Лекция 2

Системы Фреге (23.09.2010)

(Конспект: А. Бешенов)

"Программа Кука" заключается в том, чтобы доказывать нижние оценки для всё более сильных систем.

Определение 2.1. Пусть S и W — системы доказательств для одного и того же языка L.

Говорят, что S *моделирует* W (обозначение $S \leq W$), если S-доказательства не длиннее W-доказательств с точностью до полинома p.

Иными словами, для всякого $F \in L$ выполняется $|\pi_S| \leq p(|\pi_W|)$, где π_S и π_W — кратчайшие доказательства F в системах S и W соответственно.

Замечание 2.1. При сравнении систем доказательств важно, что они рассматриваются как системы для одного и того же языка.

Определение 2.2. Говорят, что S *строго моделирует* W (обозначение $S < W$), если $S \leq W$ и $\neg(W \leq S)$.

Пример 2.1. Система секущих плоскостей строго моделирует резолюцию. Строгость можно показать на принципе Дирихле.

Определение 2.3. Говорят, что система S *p-моделирует* W, если за полиномиальное время W-доказательство размера w переводится в S-доказательство для той же строки (очевидно, полиномиального размера).

2.1 Системы Фреге

Напомним, что из себя представляют системы Фреге.

Определение 2.4. *Система Фреге* состоит из корректных правил вида

$$\frac{F_1 \quad \cdots \quad F_k}{G},$$

где F_i и G — формулы логики высказываний, на место переменных в которых могут подставляться другие формулы.

Вывод начинается с аксиом, т. е. правил, для которых $k = 0$. Новые формулы выводятся правилами из ранее выведенных. Отношение выводимости за одно правило обозначается $\vdash$. Рефлексивное транзитивное замыкание отношения выводимости обозначается $\vdash^*$.

Правила могут позволять выводить формулы с тем или иным набором связок (например, $\{\supset, \neg\}$ или $\{\vee, \neg, \oplus\}$; допустимы и k-арные связки для любой константы k). Этот набор связок называется *базисом*.

Пример 2.2. Следующая система Фреге содержит четыре правила, три из которых — аксиомы.

$$\frac{}{P \supset (Q \supset P)} \quad \text{(AX I)}$$

$$\frac{}{(\neg Q \supset \neg P) \supset ((\neg Q \supset P) \supset Q)} \quad \text{(AX II)}$$

$$\frac{}{(P \supset (Q \supset R)) \supset ((P \supset Q) \supset (P \supset R))} \quad \text{(AX III)}$$

$$\frac{P \quad P \supset Q}{Q} \quad \text{(MP)}$$

Определение 2.5. Система доказательств для языка L называется *полной*, если для всякой формулы $F \in L$ в системе существует доказательство.

(Для системы Фреге "существует доказательство" соответствует $\vdash^* F$.)

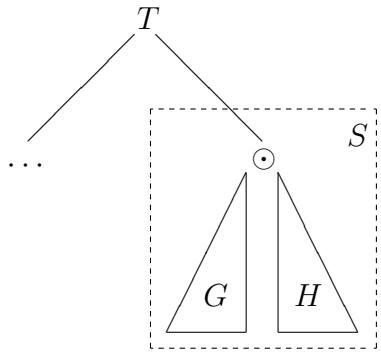
Определение 2.6. Система Фреге называется *импликативно полной*, если для всяких формул F и G, таких что $F \supset G$, также выполняется $F \vdash^* G$.

Теорема 2.1. *Все корректные полные и импликативно полные системы Фреге полиномиально p-эквивалентны (т. е. p-моделируют друг друга).*

Доказательство (схема). Если системы работают с формулами в одном базисе, то достаточно моделировать каждое правило по отдельности; правила корректны, а импликативная полнота моделирующей системы гарантирует нам наличие вывода в ней. При подстановке в этот вывод формул вместо переменных, которые были в правилах, вывод остаётся корректным. Поскольку правила константного размера, каждое из них будет моделироваться за константное число шагов; при этом общий размер вывода увеличивается в константу.

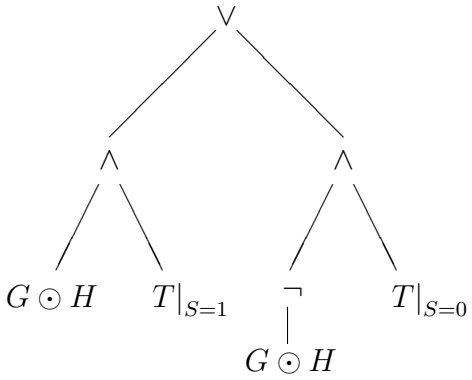
В общем случае базисы различные, и возникает необходимость переписывания формул, которое нельзя произвести наивным образом: например, переход от $\bigoplus_i x_i$ к формуле в базисе $\{\vee, \wedge, \neg\}$ дает экспоненциальное раздутие. Мы будем использовать непрямое переписывание формул.

Для простоты будет считать, что мы имеем дело с бинарными связками (с другими связками всё делается аналогично, только дерево формулы разбивается в другой пропорции). Пусть формуле F соответствует дерево T, и там есть поддерево S, корень которого находится в узле с меткой $\odot$.



Тогда можно записать эквивалентную формулу

$$F' = ((G \odot H) \wedge T|_{S=1}) \vee (\neg(G \odot H) \wedge T|_{S=0}). \qquad (*)$$



Нам потребуется вспомогательное утверждение:

Во всяком дереве T найдется узел $\odot$, которому соответствует дерево S, такое что

$$\frac{1}{3}|T| \le |S| \;\; и \;\; |T \setminus S| \le \frac{2}{3}|T|\,.$$

Иначе говоря, мы можем делить дерево «примерно пополам».

После преобразований вида (*) получится дерево, в котором все операции производятся на нижнем уровне, а всего уровней $O(\log n)$.

Остается только научиться работать с представлениями в такой сбалансированной форме — например, нужно доказать, что $b(F_1) \wedge b(F_2) \equiv b(F_1 \wedge F_2)$ (где $b(F)$ — сбалансированная форма для формулы F). □

2.2 Секвенциальное исчисление

Определение 2.7. *Секвенцией* называется запись $F_1, \ldots, F_k \to G_1, \ldots, G_l$, где F_i и G_i — пропозициональные формулы.

Такая запись означает

$$\bigwedge_{1\le i\le k} F_i \supset \bigvee_{1\le j\le l} G_j.$$

Определение 2.8. *Секвенциальное* (*генценовское*) *исчисление* есть система, в которой доказательства представляют собой последовательности секвенций, каждая из которых выводится из предшествующих при помощи следующих правил:

$$\frac{}{F \to F} \qquad \text{(Аксиома)}$$

$$\frac{\Gamma \to \Delta}{F, \Gamma \to G, \Delta} \qquad \text{(Ослабление)}$$

Введение $\vee$, $\wedge$ и $\neg$:

$$\frac{\Gamma \to F, \Delta}{\Gamma \to F \vee G, \Delta} \quad \frac{F, \Gamma \to \Delta \quad G, \Gamma \to \Delta}{F \vee G, \Gamma \to \Delta}$$

$$\frac{E, \Gamma \to \Delta}{F \wedge G, \Gamma \to \Delta} \quad \frac{\Gamma \to F, \Delta \quad \Gamma \to G, \Delta}{\Gamma \to F \wedge G, \Delta}$$

$$\frac{F, \Gamma \to \Delta}{\Gamma \to \neg F, \Delta} \quad \frac{\Gamma \to F, \Delta}{\neg F, \Gamma \to \Delta}$$

$$\frac{F, \Gamma \to \Delta \quad \Gamma \to F, \Delta}{\Gamma \to \Delta} \qquad \text{(Сечение)}$$

Здесь Γ и Δ представляют собой конечные (возможно, пустые) множества[1] формул. Выводом формулы Φ считается последовательность, завершающаяся секвенцией $\to \Phi$.

Замечание 2.2. Правило сечения нужно для того, чтобы система стала импликативно полной: если $F \supset G$, то $\to \neg F \vee G$ $(**)$, и тогда сечение позволяет из $\to F$ (т.е. $\neg F \supset$ $(***)$) вывести секвенцию $\to G$:

$$\dfrac{\dfrac{\dfrac{\neg F \supset \neg F,\ G\ \text{(Акс.+Осл.)} \qquad G \supset \neg F,\ G\ \text{(Акс.+Осл.)}}{\neg F \vee G \supset \neg F,\ G\ (\vee)} \quad \to \neg F \vee G\ (**)}{\to \neg F,\ G\ \text{(Сеч.)}} \quad \neg F \supset\ (***)}{\to G\ \text{(Сеч.)}}$$

Сечение влияет на импликативную полноту и длину вывода, но не на полноту.

Замечание 2.3. В генценовской системе "доказательство от противного"

$$\begin{array}{ll} \to & F \\ & \vdots \\ \to & \text{false} \end{array}$$

[1] Классически, рассматриваются последовательности формул и добавляются правила для перестановки членов последовательности, а также дублирования и сокращения одинаковых членов.

очевидно преобразуется в прямое доказательство

$$\begin{aligned} F &\to F \\ &\vdots \\ F &\to \text{false} \\ &\to \neg F. \end{aligned}$$

Утверждение 2.1. *Генценовские системы эквивалентны системам Фреге.*

2.3 Правило расширения

Определение 2.9. *Правило расширения* в системе доказательств позволяет вводить новую переменную для обозначения произвольной формулы F при помощи новых аксиом $x \equiv F$, где x — новая переменная, не встречавшаяся ранее в выводе.

Пример 2.3. Если добавить правило расширения к (очень слабой) системе резолюции, то она станет эквивалентна системам Фреге (тоже с правилом расширения).

2.4 Короткое доказательство принципа Дирихле при помощи правила расширения

Напомним, как принцип Дирихле для $n+1$ кролика и n клеток записывается в виде пропозициональных формул. Пусть переменная x_{ik} обозначает, что i-й кролик помещен в k-ю клетку. Условие, что всякий кролик сидит в какой-то клетке, записывается в виде

$$\bigwedge_{1\le i\le n+1} \bigvee_{1\le k\le n} x_{ik}.$$

Тогда принцип Дирихле утверждает, что в некоторой клетке сидят два кролика:

$$\bigvee_{1\le k\le n} \bigvee_{1\le i<j\le n+1} (x_{ik} \wedge x_{jk}).$$

Теорема 2.2 (Cook-Reckhow, 1979)**.** *Принцип Дирихле имеет полиномиальное доказательство в системах Фреге с правилом расширения.*

Схема доказательства. Пусть мы можем определить [многозначное] инъективное отображение

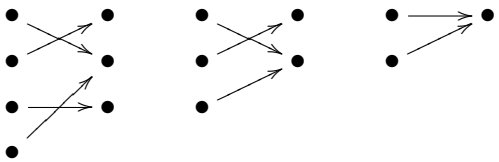
$$f\colon \{1,\dots,n+1\} \rightarrowtail \{1,\dots,n\}.$$

Тогда индуктивно определим $f_m\colon \{1,\dots,m+1\} \to \{1,\dots,m\}$, где m пробегает значения от n до 1.

$$f_n = f;$$

$$f_m(i) = \begin{cases} f_{m+1}(i), & \text{если } f_{m+1}(i) < m, \\ f_{m+1}(m+1), & \text{иначе.} \end{cases} \qquad (m \le n)$$

Далее для каждого m мы доказываем, что из инъективности f_{m+1} следует инъективность f_m, получая в конечном счете «инъекцию» $f_1\colon \{0,1\} \rightarrowtail \{0\}$ — противоречие.



В расширенной системе Фреге мы добавим переменные q_{ik}^m, каждая из которых означает $f_m(i) = k$:

$$\begin{aligned} q_{ik}^n &\equiv x_{ik}, \\ q_{ik}^m &\equiv q_{ik}^{m+1} \vee (q_{im}^{m+1} \wedge q_{m+1,k}^{m+1}), \end{aligned}$$

где $m \le n$.

При доказательстве от противного на каждом шаге будет выведено отрицание принципа Дирихле на единицу меньшего размера, то есть те же самые формулы, различающиеся только в верхнем индексе m. Каждый шаг имеет полиномиальный размер, и всего их n. □

Упражнение 2.1. Провести те же рассуждения методом резолюций.

Замечание 2.4. Для системы Фреге без правила расширения доказательство принципа Дирихле по указанной схеме не будет полиномиальным.

Однако далее мы покажем, что системы Фреге без правила расширения могут моделировать систему секущих плоскостей. Отсюда следует, что в системах Фреге без правила расширения короткое доказательство принципа Дирихле всё же существует.