

О.Рудик

Вибрані питання дискретної математики. Перелік графів і теорема Редфілда — Пойа

(Комп'ютер у школі та сім'ї — 2013. — № 7. — С. 44–51)

Публікація стисло висвітлює елементи теорії переліку ізоморфних графів, детально викладеної у роботі [1], що базується на оригінальних роботах [2–5]. Для зручності сприйняття публікації учнями загально освітніх навчальних закладів у розділі 1 викладено початки теорії груп. Публікацію адресовано:

- учням класів з поглибленим вивченням математики;
- студентам вищих навчальних закладів, які навчаються за спеціальністю "Математика" чи "Прикладна математика";
- вчителям математики й інформатики класів з поглибленим вивченням математики.

1. Група

Означення 1. Множину G називають групою, якщо справджуються такі висловлювання.

1. Задано закон множення (композиції), який впорядкованій парі $(a; b)$ елементів G ставить у відповідність добуток ab — елемент G , який називають добутком b на a зліва або добутком a на b справа.
2. Справджується сполучний закон множення: $(ab)c = a(bc)$.
3. Існує ліва одиниця множення (нейтральний елемент) групи e , тобто такий елемент групи, множення на який зліва не змінює жоден елемент групи: $ex = x$.
4. Для довільного елемента a групи існує лівий обернений до нього a^{-1} , тобто такий, при якому добуток оберненого елемента на сам елемент дорівнює лівій одиниці множення: $a^{-1}a = e$.

Групу називають комутативною (абелевою), якщо множення комутативне, тобто добуток не залежить від порядку співмножників: $ab = ba$.

Закон асоціативності множення формулюють ще й так: добуток не залежить від порядку виконання дії множення (не плутати з порядком співмножників). Саме у такій редакції його потрібно поширити на більшу кількість співмножників, розуміючи добуток як, наприклад, результат виконання дії множення у порядку запису зліва направо: $abc = (ab)c$, $abcd = ((ab)c)d$ і

т. ін. Множина взаємно однозначних відображень довільної множини в себе є групою щодо суперпозиції, тобто послідовного застосування відображень.

Теорема 1. Для довільної групи справджуються такі висловлювання.

1. Лівий обернений елемент є також правим оберненим елементом, який для кожного елемента групи єдиний: $a a^{-1} = e$.
2. Ліва одиниця є також правою одиницею, тобто множення на неї справа не змінює жоден елемент групи: $ae = a$.
3. Одиниця множення у групі єдина.

Доведення:

- помножимо зліва рівність $a^{-1} a a^{-1} = a^{-1}$ на елемент, обернений до a^{-1} і використаємо асоціативність множення. В результаті отримаємо: $a a^{-1} = e$, тобто лівий обернений елемент є також правим оберненим;
- $a = ea = (a a^{-1}) a = a (a^{-1} a) = ae$, тобто кожна ліва одиниця є одночасно правою одиницею;
- помноживши зліва і справа довільний елемент a групи на його обернені b і c та по-різному розставляючи дужки, тобто використовуючи асоціативність множення, легко пересвідчитися, що обернений елемент єдиний: $b = b (ac) = (ba) c = c$;
- обчислюючи добуток (одночасно лівих і правих) одиниць групи, легко пересвідчитися, що одиниця групи єдина: $e = ee' = e'$.

Означення 2. Запровадимо такі поняття.

1. Непорожню підмножину A групи G називають підгрупою групи G , якщо:
 - добуток двох елементів A також належить до A ;
 - елемент, обернений до елемента з A також належить до A .
2. Нехай A — підгрупа групи G . Правим класом групи G за підгрупою A називають множину вигляду $Ax = \{ax \mid a \in A\}$, де x — довільний елемент групи G (аналогічно означають лівий клас суміжності).
3. Підстановкою (перестановкою) називають взаємно однозначне відображення скінченної множини у себе. Не обмежуючи загальності міркувань, надалі будемо розглядати лише множини вигляду $\{1, 2, \dots, n\}$ — множини всіх перших n натуральних чисел.
4. Транспозицією називають підстановку, яка кожному елементу, за виключенням двох, ставить у відповідність цей самий елемент.
5. Множину всіх підстановок на множині $\{1, 2, \dots, n\}$ при сталому n називають симетричною групою і позначають S_n .
6. Порушенням порядку підстановки на множині $\{1, 2, \dots, n\}$, що числу j ставить у відповідність число i_j при $j = 1, 2, \dots, n$, називають сумісну систему таких двох нерівностей: $j < k$ та $i_j > i_k$.
7. Підстановку називають парною, якщо кількість транспозицій, у добуток яких можна розкласти дану підстановку, є парною.

8. Множину всіх парних підстановок на множині $\{1, 2, \dots, n\}$ при сталому n називають знакозмінною групою і позначають A_n .
9. Циклом довжини k називають перестановку, яка певний елемент j_1 відображає у деякий елемент j_2 , j_2 — в j_3 , ..., j_{k-1} — в j_k , j_k — в j_1 за умови, що всі елементи j_1, j_2, \dots, j_k — різні. Такий цикл позначають $(j_1 j_2 \dots j_k)$.
10. Дві групи називають ізоморфними, якщо існує взаємно однозначне відображення f однієї групи в іншу, при якому образ добутку елементів однієї групи є добутком образів співмножників у тому самому порядку: $f(ab) = f(a)f(b)$. Таке відображення f називають ізоморфізмом відповідних груп.

Зауваження 1. Справджуються такі висловлювання.

1. Транспозиція, що "міняє місцями" сусідні натуральні числа, змінює кількість порушень порядку на 1.
2. Довільна транспозиція змінює кількість порушень порядку на непарне число.
3. Парність кількості транспозицій у розкладі підстановки не залежить від конкретного подання добутком транспозицій і збігається з парністю кількості порушень порядку.
4. Цикл з непарної довжиною є добутком парної кількості транспозицій.
5. Цикл з парної довжиною є добутком непарної кількості транспозицій.
6. Підстановка є парною тоді й лише тоді, коли її подання добутком циклів без спільних елементів містить парну кількість циклів парної довжини.

Зауваження 2. Довільну підстановку можна подати добутком циклів без спільних елементів.

Наприклад:

- $S_3 = \{(1)(2)(3), (12)(3), (13)(2), (23)(1), (123), (132)\}$ — група всіх симетрій правильного трикутника (вказано дію на вершинах, занумерованих числами 1, 2 і 3);
- $A_3 = \{(1)(2)(3), (123), (132)\}$ — група поворотів правильного трикутника навколо його центра на 0, 120 і 240 градусів.

Зауваження 3. Для довільної скінченої групи множення справа (зліва) на певний елемент задає підстановку на множині елементів цієї групи. Тому довільна скінчена група ізоморфна підгрупі S_n , де $n = |G|$ — кількість елементів групи G .

Зауваження 4. Класи суміжності за однією підгрупою мають однакову кількість елементів, що збігається з кількістю елементів підгрупи.

2. Твірна функція

Означення 3. Твірною функцією послідовності a_0, a_1, a_2, \dots називають степеневий ряд такого вигляду:

$$\sum_{j=0}^{\infty} a_j x^j.$$

Надалі такі ряди будемо розглядати формально, тобто не досліджуючи питання збіжності, але використовуючи операції додавання, множення і (почленного) диференціювання твірних функцій. У задачах переліку числа a_1, a_2, \dots — кількості об'єктів з певними властивостями. Тому твірну функцію називають рядом переліку.

Теорема 2. Якщо $A(x) = e^{a(x)}$ при

$$a(x) = \sum_{j=1}^{\infty} a_j x^j, \quad A(x) = \sum_{j=0}^{\infty} A_j x^j, \quad A_0 = 1,$$

то при довільному натуральному j справджується така рівність:

$$a_j = A_j - j^{-1} \sum_{k=1}^{j-1} k a_k A_{j-k}.$$

Доведення. $A'(x) = e^{a(x)} a'(x) = A(x) a'(x)$, тобто

$$\sum_{j=1}^{\infty} j A_j x^{j-1} = \sum_{l=0}^{\infty} \frac{A_l}{x^l} \sum_{k=1}^{\infty} k a_k x^{k-1}.$$

Коефіцієнти при x^{j-1} лівої та правої частин цієї рівності відповідно дорівнюють:

$$= \sum_{k=1}^j k a_k A_{j-k},$$

звідки й випливає твердження теореми.

3. Циклові індекси групи підстановок

Означення 4. Запровадимо такі позначення й поняття.

1. Позначимо через $j_k(a)$ кількість усіх циклів довжини k , що входять у розклад підстановки a на цикли без спільних елементів. Тут k лежить в межах від 1 до n — кількості об'єктів множини, на якій діє підстановка.
2. Характеристикою підстановки a називають впорядкований набір вигляду

$$(j_1(a), j_2(a), \dots, j_n(a)).$$

3. Цикловим індексом групи підстановок G на множині n елементів називають многочлен n змінних x_1, x_2, \dots, x_n такого вигляду:

$$|G|^{-1} \sum_{a \in G} \prod_{k=1}^n x_k^{j_k(a)}.$$

4. Такий многочлен позначають $Z(G, x_1, x_2, \dots, x_n)$ або $Z(G)$.

Зауваження 5.

$$Z(G) = |G|^{-1} \sum_c h(c) \prod_{k=1}^n x_k^{j_k(a)},$$

де додавання здійснюють за всіма можливими характеристиками c елементів групи, $h(c)$ — кількість елементів групи з характеристикою $c = (j_1(a), j_2(a), \dots, j_n(a))$.

Наприклад:

- $Z(S_3) = (x_1^3 + 3x_1x_2 + 2x_3)/6$;
- $Z(A_3) = (x_1^3 + 2x_3)/3$.

Теорема 3. При всіх натуральних j справджуються такі рекурентні співвідношення:

$$Z(S_j) = j^{-1} \sum_{l=1}^j x_l Z(S_{j-l}), \quad \text{де } Z(S_0) = 1.$$

Доведення. Для довільної підстановки a позначимо через $l(a)$ довжину циклу, що містить j -ий елемент. Маємо:

$$Z(S_j) = (j!)^{-1} \sum_{\substack{a \in \\ S_j}} \prod_{k=1}^j x_k^{j_k(a)} = (j!)^{-1} \sum_{l=1}^j x_l \sum_{\substack{a \in S_j \\ l(a)=l}} x_l^{j_l(a)-1} \prod_{\substack{k \neq \\ l}} x_k^{j_k(a)}.$$

При сталому $l(a) = l$ доданки під знаком першої суми (при прогляданні виразу справа наліво — у порядку обчислення) в останньому виразі ті самі, що й для відповідної суми для $Z(S_{j-l})$. Кратність кожного такого доданку дорівнює кількості циклів довжини l , що містять j -ий елемент. Згідно з комбінаторним правилом множення таку кількість можна подати добутком:

$$1 \cdot (j-1) \cdot (j-2) \cdot (j-3) \dots (j-l+1) = (j-1)! : (j-l)! .$$

Врахувавши множник перед знаком другої суми, отримаємо твердження теореми.

Теорема 4.

∞

∞

$$\sum_{j=0}^{\infty} Z(S_j) x^j = \exp \left(\sum_{j=1}^{\infty} x_j j^{-1} x^j \right).$$

Доведення. Див. твердження попередньої теореми й доведення теореми 2.

4. Лема Коші — Фробеніуса (Бернсайда)

Означення 5. Нехай A — група підстановок на деякій множині X . Наприклад, $X = \{1, 2, \dots, n\}$. Запровадимо такі поняття.

1. Елементи x та y множини X називають A -еквівалентними, якщо існує така підстановка a з A , при якій $ax = y$.
2. Множину A -еквівалентних між собою елементів називають орбітою.
3. Для кожного x з множини X означимо стабілізатор елемента x як множину всіх тих підстановок з A , які залишають нерухомим x , і позначимо її через $A(x)$:

$$A(x) = \{a \in A \mid ax = x\}$$

Зауваження 7.

1. Відношення A -еквівалентності насправді є відношенням еквівалентності, бо A — група. Тому розбиття на орбіти є розбиттям на класи еквівалентності.
2. Стабілізатор довільного елемента є підгрупою початкової групи підстановок.
3. Якщо x та y належать до однієї орбіти, то їхні стабілізатори є спряженими підгрупами групи A . Інакше кажучи, існує такий елемент a групи A , при якому справджується рівність: $A(x) = a A(y) a^{-1}$. У цьому випадку $|A(x)| = |A(y)|$.

Теорема 5. Для довільного елемента y з орбіти Y групи A справджується така рівність:

$$|A| = |A(y)| \cdot |Y|$$

Доведення. Подамо групу A об'єднанням правих класів суміжності $a_j A(y)$ за підгрупою $A(y)$. Позначимо кількість таких класів суміжності через t . Для кожного $j = 1, 2, \dots, t$ класу суміжності $a_j A(y)$ поставимо у відповідність елемент $a_j y$ з орбіти Y .

1. При різних a_j і a_k різними також є $a_j y$ і $a_k y$, бо інакше добуток $a_j^{-1} a_k$ належить до групи $A(y)$, а тому a_k належить до $a_j A(y)$. Останнє висловлювання суперечить відсутності спільних елементів множин $a_j A(y)$ та $a_k A(y)$, тобто розбиттю на класи суміжності. Отже, вказане відображення є відображенням "в" (ін'єкцією).
2. Згідно з означенням орбіти, для довільного елемента y' орбіти Y існує елемент a групи A , при якому $y' = ay$. У свою чергу, згідно з розбиттям A на праві класи суміжності $a_j A(y)$, існують a_j та елемент b групи $A(y)$, при яких $a = a_j b$. В результаті маємо:

$$y' = ay = a_j by = a_j y.$$

Отже, вказане відображення є відображенням "на" (сюр'єкцією). Інакше кажучи, кожний елемент орбіти Y є образом деякого класу суміжності.

Таким чином, доведено існування взаємно однозначного відображення з множини класів суміжності в орбіту Y , тому вони мають однакову кількість елементів. Теорему доведено.

Теорема 6. *Кількість $N(A)$ орбіт групи підстановок A дорівнює середньому арифметичному кількості нерухомих точок групи A :*

$$N(A) = |A|^{-1} \sum_{\substack{a \in \\ A}} j_1(a).$$

Доведення. Позначимо через Y_1, Y_2, \dots, Y_m різні орбіти групи A . Для кожного $j = 1, 2, \dots, m$ виберемо довільним чином елемент $y_j \in Y_j$. Додавши праві та ліві частини рівностей у твердженні попередньої теореми, записаних для $Y = Y_j$ для кожного $j = 1, 2, \dots, m$, отримаємо таку рівність:

$$N(A) \cdot |A| = \sum_{j=1}^m |A(y_j)| \cdot |Y_j|.$$

Вже встановлено, що для елементів з однієї орбіти їхні стабілізатори спряжені, а тому мають однакову кількість елементів. Праву частину останньої рівності можна подати таким чином:

$$\sum_{\substack{x \in \\ X}} |A(x)| = \sum_{x \in X} \sum_{a \in A(x)} 1 = \sum_{a \in A} \sum_{\substack{x = \\ ax}} 1 = \sum_{a \in A} j_1(a).$$

Теорему доведено.

Теорему 4, широко відому як лема Бернсайда, опублікували раніше Огюстен Коші [2] та Фердінанд Георг Фробеніус [3].

Зауваження 8 (обмежена форма). *Якщо:*

- група підстановок A діє на множині X ;
 - Y — об'єднання орбіт групи A , що є підмножиною X ;
 - $A|Y$ — група підстановок, отримана звуженням дії A на Y ;
 - $j_1(a|Y)$ — кількість елементів Y , нерухомих відносно підстановки a ,
- то справджується така рівність:

$$N(A|Y) = |A|^{-1} \sum_{\substack{a \in \\ A}} j_1(a|Y).$$

5. Теорема Редфілда — Пойа

Означення 6. Нехай:

- A — група підстановок на множині $X = \{1, 2, \dots, n\}$;
- B — скінчена група підстановок на зліченій множині Y , що містить не менше двох елементів;
- w — вагова функція, визначена на Y , зі значеннями у множині невід'ємних цілих чисел і така, що при довільному невід'ємному цілому j кількість c_j його прообразів скінчена:

$$c_j = |\{y \in Y \mid w(y) = j\}| < \infty.$$

Запровадимо такі поняття.

1. Степенною групою підстановок, яку позначають B^A , називають таку групу:
 - група діє на множині Y^X усіх функцій з X в Y ;
 - елементом групи є впорядкована пара $(a; b)$ при $a \in A, b \in B$;
 - на функцію f елемент групи $(a; b)$ діє таким чином:
 $((a; b)f)(x) = bf(ax)$ при всіх $x \in X$.
2. Кажуть, що елемент у множині Y має вагу j , якщо $w(y) = j$.
3. Степеневий ряд змінної x , який перераховує елементи множини Y у порядку зростання їхніх ваг і має такий вигляд:

$$c(x) = \sum_{j=0}^{\infty} c_j x^j$$

називають "рядом переліку для фігур".

4. Вагу $w(f)$ функції f з Y^X означимо як суму:

$$w(f) = \sum_{x \in X} w(f(x))$$

5. Якщо $B = E$ (група, що містить лише тотожне перетворення), то функції, які належать до однієї орбіти степенної групи E^A , мають одну й ту саму вагу, яку називають вагою орбіти.
6. Степеневий ряд змінної x , який у випадку $B = E$ перераховує кількості орбіт у порядку зростання їхніх ваг і має такий вигляд:

$$C(x) = \sum_{j=0}^{\infty} C_j x^j,$$

називають "рядом переліку для конфігурацій". Тут C_j — кількість орбіт групи E^A з вагою j .

Теорема 7. Ряд $C(x)$ переліку конфігурацій отримують підстановкою в цикловий індекс $Z(A, x_1, x_2, \dots, x_n)$ групи A на місце кожної змінної x_j ряду $c(x^j)$ переліку фігур:

$$C(x) = Z(A, c(x), c(x^2), \dots, c(x^n)).$$

Доведення. Позначимо:

- e — тотожне перетворення на Y ;
- $C_j(a)$ — число функцій з вагою j , нерухомих відносно підстановки $(a; e)$.

Обмеживши для кожного k дію групи E^A на множину функцій з вагою j і застосувавши обмежену форму леми Бернсайда, маємо:

$$C_j = |A|^{-1} \sum_{a \in A} C_j(a),$$

тому

$$C(x) = |A|^{-1} \sum_{j=0}^{\infty} \sum_{a \in A} C_j(a) x^j = |A|^{-1} \sum_{a \in A} \sum_{j=0}^{\infty} C_j(a) x^j.$$

В останньому виразі ряд $\sum_j C_j(a) x^j$ перераховує всі функції, нерухомі відносно підстановки $(a; e)$. Для кожної такої функції при всіх x з X маємо:

$$((a; e)f)(x) = ef(ax) = f(ax).$$

Інакше кажучи, кожна функція, нерухома відносно підстановки $(a; e)$, стала на циклах, що не перетинаються, підстановки a . І навпаки: кожна функція, стала на циклах, що не перетинаються, підстановки a , нерухома відносно підстановки $(a; e)$.

Розглянемо цикл довжини k у довільній підстановці a . Якщо функція f відображає елементи цикла в один з c_j елементів множини $\{y \in Y \mid w(y) = j\}$, то цей цикл вносить вклад jk у вагу функції f .

При кожному невід'ємному цілому k коефіцієнт при x^{jk} у ряді

$$c(x^k) = \sum_{j=0}^{\infty} \frac{c_j x^j}{jk}$$

дорівнює числу способів, якими можна означити функцію f на елементах цикла довжини k таким чином, щоб функція f була нерухомою відносно підстановки $(a; e)$ і її вклад на вибраному циклі у вагу $w(f)$ складав jk .

Ряд $(c(x^k))^{j_k(a)}$ перераховує способи визначення функцій, сталих на всіх циклах довжини k підстановки a .

Розглянувши всі цикли підстановки a , можемо подати отриманий раніше ряд переліку функцій, сталих на циклах, що не перетинаються, добутком:

$$\sum_{j=0}^{\infty} C_j(a) x^j = \prod_{k=1}^n (c(x^k))^{j_k(a)}.$$

Для завершення доведення теореми потрібно поєднати у систему останню рівність, отриману на початку доведення подання ряду $C(x)$ та означення 4 циклового індекса.

Повідомлення про цю теорему вперше опублікував Говард Редфілд у 1927 році. Нажаль, робота [4] залишилася непоміченою, бо видалася занадто специфічною. Дьйорд Пойа (він же Джордж Поліа) опублікував своє доведення у 1937 році й виявився успішнішим популяризатором. Вже у

першій його публікації [5] на цю тему вказано на можливість застосування теореми до переліку хімічних сполук.

6. Перелік розфарбувань

Зауваження 9. Якщо в умові теореми 7: $|Y| = m$ — натуральне число; $w(y) = 1$ — стала на елементах Y вагова функція, то кількість орбіт дорівнює такій величині:

$$C(1) = Z(A, c(1), c(1), \dots, c(1)) = Z(A, m, m, \dots, m).$$

Якщо при цьому:

- A — група підстановок, що діють на множині вершин деякого неорієнтованого графа і зберігають суміжність вершин;
- m — кількість кольорів, якими можна розфарбовувати вершини деякого графа,

то знайдена кількість $C(1)$ є кількістю різних способів розфарбування вершин графа (два розфарбування вважаються однаковими, якщо одне можна отримати з іншого підстановкою на множині вершин, що зберігає суміжність вершин).

У свою чергу граф може бути моделлю геометричної фігури, наприклад, регулярного многогранника. Іншими словами, вершинами графа є вершини, ребра чи грані многогранника. Тоді знайдена кількість $C(1)$ є кількістю різних способів розфарбування геометричної фігури.

Знайдемо кількість способів розфарбування вершин (сторін) правильного трикутника жовтим і блакитним кольором: $m = 2$.

1. $Z(S_3) = (x_1^3 + 3x_1x_2 + 2x_3)/6$, тому допустивши всі рухи, маємо:
 $C(1) = (2^3 + 3 \cdot 2 \cdot 2 + 2 \cdot 2)/6 = 4$.

2. $Z(A_3) = (x_1^3 + 2x_3)/3$, тому допустивши лише повороти, маємо:
 $C(1) = (2^3 + 2 \cdot 2)/3 = 4$.

В обох розглянутих випадках є такі 4 способи розфарбування:

- три вершини пофарбовано жовтим кольором;
- дві вершини пофарбовано жовтим кольором і одну — блакитним;
- одну вершину пофарбовано жовтим кольором і дві — блакитним;
- три вершини пофарбовано блакитним кольором.

Вкажемо на зв'язок матеріалу публікації зі змістом завдань *учнівських олімпіад з інформатики*. У 2001–2006 автор публікації одноосібно упорядковував завдання орієнтовні завдання для II (районного) і III (міського) етапу Всеукраїнської учнівської олімпіади з інформатики у місті Києві. При цьому робився наголос на алгоритмічно змістовних задачах, теоретичні основи яких не виходять за межі навчальних програм поглибленого вивчення математики. Поняття симетрії і неявне запровадження групи симетрій платонових тіл — обов'язковий фрагмент такої навчальної програми. Тому:

- орієнтовні завдання II етапу учнівської олімпіади з інформатики у місті Києві 2004 року містили задачу подання підстановки добутком циклів без спільних елементів. При цьому вхідні дані містили інформацію про

підстановку на множині вершин чи граней правильного многогранника, яка (підстановка) відповідали симетрії многогранника;

- завдання III етапу учнівської олімпіади з інформатики у місті Києві 2005 року містили задачу, у якій потрібно було знайти групу симетрій регулярного многогранника за інформацією про суміжність граней. Точніше, потрібно було знайти подання групи дією на множині граней. Далі потрібно було перебрати дерева — моделі різних одноколірних розгорток многогранника.

Синтезом розв'язань вказаних двох задач з використанням теореми 7 можна отримати *оптимальне* розв'язання задачі про кількість розфарбувань вершин, ребер чи граней регулярних многогранників. У 2005 році автор не був впевнений у доступності теоретичного матеріалу для учнів. Зараз ця впевненість уже є, бо автор «випробував» текст даної публікації на учнях. Насправді від учасника олімпіади вимагають лише вміння використати кінцевий результат, а не відтворити його отримання. Алгоритм, на відміну від теорії, легкий для сприйняття і програмного втілення:

1. Зчитавши вхідні дані, встановити кількість граней і відношення суміжності.
2. За допомогою оптимізованого перебору встановити групу симетрій S — взаємно однозначних відображень множини граней многогранника у себе — і кількість елементів цієї групи $|S|$.
3. При всіх k в межах від 1 до $|S|$ змінній p_k надати величину 0.
4. Для кожного елемента групи симетрій:
 - знайти j — кількість циклів, на які він розкладається;
 - збільшити на 1 величину p_j .
5. Обчислити $n_{\text{out}} = (p_1 \cdot m + p_2 \cdot m^2 + p_3 \cdot m^3 + \dots + p_{|S|} \cdot m^{|S|}) : |S|$.
6. Вивести величину n_{out} .

Розглянемо популярну у навчальній літературі задачу про знаходження кількості різних намист, що складаються з намистинок k кольорів і містять по p намистинок. Два намиста вважають різними, якщо їх не можна сумістити рухами у площині.

Нехай p — просте число. У цьому випадку група поворотів намиста має вигляд $Z_p = \{e, a, a^2, \dots, a^{p-1}\}$, де:

- $e = (1)(2)\dots(p)$ — тотожне перетворення, що має характеристику $(p, 0, 0, 0, 0)$ і якому відповідає доданок x_1^p у цикловому індексі;
- $a = (2, 3, \dots, p, 1)$ — поворот на одну намистинку, що має характеристику $(0, 0, \dots, 0, 1)$ і якому відповідає доданок x_n у цикловому індексі;
- повороти a^2, a^3, \dots, a^{p-1} мають таку саму характеристику, що й a . Тому їм відповідає той самий доданок x_n у цикловому індексі.

Цикловий індекс групи: $Z(Z_p, x_1, x_2, \dots, x_p) = (x_1^p + (p-1)x_p) : p$.

Шукана кількість різних намист: $Z(Z_p, k, k, \dots, k) = (k^p + (p-1)k) : p$.

Якщо p — відмінне від 1 не просте натуральне число, то $Z(A, x_1, x_2, \dots, x_n)$ дорівнює такій сумі:

$$n^{-1} \sum (x_n : \text{НСД}(k, n))^{\text{НСД}(k, n)} = n^{-1} \sum \varphi(n/d) (x_{n/d})^d = n^{-1} \sum \varphi(d) x_d^{n/d}.$$

$$k = 1 \qquad \qquad \qquad d \mid n \qquad \qquad \qquad d \mid n$$

Тут:

- НСД(k, n) — найбільший спільний дільник натуральних k і n ;
- $\varphi(d)$ — функція Ейлера — кількість натуральних чисел, які не перевищують d і взаємно прості з ним;
- додавання здійснюють за всіма d — натуральними дільниками n .

У загальному випадку шукана кількість різних намист така:

$$n^{-1} \sum_{\substack{d \mid n}} \varphi(d) k^{n/d}.$$

7. Перелік неорієнтованих дерев з виділеною вершиною-коренем

Означення 7. Запровадимо такі поняття.

1. Графи називають ізоморфними, якщо існує взаємно однозначне відображення вершин одного графа у вершини іншого графа, що зберігає суміжність вершин.
2. Взаємно однозначне відображення вершин одного графа у вершини іншого графа, що зберігає суміжність вершин, називають ізоморфізмом графів.
3. Підстановка на множині вершин графа, що зберігає суміжність вершин, називають автоморфізмом графа.
4. Коли говорять про ізоморфізм чи автоморфізм графа з виділеною вершиною-коренем чи виділеним ребром, то крім збереження суміжності вершин вимагають, щоб образ виділеного елемента був виділеним.

Запровадимо такі позначення:

T_j — кількість різних (неізоморфних) неорієнтованих дерев з виділеною вершиною-коренем, що мають j вершин;

$$T(x) = \sum_{j=1}^{\infty} T_j x^j = x + x^2 + 2x^3 + 4x^4 + \dots$$

— твірна функція неорієнтованих дерев з виділеною вершиною-коренем.

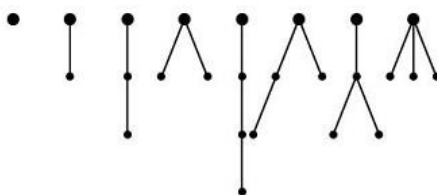


Рис.1. Неізоморфні кореневі дерева, порядок яких не перевищує 4. Корені виділено кругами більшого радіусу.

Теорема 8. Ряд $T(x)$ переліку неорієнтованих кореневих дерев задовольняє таке співвідношення:

$$T(x) = x \exp\left(\sum_{j=1}^{\infty} T(x^j) / j\right).$$

Доведення. Спочатку розглянемо лише такі неорієнтовані кореневі дерева, у яких степінь кореня сталий і дорівнює деякому натуральному n . Інакше кажучи, у таких деревах корінь є кінцем n різних ребер. Зауважимо, що довільне таке дерево можна подати як результат такого перетворення сукупності n кореневих дерев: долучається ще одна точка-корінь, що стає безпосереднім предком коренів n кореневих дерев, заданих спочатку. Запровадимо такі позначення: $X = \{1, 2, \dots, n\}$; Y — множина всіх неорієнтованих кореневих дерев; E — група з одним елементом (одиницею групи); E_n^S — степенева група з множиною об'єктів Y^X . Кожна функція з Y^X задає впорядкований набір (кортеж) n неорієнтованих кореневих дерев. Означимо вагу довільного дерева з Y як кількість його вершин. Тоді твірна функція $T(x)$ є рядом, що перераховує фігури (неорієнтовані кореневі дерева) у порядку зростання їхніх ваг. Згідно з зауваженням, виділеним курсивом, кожна орбіта степеневої групи E_n^S відповідає деякому кореневому дереву, корінь якого має степінь n . Вага такої орбіти на 1 менша від кількості вершин того кореневого дерева, що ставлять у взаємно однозначну відповідність орбіті. Взевши у теоремі 7 $A = S_n$ і $s(x) = T(x)$, отримаємо ряд переліку функцій (конфігурацій):

$$Z(S_n, T(x), \dots) = Z(S_n, T(x), T(x^2), \dots, T(x^n)).$$

Коефіцієнт при x^j у степеневому розкладі $x Z(S_n, T(x), \dots)$ дорівнює числу неорієнтованих кореневих дерев з j вершинами. При цьому степінь кореня всіх таких дерев дорівнює n . Здійснивши додавання за всіма можливими невід'ємними цілими n , отримаємо таке:

$$T(x) = \sum_{n=0}^{\infty} Z(S_n, T(x), T(x^2), \dots, T(x^n)).$$

Для завершення доведення теореми достатньо записати твердження теореми 4 для $x = 1$, а після "вивільнення" змінної x покласти $x_j = T(x^j)$ при всіх натуральних j .

Теорема 9. Кількості неорієнтованих кореневих дерев при довільному натуральному k задовольняють таке рекурентне співвідношення:

$$T_{j+1} = j^{-1} \sum_{k=1}^j k a_k T_{j-k+1}, \quad \text{де} \quad a_k = k^{-1} \sum_{\substack{d|k \\ k}} d T_d$$

Доведення. Справдження останньої рівності при довільному натуральному k означає рівність степеневих рядів:

$$\sum_{k=1}^{\infty} a_k x^k = \sum_{l=1}^{\infty} T(x^l) / l.$$

Для завершення доведення теореми потрібно скористатися попередньою теоремою 8 та теоремою 2 про експоненту твірної функції.

Перші 333 члени послідовності $\{T_j\}$ опубліковано на сайті "Київські учнівські олімпіади з інформатики" за адресою:
<http://kievoi.narod.ru/lectures/roottree.html>.

8. Перелік неорієнтованих дерев з виділеним ребром

Означення 8. *Запровадимо такі поняття.*

1. *Граф, у якому виділено ребро, називають реберно-кореневим графом.*
2. *Виділене ребро в реберно-кореновому графі називають кореневим ребром.*
3. *Ребро графа називають симетричним, якщо існує автоморфізм графа, що міняє кінці цього ребра місцями.*

Запровадивши серед вершин графа відношення еквівалентності "розташування по один бік від обраного ребра", можна пересвідчитися в істинності такого висловлювання.

Зауваження 10. *Кількість симетричних ребер у довільному дереві не перевищує 1.*

Теорема 10. *Запровадимо такі позначення:*

L_j — кількість різних (тобто неізоморфних) реберно-коренових неорієнтованих дерев порядку j (тобто дерев, що мають j вершин);

$$L(x) = \sum_{j=1}^{\infty} L_j x^j \text{ — твірна функція реберно-коренових неорієнтованих дерев.}$$

Маємо: $L(x) = (T^2(x) - T(x^2))/2$.

Доведення. Кореневе ребро розбиває реберно-кореневе неорієнтоване дерево на два кореневі неорієнтовані дерева. Тому L_j дорівнює кількості різних неупорядкованих пар коренових неорієнтованих дерев за умови, що у кожній такій парі загальна кількість вершин дорівнює j .

При непарному j кожна така пара містить різні кореневі дерева:

$$L_j = \sum_{k=1}^{j-1} T_k T_{j-k} / 2.$$

При парному j серед усіх таких пар знайдеться $T_{j/2}$ пар, що мають однакові елементи:

$$L_j = \left(\sum_{k=1}^{J-1} T_k T_{j-k} - T_{j/2} \right) / 2.$$

Помноживши обидві частини останніх двох рівностей на x^j і здійснивши додавання за всіма натуральними j , отримуємо твердження теореми.

9. Перелік неорієнтованих дерев

Означення 9. Запровадимо такі поняття.

1. Вершину графа називають точкою сполучення, якщо при видаленні її разом з інцидентними ребрами кількість компонент зв'язності графа зростає щонайменше на 1.
2. Зв'язний граф без точок сполучення називають двозв'язним.
3. Максимальні за вмістом (вершин і ребер) двозв'язні підграфи називають двозв'язними компонентами або блоками.
4. Нехай $A(G)$ — група автоморфізмів графа G . Дві вершини (два ребра, два блоки) цього графа називають $A(G)$ -еквівалентними (подібними), якщо існує автоморфізм графа G , що відображає одну вершину в іншу (одне ребро в інше, один блок в інший).
5. Дві вершини (два ребра, два блоки) графа G називають неподібними, якщо вони не є еквівалентними щодо групи $A(G)$ автоморфізмів цього графа.

Теорема 11. Для довільного графа G запровадимо такі позначення:

p — кількість неподібних вершин, тобто кількість класів еквівалентності подібних вершин;

b — кількість неподібних блоків, тобто кількість класів еквівалентності подібних блоків;

p_j — кількість неподібних вершин j -го блоку при $j = 1, 2, \dots, b$.

Маємо:

$$p - 1 = \sum_{j=1}^b (p_j - 1).$$

Доведення (методом математичної індукції за кількістю класів еквівалентності подібних блоків).

1. **База індукції.** При $b = 1$ маємо: $p = p_1$, тому твердження теореми справджується.
2. **Припущення індукції.** Припустимо, що твердження теореми справджується для довільного графа, у якому кількість неподібних блоків не перевищує певне натуральне b .
3. **Крок індукції.** Нехай кількість різних класів еквівалентності блоків графа дорівнює $b + 1$. Розглянемо серед блоків той, що має лише одну точку сполучення. Необмежуючи загальності міркувань, занумеруємо класи еквівалентності таким чином, щоб вибраний клас мав номер

$b + 1$. Вилучимо з графа вершини всіх блоків, що належать до цього класу еквівалентності, за виключенням точок сполучення. Новостворений граф має b різних класів блоків, тому для нього справджується припущення індукції. При цьому кількість різних класів еквівалентності вершин новоствореного графа дорівнює $p - (p_{b+1} - 1)$. Тому твердження теореми справджується і для початкового графа.

Зауваження 11. У довільному неорієнтованому дереві блоком є ребро, тому для кожного такого блоку-ребра маємо: $p_j = 2$. Виключення складає симетричне ребро, у якому ця кількість дорівнює 1. Позначивши через s кількість симетричних ребер, що не перевищує 1, твердження теореми 11 запишемо таким чином: $p - (b - s) = 1$.

Теорема 12. Запровадимо такі позначення:

t_j — кількість різних (тобто неізоморфних) неорієнтованих дерев порядку j (тобто дерев, що мають j вершин);

$$t(x) = \sum_{j=1}^{\infty} t_j x^j \text{ — твірна функція неорієнтованих дерев.}$$

Маємо: $t(x) = T(x) - (T^2(x) - T(x^2))/2$, де $T(x)$ — твірна функція кореневих неорієнтованих дерев.

Доведення. Розглянемо рівність $1 = p - (b - s)$ у позначеннях теореми 11 і зауваження 11 для усіх неорієнтованих дерев, що мають сталу кількість вершин j . Здійснивши додавання за всіма такими деревами, отримаємо: $t_j = T_j - L_j$ при довільному натуральному j . Перейшовши до твірних функцій, отримаємо: $t(x) = T(x) - L(x)$ і скористаємося твердженням теореми 10 для завершення доведення.

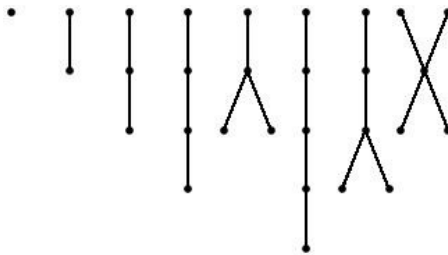


Рис.2. Неізоморфні дерева, порядок яких не перевищує 5.

Перші 333 члени послідовності $\{t_j\}$ опубліковано за адресою: <http://kievoi.narod.ru/lectures/tree.html>.

Маємо:

$$t(x) = x + x^2 + x^3 + 2x^4 + 3x^5 + \dots$$

10. Перелік орієнтованих дерев з виділеною вершиною-коренем

Запровадимо такі позначення:

R_j — кількість різних (неізоморфних) орієнтованих дерев з виділеною вершиною-коренем, що мають по j вершин;

$$R(x) = \sum_{j=1}^{\infty} R_j x^j = x + 2x^2 + 7x^3 + \dots$$

— твірна функція кореневих орієнтованих дерев.

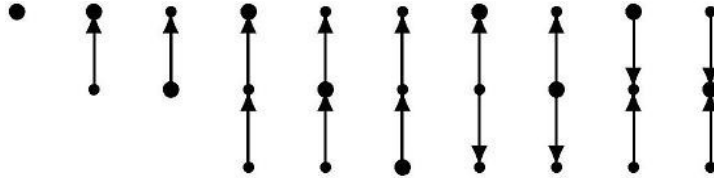


Рис.3. Неізоморфні кореневі орієнтовані дерева, порядок яких не перевищує 3. Корені виділено кругами більшого радіусу.

Теорема 13. Ряд $R(x)$ переліку кореневих орієнтованих дерев задовольняє таке співвідношення:

$$R(x) = x \exp^2\left(\sum_{j=1}^{\infty} R(x^j) / j\right).$$

Доведення. Позначимо через $R^*(x)$ ряд переліку орієнтованих дерев з виділеним коренем, що має степінь 1 (корінь є початком чи кінцем лише однієї дуги). Існує взаємно однозначна відповідність між довільною n -елементною (невпорядкованою) множиною таких дерев і орієнтованим деревом, у якому корінь інцидентний n вершинам. Застосувавши теорему 7 Редфілда — Пойа до симетричної групи S_n з використанням ряду переліку фігур $R^*(x)/x$, отримаємо ряд переліку функцій $Z(S_n, R^*(x)/x, \dots)$. У цьому ряді коефіцієнт при x^j дорівнює кількості орієнтованих кореневих дерев, що містять по $j+1$ вершині та у яких корені інцидентні n вершинам. Здійснивши додавання за всіма невід'ємними цілими n , отримаємо таке подання:

$$R(x) = \sum_{n=0}^{\infty} Z(S_n, R^*(x)/x, R^*(x^2)/x^2, \dots, R^*(x^n)/x^n).$$

Для кожного орієнтованого дерева з j вершинами і виділеним коренем можна побудувати два різних дерева, у яких корінь має степінь 1 і які містять $j+1$ вершину. Для цього достатньо додати дугу, що входить у корінь або виходить з кореня початкового дерева, а інший кінець цієї дуги не є вершиною початкового дерева. У термінах твірних функцій маємо: $R^*(x) = 2x R(x)$. Для завершення доведення достатньо скористатися твердженням теореми 4.

Теорема 14. Кількості орієнтованих кореневих дерев при довільному натуральному k задовольняють таке рекурентне співвідношення:

$$R_{j+1} = j^{-1} \sum_{k=1}^j k a_k R_{j-k+1}, \quad \text{де} \quad a_k = 2k^{-1} \sum_{\substack{d|k \\ d < k}} d R_d$$

Доведення. Справдження останньої рівності при довільному натуральному k означає рівність степеневих рядів:

$$\sum_{k=1}^{\infty} a_k x^k = 2 \sum_{l=1}^{\infty} R(x^l) / l.$$

Для завершення доведення теореми потрібно скористатися попередньою теоремою 13 і теоремою 2 про експоненту твірної функції.

Перші 222 члени послідовності $\{R_j\}$ опубліковано за адресою <http://kievoi.narod.ru/lectures/rootort.html>.

11. Перелік орієнтованих дерев

Теорема 15. *Запровадимо такі позначення:*

L_j — кількість різних (неізоморфних) орієнтованих дерев з виділеною дугою, що мають j вершин. Зміст цього позначення у цьому розділі відрізняється від того, що був у розділах 8 і 9;

$$L(x) = \sum_{j=1}^{\infty} L_j x^j \text{ — твірна функція орієнтованих дерев з виділеною дугою.}$$

Маємо: $L(x) = R^2(x)$.

Доведення. Існує взаємно однозначна відповідність між орієнтованими деревами з виділеною дугою та функціями f з двоелементної множини $\{1, 2\}$ у множину всіх орієнтованих дерев з виділеним коренем: орієнтоване дерево з виділеною дугою отримують об'єднанням кореневих дерев $f(1)$ і $f(2)$ та долученням кореневої дуги, спрямованої з кореня $f(1)$ у корінь $f(2)$. Тому при довільному натуральному j справджується така рівність:

$$L_j = \sum_{k=1}^{j-1} T_k T_{j-k}.$$

Помноживши обидві частини останніх двох рівностей на x^j і здійснивши додавання за всіма натуральними j , отримаємо твердження теореми.

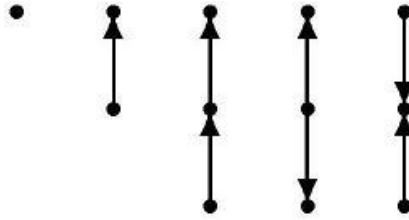


Рис. 4. Неізоморфні орієнтовані дерева, порядок яких не перевищує 3.

Теорема 16. *Запровадимо такі позначення:*

r_j — кількість різних (неізоморфних) орієнтованих дерев, що мають по j вершин;

$$r(x) = \sum_{j=1}^{\infty} r_j x^j = x + x^2 + 3x^3 + \dots \text{ — твірна функція таких орієнтованих дерев.}$$

Тоді ряди $r(x)$ і $R(x)$ задовольняють таку рівність: $r(x) = R(x) - R^2(x)$.

Доведення. Поняття симетричної дуги в орієнтованому графі відсутнє, тому у такому графі справджується рівність $1 = p - b$ у позначеннях теореми 11. Як і для неорієнтованих дерев, з останньої рівності маємо: $r(x) = R(x) - L(x)$, де ряд $L(x)$ перераховує орієнтовані дерева з виділеною дугою і згідно з твердженням теореми 15 дорівнює $R^2(x)$.

Перші 222 члени послідовності $\{r_j\}$ опубліковано за адресою <http://kievoi.narod.ru/lectures/ortree.html>.

Література

1. Харари Ф., Палмер Э. Перечисление графов: Пер. с. англ. — М.: Мир, 1977, 324 с.
2. Cauchy, A. "Memoire sur diverses proprietes remarquables des substitutions regulieres ou irregulieres, et des systemes de substitutions conjugees." Comptes Rendus Acad. Sci. Paris 21, 835, 1845. Reprinted in Ouvres Completes d'Augustin Cauchy, Tome IX. Paris: Gauthier-Villars, 1896, pp. 342-360.
3. Frobenius, F. G. "Uber die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul." J. reine angew. Math. 101, 1887, pp. 273-299. Reprinted in Ferdinand Georg Frobenius Gesammelte Abhandlungen, Band II. Berlin: Springer-Verlag, 1968, pp. 304-330.
4. Redfield, J. Howard. The Theory of Group-Reduced Distributions, American Journal of Mathematics, Vol. 49, No. 3 (Jul., 1927), pp. 433-455.
5. Polya, G. "Kombinatorische Anzahlbestimmungen fur Gruppen, Graphen und chemische Verbindungen". Acta Mathematica, 1937, 68 (1): pp. 145-254.