Лекция 5: упорядоченные множества

Дискретная математика, ВШЭ, факультет компьютерных наук

(Осень 2014 – весна 2015)

1 Отношения порядка

Отношения порядка возникают, когда мы хотим сравнивать элементы множеств. При этом мы ожидаем от результатов сравнения свойств, похожих на свойства сравнения чисел по величине. В зависимости от того, насколько много свойств мы хотим сохранить, получаются более или менее далёкие обобщения.

Начнём с того, что укажем свойства, которые мы хотим сохранить обязательно. Это свойство транзитивности: если a «меньше» b, b «меньше» c, то a «меньше» c. И свойство *антирефлексивности*: неверно, что a «меньше» a.

Назовём транзитивное и антирефлексивное отношение *отношением строгого частичного порядка*. Используем обычный знак строгого сравнения для такого отношения. Тогда два свойства, которые мы указали, запишутся так:

$$\text{Свойства строгого частичного порядка:} \quad \begin{cases} a \not< a, \\ (a < b) \text{ и } (b < c) \text{ влечет } a < c. \end{cases} \tag{1}$$

Слово «частичный» в названии отношения подчёркивает, что не все пары сравнимы.

Пример 1 (Покоординатное сравнение векторов.)**.** Часто приходится сравнивать альтернативы, которые задаются не одним числом, а несколькими. Один из самых распространённых способов сравнения в таком случае таков.

Зададим порядок на последовательностях чисел длины n таким образом:

$$(x_1, \dots, x_n) < (y_1, \dots y_n)$$

тогда и только тогда, когда для любого i выполняется либо $x_i = y_i$, либо $x_i < y_i$, причём хотя бы в одной координате сравнение строгое.

Последнее уточнение гарантирует антирефлексивность. Транзитивность легко проверяется разбором случаев.

При этом легко видеть, что $(1, 2) \not< (2, 1)$ и $(2, 1) \not< (1, 2)$, то есть эти пары несравнимы.

Пример 2. На подмножествах некоторого множества U определено отношение строгого включения $A \subset B$. Легко видеть, что это отношение строгого частичного порядка.

Множества в общем положении ($A \setminus B \neq \varnothing$ и $B \setminus A \neq \varnothing$) в этом отношении несравнимы.

Эти примеры показывают техническое несовершенство нашего определения: приходится при проверке свойств строгого порядка разбирать разные случаи сочетания равенства и строгого неравенства. По этой причине принято использовать родственное понятие нестрогого порядка (так же, как это мы делаем с числами): $x \leqslant y$ (x «меньше или равно» y) означает, что $x < y$ или $x = y$.

Отношение частичного порядка получается из отношения строгого частичного порядка указанным выше способом. Но такие отношения несложно задать и набором свойств:

$$\text{Свойства частичного порядка:} \quad \begin{cases} a \leqslant a, & \text{рефлексивность;} \\ \text{если } (a \leqslant b) \text{ и } (b \leqslant a), \text{ то } a = b, & \text{антисимметричность;} \\ (a \leqslant b) \text{ и } (b \leqslant c) \text{ влечет } a \leqslant c, & \text{транзитивность.} \end{cases} \tag{2}$$

Из такого определения видно, что, выбросив из отношения пары (a, a), получим отношение строгого частичного порядка. И наоборот, если по отношению строгого порядка определить отношение «меньше или равно» как описано выше, то для него очевидно выполняются рефлексивность и транзитивность. Антисимметричность чуть менее очевидна, но легко проверяется. Для этого полезно заметить, что одновременное выполнение сравнений $a < b$ и $b < a$ невозможно (по транзитивности из них следует $a < a$). Значит, из $a \leqslant b$ и $b \leqslant a$ следует выполнение равенства.

Замечание 1. Для обычного сравнения чисел отношения «меньше или равно» и «не больше» совпадают. В общем случае это не так. Скажем множество $\{1, 2\}$ «не больше» множества $\{2, 3\}$ в порядке включения подмножеств. Но неверно, что $\{1, 2\}$ «меньше или равно» $\{2, 3\}$ в том же порядке.

Для краткости мы дальше называем порядком пару $(P, \leqslant)$ из множества и отношения частичного порядка на нем.

Если любые два элемента порядка сравнимы ($x \leqslant y$ или $y \leqslant x$), такой порядок называется *линейным* (хотя по аналогии с функциями его нужно бы называть тотальным, но терминология уже устоялась).

2 Операции с порядками

Из одних порядков можно получать другие с помощью операций.

Пример 1 демонстрирует операцию *покоординатного произведения порядков*. Покоординатный порядок на $P \times Q$ задаётся правилом:

$$(p_1, q_1) \leqslant (p_2, q_2) \text{ по определению означает } p_1 \leqslant p_2 \text{ и } \; q_1 \leqslant q_2.$$

Пример 3 (покоординатный порядок на словах)**.** Напомним, что слова — это конечные последовательности элементов некоторого множества A (которое называется алфавитом, а его элементы — символами).

Во многих случаях алфавит упорядочен и даже линейно упорядочен (числа, буквы латиницы или кириллицы). В этом случае слова одинаковой длины сравниваются покоординатно.

Покоординатное произведение линейных порядков не обязательно линейно (пример 1). Поэтому используется ещё одно определение произведения: лексикографическое. Лексикографический порядок на $P \times Q$ задаётся правилом:

$$(p_1, q_1) \leqslant (p_2, q_2) \text{ по определению означает, что } (p_1 < p_2) \text{ или } \; (p_1 = p_2) \text{ и } (q_1 \leqslant q_2).$$

Лексикографическое произведение линейных порядков линейно. Дальше мы по умолчанию предполагаем лексикографический порядок на $P \times Q$.

Лексикографическое произведение определено не только для декартовых степеней P^n, но и для «бесконечной декартовой степени» $P^{\mathbb{N}}$, то есть на множестве бесконечных последовательностей элементов частичного порядка P.

Пример 4 (лексикографический порядок на всех словах)**.** Лексикографическое произведение задаёт линейный порядок на словах одинаковой длины.

А как сравнивать слова разной длины? Общепринятый способ, применяемый в словарях, таков: если слово u является началом слова w, то $u \leqslant w$. Если ни одно из слов u, v не является началом другого, то найдётся позиция, в которой эти слова различаются. Тогда меньше то слово, в котором на этой позиции стоит меньший символ.

То же самое правило получится, если добавить к алфавиту ещё один символ — пробел — и считать его наименьшим символом в алфавите. Слову в исходном алфавите сопоставим бесконечную последовательность в новом алфавите, которая начинается с символов слова и продолжается пробелами.

Легко видеть, что описанное выше правило задаётся лексикографическим сравнением полученных бесконечных последовательностей. Поэтому указанный порядок на всем множестве слов также называют лексикографическим.

Мы уже видели, что произведение порядков можно определять по-разному. То же самое и с суммой. Сумма порядков определяется для порядков, заданных на непересекающихся множествах. Если нужно сложить два порядка, множества которых пересекаются, то нужно изготовить копию одного из порядков на элементах, не входящих в множество второго порядка и лишь потом их складывать.

Самый осторожный способ определить сумму порядков — это больше ничего не делать. (Пары элементов из разных порядков несравнимы.) Недостаток этого способа в том, что он не сохраняет свойство линейности порядка.

Второй способ состоит в том, чтобы объявить все элементы первого порядка меньшими элементов второго порядка. При таком определении сумма линейных порядков является линейным порядком.

Пример 5. Рассмотрим сумму $\mathbb{N}+\mathbb{N}$. Её элементами будут обычные натуральные числа и их «копии». Копию числа n обозначим n'. Тогда полученный линейный порядок выглядит так:

$$0 < 1 < 2 < \dots < n < \dots < 0' < 1' < \dots .$$

Есть ещё один общий способ получить из одного порядка другой: ограничение на подмножество. Если множество X является подмножеством частичного порядка P, то отношение частичного порядка, *индуцированное* на X порядком P задаётся так: x меньше или равно y если это выполняется в порядке P. Так мы получаем, например, порядок на каждом подмножестве действительных чисел, ограничивая общий порядок сравнения чисел.

3 Какие порядки считать «одинаковыми»?

Рассмотрим два порядка: порядок на подмножествах n-элементного множества по включению и покоординатный порядок на двоичных словах длины n. Это два разных отношения, заданные на разных множествах. Но по сути они одинаковы. Вспомним, что между подмножествами множества $\{1,\dots,n\}$ и двоичными словами длины n есть биекция: подмножеству S сопоставляется слово x_S, в котором на i-й позиции стоит 1 тогда и только тогда, когда $i \in S$.

Эта биекция «уважает» порядок: если $A \subseteq B$, то $x_A \leqslant x_B$ в отношении покоординатного порядка.

Поэтому естественно рассматривать два таких порядка как разные записи одного и того же. Для точных рассуждений используется специальный термин «изоморфизм».

Определение 1. Порядки P и Q называются *изоморфными*, если есть такая биекция $\varphi\colon P \to Q$, что $x \leqslant y$ равносильно $\varphi(x) \leqslant \varphi(y)$ для всех пар x, y.

Чтобы установить изоморфизм порядков достаточно указать такую биекцию. А как обосновать неизоморфность порядков? Разбирать все мыслимые биекции? Это затруднительно даже для конечных порядков.

Есть другой способ — указать различающее порядки *инвариантное* свойство. Если в формулировке свойства используются только сравнения пар элементов, то такое свойство должно сохраняться при изоморфизме.

Одним из простейших инвариантных свойств является наличие *минимального* элемента: такого элемента, что нет меньшего его. Аналогично определяется *максимальный* элемент.

В некоторых порядках минимальные элементы есть (скажем, порядок, индуцированный сравнением чисел на отрезке $[0,1]$). В других минимальных элементов нет (индуцированный на интервале $(0,1)$ порядок). Поэтому порядок на отрезке неизоморфен порядку на интервале.

Есть близкие понятия *наибольшего* и *наименьшего* элементов, которые нужно не путать с максимальными и минимальным элементами. Наименьший элемент меньше всех других элементов в порядке, наибольший — больше всех других.

Для линейных порядков эти понятия совпадают. В общем случае это не так.

Пример 6. Рассмотрим два единичных квадрата на координатной плоскости $\mathbb{R}^2$:

$$P = \{(x,y) : 0 \leqslant x \leqslant 1,\ 0 \leqslant y \leqslant 1\}, \qquad Q = \{(x,y) : |x| + |y| \leqslant \frac{1}{\sqrt{2}}\}$$

и порядки на них, индуцированные покоординатным порядком на $\mathbb{R}^2$.

В порядке P есть наименьший элемент $(0,0)$, он же единственный минимальный. В порядке Q наименьшего элемента нет, а минимальных — бесконечно много, весь отрезок между вершинами $(-1/\sqrt{2}, 0)$ и $(0, -1/\sqrt{2})$.

На порядки обобщается определение отрезка числовой прямой. Пусть $x \leqslant y$, тогда отрезком с концами x, y называется множество

$$[x,y] = \{z : x \leqslant z \leqslant y\}$$

и порядок, индуцированный на этом множестве.

Изоморфизм порядков должен порождать изоморфизм отрезков. В частности, отрезку из конечного числа элементов должен соответствовать отрезок из конечного числа элементов.

Поэтому $\mathbb{Z}$ неизоморфен $\mathbb{Q}$: в первом случае все отрезки конечны, а во втором — все бесконечны.

Порядок $\mathbb{Z}$ неизоморфен (линейному) порядку $\mathbb{Z} + \mathbb{Z}$: во втором случае есть бесконечные отрезки, скажем, $[0, 0']$.

Два элемента x, y называют соседними, если между ними нет других элементов (то есть ни один элемент z не удовлетворяет сразу двум неравенствам $x < z < y$). Отрезок с концами в соседних элементах состоит в точности из своих концов.

Если соседних элементов нет, то порядок называется *плотным*. Примеры плотных порядков — $\mathbb{Q}$, $\mathbb{R}$.

Поскольку между любыми двумя элементами плотного порядка есть ещё хотя бы один, любой отрезок плотного порядка бесконечен.

4 Конечные линейные порядки

Проще всего разобраться с конечными линейными порядками.

Лемма 1. *В конечном линейном порядке есть наибольший и наименьший элементы.*

Доказательство. Рассмотрим *убывающие цепи*: последовательности элементов порядка $x_1 > x_2 > \dots$, в которой каждый следующий элемент меньше предыдущего. Будем дополнять убывающую цепь новыми элементами, пока это возможно. Поскольку всего элементов конечное число, процесс рано или поздно остановится. Последний элемент такой убывающей цепи обязан быть наименьшим: в противном случае её можно было бы продолжить.

Аналогичное рассуждение с *возрастающими цепями* показывает существование наибольшего элемента. $\square$

Теорема 1. *Все конечные линейные порядки с одинаковым числом элементов изоморфны.*

Доказательство. Индукция по числу элементов. База — один элемент в порядке — очевидна.

Индуктивный переход. Предположим, что все линейные порядки с n элементами изоморфны. Рассмотрим два линейных порядка P и Q. Выделим в них наименьшие элементы p_0, q_0. Порядки на оставшихся элементах изоморфны по предположению индукции. Продолжая этот изоморфизм соответствием $p_0 \mapsto q_0$, получаем искомый изоморфизм порядков P и Q. $\square$

5 Порядки и индукция

Принцип математической индукции можно переформулировать таким образом:

> **Математическая индукция «без базы».** *Пусть для утверждения $A(n)$, зависящего от натурального параметра n, для любого n верно утверждение «если $A(m)$ верно при всех $m < n$, то и $A(n)$ верно». Тогда утверждение $A(n)$ верно при любом n.*

Отсутствие базы индукции тут мнимое. База скрыта в более сложном индуктивном предположении. Действительно, для $n = 0$ посылка условного индуктивного предположения всегда истинна (так как нет натуральных чисел, меньших n). Поэтому $A(0)$ обязано быть истинным.

В формулировке принципа математической индукции используется порядок на натуральных числах. Разберёмся, какие свойства этого порядка существенны для справедливости принципа математической индукции.

Теорема 2. *Следующие свойства порядка P равносильны:*

1° каждое непустое подмножество имеет минимальный элемент;

2° любая убывающая цепь конечна;

3° для порядка P справедлив принцип индукции: если для утверждения $A(p)$, зависящего от элемента порядка, для любого p верно утверждение «если $A(q)$ верно при всех $q < p$, то и $A(p)$ верно». Тогда утверждение $A(p)$ верно при любом $p \in P$.

Доказательство. Из 1 следует 2. Это равносильно тому, что из отрицания 2 следует отрицание 1. Возьмём бесконечную убывающую цепь $y_1 > y_2 > \dots$. По определению в ней нет минимального элемента.

Из 2 следует 1 будем доказывать аналогично, проверив, что из отрицания 1 следует отрицание 2. Возьмём множество X без минимальных элементов и построим бесконечную убывающую цепь. Выберем какой-нибудь $x_0 \in X$. Он не минимален, поэтому есть $x_1 < x_0$. Аналогично рассуждаем с x_1 и так далее. Получаем бесконечную убывающую цепь.

Теперь выведем принцип индукции для P из существования минимальных элементов. Рассмотрим множество тех x, для которых не выполняется $A(x)$. Если оно непусто, в нем есть минимальный элемент m. Но тогда для всех $y < m$ утверждение $A(y)$ верно и в силу предположения индукции $A(m)$ тоже верно. Получили противоречие, так как по выбору m утверждение $A(m)$ ложно. Значит, имеет место единственная оставшаяся возможность: множество тех x, для которых не выполняется $A(x)$, пусто.

Осталось сделать ещё одну проверку: что из принципа индукции следует существование минимальных элементов в непустых множествах. Предположим, что множество X не имеет минимальных элементов. Возьмём в качестве утверждения $A(p)$ такое: $p \notin X$.

Индуктивное предположение выполняется: если для всех $q < p$ выполняется $q \notin X$, то и $p \notin X$ (иначе p — минимальный элемент). Поэтому $p \notin X$ для всех p, то есть $X = \varnothing$. □

Определение 2. Множество, удовлетворяющее условиям теоремы 2, называется *фундированным*.

Приведём примеры фундированных множеств, отличных от множества натуральных чисел.

Первый пример: лексикографическое произведение $\mathbb{N} \times \mathbb{N}$. В убывающей цепи пар натуральных чисел первые компоненты будут одинаковыми, начиная с некоторого места (так как $\mathbb{N}$ фундированное). Начиная с этого места, вторые компоненты образуют убывающую цепь в $\mathbb{N}$. Поэтому любая убывающая цепь в $\mathbb{N} \times \mathbb{N}$ конечна.

Точно такое же рассуждение показывает, что лексикографическое произведение любых фундированных множеств фундировано. Поэтому всякое $\mathbb{N}^d$ фундировано.

Покажем как использовать индукцию по фундированному множеству на примере известной олимпиадной задачи.

Задача 1. Купец заключил сделку с чёртом: каждый день он отдаёт черту одну монету и получает взамен любое количество монет меньшего достоинства. Брать монеты из других источников купцу запрещается. Когда монет не останется, купец проигрывает черту (душу).

Докажите, что черт выигрывает при любых действиях купца.

Состояние купца в любой момент времени выражается набором натуральных чисел

$$(n_1, n_2, \ldots, n_d),$$

где d — количество видов монет, n_1 — количество монет наибольшего номинала, n_2 — количество монет следующего номинала и т.д.

Тогда из условия задачи сразу следует, что состояние купца каждый день уменьшается в лексикографическом порядке. Поскольку бесконечных убывающих цепей нет, купец рано или поздно останется без монет.

6 Антицепи

Мы уже пользовались понятием цепи. Цепь — это линейный порядок. *Антицепь* — это множество попарно несравнимых элементов.

Неформально говоря, цепи и антицепи отвечают за «высоту» и «ширину» порядка. Более строго это соотношение демонстрирует следующее утверждение.

Задача 2. В конечном порядке на $mn + 1$ элементах есть либо конечная цепь размера $n + 1$, либо конечная антицепь размера $m + 1$.

Решение. Множество максимальных элементов порядка образует антицепь.

Построим такое разбиение элементов некоторого конечного порядка P_1. Первое множество разбиения M_1 — это максимальные элементы P_1. Отбросив эти элементы, получим порядок $P_2 = P_1 \setminus M_1$. Множество максимальных элементов этого порядка обозначим M_2. Продолжая этот процесс, получаем разбиение $P_1 = M_1 \cup M_2 \cup \cdots \cup M_h$, где

$$P_{i+1} = P_i \setminus M_i, \quad M_i \text{ — максимальные элементы } P_i.$$

Заметим, что по определению для любого немаксимального элемента x в любом порядке найдётся максимальный элемент y, который больше x. Это позволяет построить возрастающую цепь $y_h < y_{h-1} < \cdots < y_1$, в которой $y_i \in M_i$, то есть из каждого множества разбиения взято по одному элементу. Для этого начнём с любого $y_h \in M_h$. Найдём для него максимальный в порядке P_{h-1} элемент y_{h-1}, который больше y_h, и так далее.

Осталось сделать простое арифметическое наблюдение: если в порядке на N элементах размер любой антицепи не превосходит s, то для построенного разбиения должно выполняться неравенство $N \leqslant sh$, то есть в этом порядке есть цепь длины $\geqslant N/s$. □

Задача 3. Докажите, что в любом бесконечном порядке есть либо бесконечная цепь, либо бесконечная антицепь.

Есть более точная характеризация наибольшего размера антицепи в порядке через свойства цепей порядка.

Теорема 3 (Дилуорс)**.** *Наибольший размер антицепи в порядке равен наименьшему количеству цепей в разбиениях порядка на непересекающиеся цепи.*

Доказательство. В одну сторону очевидно: если порядок разбит на k непересекающихся цепей, то любая антицепь пересекается с каждой из цепей не более чем по одному элементу и в антицепи не больше k элементов.

В другую сторону сложнее. Индукция по числу элементов в порядке. База — порядок из одного элемента — очевидно выполнена.

Пусть утверждение теоремы справедливо для порядков с количеством элементов не больше n.

Рассмотрим порядок P, в котором $n+1$ элемент. В любом конечном порядке есть минимальные элементы. Пусть m — минимальный элемент в порядке P. Отбрасывая этот элемент, получаем порядок Q, для которого утверждение теоремы выполнено. Обозначим наибольший размер антицепи в Q через s. По предположению индукции порядок Q можно разбить на s непересекающихся цепей.

Наибольший размер антицепи в P либо равен s, либо равен $s+1$. В последнем случае m содержится в антицепи размера $s+1$ и порядок P легко разбивается на $s+1$ цепь: одна состоит только из элемента m, а остальные разбивают Q на s непересекающихся цепей.

Осталось рассмотреть случай, когда наибольший размер антицепи в P равен s. Элемент m тогда сравним с какими-то элементами порядка Q, а поскольку он минимальный, то он меньше каких-то элементов.

Выберем такой элемент $q \in Q$, что $m < q$, а все элементы, меньшие q в цепи C разбиения Q на s непересекающихся цепей, не входят в антицепи размера s.

Выделим цепь, состоящую из m и всех элементов цепи C, начиная с q и больше. Порядок на оставшихся элементах не содержит антицепей размера s (так как любая такая антицепь обязана пересекать остаток от цепи C) и в нем не больше n элементов. Значит, для этого порядка утверждение теоремы справедливо и его можно разбить на $s-1$ непересекающуюся цепь. Добавляя выделенную цепь, получаем разбиение исходного порядка P на s цепей.

Таким образом, утверждение теоремы справедливо и для порядка P. По принципу математической индукции теорема справедлива для всех конечных порядков. $\square$

С помощью теоремы Дилуорса легко решить задачу 2.