МГТУ им. Н.Э. Баумана

Кафедра «Теоретическая информатика и компьютерные технологии»

Порядки и фундированность

Вводная лекция по ДМА

А.Н. Непейвода

a_nevod@mail.ru, ***@TonitaN***

Частичный порядок

Каркас определения

Бинарное отношение $\prec$ на множестве P ($\prec \subseteq P \times P$) определяет порядок, если оно:

- транзитивно: $\forall a, b, c \in P(a \prec b \wedge b \prec c \Rightarrow a \prec c)$;
- антисимметрично: $\forall a, b \in P(a \prec b \wedge b \prec a \Rightarrow a = b)$

Поведение на диагонали (элементах $(a, a) \in P \times P$):

- строгий порядок: $\forall a \in P(\neg(a \prec a))$ — антирефлексивность;
- нестрогий порядок: $\forall a \in P(a \prec a)$ — рефлексивность.

Частичный порядок

Каркас определения

Бинарное отношение $\prec$ на множестве P ($\prec \subseteq P \times P$) определяет порядок, если оно:

- транзитивно: $\forall a, b, c \in P(a \prec b \wedge b \prec c \Rightarrow a \prec c)$;
- антисимметрично: $\forall a, b \in P(a \prec b \wedge b \prec a \Rightarrow a = b)$

То есть частичный порядок соответствует отношению достижимости в ориентированном графе без циклов, за исключением, возможно, петель.

Граф, соответствующий порядку:

Порядок: $a \prec b$, $a \prec c$, $c \prec e$, $d \prec e$, $\underbrace{a \prec e}_{a \prec c \wedge c \prec e}$.

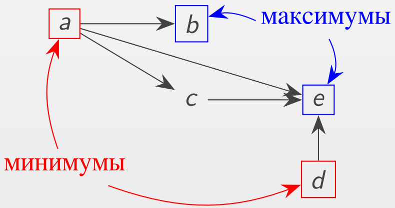

Диаграмма Хассе

Удобно перерисовать граф, изоморфный порядку, удалив визуальный мусор:

- рёбра — каркас, по которому однозначно восстанавливается достижимость;
- расположение вершин — минимумы снизу, максимумы сверху.

Какой-то граф, соответствующий порядку:

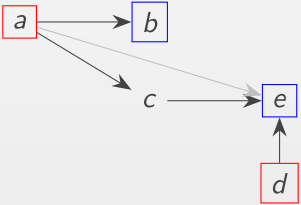

Диаграмма Хассе:

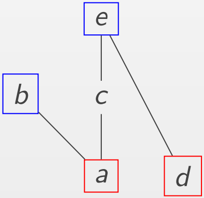

Диаграмма Хассе

Определение

Пусть P — множество элементов, $R \subset P \times P$ — отношение частичного порядка на нём. Диаграммой Хассе для пары $\langle P, R \rangle$ называется неориентированный граф $\langle V, E \rangle$ такой, что:

- множество вершин V есть P;
- $(a, b) \in E$ **только если** $(a, b) \in R \ \wedge a \neq b \wedge \ \nexists c \in P (c \neq a \wedge c \neq b \wedge (a, c) \in R \wedge (c, b) \in R)$;
- если $(a, b) \in R$, то вершина a располагается в графе ниже вершины b. Обратное не обязательно выполняется.

Диаграммы Хассе и запрещённые подграфы

Если G — диаграмма Хассе, то в G запрещены подграфы-треугольники K_3 (это необходимое, но не достаточное свойство).

Связные диаграммы Хассе, в которых запрещены ветвления, описывают порядки, позволяющие сравнивать любые два элемента: формально $\forall a, b \in P(a \prec b \vee b \prec a)$. Такие порядки называются линейными (и их граф Хассе — это цепочка).

Какие ещё запрещённые подграфы в диаграммах Хассе приводят к полезным свойствам порядков, ими описываемых? Важный класс таких порядков будет приведён чуть позже.

Несколько примеров

- диаграммы без рёбер: $\begin{cases} \varnothing \text{ — пустой строгий частичный порядок} \\ a \preceq b \iff a = b \text{ — нестрогий порядок} \end{cases}$
- Все конечные линейно упорядоченные множества одного размера имеют одну и ту же структуру. Если P — конечное множество, и все его элементы сравнимы, то диаграмма Хассе такого порядка — цепочка из $|P| - 1$ звеньев.
- Если P бесконечно, то даже линейно его можно упорядочить по-разному.

В стиле $\mathbb{N}$:

В стиле $\mathbb{Z}^-$:

В стиле $\mathbb{Z}$:

В стиле $(a_1, b_1) \prec (a_2, b_2) \iff a_1 < a_2 \vee (a_1 = a_2 \wedge b_1 < b_2)$ на $\mathbb{N} \times \mathbb{N}$

Примеры практичных частичных порядков

- Стандартные порядки ($<$, $\leq$) на множествах чисел ($\mathbb{N}$, $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{Q}$ и их подмножества).
- Любые порядки, основанные на оценке структур в $\mathbb{N}$:
  - слов по длине
  - графов по числу вершин и рёбер
  - многочленов по старшей степени
  - фигур по площади, et cetera
- Словарный порядок слов, заданный линейным порядком на их алфавите (лексикографический):
  $a_1 w_1 \prec a_2 w_2 \iff a_1 \prec a_2 \vee (a_1 = a_2 \wedge w_1 \prec w_2)$. Пустое слово предполагается наименьшим.
- Структурные порядки:
  - слов по отношению вхождения
  - натуральных чисел по делимости
  - множеств по включению, et cetera

Зачем порядки программисту?

Алгоритм	Свойство порядка
Быстрый доступ к элементам упорядоченных множеств и сравнение таких множеств	линейность
Рекурсия "от большего к меньшему"	???
Итерация "пока есть изменения"	???

Полезно формализовать свойство завершимости вычислений по рекурсии — если они согласованы с порядком, в котором не может быть бесконечных убывающих цепей (как в $<$ на $\mathbb{N}$), то завершимость строго обоснована.

Фундированный порядок

Скажем, что пара $\langle P, \prec \rangle$ задаёт фундированное ("хорошо основанное") множество, если любое подмножество множества P имеет минимальный элемент.
Эквивалентное определение: граф Хассе отношения не содержит бесконечных цепей вниз, подграф "в стиле $\mathbb{Z}^-$"запрещён.

Фундированные

- $\langle \mathbb{N}, < \rangle$
- Конечные деревья, порядок "быть поддеревом"
- Множество строк, порядок "быть префиксом"

Не фундированные

- $\mathbb{Z}$ (целые числа): $0 > -1 > -2 > \cdots$
- $(0, 1]$ рациональные: $1 > \frac{1}{2} > \frac{1}{3} > \cdots$
- Множество строк, словарный порядок: $b > ab > abb > \cdots$

Доказательство эквивалентности определений

$1 \Rightarrow 2$: Если любое подмножество имеет минимум, нет бесконечных убывающих цепей

- Предположим, есть бесконечная убывающая цепь: $a_1 > a_2 > a_3 > \cdots$
- Рассмотрим множество $S = \{a_1, a_2, a_3, \dots\}$
- По условию 1, S имеет минимальный элемент a_k
- Но тогда $a_k > a_{k+1} > \cdots$ — противоречие с минимальностью a_k

$2 \Rightarrow 1$: Если нет бесконечных убывающих цепей, любое подмножество имеет минимум

- Возьмём любое непустое $S \subseteq P$
- Выберем $a_1 \in S$
- Если a_1 минимален — доказано
- Иначе существует $a_2 < a_1$, $a_2 \in S$
- Продолжая, получим цепь $a_1 > a_2 > a_3 > \cdots$
- По условию 2, цепь конечна $\Rightarrow$ последний элемент минимален

Свойства практичных частичных порядков

- Порядки, основанные на оценке структур в $\mathbb{N}$:

$$\left\{\begin{array}{l}\text{слов по длине}\\ \text{графов по числу вершин и рёбер}\\ \text{многочленов по старшей степени}\\ \text{фигур по площади, et cetera}\end{array}\right. \quad \text{—} \quad \begin{array}{l}\text{обычно нелинейны,}\\ \text{но фундированы}\end{array}$$

- Лексикографический порядок:
  $a_1 w_1 \prec_{lex} a_2 w_2 \iff a_1 \prec a_2 \vee (a_1 = a_2 \wedge w_1 \prec w_2)$. Линеен, не фундирован. Shortlex-порядок:
  $w_1 \prec_{slex} w_2 \iff |w_1| < |w_2| \vee (|w_1| = |w_2| \wedge w_1 \prec_{lex} w_2)$.
  Линеен и фундирован.
- Структурные порядки:

$$\left\{\begin{array}{l}\text{слов по отношению вхождения}\\ \text{натуральных чисел по делимости}\\ \text{множеств по включению, et cetera}\end{array}\right. \quad \text{—} \quad \begin{array}{l}\text{обычно нелинейны,}\\ \text{фундированны}\end{array}$$

Индукция по фундированному порядку

Формулировка

Пусть $(P, \leq)$ — фундированное множество. Чтобы доказать, что свойство $Q(x)$ верно для всех $x \in P$, достаточно доказать:

$$\forall x \in P \left(\forall y \left(y < x \Rightarrow Q(y) \right) \Rightarrow Q(x) \right)$$

- Основание индукции скрыто: Для минимальных элементов посылка $\forall y(y < x \Rightarrow Q(y))$ верна всегда
- Требуется доказать $Q(x)$ для минимальных элементов напрямую
- Обобщение полной математической индукции на произвольные фундированные множества

Важность учёта всех минимумов

Ложное утверждение

$\forall x Q(x)$: "Любое натуральное число, большее 1, либо равно 2, либо составное"

1. База индукции для минимума: для 2 утверждение тривиально истинно.
2. Индукционное предположение: Выберем фундированный порядок $\prec$ по отношению делимости
3. Шаг: Рассмотрим элемент x и произвольный y такой, что $y \prec x$
4. Поскольку мы предполагаем, что $Q(y)$, то y либо равен 2, либо составной. Значит, $x = k \cdot y$ $(k > 1)$ уж тем более составной.
5. Ошибка: Выбор минимума по порядку $<$, а индукция по порядку $\prec$. Проигнорированы почти все минимумы по $\prec$ — нечётные простые числа.

Важность свойства фундированности

Ложное утверждение

$\forall x(x > 0)$ на целых числах со стандартным порядком $\dots < -2 < -1 < 0 < 1 < 2 < \cdots$

1. Индукционное предположение: $\forall y(y < x \Rightarrow Q(y)) \Rightarrow Q(x)$ верно! У каждого числа найдётся меньшее его отрицательное число. Поэтому $\forall y(y < x \Rightarrow (y > 0))$ ложно для всех x, а из лжи следует всё что угодно.
2. Можем "заключить", что все числа неотрицательны

Применения индукции

Теоретические

- Теория множеств (индукция по $\in$)
- Теория доказательств (индукция по длине вывода)
- Теория рекурсии
- Теория графов (индукция по подграфам)

Практические

- Доказательство корректности алгоритмов
- Анализ программ с рекурсией
- Доказательство завершаемости
- Структурная индукция в формальных методах