = \sum_{k=1}^{n} k^m$ є многочленом від n степеня $m+1$. Чому дорівнює старший коефіцієнт цього многочлена?

(2) Знайдіть многочлени $S_m(n)$ при $n \leq 4$.

3. Визначимо *вищі різниці* $\Delta^n f(x)$ функції $f(x)$ рекурентними формулами:

$$\Delta^0 f(x) = f(x), \quad \Delta^{n+1} f(x) = \Delta\Delta^n f(x).$$

Доведіть, що кожен многочлен $f(x)$ степеня n можна подати у вигляді

$$f(x) = \sum_{m=0}^{n} \Delta^m f(0) \binom{x}{m}.$$

Вказівка: Можна скористатися тим, що $\Delta^m \binom{x}{m} = 1$ для кожного m.

4. *Поліноміальними коефіцієнтами* звуться многочлени

$$\binom{x}{m_1, m_2, \dots, m_k} = \frac{x(x-1)\dots(x-m+1)}{m_1!\, m_2! \dots m_k!},$$

де $m_1, m_2, \dots, m_k$ — деякі натуральні числа, $m = m_1 + m_2 + \dots + m_k$. Доведіть, що:

(1) Якщо $m' = m_1 + m_2 + \dots + m_{k-1}$, то

$$\binom{x}{m_1, m_2, \dots, m_k} = \binom{x}{m_1, m_2, \dots, m_{k-1}} \binom{x-m'}{m_k}.$$

(2) $\Delta \binom{x}{m_1, m_2, \dots, m_k} = \sum_{i=1}^{k} \binom{x}{m_1, \dots, m_i - 1, \dots, m_k}$.

(3) (*Поліноміальна формула*)

$$(x_1 + x_2 + \dots + x_k)^n = \sum_{m_1+m_2+\dots+m_k=n} \binom{n}{m_1, m_2, \dots, m_{k-1}} x_1^{m_1} x_2^{m_2} \dots x_k^{m_k}.$$

(4) Якщо x — натуральне число, то й $\binom{x}{m_1, m_2, \dots, m_k}$ — натуральне число для довільних m_i і k.

Завдання 2.

1 (Кратні сполучення). (1) Нехай M — множина з n елементами, а $K = \{ a_1, a_2, \dots, a_k \}$ — множина з k елементами. Довести, що кількість відображень $f : M \to K$, таких що $\#\bigl(f^{-1}(a_k)\bigr) = m_k$, дорівнює

$$\binom{n}{m_1, m_2, \dots, m_{k-1}} = \frac{n!}{m_1!\, m_2!\, \dots\, m_k!}.$$

Якщо $k = 2$, таке відображення повністю визначається підмножиною $f^{-1}(a_1)$. Тому цей результат узагальнює формулу для числа сполучень.

(2) Довести, що

(а) $$\sum_{m_1+\dots+m_k=n} \binom{n}{m_1, m_2, \dots, m_{k-1}} = k^n.$$

(б) $$\sum_{\substack{m_i>0\\ m_1+\dots+m_k=n}} \binom{n}{m_1, m_2, \dots, m_{k-1}} = \sum_{l=0}^{k-1} (-1)^l \binom{k}{l} (k-l)^n.$$

2 (Розбиття з фіксованою кількістю елементів). Нехай множина M складається з n елементів. Розглядаємо розбиття M на r частин, з яких r_1 має по m_1 елементів, r_2 має по m_2 елементів, ..., r_k має по m_k елементів, де, звичайно, $r = \sum_{i=1}^{k} r_i$, а $\sum_{i=1}^{k} r_i m_i = n$. Довести, що кількість таких розбиттів дорівнює

$$\frac{n!}{(m_1!)^{r_1}(m_2!)^{r_2}\dots(m_k!)^{r_k} r_1!\, r_2!\, \dots\, r_k!}.$$

Зокрема, цей вираз завжди є натуральним числом (що вельми неочевидно)

Завдання 3.

1. Довести, що

$$\sum_{k=1}^{n}(-1)^{k-1}\binom{n}{k}k^m = \begin{cases} 0, & \text{якщо } m < n, \\ n!, & \text{якщо } m = n. \end{cases}$$

2. Означимо *експоненційний ряд* $\exp t$ формулою

$$\exp t = \sum_{n=0}^{\infty}\frac{t^n}{n!}.$$

Довести, що $\exp(t+z) = (\exp t)(\exp z)$, зокрема, $\exp(-t) = (\exp t)^{-1}$.

3. Розглянемо множину *рядів Лорана*, тобто виразів вигляду

$$f(t) = \sum_{n=-m}^{\infty} a_n t^n = a_{-m}t^{-m} + a_{-m+1}t^{-m+1} + \\ + \dots + a_{-1}t^{-1} + a_0 + a_1 t + \dots + a_n t^n + \dots$$

(із *скінченною*, але довільною кількістю членів з від'ємними степенями). Означимо дії над ними так само, як дії над степеневими рядами. Довести, що відносно цих дій множина рядів Лорана є полем (тобто, у кожного ненульового елемента є обернений).

Завдання 4.

1 (Біноміальна формула обертання). (1) Доведіть, що

$$\sum_{k=m}^{n}(-1)^k\binom{n}{k}\binom{k}{m}=\begin{cases}0, & \text{якщо } m<n,\\ (-1)^n, & \text{якщо } m=n.\end{cases}$$

Вказівка: Скористайтеся рівністю $\binom{n}{k}\binom{k}{m}=\binom{n}{m}\binom{n-m}{k-m}$.

(2) Доведіть, що коли для кожного n

$$b_n=\sum_{k=0}^{n}(-1)^k\binom{n}{k}a_k,$$

то також для кожного n

$$a_n=\sum_{k=0}^{n}(-1)^k\binom{n}{k}b_k.$$

2 (Числа Стірлінга). Нагадіємо, що D_n^m позначає кількість сюр'єкцій $N\to M$, де $\#(N)=n$, $\#(M)=m$, S_n^m (числа Стірлінга другого роду) — кількість розбиттів множини з n елементами на m непорожніх частин.

(1) Доведіть рекурентні формули

$$D_{n+1}^m=m(D_n^m+D_n^{m-1}),$$
$$S_{n+1}^m=mS_n^m+S_n^{m-1}.$$

(2) Доведіть, що для кожного натурального n

$$x^n=\sum_{k=0}^{n}D_m^k\binom{x}{k}.$$

(3) Доведіть, що існує єдиний набір чисел s_n^m, такий що для довільних m і n виконується рівність

$$\sum_{k=0}^{n}s_n^kS_k^m=\begin{cases}0, & \text{якщо } m\neq n,\\ 1, & \text{якщо } m=n.\end{cases}$$

Числа s_n^m звуться *числами Стірлінга першого роду.*

(4) Доведіть, що для кожного натурального n

$$\binom{x}{n}=\sum_{k=0}^{n}s_n^k\frac{x^k}{k!}.$$

3 (Задача про розмін). (1) Знайдіть твірну функцію послідовності V_n, де V_n — кількість розв'язків у невід'ємних цілих числах рівняння $a_1x_1+a_2x_2+\cdots+a_kx_k$, де $a_1,a_2,\ldots,a_k$ — фіксовані натуральні числа.

Якщо всі a_i різні, V_n можна розглядати, як кількість способів, якими можна розміняти n гривень, маючи купюри вартістю $a_1,a_2,\ldots,a_k$.

(2) Якою буде твірна функція, якщо в задачі про розмін накласти додаткову умову: $x_i\le m$ для всіх i («обмежена кількість купюр»)?

Завдання 5.

1. Доведіть рекурентне співвідношення для чисел Стірлінга першого роду:

$$s_{n+1}^k = s_n^{k-1} + n s_n^k.$$

2. Доведіть наступні властивості чисел Фібоначчі Φ_n:

(i) $$\Phi_{n+k} = \Phi_n \Phi_{k+1} + \Phi_{n-1}\Phi_k,$$

(ii) $$\Phi_{kn} \text{ ділиться на } \Phi_n,$$

(iii) $$\Phi_{n+1} = \sum_{k=0}^{[n/2]} \binom{k}{n-k}.$$

3. Позначимо через $\tau(n)$ кількість дільників числа n. Доведіть, що функція $\tau(n)$ мультиплікативна і для кожного n

$$\sum_{d|n} \tau(d)\mu(n/d) = 1.$$

4. Позначимо через $\sigma(n)$ суму всіх дільників числа n. Доведіть, що функція $\sigma(n)$ мультиплікативна і для кожного n

$$\sum_{d|n} \sigma(n)\mu(n/d) = n.$$

5 (Ойлерів добуток). Доведіть, що

$$\zeta(s) = \sum_{n=1}^{s} \frac{1}{n^s} = \prod_p \frac{1}{1 - \frac{1}{p^s}},$$

де p пробігає всі первинні числа.

Тут, як і раніше, ми маємо на увазі формальну тотожність у кільці рядів Діріхле. Інакше кажучи, якщо формально виконати дії в правій частині, то одержимо ряд з лівої частини.

Завдання 6.

1. Розглянемо висловлювання:

(1) «Якщо Київ — столиця Португалії, то кожна неперервна функція диференційовна»

(2) «Якщо кожна диференційовна функція неперервна, то жирафи живуть на південному полюсі»

(3) «Якщо на Марсі є життя, то взимку кожного дня ллє дощ або це речення написано українською мовою»

Які їхні логічні значення? Чому?

2. Обчисліть значення наступних виразів у залежності від значень елементарних висловлювань, які до них входять:

(i) $$(B \Rightarrow \neg A) \vee C \Leftrightarrow (A \wedge \neg C),$$

(ii) $$A \wedge (\neg B \vee \neg C) \Rightarrow (B \Rightarrow \neg A),$$

(iii) $$(\neg A \Rightarrow C) \vee ((A \Leftrightarrow B) \oplus \neg C).$$

3. Перевірте наступні тотожності:

(i) $$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C),$$

(ii) $$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C),$$

(iii) $$\neg(A \vee B) = \neg A \wedge \neg B,$$

(iv) $$\neg(A \wedge B) = \neg A \vee \neg B.$$

4. Нехай $\mathcal{X}$ — деякий логічний вираз, до якого входять лише сполучники $\neg, \vee, \wedge$. Доведіть, що вираз $\neg\mathcal{X}$ еквівалентний виразу $\mathcal{X}^*$, який одержується в наступний спосіб:

- кожне елементарне висловлювання A замінюється на $\neg A$; якщо при цьому виникає вираз $\neg\neg A$, він замінюється на A;
- кожен сполучник $\vee$ замінюється на $\wedge$ і навпаки.

5. *Тавтологією* зветься логічний вираз, який приймає значення **1** при всіх значеннях елементарних висловлювань, які до нього входять. Перевірити, що наступні вирази є тавтологіями:

(i) $$(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C)),$$

(ii) $$(A \Rightarrow C) \Rightarrow ((B \Rightarrow C)) \Rightarrow (A \vee B \Rightarrow C)),$$

(iii) $$(A \Rightarrow B) \Rightarrow ((A \Rightarrow C) \Rightarrow (A \Rightarrow B \wedge C)),$$

(iv) $$(A \Rightarrow B) \Rightarrow ((\neg A \Rightarrow B) \Rightarrow B).$$

Завдання 7.

1. Побудуйте ДДНФ, еквівалентні функціям:

(1) $$(x \Rightarrow y) \vee (\neg y \Leftrightarrow \neg z),$$

(2) $$(x \wedge (y \Rightarrow \neg z)) \oplus (\neg z \vee x \Rightarrow \neg y).$$

2. Побудуйте ДКНФ, еквівалентні функціям:

(1) $$(x \oplus y \Rightarrow z \vee \neg x) \Leftrightarrow (\neg y \wedge z \Rightarrow x),$$

(2) $$(\neg x \wedge (y \Rightarrow \neg z)) \vee ((\neg y \Rightarrow x) \vee (\neg x \Leftrightarrow z)).$$

3. Користуючись тотожностями

$$(A \wedge F) \vee (\neg A \wedge F) = F \quad \text{та} \quad (A \vee F) \wedge (\neg A \vee F) = F$$

для довільної F, спростити вирази, одержані в задачах 1 і 2.

4. Побудуйте булеві многочлени, еквівалентні функціям:

(1) $$(x \Rightarrow \neg y) \vee (\neg z \wedge x),$$

(2) $$(\neg z \Leftrightarrow y) \Rightarrow x \wedge (y \vee z).$$

5. Доведіть, що для кожної булевої функції існує еквівалентна їй, яка містить лише сполучники $\Rightarrow$ та $\neg$. Виразіть через них сполучники $\vee$, $\wedge$, $\oplus$, $\Leftrightarrow$.

6. Виразіть:

(1) кон'юнкцію через логчну суму та диз'юнкцію;
(2) диз'юнкцію через логічну суму та кон'юнкцію.

Завдання 8.

1. Складіть таблицю приналежності всіх булевих функцій від 2 змінних до класів $\mathfrak{F}_0, \mathfrak{F}_1, \mathfrak{F}_2, \mathfrak{F}_3, \mathfrak{F}_4$ з теореми Поста.

2. Знайдіть усі пари $\{ f, g \}$ булевих функцій від 2 змінних, які утворюють повний набір, причому не містять ані штрих Шеффера, ані стрілку Пірса. У кожному випадку виразіть через функції цього набору всі двомісні сполучники.

3. Виразіть усі двомісні сполучники через штрих Шеффера та через стрілку Пірса. (В тому числі виразіть штрих Шеффера через стрілку Пірса й навпаки.)

4. (1) Доведіть, що з кожного повного набору булевих функцій $\mathfrak{M}$ можна вибрати 4 (або менше) функції, які вже складають повний набір.

   (2) Побудуйте набір з 4 булевих функцій, який є повним, але якщо з нього вилучити хоча б одну функцію, він перестає бути таким.

   Вказівка: У цій задачі не можна обмежуватись функціями від 2 змінних. Наспрвді, можна довести, що з будь-якого повного набору функцій від 2 змінних можна вибрати 3 (або менше) функцій, які вже складають повний набір.

Завдання 9.

1. Які з наступних відношень є: а) відношеннями еквівалентності? б) відношеннями порядку (часткового чи лінійного)?

(1) А старший за Б.
(2) Натуральне число a ділить натуральне число b.
(3) Вектори $\mathbf{u}$ та $\mathbf{v}$ пропорційні.
(4) Ненульові вектори $\mathbf{u}$ та $\mathbf{v}$ пропорційні.
(5) А — брат або сестра Б.
(6) А та Б мають тих самих батьків.

2. Нехай M — множина з m елементами. Скільки на ній існує:

(1) симетричних відношень?
(2) антисиметричних відношень?
(3) відношень лінійного порядку?
(4) відношень лінійного квазіпорядку?

3. Скільки існує неізоморфних відношень (часткового) порядку на множині з m елементами при $m \leq 4$?

4. Нехай R і S — відношення на множинах, відповідно, M і N. Їхнім *прямим добутком* звуть відношення $R \times S$ на множині $M \times N$, таке що $((a,b),(a',b')) \in R \times S$ тоді й лише тоді, коли $(a,a') \in R$ і $(b,b') \in S$. Доведіть, що коли R і S обидва є відношеннями еквівалентності (або часткового порядку), то таким є й $R \times S$. Чи вірне таке ж твердження для відношень лінійного порядку?

5. Нехай R і S — відношення строгого порядку на множинах, відповідно, M і N. Їхнім *лексікографічним добутком* звуть відношення $R \circ S$ на множині $M \times N$, таке що $((a,b),(a',b')) \in R \times S$ тоді й лише тоді, коли або $(a,a') \in R$, або $a = a'$ і $(b,b') \in S$. Доведіть, що $R \circ S$ — відношення строгого порядку, причому якщо R і S — відношення лінійного строгого порядку, то таким є й $R \circ S$.

Завдання 10.

В усіх задачах граф Γ вважається неорієнтованим, простим і зв'язним.

1. Доведіть, що $d(a,b)+d(b,c)=d(a,c)$ тоді й лише тоді, коли b лежить на одному з найкоротших шляхів з a до c.

2. Доведіть, що коли p і q — такі прості шляхи, що $\mathrm{L}(p)=\mathrm{L}(q)=\mathrm{L}(\Gamma)$, вони мають спільну вершину.

3. Нехай $l=\mathrm{L}(\Gamma)$. Довести, що $e(a)\geq[(l+1)/2]$ для довільної вершини a, причому рівність досягається тоді й лише тоді, коли a належить кожному найдовшому простому шляху.

4. Нехай $r=r(\Gamma)$, $\rho=\rho(\Gamma)$, причому $\rho>2$. Довести, що

$$\nu_v(\Gamma)\leq 1+\rho\frac{(\rho-1)^r-1}{\rho-2},$$

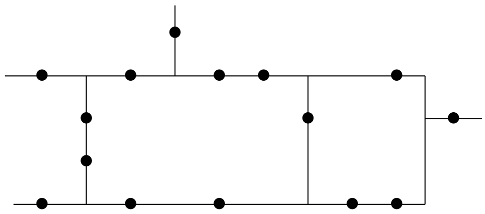
причому рівність досягається (на якому графі?). Що буде, коли $\rho=2$?

5. Нехай $\rho(b)>1$ і $p:a\to b$ — такий простий шлях, що $\mathrm{L}(p)=\mathrm{L}(a,b)$. Доведіть, що вершина b належить простому циклу довжини принаймні $\rho(b)+1$.

Завдання 11.

1. Доведіть, що розмах $\mathrm{L}(a,b)$ (найбільша довжина простого шляху між вершинами a та b) задовольняє правилу трикутника $\mathrm{L}(a,c) \leq \mathrm{L}(a,b)+\mathrm{L}(b,c)$.

2 (Задача Ойлера, з якої розпочалася теорія графів). План Кенігсберзьких мостів схематично виглядає так:



(Лінії — це річки, жирні крапки — мости.) Чи можна, вийшовши з якоїсь точки, перейти кожен міст по одному разу: а) і повернутися в ту саму точку? б) не обов'язково повертаючись?

3. Нехай Δ — підграф зв'язного графа Γ. Доведіть, що кількість зв'язних компонент доповнення $\complement\Delta$ не перебільшує кількості вершин у графі Δ.

4. Нехай простий шлях $p : a \to b$ (у простому графі) не можна продовжити до більшого простого шляху з тим самим початком a, причому $\rho(b) > 1$. Доведіть, що через вершину b проходить простий цикл довжини $l > \rho(b)$.

5. Нехай Γ — скінченний орієнтований зв'язний граф. Доведіть, що:

(1) У графі Γ існує орієнтований ойлерів цикл тоді й лише тоді, коли $\rho^+(a) = \rho^-(a)$ для кожної вершини a.

(2) Найменша кількість орієнтованих шляхів, які разом містять кожну стрілку графа Γ по одному разу, дорівнює
$$\frac{1}{2}\sum_{a\in \mathrm{Ver}\,\Gamma} \left|\rho^+(a)-\rho^-(a)\right| = \sum_{a\in \mathrm{Ver}^+\Gamma} \bigl(\rho^+(a)-\rho^-(a)\bigr),$$
де $\mathrm{Ver}^+\Gamma = \{\, a \in \mathrm{Ver}\,\Gamma \mid \rho^+(a) > \rho^-(a)\,\}$.

6. Скільки гамільтонових циклів є у повному графі з m вершинами?

Завдання 12.

1. Доведіть, що циклове число $\gamma(\Gamma)$ дорівнює 1 тоді й лише тоді, коли в графі Γ є рівно один цикл.

2. Знайдіть необхідну й достатню умову того, що $\gamma(\Gamma) = 2$.

3. Доведіть, що зв'язний граф Γ є деревом тоді й лише тоді, коли перетин його довільних зв'язних підграфів або порожній, або зв'язний.

4. Скільки існує кореневих дерев Δ з коренем o і фіксованими множинами $M_n = \{\, a \in \operatorname{Ver}\Delta \mid d(o,b) = n \,\}$, якщо відомо, що $\#(M_n) = m_n$, а $r(a) = r$.

5. Нехай $f : M \to M$ — деяке відображення. Утворимо граф $\Gamma(f)$, в якому $\operatorname{Ver}\Gamma = M$, а ребра сполучають точки a та $f(a)$. Доведіть, що (скінченний) граф ізоморфний $\Gamma(f)$ для деякого відображення f тоді й лише тоді, коли кожна його компонента містить рівно один цикл. Скільки є різних відображень $f : M \to M$, для який графи $\Gamma(f)$ збігаються?

Завдання 13.

1. Нехай Γ — неорієнтований зв'язний граф. Доведіть, що наступні умови рівносильні:

(1) Граф Γ дводольний.
(2) Γ не має простих циклів непарної довжини.
(3) $d(a,b) \neq d(a,c)$ для кожної вершини a і кожної пари вершин $\{ b,c \}$, сполучених ребром.

2. Припустимо, що у дводольному графі без кратних ребер існує повне парування. Доведіть, що кількість таких парувань не менша, ніж $n!$, де $n = \min\{ \rho(a) \mid a \in V_0 \}$.

3. Нехай Γ — однорідний дводольний граф степеня n (тобто $\rho(a) = n$ для кожної вершини a). Доведіть, що:

(1) У графі Γ є повне парування.
(2) Множину всіх стрілок цього графа можна розбити на n повних парувань.
(3) Якщо Γ — без кратних ребер, кількість таких розбиттів не менша, ніж $1!2!\dots(n-1)!n!$

4. Нехай $A_1, A_2, \dots, A_n$ і $B_1, B_2, \dots, B_n$ — дві сім'ї множин.

(1) Знайдіть необхідну й достатню умову того, щоб ці множини можна було перенумерувати так, що $A_i \cap B_i \neq \emptyset$ для всіх $i = 1, 2, \dots, n$.
(2) Якщо це не можливо, яку найменшу кількість множин треба вилучити з цього списку, щоб це вже стало можливим?

Завдання 14.

1. Нехай M — множина з n елементів. *Латинським квадратом* на множині M зветься $n \times n$ матриця (a_{ij}), де всі $a_{ij} \in M$, причому $a_{ij} \neq a_{ik}$ при $j \neq k$ і $a_{ij} \neq a_{kj}$ при $i \neq k$ (тобто ані в рядках, ані у стовпчиках елементи не повторюються).

(1) Ототожнити кожен латинський квадрат з розбиттям на повні парування множини стрілок дводольного графа, у якого V і V' — копії множини M і з кожної вершини $a \in V$ до кожної вершини $a' \in V'$ веде стрілка.

(2) Вивести звідси, що кількість латинських квадратів на множині з n елементами не менша за $n!(n-1)!\dots 2!1!$.

2. *Перманентом* квадратної матриці $A = (a_{ij})$ розміру $n \times n$ зветься число

$$\operatorname{Per}(A) = \sum a_{1i_1} a_{2i_2} \dots a_{ni_n},$$

де сума береться за всіма перестановками $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$. Довести, що кількість повних паросполучень у неорієнтованому дводольному графі дорівнює $\sqrt{\operatorname{Per}(S)}$, де S — його матриця суміжності.

3. Нехай $A = (a_{ij})$ — матриця з невід'ємними дійсними коефіцієнтами. Її *терм-рангом* $\operatorname{ter}(A)$ назвемо найбільше натуральне t, таке що в A існує квадратна підматриця розміру $t \times t$ з ненульовим перманентом. Довести, що для квадратної матриці розміру $n \times n$

$$\operatorname{ter}(A) = \min(n, 2n - \delta), \tag{1}$$

де δ — найбільша серед таких сум $k + l$, що в A є нульова підматриця розміру $k \times l$. Зокрема, $\operatorname{Per}(A) = 0$ тоді й лише тоді, коли в A є нульова підматриця розміру $k \times l$, де $k + l > n$. Як треба змінити формулу (1), щоб вона залишилася вірною для прямокутних матриць?

Вказівка: Зведіть цю задачу до розгляду деякого дводольного графа.