

Сложность пропозициональных доказательств

Эдуард Алексеевич Гирш

<http://logic.pdmi.ras.ru/~hirsch>

ПОМИ РАН

23 сентября 2010 г.

Определение

Пусть S, W — системы для *одного и того же* языка L .

S моделирует W (пишем $S \leq W$) \iff

S -док-ва — не длиннее W -док-в (с точностью до полинома p):

$\forall F \in L \mid \text{кратчайшее } S\text{-док-во для } F \mid \leq p(\mid \text{кратчайшее } W\text{-док-во для } F \mid)$.

Определение

Пусть S, W — системы для *одного и того же* языка L .

S моделирует W (пишем $S \leq W$) \iff

S -док-ва — не длиннее W -док-в (с точностью до полинома p):

$\forall F \in L$ |кратчайшее S -док-во для F | $\leq p$ (|кратчайшее W -док-во для F |).

S строго моделирует W (пишем $S < W$), если ещё и $W \not\leq S$.

Например, CP (секущие плоскости) $<$ Res (метод резолюций).

Определение

Пусть S, W — системы для *одного и того же* языка L .

S моделирует W (пишем $S \leq W$) \iff

S -док-ва — не длиннее W -док-в (с точностью до полинома p):

$\forall F \in L \mid \text{кратчайшее } S\text{-док-во для } F \mid \leq p(\mid \text{кратчайшее } W\text{-док-во для } F \mid)$.

S строго моделирует W (пишем $S < W$), если ещё и $W \not\leq S$.

Например, CP (секущие плоскости) $<$ Res (метод резолюций).

Определение

p -моделирование (\leq_p) — конструктивная версия:

за полиномиальное время можно трансформировать

W -доказательство размера w в S -доказательство размера $p(w)$.

Полиномиальное моделирование

Определение

Пусть S, W — системы для *одного и того же* языка L .

S моделирует W (пишем $S \leq W$) \iff

S -док-ва — не длиннее W -док-в (с точностью до полинома p):

$\forall F \in L \mid \text{кратчайшее } S\text{-док-во для } F \mid \leq p(\mid \text{кратчайшее } W\text{-док-во для } F \mid)$.

S строго моделирует W (пишем $S < W$), если ещё и $W \not\leq S$.

Например, CP (секущие плоскости) $<$ Res (метод резолюций).

Определение

p -моделирование (\leq_p) — конструктивная версия:

за полиномиальное время можно трансформировать

W -доказательство размера w в S -доказательство размера $p(w)$.

Определение

(p) -оптимальная система док-в — наименьший элемент для $\leq (\leq_p)$.

Системы Фреге

Определение

Системой Фреге называется система, состоящая из корректных правил вида

$$\frac{F_1 \quad F_2 \quad \dots \quad F_k}{G},$$

- ▶ F_i, G — формулы логики высказываний,
- ▶ в качестве переменных можно подставлять произвольные формулы с выбранным множеством операций (“**базисом**”),
- ▶ вывод начинается с аксиом (где $k = 0$),
- ▶ новые формулы выводятся (\vdash) правилами из ранее выведенных.

Пример

$$\frac{}{P \supset (Q \supset P)},$$

$$\frac{}{(\neg Q \supset \neg P) \supset ((\neg Q \supset P) \supset Q)},$$

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

$$\frac{}{(P \supset (Q \supset R)) \supset ((P \supset Q) \supset (P \supset R))}.$$

Системы Фреге

Эквивалентность

Система **полна**, если $F \in L \implies \exists$ док-во F .

Системы Фреге

Эквивалентность

Система Фреге **полна**, если $F \in L \implies \vdash^* F$.

Система Фреге **импликативно полна**, если $\check{\forall}(F \supset G) \implies F \vdash^* G$.

Системы Фреге

Эквивалентность

Система Фреге **полна**, если $F \in L \implies \vdash^* F$.

Система Фреге **импликативно полна**, если $\check{\forall}(F \supset G) \implies F \vdash^* G$.

Теорема

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

Системы Фреге

Эквивалентность

Система Фреге **полна**, если $F \in L \implies \vdash^* F$.

Система Фреге **импликативно полна**, если $\check{\forall}(F \supset G) \implies F \vdash^* G$.

Теорема

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

- ▶ Док-во для одинаковых базисов: промоделируем каждое правило.

Системы Фреге

Эквивалентность

Система Фреге **полна**, если $F \in L \implies \vdash^* F$.

Система Фреге **импликативно полна**, если $\check{\forall}(F \supset G) \implies F \vdash^* G$.

Теорема

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

- ▶ Док-во для одинаковых базисов: промоделируем каждое правило.
- ▶ При смене базиса *глубокие* формулы могут вырасти!

Системы Фреге

Эквивалентность

Система Фреге **полна**, если $F \in L \implies \vdash^* F$.

Система Фреге **импликативно полна**, если $\check{\vee}(F \supset G) \implies F \vdash^* G$.

Теорема

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

- ▶ Док-во для одинаковых базисов: промоделируем каждое правило.
- ▶ При смене базиса *глубокие* формулы могут вырасти!
- ▶ Непрямой перевод:

$$F = T[G \odot H],$$
$$F' = ((G \odot H) \wedge T[1]) \vee (\neg(G \odot H) \wedge T[0]).$$

Ясно, что собственно операции переводятся на нижнем уровне, а уровней получается $O(\log \dots)$.

Системы Фреге

Эквивалентность

Система Фреге **полна**, если $F \in L \implies \vdash^* F$.

Система Фреге **импликативно полна**, если $\check{\forall}(F \supset G) \implies F \vdash^* G$.

Теорема

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

- ▶ Док-во для одинаковых базисов: промоделируем каждое правило.
- ▶ При смене базиса *глубокие* формулы могут вырасти!
- ▶ Непрямой перевод:

$$F = T[G \odot H],$$
$$F' = ((G \odot H) \wedge T[1]) \vee (\neg(G \odot H) \wedge T[0]).$$

Ясно, что собственно операции переводятся на нижнем уровне, а уровней получается $O(\log \dots)$.

- ▶ Остаётся научиться работать с таким представлением.

Секвенциальное (генценовское) исчисление

- ▶ Секвенция $F_1, \dots, F_k \rightarrow G_1, \dots, G_l$
- ▶ Смысл: $\bigwedge_i F_i \supset \bigvee_j G_j$.

Секвенциальное (генценовское) исчисление

▶ Секвенция $F_1, \dots, F_k \rightarrow G_1, \dots, G_l$ (списки как множества!).

▶ Смысл: $\bigwedge_i F_i \supset \bigvee_j G_j$.

▶ Аксиомы $F \rightarrow F$, ослабление $\frac{\Gamma \rightarrow \Delta}{F, \Gamma \rightarrow G, \Delta}$.

▶ Правила введения \wedge, \vee, \neg :

$$\frac{\Gamma \rightarrow F, \Delta}{\Gamma \rightarrow F \vee G, \Delta},$$

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

$$\frac{F, \Gamma \rightarrow \Delta}{\Gamma \rightarrow \neg F, \Delta},$$

$$\frac{F, \Gamma \rightarrow \Delta}{F \wedge G, \Gamma \rightarrow \Delta},$$

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

$$\frac{\Gamma \rightarrow F, \Delta}{\neg F, \Gamma \rightarrow \Delta}.$$

Секвенциальное (генценовское) исчисление

▶ Секвенция $F_1, \dots, F_k \rightarrow G_1, \dots, G_l$ (списки как множества!).

▶ Смысл: $\bigwedge_i F_i \supset \bigvee_j G_j$.

▶ Аксиомы $F \rightarrow F$, ослабление $\frac{\Gamma \rightarrow \Delta}{F, \Gamma \rightarrow G, \Delta}$.

▶ Правила введения \wedge, \vee, \neg :

$$\frac{\Gamma \rightarrow F, \Delta}{\Gamma \rightarrow F \vee G, \Delta},$$

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

$$\frac{F, \Gamma \rightarrow \Delta}{\Gamma \rightarrow \neg F, \Delta},$$

$$\frac{F, \Gamma \rightarrow \Delta}{F \wedge G, \Gamma \rightarrow \Delta},$$

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

$$\frac{\Gamma \rightarrow F, \Delta}{\neg F, \Gamma \rightarrow \Delta}.$$

▶ Правило сечения:

$$\frac{F, \Gamma \rightarrow \Delta \quad \Gamma \rightarrow F, \Delta}{\Gamma \rightarrow \Delta}.$$

Секвенциальное (генценовское) исчисление

▶ Секвенция $F_1, \dots, F_k \rightarrow G_1, \dots, G_l$ (списки как множества!).

▶ Смысл: $\bigwedge_i F_i \supset \bigvee_j G_j$.

▶ Аксиомы $F \rightarrow F$, ослабление $\frac{\Gamma \rightarrow \Delta}{F, \Gamma \rightarrow G, \Delta}$.

▶ Правила введения \wedge, \vee, \neg :

$$\frac{\Gamma \rightarrow F, \Delta}{\Gamma \rightarrow F \vee G, \Delta},$$

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

$$\frac{F, \Gamma \rightarrow \Delta}{\Gamma \rightarrow \neg F, \Delta},$$

$$\frac{F, \Gamma \rightarrow \Delta}{F \wedge G, \Gamma \rightarrow \Delta},$$

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

$$\frac{\Gamma \rightarrow F, \Delta}{\neg F, \Gamma \rightarrow \Delta}.$$

▶ Правило сечения:

$$\frac{F, \Gamma \rightarrow \Delta \quad \Gamma \rightarrow F, \Delta}{\Gamma \rightarrow \Delta}.$$

▶ Эквивалентны системам Фреге.

▶ Сечение важно для длины вывода, но не для полноты.

Секвенциальное (генценовское) исчисление

▶ Секвенция $F_1, \dots, F_k \rightarrow G_1, \dots, G_l$ (списки как множества!).

▶ Смысл: $\bigwedge_i F_i \supset \bigvee_j G_j$.

▶ Аксиомы $F \rightarrow F$, ослабление $\frac{\Gamma \rightarrow \Delta}{F, \Gamma \rightarrow G, \Delta}$.

▶ Правила введения \wedge, \vee, \neg :

$$\frac{\Gamma \rightarrow F, \Delta}{\Gamma \rightarrow F \vee G, \Delta},$$

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

$$\frac{F, \Gamma \rightarrow \Delta}{\Gamma \rightarrow \neg F, \Delta},$$

$$\frac{F, \Gamma \rightarrow \Delta}{F \wedge G, \Gamma \rightarrow \Delta},$$

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

$$\frac{\Gamma \rightarrow F, \Delta}{\neg F, \Gamma \rightarrow \Delta}.$$

▶ Правило сечения:

$$\frac{F, \Gamma \rightarrow \Delta \quad \Gamma \rightarrow F, \Delta}{\Gamma \rightarrow \Delta}.$$

▶ Эквивалентны системам Фреге.

▶ Сечение важно для длины вывода, но не для полноты.

▶ Доказательство от противного очевидно преобразуется в прямое.^{5/6}

Правило расширения

Разрешим вводить новые переменные: аксиома $x \equiv F$.

Фреге с правилом расширения \equiv резолюции с правилом расширения!

(Для резолюции: аксиомы $(\neg x \vee a_1 \vee \dots \vee a_k)$ и $(\neg a_1 \vee x), \dots, (\neg a_k \vee x)$).

Правило расширения

Разрешим вводить новые переменные: аксиома $x \equiv F$.

Фреге с правилом расширения \equiv резолюции с правилом расширения!
(Для резолюции: аксиомы $(\neg x \vee a_1 \vee \dots \vee a_k)$ и $(\neg a_1 \vee x), \dots, (\neg a_k \vee x)$).

Короткое доказательство принципа Дирихле:

доказываем по индукции $(n + 1 \rightarrow n \rightarrow \dots)$, вводя новые переменные,
очередное m -е отображение селит m кроликов в $m - 1$ клеток;
тех, кто сидел, как надо ($j < m$), оставляем;
в клетку, где был $(m + 1)$ -й, селим того, кто сидел в m -й клетке:

Правило расширения

Разрешим вводить новые переменные: аксиома $x \equiv F$.

Фреге с правилом расширения \equiv резолюции с правилом расширения!
(Для резолюции: аксиомы $(\neg x \vee a_1 \vee \dots \vee a_k)$ и $(\neg a_1 \vee x), \dots, (\neg a_k \vee x)$).

Короткое доказательство принципа Дирихле:

доказываем по индукции $(n + 1 \rightarrow n \rightarrow \dots)$, вводя новые переменные, очередное m -е отображение селит m кроликов в $m - 1$ клеток; тех, кто сидел, как надо ($j < m$), оставляем; в клетку, где был $(m + 1)$ -й, селим того, кто сидел в m -й клетке:

$$q_{i,j}^{(m)} \equiv q_{i,j}^{(m+1)} \vee (q_{m+1,j}^{(m+1)} \wedge q_{i,m}^{(m+1)}),$$
$$q_{i,j}^{(n+1)} \equiv p_{i,j}.$$