Дискретная математика

Глава 9. Перечисление непомеченных объектов

А. В. Пастор

29.05.2023

Помеченные и непомеченные объекты

- Во многих комбинаторных задачах ответ и трудность его нахождения существенно зависят от того, рассматриваются ли помеченные или непомеченные объекты.
- Например, сколько существует различных графов на n вершинах? Ответ на этот вопрос зависит от того, какие графы мы будем считать различными.

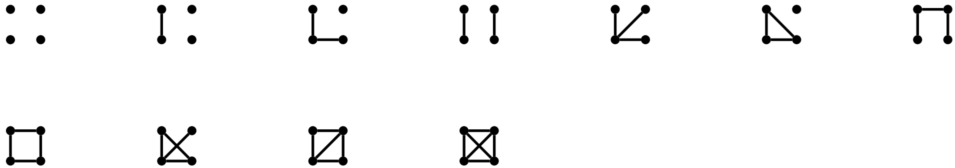
1. Пусть n вершин занумерованы числами от 1 до n. Тогда у нас есть C_n^2 пар вершин, каждую из которых можно соединить или не соединить ребром. Итого, получаем $2^{C_n^2} = 2^{\frac{n(n-1)}{2}}$ различных графов.
   - Графы, все вершины которых занумерованы натуральными числами от 1 до $v(G)$ называют *помеченными*, а полученное выше количество графов — это *число помеченных графов* на n вершинах.
2. Совсем другой результат получается, если никаких пометок на вершинах нет и все вершины считаются идентичными.
   - Напомним, что *изоморфизмом* графов G_1 и G_2 называется биекция $\varphi\colon V(G_1) \to V(G_2)$, удовлетворяющая условию $\forall x, y \in V(G_1)\,(xy \in E(G_1) \longleftrightarrow \varphi(x)\varphi(y) \in E(G_2))$.
   - Сами графы G_1 и G_2 в этом случае называют *изоморфными*. Обозначение: $G_1 \cong G_2$.

Графы с точностью до изоморфизма

- По сути, если мы стираем пометки на вершинах графа, то мы перестаем различать изоморфные друг другу графы. Тогда возникает вопрос о количестве графов *с точностью до изоморфизма*.
    - Легко видеть, что изоморфность двух помеченных графов — это отношение эквивалентности. А интересующее нас количество графов с точностью до изоморфизма — это число классов эквивалентности.

Пример

Есть $2^6 = 64$ помеченных графов на 4 вершинах, но всего 11 попарно неизоморфных графов на 4 вершинах.



Расстановка пометок и автоморфизмы графа

- Посмотрим на этот вопрос с другой стороны. Сколько есть способов расставить пометки на вершинах данного непомеченного графа?
- Другими словами, сколько помеченных графов входят в данный класс эквивалентности?
  - Количество классов эквивалентности было бы легко посчитать, если бы все классы содержали одинаковое число элементов. Однако, это, увы, не так.
  - Например, очевидно, что полный граф является единственным элементом своего класса эквивалентности. Но есть $n(n-1)/2$ помеченных графов на n вершинах ровно с одним ребром — и все они изоморфны.
- Всего есть $n!$ способов расставить пометки на данных n вершинах. Но некоторые из этих способов могут давать один и тот же помеченный граф.
  - То есть граф может оказаться изоморфен сам себе.

Определение

- *Автоморфизмом* графа G называется изоморфизм из G в G.
- Множество всех автоморфизмов графа G обозначается $\mathrm{Aut}(G)$.

Группа автоморфизмов графа

Замечание

• Итак, автоморфизм графа — это перестановка на множестве его вершин, сохраняющая отношение смежности.

• Пусть вершины графа G занумерованы числами от 1 до n. Тогда $\mathrm{Aut}(G) \subset S_n$.

Утверждение

$\mathrm{Aut}(G) < S_n$.

Доказательство. Очевидно, что $e \in \mathrm{Aut}(G)$. Далее нужно проверить замкнутость относительно умножения и взятия обратного элемента.

• Пусть $\varphi, \psi \in \mathrm{Aut}(G)$. Поскольку φ и ψ — биекции, их композиция — также биекция. Далее, для любых $x, y \in V(G)$ имеем
$xy \in E(G) \iff \psi(x)\psi(y) \in E(G) \iff \varphi(\psi(x))\varphi(\psi(y))$.

• Пусть $\varphi \in \mathrm{Aut}(G)$. Поскольку φ — биекция, сохраняющая отношение смежности, то φ^{-1} — также биекция, сохраняющая отношение смежности. $\square$

Группа автоморфизмов и её свойства

Определение

Определенная выше группа $\mathrm{Aut}(G)$ называется *группой автоморфизмов* графа G.

Утверждение

1. *Если* $G_1 \cong G_2$, *то* $\mathrm{Aut}(G_1) \cong \mathrm{Aut}(G_2)$;
2. *для любого графа* G *выполнено* $\mathrm{Aut}(G) \cong \mathrm{Aut}(\overline{G})$.

Замечание

• То есть группы автоморфизмов изоморфных графов всегда изоморфны.

• Но обратное наверное. Например, легко построить граф, не изоморфный своему дополнению. У этих графов группы автоморфизмов будут изоморфны, а сами графы — нет.

• Порядок группы автоморфизмов тесно связан с числом способов расставить пометки на вершинах данного непомеченного графа (или, что тоже самое, с размером класса эквивалентности по отношению изоморфности, содержащего данный помеченный граф).

Группа автоморфизмов и число способов расставить пометки

Лемма

Пусть G — помеченный граф и $n = v(G)$. Тогда существует ровно $\frac{n!}{|\mathrm{Aut}(G)|}$ помеченных графов на том же множестве вершин, изоморфных G.

Доказательство. Не умаляя общности будем считать, что $V(G) = [1..n]$.

- Пусть $\mathcal{G}_n$ — множество всех помеченных графов на множестве $[1..n]$.
- Рассмотрим следующее действие группы S_n на множестве $\mathcal{G}_n$:
  - для любых $\sigma \in S_n$ и $H \in \mathcal{G}_n$ обозначим через σH граф с $V(\sigma H) = [1..n]$ и $E(\sigma H) = \{\sigma(x)\sigma(y) \mid xy \in E(H)\}$.
- Тогда
  - $\langle G \rangle$ — множество всех графов на множестве $[1..n]$, изоморфных G;
  - $\mathrm{St}(G) = \mathrm{Aut}(G)$.
- Следовательно, по теореме из курса алгебры получаем, что

$$|\langle G \rangle| = \frac{|S_n|}{|\mathrm{St}(G)|} = \frac{n!}{|\mathrm{Aut}(G)|}.$$

$\square$

Задачи о раскрашивании ожерелья

- Сейчас мы отложим на некоторое время задачу о перечислении непомеченных графов и рассмотрим две более простые задачи о перечислении непомеченных объектов.

1. На окружности расставлены n точек, разбивающие её на равные дуги. Сколькими способами можно раскрасить эти точки в a цветов, если раскраски, отличающиеся друг от друга поворотом окружности, считаются одинаковыми?
   - Как обычно, под раскраской множества M в a цветов мы понимаем отображение $c: M \to [1..a]$.
   - Неформальная формулировка: Дана карусель с n одинаковыми кабинками. Сколькими способами можно раскрасить кабинки в a цветов?
2. Тот же вопрос, но одинаковыми считаются раскраски, отличающиеся либо поворотом, либо осевой симметрией.
   - Неформальная формулировка: Дано ожерелье с n одинаковыми бусинками. Ожерелье можно как угодно поворачивать и переворачивать. Сколькими способами можно раскрасить бусинки в a цветов?

Простой частный случай задачи о каруселях

Утверждение

Пусть $p \in \mathbb{P}$. Тогда существует ровно $\frac{a^p-a}{p} + a = \frac{a^p+(p-1)a}{p}$ раскрасок p точек на окружности в a цветов, если раскраски, отличающиеся друг от друга поворотом окружности, считаются одинаковыми.

Доказательство. Занумеруем все точки в порядке обхода по часовой стрелке числами от 0 до $p-1$.

- Номера точек мы будем рассматривать по модулю p.
  - То есть можно считать, что мы нумеруем точки элементами кольца $\mathbb{Z}/p\mathbb{Z}$.
- Тогда поворот окружности на угол $\frac{2\pi k}{n}$ переводит точку с номером i в точку номер $i+k$.
  - Число k также можно рассматривать как элемент кольца $\mathbb{Z}/p\mathbb{Z}$.
  - То есть всего получаем p различных поворотов.
- Рассмотрим произвольную раскраску $c\colon \mathbb{Z}/p\mathbb{Z} \to [1..a]$ точек окружности в a цветов.

Простой частный случай задачи об ожерелье

- Докажем, что для раскраски c выполнено ровно одно из следующих двух утверждений:
  - либо раскраска не изменяется ни при каком повороте (и тогда цвета всех точек одинаковы);
  - либо все p возможных поворотов приводят к различным раскраскам.
- Пусть раскраска c не изменилась при повороте на угол $\frac{2\pi k}{n}$, где $0 < k < p$.
  - Тогда $c(0) = c(k) = c(2k) = \ldots = c((p-1)k)$.
  - Заметим, что $0, k, 2k, \ldots, (p-1)k$ — это все элементы кольца $\mathbb{Z}/p\mathbb{Z}$.
  - Следовательно, цвета всех точек при раскраске c одинаковы.
- Всего есть a^p различных раскрасок помеченных точек. Среди них есть a одноцветных. Остальные $a^p - a$ раскрасок разбиваются на $\frac{a^p-a}{p}$ классов эквивалентности, по p раскрасок в каждом.
- Итого, получаем $\frac{a^p-a}{p} + a$ раскрасок с точностью до поворота. $\square$

Следствие (Малая теорема Ферма)

Пусть $a \in \mathbb{N}$ *и* $p \in \mathbb{P}$. *Тогда* $a^p - a \,\vdots\, p$.

Классы эквивалентности и действие группы на множестве

- Описанный выше метод трудно применять к общему случаю задачи о раскраске ожерелья (или карусели), поскольку при составном n возможны нетривиальные раскраски, переходящие в себя при повороте на ненулевой угол.
- Поэтому давайте посмотрим на эти задачи с точки зрения теории групп.
- Во всех задачах о перечислении непомеченных объектов мы ищем количество классов эквивалентности, на которые разбивается множество помеченных объектов.
- Классы эквивалентности образуются в результате применения к помеченным объектам некоторых преобразований. Как правило, эти преобразования образуют группу.
  - В случае задачи о раскраски карусели, преобразование — это поворот;
  - в случае задачи о раскраски ожерелья — поворот или осевая симметрия;
  - в случае задачи о перечислении графов, преобразование – это любая перестановка на множестве его вершин.
- В любом из этих случаев, мы имеем дело с действием некоторой группы на множестве помеченных объектов. Интересующие нас классы эквивалентности — это орбиты элементов множества при данном действии.

Лемма Бернсайда

Определение

Пусть задано действие группы A на множестве X. Тогда для любого $\alpha \in A$

- $\mathrm{Fix}(\alpha) \stackrel{\mathrm{def}}{=} \{x \in X \mid \alpha x = x\}$ — *множество неподвижных точек* элемента α;
- элементы множества $\mathrm{Fix}(\alpha)$ — *неподвижные точки* элемента α.

Утверждение

$$\sum_{\alpha \in A} |\mathrm{Fix}(\alpha)| = \sum_{x \in X} |\mathrm{St}(x)|.$$

Доказательство. Обе части равны $|\{(\alpha, x) \in A \times X \mid \alpha x = x\}|$. □

Теорема (Лемма Бернсайда)

Количество орбит действия группы A на множестве X равно $\frac{1}{|A|} \sum_{\alpha \in A} |\mathrm{Fix}(\alpha)|$.

Доказательство. Присвоим каждому элементу $x \in X$ вес $w(x) \stackrel{\mathrm{def}}{=} \frac{1}{|\langle x \rangle|}$.

- Тогда сумма весов элементов любой орбиты равна 1.

Доказательство леммы Бернсайда

- Следовательно, сумма весов всех элементов множества X равна количеству орбит (обозначим его N).
- Тогда $N = \sum\limits_{x \in X} \frac{1}{|\langle x \rangle|} = \sum\limits_{x \in X} \frac{|\mathrm{St}(x)|}{|\langle x \rangle||\mathrm{St}(x)|} = \frac{1}{|A|} \sum\limits_{x \in X} |\mathrm{St}(x)| = \frac{1}{|A|} \sum\limits_{\alpha \in A} |\mathrm{Fix}(\alpha)|$. $\square$

Замечание

Доказанное выше утверждение обычно называют леммой Бернсайда. Но оно было известно и ранее. Сам William Burnside в своей книге “Theory of Groups of Finite Order” 1897 года называл первооткрывателем этой леммы Фробениуса. Но судя по всему, это утверждение было известно еще раньше.

Задача о каруселях: общий случай

Теорема

Пусть $a, n \in \mathbb{N}$. Тогда существует ровно $\frac{1}{n}\sum\limits_{d|n}\varphi(\frac{n}{d})a^d$ раскрасок n точек на окружности в a цветов, если раскраски, отличающиеся друг от друга поворотом окружности, считаются одинаковыми.

Доказательство. Как и ранее, занумеруем точки на окружности элементами кольца $\mathbb{Z}/n\mathbb{Z}$.

- Пусть $X = \{c \mid c\colon \mathbb{Z}/n\mathbb{Z} \to [1..a]\}$ — множество всех раскрасок точек в a цветов.
- Повороты окружности можно рассматривать как действие циклической группы C_n порядка n на этом множестве.
  - Пусть образующая ε группы C_n соответствует повороту на угол $\frac{2\pi}{n}$.
  - Тогда элемент ε^k соответствует повороту на угол $\frac{2\pi k}{n}$.
- Пусть раскраска c является неподвижной точкой для элемента ε^k.
- Докажем, что раскраска c является d-периодичной, где $d = (k, n)$ (т. е. что $\forall i\,(c(i) = c(i + d))$).

Задача о каруселях: общий случай

- Пусть $d = sk + tn$ — линейное представление НОД.
- Тогда $c(i) = c(i + sk) = c(i + sk + tn) = c(i + d)$.
- Обратно, любая d-периодичная раскраска, очевидно, является неподвижной точкой для элемента ε^k.
- Итак, $\mathrm{Fix}(\varepsilon^k)$ — это в точности множество всех d-периодичных раскрасок, где $d = (k, n)$.
- Тогда $|\mathrm{Fix}(\varepsilon^k)| = a^d$, поскольку любая d-периодичная раскраска однозначно задается цветами точек $0, 1, \ldots, d - 1$.
- Следовательно, по лемме Бернсайда, число раскрасок с точностью до поворота равно $\frac{1}{n}\sum\limits_{k=0}^{n-1} a^{(k,n)}$.
- Далее, запишем числа k и n в виде $k = k_1 d$ и $n = n_1 d$. Тогда $(k_1, n_1) = 1$. То есть число k_1 можно выбрать $\varphi(n_1)$ способами. Следовательно, существует ровно $\varphi(\frac{n}{d})$ таких k, что $d = (k, n)$.
- Таким образом, число раскрасок равно $\frac{1}{n}\sum\limits_{k=0}^{n-1} a^{(k,n)} = \frac{1}{n}\sum\limits_{d|n} \varphi(\frac{n}{d}) a^d$. $\square$

Задача об ожерелье: общий случай

Теорема

Пусть $a, n \in \mathbb{N}$. Обозначим через $B(n, a)$ количество раскрасок n точек на окружности в a цветов, если раскраски, отличающиеся друг от друга поворотом окружности или осевой симметрией, считаются одинаковыми. Тогда

- $B(n,a) = \frac{1}{2n}\sum\limits_{d|n}\varphi(\frac{n}{d})a^d + \frac{a^k}{2}$, *при* $n = 2k-1$;
- $B(n,a) = \frac{1}{2n}\sum\limits_{d|n}\varphi(\frac{n}{d})a^d + \frac{a^k(a+1)}{4}$, *при* $n = 2k$.

Доказательство. В отличии от предыдущей теоремы, здесь нужно рассматривать на множестве всех раскрасок действие группы D_n.

- D_n — это *группа самосовмещений правильного n-угольника* или *диэдральная группа*.
- В этой группе $2n$ элементов: n из них соответствуют поворотам, оставшиеся n — осевым симметриям.
- Также эту группу можно представлять себе как группу автоморфизмов цикла на n вершинах.

Задача об ожерелье: общий случай

- Мы уже знаем, что число неподвижных точек поворота на угол $\frac{2\pi k}{n}$ равно $a^{(k,n)}$.
- Посчитаем число неподвижных точек для осевой симметрии. То есть количество раскрасок, симметричных относительно данной оси.
  - При $n = 2k - 1$ любая ось симметрии проходит через одну из отмеченных точек. Остальные $2k - 2$ точки разбиваются на пары симметричных. Точки в каждой паре должны быть одного цвета. Итого, нам нужно выбрать цвета k точек: по одной точке в каждой паре и точки, лежащей на оси симметрии. Таких раскрасок a^k.
  - При $n = 2k$ оси симметрии бывают двух видов: $n/2$ осей не проходят через отмеченные точки и $n/2$ проходят через две отмеченные точки. В первом случае раскраска однозначно задается выбором цветов k точек, а во втором — выбором цветов $k + 1$ точки. То есть в первом случае получаем a^k раскрасок, а во втором — a^{k+1}.

Задача об ожерелье: общий случай

- Тогда при $n = 2k - 1$ получаем, что

$$B(n,a) = \frac{1}{2n}\left(\sum_{k=0}^{n-1} a^{(k,n)} + na^k\right) = \frac{1}{2n}\sum_{d|n}\varphi(\tfrac{n}{d})a^d + \frac{a^k}{2}.$$

- А при $n = 2k$ получаем

$$B(n,a) = \frac{1}{2n}\left(\sum_{k=0}^{n-1} a^{(k,n)} + \frac{n}{2}a^k + \frac{n}{2}a^{k+1}\right) = \frac{1}{2n}\sum_{d|n}\varphi(\tfrac{n}{d})a^d + \frac{a^k(a+1)}{4}. \qquad \square$$

Асимптотика числа графов с точностью до изоморфизма

- Введем следующие обозначения.
  - G_n — число помеченных графов на n вершинах;
  - g_n — число графов на n вершинах с точностью до изоморфизма.
- Мы уже знаем, что $G_n = 2^{\frac{n(n-1)}{2}}$.
- Оказывается, что g_n примерно в $n!$ раз меньше.
  - Неформально это означает, что почти у всех графов группа автоморфизмов тривиальна (т. е. состоит из единственного элемента: тождественного преобразования).

Теорема

$g_n \sim \frac{G_n}{n!} = \frac{2^{\frac{n(n-1)}{2}}}{n!}$.

Доказательство. Пусть $\mathcal{G}_n$ — множество всех помеченных графов на множестве вершин $V = [1..n]$.

- Как и ранее, рассмотрим следующее действие группы S_n на множестве $\mathcal{G}_n$:
  - для любых $\sigma \in S_n$ и $H \in \mathcal{G}_n$ обозначим через σH граф с $V(\sigma H) = V$ и $E(\sigma H) = \{\sigma(x)\sigma(y) \mid xy \in E(H)\}$.

Асимптотика числа графов с точностью до изоморфизма

- Нам нужно посчитать число неподвижных точек для перестановки $\sigma \in S_n$.
- Для этого рассмотрим множество $V^{(2)}$ двухэлементных подмножеств множества V.
  - Другими словами, $V^{(2)}$ — это множество ребер полного графа K_n на множестве вершин V.
- Заметим, что группа S_n действует также и на множестве $V^{(2)}$: $\sigma \cdot xy \stackrel{\text{def}}{=} \sigma(x)\sigma(y)$. Тем самым, каждая перестановка $\sigma \in S_n$ индуцирует перестановку $\sigma' \in S(V^{(2)})$, а группа S_n индуцирует подгруппу $S_n^{(2)} < S(V^{(2)})$, состоящую из всех перестановок множества $V^{(2)}$ вида σ'.
  - Группа $S_n^{(2)}$ называется *парной группой* группы S_n.
  - Фактически, мы построили гомоморфизм групп $S_n \to S(V^{(2)})$. Группа $S_n^{(2)}$ — это образ данного гомоморфизма.
  - Нетрудно проверить, что при $n > 2$ группы S_n и $S_n^{(2)}$ изоморфны.
- Для перестановки $\sigma \in S_n$ нас будут интересовать циклы соответствующей ей перестановки $\sigma' \in S_n^{(2)}$. Эти циклы мы будем называть *рёберными циклами* перестановки σ.

Асимптотика числа графов с точностью до изоморфизма

- Заметим, что граф $G \in \mathcal{G}_n$ является неподвижной точкой для перестановки $\sigma \in S_n$, если и только если для любого рёберного цикла C перестановки σ либо $C \subset E(G)$, либо $C \cap E(G) = \varnothing$.
- Тем самым, $|\mathrm{Fix}(\sigma)| = 2^{q(\sigma)}$, где $q(\sigma)$ — число рёберных циклов перестановки σ.
- Тогда по лемме Бернсайда, $g_n = \frac{1}{n!} \sum\limits_{\sigma \in S_n} 2^{q(\sigma)}$.
- Обозначим через $S_{n,k}$ множество перестановок из S_n, имеющих ровно $n-k$ неподвижных точек.
- Пусть $g_n^{(k)} = \frac{1}{n!} \sum\limits_{\sigma \in S_{n,k}} 2^{q(\sigma)}$. Тогда $g_n = \sum\limits_{k=0}^{n} g_n^{(k)}$.
  - Очевидно, что $g_n^{(0)} = \frac{1}{n!} 2^{\frac{n(n-1)}{2}}$.
  - То есть нам нужно доказать, что $g_n \sim g_n^{(0)}$.

Асимптотика числа графов с точностью до изоморфизма

Лемма

Если $\sigma \in S_{n,k}$, *то* $q(\sigma) \le C_n^2 + \frac{1}{2}(k - nk + \frac{k^2}{2})$.

Доказательство. Пусть перестановка σ имеет t рёберных циклов длины 1.

- Тогда оставшиеся $\frac{n(n-1)}{2} - t$ пар вершин разбиты на рёберные циклы длины хотя бы 2.
- Следовательно, рёберных циклов длины хотя бы 2 не более $\frac{n(n-1)}{4} - \frac{t}{2}$.
- Это означает, что $q(\sigma) \le \frac{n(n-1)}{4} - \frac{t}{2} + t = \frac{n(n-1)}{4} + \frac{t}{2}$.
- Осталось заметить, что рёберными циклами длины 1 перестановки σ могут быть лишь
  - пары из двух неподвижных точек перестановки σ (их $\frac{(n-k)(n-k-1)}{2}$);
  - пары вершин, образующих цикл длины 2 перестановки σ (их не более, чем $\frac{k}{2}$).
- Итого, $t \le \frac{(n-k)(n-k-1)}{2} + \frac{k}{2} = \frac{n^2-2nk+k^2-n+2k}{2} = \frac{n(n-1)}{2} + (k - nk + \frac{k^2}{2})$.
- Таким образом, $q(\sigma) \le \frac{n(n-1)}{4} + \frac{t}{2} \le \frac{n(n-1)}{2} + \frac{1}{2}(k - nk + \frac{k^2}{2})$. $\square$

Асимптотика числа графов с точностью до изоморфизма

- Заметим, что $|S_{n,k}| \le C_n^k \cdot k! = \frac{n!}{(n-k)!} \le n^k$.
- Тогда $g_n^{(k)} \le \frac{1}{n!}|S_{n,k}|2^{C_n^2+\frac{1}{2}(k-nk+\frac{k^2}{2})} \le g_n^{(0)} n^k 2^{\frac{k}{2}(1-n+\frac{k}{2})} \le$

$$\le g_n^{(0)}\left(\frac{n}{2^{\frac{1}{2}(n-1-\frac{k}{2})}}\right)^k \le g_n^{(0)}\left(\frac{n}{2^{\frac{n-2}{4}}}\right)^k = g_n^{(0)}\left(\frac{n\sqrt{2}}{2^{\frac{n}{4}}}\right)^k.$$

- Следовательно, $1 \le \frac{g_n}{g_n^{(0)}} \le \sum_{k=0}^{n}\left(\frac{n\sqrt{2}}{2^{\frac{n}{4}}}\right)^k \le \frac{1}{1-\frac{n\sqrt{2}}{2^{\frac{n}{4}}}} \xrightarrow[n\to\infty]{} 1$.
- Тогда по теореме о двух милиционерах $\frac{g_n}{g_n^{(0)}} \xrightarrow[n\to\infty]{} 1$,

а это и означает, что

$$g_n \sim g_n^{(0)} = \frac{G_n}{n!} = \frac{2^{\frac{n(n-1)}{2}}}{n!}.$$

$\square$