Лекция 1

Основные определения и примеры (09.09.2010)

(Конспект: А. Бешенов)

1.1 Введение. Основные определения

(Детерминированный) алгоритм решает (индивидуальную) задачу, давая правильный ответ. Проверять его не надо, и нас интересует лишь чтобы время работы было поменьше.

Напротив, доказательство — это то, что любой посторонний наблюдатель может эффективно проверить. Для нас "эффективно" означает "за полиномиальное время" (от длины доказательства и доказываемого утверждения). Само доказательство при этом может быть весьма длинным (хотя мы и заинтересованы, чтобы оно было покороче).

Главным образом нас будет интересовать сложность (то есть длина) доказательств для формул логики высказываний, хотя доказывать можно элементы любого другого языка, например, доказывать, что два данных графа не являются изоморфными.

Пример 1.1. Рассмотрим вопрос: является ли формула $x \vee (\overline{x} \wedge y) \vee (\overline{x} \wedge \overline{y})$ тавтологией (т.е. верно ли, что она истинна для любых значений переменных x и y)? "Общематематическое" доказательство того, что это тавтология, может выглядеть так:

$$x \vee \overline{x}$$
$$\vdots$$
$$x \vee (\overline{x} \wedge \text{true})$$
$$\vdots$$
$$x \vee (\overline{x} \wedge (y \vee \overline{y}))$$
$$\vdots$$
$$x \vee ((\overline{x} \wedge y) \vee (\overline{x} \wedge \overline{y}))$$

Мы применяли известные нам аксиомы (правило исключённого третьего, дистрибутивность логических операций) в произвольном порядке, никакого алгоритма при этом не применяя. Однако всякий может быстро проверить это доказательство очевидным алгоритмом (особенно если мы укажем в каждом случае, какое именно правило мы применяли).

Как правило, формальные системы доказательств, использующиеся в учебниках по математической логике, в качестве пропозиционального фрагмента содержат то, что в сложности доказательств называется "системами Фреге".

Определение 1.1. *Системой Фреге* называется любая система, которая включает некоторые правила, например

$$\frac{F \qquad G}{F \wedge G}, \qquad\qquad \frac{F \qquad F \supset G}{G},$$

и некоторые аксиомы, например

$$\frac{}{F \vee \neg F}.$$

При применении этих правил и аксиом $F, G, \ldots$ могут заменяться на произвольные формулы, состоящие из логических переменных и выбранного (фиксированного для данной системы) множества операций (например, $\vee, \wedge, \supset, \neg$, и т. д., допустимы любые операции $\{\mathrm{false}, \mathrm{true}\}^k \to \{\mathrm{false}, \mathrm{true}\}$). (Конечно, не всякий набор правил и аксиом составляет разумную систему доказательств, об этом мы поговорим позже.)

Пример 1.2. Пример системы Фреге: язык со связками $\kappa = \{\neg, \vee, \wedge, \supset\}$, правилом вывода *modus ponens*

$$\frac{P \quad P \supset Q}{Q}$$

и следующим набором аксиом:

$$\begin{gathered}
(P \wedge Q) \supset P, \\
(P \wedge Q) \supset Q, \\
P \supset (P \vee Q), \\
Q \supset (P \vee Q), \\
(P \supset Q) \supset ((P \supset \neg Q) \supset \neg P), \\
(\neg\neg P) \supset P, \\
P \supset (Q \supset P \wedge Q), \\
(P \supset R) \supset ((Q \supset R) \supset (P \vee Q \supset R)), \\
P \supset (Q \supset P), \\
(P \supset Q) \supset (P \supset (Q \supset R)) \supset (P \supset R).
\end{gathered}$$

Пример 1.3. Другой пример системы Фреге — *Гильбертовская система* (вернее, её пропозициональная часть) с тремя аксиомами:

1. $P \supset (Q \supset P)$,
2. $(\neg Q \supset \neg P) \supset ((\neg Q \supset P) \supset Q)$,
3. $(P \supset (Q \supset R)) \supset ((P \supset Q) \supset (P \supset R))$;

и правилом вывода modus ponens.

Разные системы Фреге могут различаться по длине доказательств (но, как мы узнаем далее, «разумные» системы Фреге имеют доказательства сходной длины).

От системы доказательств разумно требовать *полноту* (все тавтологии выводимы) и *корректность* (противоречия не выводимы).

Помимо языка тавтологий TAUT, конечно, можно рассматривать и другие — например, язык не разрешимых в целых числах уравнений.

Дадим теперь формальные определения.

Определение 1.2. *Системой доказательств* для языка L называется полиномиальный по времени алгоритм проверки доказательств для строк этого языка. Пусть V — такой алгоритм.

Система доказательств называется *корректной*, если

$$\forall x \ (\exists \pi \ (V(x, \pi) = 1 \Rightarrow x \in L)),$$

где x — строка в языке, π — доказательство.

Система доказательств называется *полной*, если

$$\forall x \ (x \in L \Rightarrow \exists \pi \ V(x, \pi) = 1)\,.$$

Говоря в дальнейшем "система доказательств", мы будем иметь в виду корректную и полную систему.

Имеется также классическое определение (Cook, Reckhow, 70-е гг.):

Определение 1.3. *Системой доказательств* называется сюръективное полиномиальное по времени отображение строк в доказываемый язык:

$$\Pi\colon \{0,1\}^* \twoheadrightarrow L.$$

Это определение практически[1] эквивалентно предыдущему (в частности, сюръективность означает полноту системы). Отображение выдает тот элемент языка, который был доказан, если доказательство верное, и какой-то фиксированный простой элемент языка, если доказательство неверное.

Алгоритм есть частный случай системы доказательств: доказательством является протокол работы алгоритма, а проверку делает сам же алгоритм, убеждаясь в том, что последовательность шагов правильная (на самом деле, вместо протокола достаточно написать столько единичек, каково было время работы; тогда вновь запущенный алгоритм отработает время, ограниченное длиной такого "доказательства", и убедится, что принял за это время входную строку). Система доказательств

[1] До тех пор, пока нас всё интересует с точностью до полинома от длины доказательства и длины доказываемой строки.

не обязательно является алгоритмом — мы можем не знать, как находить доказательство за время, полиномиальное от его длины.

Существуют языки, для которых имеются системы с короткими доказательствами, например, уравнения, разрешимые в целых числах (в противоположность неразрешимым, здесь достаточно предъявить корни).

Определение 1.4. Система доказательств V для языка L называется *полиномиально ограниченной*, если имеется такой полином p, что для каждой строки $x \in L$ имеется доказательство π (т.е. $V(x, \pi) = 1$) длины, не превосходящей $p(|x|)$.

Класс языков **NP** (известный многим из курса теории сложности) может быть эквивалентно определён как класс языков, с полиномиально ограниченными системами доказательств. Нас интересует класс дополнительных задач **co-NP**, то есть языков L, таких что для $\overline{L}$ существует полиномиально ограниченная система доказательств. Следующее утверждение является очевидным следствием определений.

Утверждение 1.1. **NP** = **co-NP** *тогда и только тогда, когда существует полиномиально ограниченная система доказательств для каждого языка из* **co-NP**.

Из того, что язык булевых тавтологий является **co-NP**-полным (иначе говоря, задача выполнимости булевых формул `SAT` является **NP**-полной, см. курс теории сложности), следует, что достаточно найти полиномиально ограниченную систему для этого языка.

Утверждение 1.2. **NP** = **co-NP** *тогда и только тогда, когда существует полиномиально ограниченная система доказательств для языка булевых тавтологий.*

Помимо вопроса о существовании полиномиально ограниченной системы доказательств для языка булевых тавтологий, могут быть интересны и другие. Возможно, для какого-то интересного не **co-NP**-полного языка полиномиально ограниченная система всё-таки есть. Интересно также рассматривать задачи из других классов, например **PSPACE**: истинные булевы формулы с кванторами $\forall$ и $\exists$, интуиционистские тавтологии и т. д.

1.2 Примеры систем доказательств

Пример 1.4 (Метод резолюций)**.** Формула F является тавтологией тогда и только тогда, когда $\overline{F}$ невыполнима. Как хорошо известно из теории сложности, выполнимость достаточно выяснять для формул в *конъюнктивной нормальной форме* (КНФ), таких как

$$(x \vee y \vee z) \wedge (\overline{x} \vee y \vee z) \wedge (x \vee \overline{y} \vee \overline{z}),$$

остальные к ним сводятся (напоминание см. ниже).

Резолюцией называется правило

$$\frac{(x \vee \alpha) \quad (\overline{x} \vee \beta)}{\alpha \vee \beta},$$

полученная новая дизъюнкция *резольвентой* двух прежних.

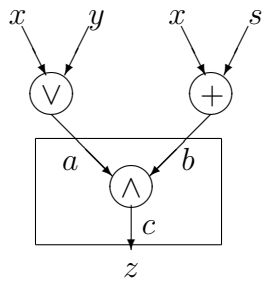
Если, применяя такие правила к дизъюнкциям (исходным и выведенным нами), мы получим

$$\frac{P \quad \overline{P}}{\text{false}},$$

то доказательство невыполнимости готово, поскольку, очевидно, если существовал набор значений, выполнявший исходные дизъюнкции, то он же должен выполнять и все выведенные (в частности, тождественно ложную false). Такой метод доказательства называется *методом резолюций*.

(Заметим, что хорошего алгоритма, который находит оптимальный порядок резолюций, у нас нет.)

Пример 1.5. Напомним, как из произвольной логической формулы построить КНФ, которая будет выполнима тогда и только тогда, когда исходная формула была выполнима. Возьмем дерево для нужной функции, припишем каждому ребру новую переменную и запишем для каждой вершины конъюнкцию нескольких дизъюнкций, означающую, что выходная переменная этой вершины правильно вычислена по входным. Также добавим $\ldots \wedge z$ для результата всего дерева.



$$\begin{aligned}&(\overline{c} \vee a) \wedge\\ &(\overline{c} \vee b) \wedge\\ &(\overline{a} \vee \overline{b} \vee c) \wedge\\ &\vdots\\ &z\end{aligned}$$

Итак, для доказательства тавтологичности любых формул достаточно уметь доказывать невыполнимость формул в КНФ.

Пример 1.6 (Nullstellensatz)**.** Снова доказываем невыполнимость формулы в КНФ, но переделаем эту формулу в систему полиномиальных уравнений.

- От булевых переменных перейдем к переменным, принимающим целые значения 0 и 1.
- $\neg x$ заменим на $(1 - x)$.
- Все дизъюнкции $a \vee b \vee c \vee \cdots$ заменим многочленами $(1 - a)\,(1 - b)\,(1 - c) \cdots$
- Также введем для каждой переменной x многочлен $x^2 - x$.

Тогда булева формула невыполнима тогда и только тогда, когда полученные многочлены p_i не имеют общего корня.

Используем *теорему Гильберта о нулях* (*Nullstellensatz*; слабая форма): многочлены не имеют общего корня над алгебраически замкнутым полем тогда и только тогда, когда в порожденном идеале лежит постоянный многочлен 1. То есть, существуют такие многочлены g_i, что

$$\sum_i p_i\, g_i \equiv 1.$$

Множество $\{g_i\}$ и является доказательством в системе *Nullstellensatz*.

Пример 1.7 (Секущие плоскости)**.** Будем работать с системами линейных неравенств.

Дизъюнкции вида $(\overline{a} \vee b)$ заменяются неравенствами $(1-a)+b \geq 1$, где $1 \geq a \geq 0$; рассматриваются целые решения.

В системе *секущих плоскостей* (*Cutting Plane*) используется два правила вывода:

$$\frac{A \geq 0 \quad B \geq 0}{k\,A + l\,B \geq 0}, \qquad \frac{k\,A \geq l}{A \geq \lceil l/k \rceil},$$

где k и l — положительные целые числа.

Доказательство будет завершено, как только мы получим противоречие $-1 \geq 0$.

Пример 1.8. В качестве важного в дальнейшем примера рассмотрим *принцип Дирихле* (*pigeon-hole principle*, *PHP*). Пусть переменная x_{ij} означает, что i-й кролик $(1 \leq i \leq n+1)$ сидит в j-й клетке $(1 \leq j \leq n)$.

Условие, что i-й кролик где-то сидит:

$$\bigvee_j x_{ij}.$$

Условие, что два кролика не могут сидеть в одной клетке:

$$\neg x_{ij} \vee \neg x_{i'j}.$$

Из этих условий следует противоречие (кроликов больше, чем клеток).

Известно, что у принципа Дирихле не существует доказательств полиномиальной длины при помощи метода резолюций (Хакен, 80-е гг.). Но в системе секущих плоскостей такое доказательство есть.

Теорема 1.1. *В системе секущих плоскостей принцип Дирихле имеет доказательство полиномиальной длины.*

Доказательство. Переменная x_{ij} означает, что i-й кролик $(1 \leq i \leq n+1)$ сидит в j-й клетке $(1 \leq j \leq n)$.

Условие, что i-й кролик где-то сидит:

$$\sum_j x_{ij} \geq 1. \qquad (*)$$

Условие, что два кролика не могут сидеть в одной клетке:

$$x_{ij} + x_{i'j} \leq 1.$$

Вывод в системе секущих плоскостей:

$$\dfrac{\dfrac{\dfrac{x_{ij}+x_{i'j}\le 1 \quad x_{i'j}+x_{i''j}\le 1 \quad x_{i''j}+x_{ij}\le 1}{2\left(x_{ij}+x_{i'j}+x_{i''j}\right)\le 3}}{x_{ij}+x_{i'j}+x_{i''j}\le 1}}{\vdots}}{\sum_i x_{ij}\le 1}$$

Этот вывод имеет полиномиальную длину[2].

Всего, складывая по j, имеем

$$\sum_{i\,j} x_{i\,j} \le m,$$

но условие (*) дает (после сложения по i)

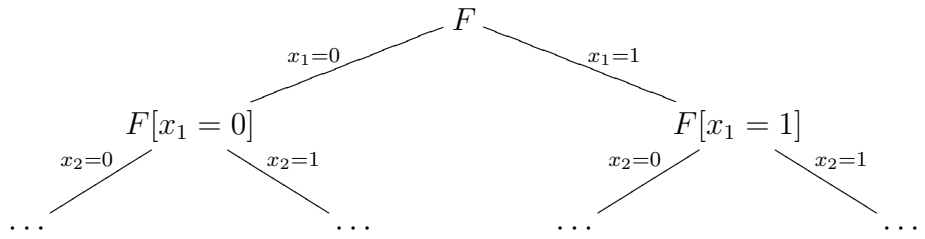
$$\sum_{ij} x_{ij} \ge m+1.$$

Получили противоречие. □

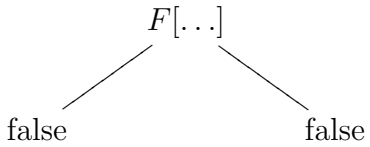
1.2.1 Полнота систем доказательств

Теорема 1.2. *Метод резолюции является полным.*

Доказательство. Сначала рассмотрим, как выглядит доказательство невыполнимости формулы через разбор случаев. Изобразим это в виде дерева:



В результате должны получиться листья вида



Теперь индуктивно преобразуем это в доказательство резолюцией. База индукции очевидна. В качестве шага индукции предположим, что $F[x_1=0]$ доказывается резолюцией, в которой участвуют формулы $A, B, C, \ldots$, и которая заканчивается false. Если дополнить каждую дизъюнкцию этого доказательства переменной x_1,

[2]Упражнение: объясните, как именно следует продолжить вывод вместо многоточия, чтобы его длина получилась полиномиальной

получится снова корректный резолюционный вывод $A \vee x_1, B \vee x_1, C \vee x_1, \ldots$, заканчивающийся x_1. Заметим, что в этом выводе используются "аксиомы" из исходной формулы F (раз уж с отрезанным x_1 они встречались в формуле $F[x_1 = 0]$).

Аналогично выводится $\overline{x_1}$.

Далее переход индукции завершает резолюция

$$\frac{x_1 \quad \overline{x_1}}{\text{false}}.$$

□

Теорема 1.3. *Метод секущих плоскостей является полным.*

Доказательство. Покажем, как из доказательства методом резолюций можно получить доказательство методом секущих плоскостей.

Резолюции можно поставить в соответствие первое правило метода секущих плоскостей.

$$\frac{x \vee \alpha \qquad \overline{x} \vee \beta}{\alpha \vee \beta} \quad \mapsto \quad \frac{x + \alpha \geq 1 \qquad (1 - x) + \beta \geq 1}{\alpha + \beta \geq 1}$$

Но здесь есть проблема: в методе секущих плоскостей перед переменными могут стоять какие-то коэффициенты. Например, если в указанном правиле α и β одновременно содержат z, то $\alpha + \beta$ содержит $2z$.

Но от коэффициента в $2z$ можно избавиться. Пусть γ есть сумма "литералов" γ_i, то есть переменных либо отрицаний переменных (возможно, с натуральными коэффициентами). Мы знаем, что $\gamma \geq 0$. Имеем вывод в системе секущих плоскостей:

$$\frac{\dfrac{\gamma + 2z \geq 1}{2\gamma + 2z \geq 1}}{\gamma + z \geq 1}$$

(Здесь использовано второе правило метода секущих плоскостей.) □

Теорема Гильберта о нулях дает нам следующий результат.

Теорема 1.4. *Система Nullstellensatz является полной.*