Математическая логика

(mk.cs.msu.ru → Лекционные курсы → Математическая логика (группы 318, 241))

Лекция 5

Полнота табличного вывода
Теорема Лёвенгейма-Сколема
Теорема компактности Мальцева
Теорема Чёрча
Автоматизация доказательства теорем

Лектор:
Подымов Владислав Васильевич

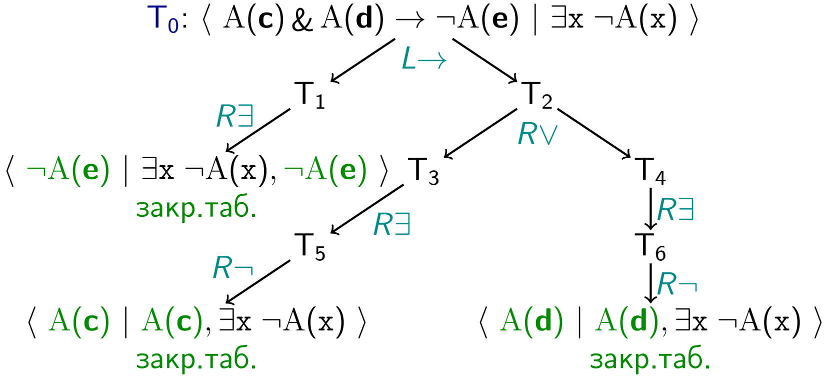
E-mail:
valdus@yandex.ru

ВМК МГУ, 2019, весенний семестр

Напоминание

Корректность табличного вывода в логике предикатов:

если для таблицы T_0 существует **успешный** табличный вывод, то таблица T_0 невыполнима



Полнота табличного вывода

А верно ли обратное утверждение?
(*если таблица невыполнима,*
то для неё существует успешный табличный вывод)

То есть

всегда ли можно обосновать общезначимость формулы, используя только метод семантических таблиц?

Это и есть полнота табличного вывода

Теорема(***о полноте табличного вывода***)
Для любой невыполнимой семантической таблицы существует успешный табличный вывод

Теорема о полноте табличного вывода: доказательство

Пусть $T_0 = \langle\, \Gamma_0 \mid \Delta_0 \,\rangle$ — невыполнимая таблица

Для простоты считаем, что

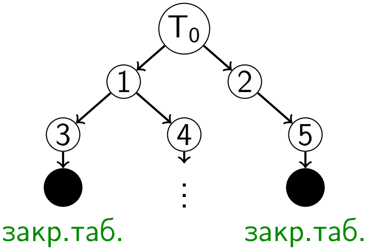
- множества Γ_0, Δ_0 конечны
- все формулы из Γ_0, Δ_0 замкнуты
- формулы из Γ_0, Δ_0 не содержат функциональных символов

Опишем **стратегию построения табличного вывода**, позволяющую доказать невыполнимость таблицы T_0

Теорема о полноте табличного вывода: доказательство

При построении табличного вывода для T_0 будем придерживаться трёх правил:

1. Незакрытые неатомарные таблицы обрабатываются в порядке появления при построении вывода (*то есть дерево вывода обходится в ширину*)



Результат: каждая таблица каждой ветви вывода рано или поздно будет построена

Теорема о полноте табличного вывода: доказательство

При построении табличного вывода для T_0 будем придерживаться трёх правил:

2. Все неатомарные формулы таблицы упорядочены, правило вывода применяется к первой формуле, результат применения записывается последним

$$\langle\ 1{:}\forall x\ \varphi,\ 3{:}\psi_1 \to \psi_2 \mid 2{:}\chi_1 \vee \chi_2\ \rangle$$
$$\downarrow$$
$$\langle\ 2{:}\psi_1 \to \psi_2,\ 3{:}\forall x\ \varphi,\ 4{:}\varphi' \mid 1{:}\chi_1 \vee \chi_2\ \rangle$$
$$\downarrow$$
$$\langle\ 1{:}\psi_1 \to \psi_2,\ 2{:}\forall x\ \varphi,\ 3{:}\varphi' \mid 4{:}\chi_1,\ 5{:}\chi_2\ \rangle$$
$$\swarrow \qquad \searrow$$
$$\langle 1{:}\forall x\ \varphi, 2{:}\varphi', 5{:}\psi_2 \mid 3{:}\chi_1, 4{:}\chi_2 \rangle \qquad \langle 1{:}\forall x\ \varphi, 2{:}\varphi' \mid 3{:}\chi_1, 4{:}\chi_2, 5{:}\psi_1 \rangle$$
$$\dots \qquad\qquad\qquad \dots$$

Результат: в каждой бесконечной ветви вывода каждая неатомарная формула рано или поздно будет обработана

Теорема о полноте табличного вывода: доказательство

При построении табличного вывода для T_0 будем придерживаться трёх правил:

3. При применении правил $L\forall$, $R\exists$ подставляются **все имеющиеся в таблице константы** (**c**, если констант нет)

$$\begin{array}{c}
\langle\ \forall \mathrm{x}\ \varphi,\ \exists \mathrm{x}\ \psi \mid \exists \mathrm{x}\ \chi\ \rangle \\
\big\downarrow L\forall \\
\langle\ \forall \mathrm{x}\ \varphi,\ \exists \mathrm{x}\ \psi,\ \varphi\{\mathrm{x}/\mathbf{c}\} \mid \exists \mathrm{x}\ \chi\ \rangle \\
\big\downarrow L\exists \\
\langle\ \forall \mathrm{x}\ \varphi,\ \psi\{\mathrm{x}/\mathbf{d}\},\ \varphi\{\mathrm{x}/\mathbf{c}\} \mid \exists \mathrm{x}\ \chi\ \rangle \\
\big\downarrow R\exists \times 2 \\
\langle\ \forall \mathrm{x}\ \varphi,\ \psi\{\mathrm{x}/\mathbf{d}\},\ \varphi\{\mathrm{x}/\mathbf{c}\} \mid \exists \mathrm{x}\ \chi,\ \chi\{\mathrm{x}/\mathbf{c}\},\ \chi\{\mathrm{x}/\mathbf{d}\}\ \rangle \\
\cdots
\end{array}$$

Результат: в каждой бесконечной ветви вывода каждая константа рано или поздно будет подставлена для каждого неустраняемого квантора

Теорема о полноте табличного вывода: доказательство

Покажем, что вывод $\mathfrak{D}$, построенный по этой стратегии для невыполнимой таблицы $\mathsf{T}_0 = \langle\ \Gamma_0 \mid \Delta_0\ \rangle$, успешен

Предположим, что это не так: вывод $\mathfrak{D}$ неуспешен — получим из этого выполнимость таблицы T_0, *противоречащую условию теоремы*

Заменим в $\mathfrak{D}$ каждую незакрытую атомарную таблицу T_{atom} на бесконечную ветвь $\mathsf{T}_{atom} \to \mathsf{T}_{atom} \to \mathsf{T}_{atom} \to \dots$

Тогда в полученном дереве обязательно найдётся бесконечная ветвь $\mathcal{T}$, состоящая только из незакрытых таблиц:

$$\mathsf{T}_0 \to \mathsf{T}_1 \to \mathsf{T}_2 \to \dots$$

По этой ветви построим интерпретацию $\mathcal{I}$, такую что:

- каждая формула из Γ_0 выполнима в $\mathcal{I}$
- каждая формула из Δ_0 невыполнима в $\mathcal{I}$

Теорема о полноте табличного вывода: доказательство

$$\mathfrak{T}\colon \mathrm{T}_0 \to \mathrm{T}_1 \to \mathrm{T}_2 \to \ldots, \quad \mathrm{T}_i = \langle\ \Gamma_i \mid \Delta_i\ \rangle$$

$\mathcal{I} = \left\langle \mathrm{D}, \overline{\mathrm{Const}}, -, \overline{\mathrm{Pred}} \right\rangle$, где

- предметная область D — это все константы всех формул в $\mathfrak{T}$:
  $$\mathrm{D} = \bigcup_{i \geq 0} \mathrm{Const}_i = \mathrm{Const}_\omega, \text{ где } \mathrm{Const}_i \text{ — все константы в } \mathrm{T}_i$$
- значение каждой константы — это её изображение (*она сама*):
  $$\bar{\mathbf{c}} = \mathbf{c}$$
- предикат истинен = он встречается в левых частях таблиц $\mathfrak{T}$:
  $$\overline{\mathrm{P}}(\mathbf{c_1}, \ldots, \mathbf{c_k}) = \mathbf{t} \quad \Leftrightarrow \quad \mathrm{P}(\mathbf{c_1}, \ldots, \mathbf{c_k}) \in \bigcup_{i \geq 0} \Gamma_i = \Gamma_\omega$$

Осталось показать *индукцией по структуре формулы*, что

- каждая формула из Γ_ω выполнима в $\mathcal{I}$
- каждая формула из $\Delta_\omega = \bigcup_{i \geq 0} \Delta_i$ невыполнима в $\mathcal{I}$

Теорема о полноте табличного вывода: доказательство

$$\mathfrak{T}\colon \mathsf{T}_0 \to \mathsf{T}_1 \to \mathsf{T}_2 \to \dots, \quad \mathsf{T}_i = \langle\, \Gamma_i \mid \Delta_i \,\rangle$$

$$\varphi \in \Gamma_\omega \overset{?}{\Rightarrow} \mathcal{I} \models \varphi \qquad\qquad \varphi \in \Delta_\omega \overset{?}{\Rightarrow} \mathcal{I} \not\models \varphi$$

База индукции: φ — атом

Тогда φ имеет вид $\mathrm{P}(\mathbf{c_1}, \dots, \mathbf{c_k})$, где $\mathbf{c_1}, \dots, \mathbf{c_k} \in \mathsf{Const}_\omega$ (почему?)

Подслучай 1: $\mathrm{P}(\mathbf{c_1}, \dots, \mathbf{c_k}) \in \Gamma_\omega$
Тогда $\overline{\mathrm{P}}(\mathbf{c_1}, \dots, \mathbf{c_k}) = \mathbf{t}$, а значит, $\mathcal{I} \models \varphi$

Подслучай 2: $\mathrm{P}(\mathbf{c_1}, \dots, \mathbf{c_k}) \in \Delta_\omega$
Тогда $\mathrm{P}(\mathbf{c_1}, \dots, \mathbf{c_k}) \notin \Gamma_\omega$ (почему?)
Значит, $\overline{\mathrm{P}}(\mathbf{c_1}, \dots, \mathbf{c_k}) = \mathbf{f}$ и $\mathcal{I} \not\models \varphi$

Индуктивный переход
Предположение индукции: для каждой формулы, содержащей менее N логических операций, утверждение доказано
Рассматриваемый случай: формула φ содержит ровно N логических операций

Теорема о полноте табличного вывода: доказательство

$$\mathfrak{T}\colon \mathsf{T}_0 \to \mathsf{T}_1 \to \mathsf{T}_2 \to \ldots, \quad \mathsf{T}_i = \langle\, \Gamma_i \mid \Delta_i \,\rangle$$

$$\varphi \in \Gamma_\omega \overset{?}{\Rightarrow} \mathcal{I} \models \varphi \qquad\qquad \varphi \in \Delta_\omega \overset{?}{\Rightarrow} \mathcal{I} \not\models \varphi$$

Переход 1: φ имеет вид $\psi \to \chi$

Подслучай 1: $\varphi \in \Gamma_\omega$

В ветви $\mathfrak{T}$ существует таблица T_i, такая что правило вывода применяется к φ в левой части этой таблицы (почему?)

Значит, верно хотя бы одно из двух: (почему?)

- $\chi \in \Gamma_{i+1}$, и тогда $\mathcal{I} \models \chi$ и $\mathcal{I} \models \varphi$
- $\psi \in \Delta_{i+1}$, и тогда $\mathcal{I} \not\models \psi$ и $\mathcal{I} \models \varphi$

Подслучай 2: $\varphi \in \Delta_\omega$ — рассуждения аналогичны

Переход 2/3/4: формула φ имеет вид $\psi \,\&\, \chi / \psi \vee \chi / \neg\psi$ — рассуждения аналогичны

Теорема о полноте табличного вывода: доказательство

$$\mathfrak{T}\colon \mathrm{T}_0 \to \mathrm{T}_1 \to \mathrm{T}_2 \to \dots, \quad \mathrm{T}_i = \langle\, \Gamma_i \mid \Delta_i \,\rangle$$

$$\varphi \in \Gamma_\omega \overset{?}{\Rightarrow} \mathcal{I} \models \varphi \qquad\qquad \varphi \in \Delta_\omega \overset{?}{\Rightarrow} \mathcal{I} \not\models \varphi$$

Переход 5: формула φ имеет вид $\forall \mathtt{x}\ \psi$

Подслучай 1: $\varphi \in \Gamma_\omega$

Тогда $\varphi\{\mathtt{x}/\mathbf{c}\} \in \Gamma_\omega$ для любой константы $\mathbf{c} \in \mathrm{Const}_\omega$ (почему?)

Значит, для любой константы $\mathbf{c} \in \mathrm{Const}_\omega$ верно: $\mathcal{I} \models \varphi\{\mathtt{x}/\mathbf{c}\}$

Но это и означает $\mathcal{I} \models \forall \mathtt{x}\ \varphi$

Подслучай 2: $\varphi \in \Delta_\omega$

В ветви $\mathfrak{T}$ существует таблица T_i, такая что правило вывода применяется к φ в правой части этой таблицы

Значит, $\varphi\{\mathtt{x}/\mathbf{c}\} \in \Delta_{i+1}$ для некоторой $\mathbf{c} \in \mathrm{Const}_{i+1} \subseteq \mathrm{Const}_\omega$

Тогда $\mathcal{I} \not\models \varphi\{\mathtt{x}/\mathbf{c}\}$, и следовательно, $\mathcal{I} \not\models \forall \mathtt{x}\ \varphi$

Переход 6: формула φ имеет вид $\exists \mathtt{x}\ \psi$ — рассуждения аналогичны

Теорема о полноте табличного вывода: доказательство

$\mathfrak{T}$: $\mathsf{T}_0 \to \mathsf{T}_1 \to \mathsf{T}_2 \to \dots$, $\mathsf{T}_i = \langle\, \Gamma_i \mid \Delta_i \,\rangle$

Итоги рассуждений

Существует (*и явно описана*) интерпретация $\mathcal{I}$, такая что

- все формулы в левых частях таблиц из $\mathfrak{T}$ выполнимы в $\mathcal{I}$
- все формулы в правых частях таблиц из $\mathfrak{T}$ невыполнимы в $\mathcal{I}$

В частности, все формулы из Γ_0 выполнимы в $\mathcal{I}$,
и все формулы из Δ_0 невыполнимы в $\mathcal{I}$

Значит, таблица T_0 выполнима, *что противоречит условию теоремы*

Противоречие получено в предположении о том, что вывод, построенный для T_0, неуспешен

Значит, предположение неверно: **любой вывод, построенный согласно предложенной стратегии для невыполнимой таблицы T_0, успешен**

Теорема о полноте табличного вывода: доказательство

А что изменится в доказательстве для общего случая?

То есть:

- какой порядок обработки формул позволит "справедливо" обращаться с бесконечными множествами формул? (*хотя бы со счётно-бесконечными*)
- какие термы подставлять, если в сигнатуре алфавита есть функциональные символы?
- как описать и что делать с интерпретацией $\mathcal{I}$, если в таблицах встречаются незамкнутые формулы?

Полнота табличного вывода

Следствие(*вариант теоремы Гёделя о полноте для исчисления семантических таблиц*)
$\models \varphi \quad \Leftrightarrow \quad$ **для семантической таблицы $\langle \ \mid \varphi \ \rangle$ существует успешный табличный вывод**

Доказательство.
Следует из *корректности* и *полноты* табличного вывода и теоремы *о табличной проверке общезначимости формул* ▼

Более того, в доказательстве *теоремы о полноте* сказано, **как построить** успешный табличный вывод, *если он существует*

Кроме того, из теорем о корректности и полноте табличного вывода можно легко получить полезные следствия, не относящиеся к табличным выводам как таковым

Теорема Лёвенгейма-Сколема

Для любого предложения φ справедлива равносильность:
$\models \varphi \;\Leftrightarrow\; \varphi$ **имеет модель с <u>конечной</u> или <u>счётно-бесконечной</u> предметной областью**

Доказательство.

Корректность и *полнота*: φ выполнима $\Leftrightarrow$ для таблицы $T_0 = \langle\, \varphi \mid \;\rangle$ не существует успешного табличного вывода

Построив вывод согласно *стратегии из доказательства полноты*, получим

- бесконечную ветвь $T_0 \to T_1 \to \dots$, состоящую только из незакрытых таблиц
- интерпретацию $\mathcal{I}$ с **не более чем счётно-бесконечной** предметной областью, в которой выполнимы все таблицы этой ветви — в том числе таблица T_0 ▼

Теорема компактности Мальцева

Для любого предложения φ и любого множества предложений Γ справедлива равносильность:

$\Gamma \models \varphi \quad \Leftrightarrow$ **существует <u>конечное</u> подмножество Γ' множества Γ, такое что $\Gamma' \models \varphi$**

Доказательство.

$\Gamma \models \varphi \Leftrightarrow$ таблица $T = \langle\, \Gamma \mid \varphi \,\rangle$ невыполнима (почему?)
$\Leftrightarrow$ существует успешный табличный вывод $\mathfrak{D}$ для T

Подмножество Γ' формул множества Γ, к которым применяются правила и которые приводят к закрытости таблиц в $\mathfrak{D}$, <u>конечно</u> (почему?)

Тогда для таблицы $\langle\, \Gamma' \mid \varphi \,\rangle$ также существует успешный табличный вывод (почему?)

Значит, $\Gamma' \models \varphi$ ▼

Автоматическое доказательство теорем

Если программно реализовать стратегию[1] построения логического вывода[2], то в результате получится средство **автоматического доказательства теорем**:

First-order theorem prover

Основная задача прувера — предоставлять доказательство общезначимости формулы (успешный вывод)

Требования, предъявляемые к пруверу:

- корректность: обязательно
- полнота: очень желательно
- эффективность: желательно

[1] Не обязательно озвученную в доказательстве теоремы полноты, и даже не обязательно полную

[2] Не обязательно табличного вывода

Автоматическое доказательство теорем

Если программно реализовать стратегию построения логического вывода, то в результате получится средство **автоматического доказательства теорем**:

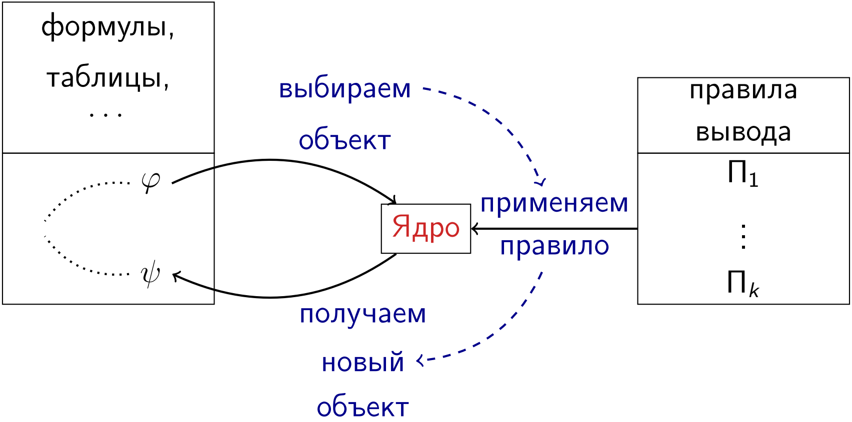
First-order theorem prover

Один из **многих** примеров того, чего позволило добиться использование пруверов:[1] строго доказана корректность *nix-микроядра L4, и в процессе доказательства найдены и исправлены сотни ошибок в коде

[1] Klein et al. seL4: formal verification of an OS kernel. 2009.
Конкретно этот пример выбран из-за наглядности, понятности и при этом "неоспоримой полезности" формулировки результата

Автоматическое доказательство теорем

Как устроены пруверы:



Автоматическое доказательство теорем: теоретический взгляд. Теорема Чёрча

Теорема(*Чёрча*). **Проблема общезначимости формул логики предикатов алгоритмически неразрешима**

Иными словами, **никакой алгоритм**
не способен достоверно и за конечное время
решить проблему "$\models \varphi$?" для произвольной формулы φ

Но при этом существует алгоритм, способный подтвердить общезначимость формулы (например, метод семантических таблиц с полной стратегией построения успешного вывода)

Это означает, что проблема "$\models \varphi$?" полуразрешима, или
частично разрешима

Автоматическое доказательство теорем: теоретический взгляд

Неразрешимость проблемы общезначимости можно доказать так: взять известную неразрешимую проблему и **свести** её к "$\models \varphi$?"

Проблема останова машин Тьюринга (*как известно, неразрешимая*)
Дано: машина Тьюринга M, слово w
Вопрос $\mathbf{HALT}(M, w)$: остановится ли M на входном слове w?

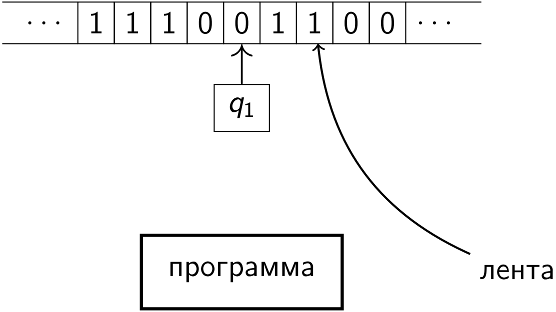
Что такое "свести"?

Предложить алгоритм, по M и w строящий формулу $\varphi_{M,w}$, такую что

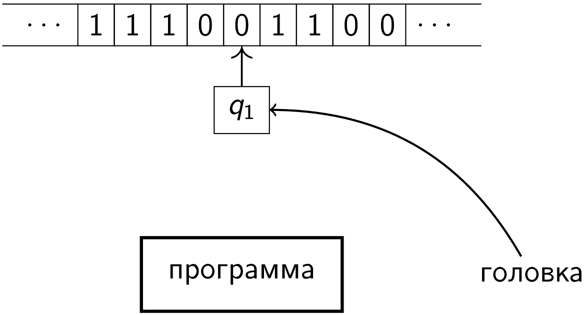
$$\mathbf{HALT}(M, w) \quad \Leftrightarrow \quad \models \varphi_{M,w}$$

Перед тем как описать такой алгоритм, вспомним, как выглядят **машины Тьюринга**

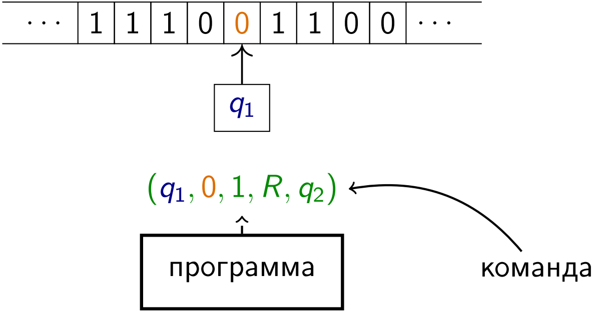
Машины Тьюринга (МТ)



Машины Тьюринга (МТ)



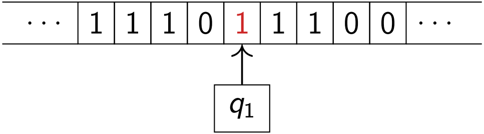
Машины Тьюринга (МТ)



Шаг вычисления выглядит так:

- по текущему состоянию и обозреваемому символу выбираем команду

Машины Тьюринга (МТ)



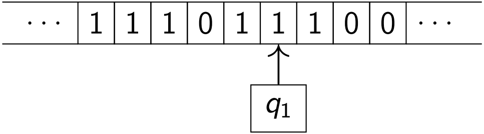
$$(q_1, 0, 1, R, q_2)$$

программа

Шаг вычисления выглядит так:

- по текущему состоянию и обозреваемому символу выбираем команду
- записываем в ячейку новый символ

Машины Тьюринга (МТ)



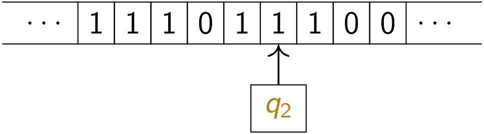
$$(q_1, 0, 1, R, q_2)$$

программа

Шаг вычисления выглядит так:

- по текущему состоянию и обозреваемому символу выбираем команду
- записываем в ячейку новый символ
- сдвигаем головку

Машины Тьюринга (МТ)



$$(q_1, 0, 1, R, q_2)$$

программа

Шаг вычисления выглядит так:

- по текущему состоянию и обозреваемому символу выбираем команду
- записываем в ячейку новый символ
- сдвигаем головку
- меняем состояние

Машины Тьюринга (МТ)

Определим всё с начала, по порядку и строго

$\mathcal{A}$ — конечный ленточный алфавит, Λ — пустой символ $(\Lambda \in \mathcal{A})$

Ленточное слово — это слово в алфавите $\mathcal{A}$

$\mathcal{A}^*$ — множество всех конечных ленточных слов

$\mathcal{Q}$ — конечный алфавит состояний

q_0 — начальное состояние $(q_0 \in \mathcal{Q})$

Ленточная конфигурация — это слово вида $u\ q\ x\ v$, где

$$q \in \mathcal{Q}, \quad x \in \mathcal{A}, \quad u, v \in \mathcal{A}^*$$

Пояснение: $(u = u_1 \dots u_l,\ v = v_1 \dots v_s)$

$\cdots$	Λ	$\cdots$	Λ	u_1	$\cdots$	u_l	x	v_1	$\cdots$	v_s	Λ	$\cdots$	Λ	$\cdots$

$$\boxed{q}$$

Машины Тьюринга (МТ)

Команда — это пятёрка вида (q, a, b, D, q'), где

$$q, q' \in \mathcal{Q}, \quad a, b \in \mathcal{A}, \quad D \in \{L, R\}$$

Пояснение: если МТ находится в состоянии q и обозревает символ a в текущей ячейке, то записать в эту ячейку b, сдвинуться влево ($D = L$) или вправо ($D = R$) и перейти в состояние q'

Командой C задаётся бинарное отношение переходов $\to_C$ на множестве конфигураций: $(z \in \mathcal{A})$

- $u\ z\ q\ x\ v \to_{(q,x,y,L,q')} u\ q'\ z\ y\ v$
- $q\ x\ v \to_{(q,x,y,L,q')} q'\ \Lambda\ y\ v$
- $u\ q\ x\ z\ v \to_{(q,x,y,R,q')} u\ y\ q'\ z\ v$
- $u\ q\ x \to_{(q,x,y,R,q')} u\ y\ q'\ \Lambda$

Машины Тьюринга (МТ)

Машина Тьюринга — это конечное множество команд

Детерминированная МТ: для любых $q \in \mathcal{Q}$, $a \in \mathcal{A}$ **не более чем одна** команда имеет вид (q, a, b, D, q')

Будем рассматривать **только** детерминированные МТ

Отношение переходов $\to_M$, задаваемое МТ M на множестве ленточных конфигураций, определяется так:

$$\to_M = \bigcup_{C \in M} \to_C$$

Конфигурация α МТ M — заключительная, если не существует конфигурации β, такой что $\alpha \to_M \beta$

МТ M останавливается на слове w (**HALT**(M, w)), если какая-либо заключительная конфигурация α_{fin} **достижима** из начальной конфигурации $(q_0\ w)$:

$$q_0\ w \to_M \cdots \to_M \alpha_{fin} \not\to_M$$

Теорема Чёрча: доказательство

Сведём проблему останова детерминированных МТ
к проблеме общезначимости формул логики предикатов

Для этого опишем, как можно по МТ M и ленточному слову w
построить формулу $\varphi_{M,w}$, такую что

$$\mathbf{HALT}(M, w) \qquad \Leftrightarrow \qquad \models \varphi_{M,w}$$

Что будет записано в формуле:

Если начальная конфигурация достижима и
конфигурация, следующая за достижимой, также достижима,
то достижима некоторая заключительная конфигурация

$$\varphi_{start} \mathbin{\&} \varphi_{step} \to \varphi_{finish}$$

Теорема Чёрча: доказательство

Сигнатура формулы $\varphi_{M,w}$*:*

- константа $\mathbf{a}$ для каждого $a \in \mathcal{A}$
- константа $\mathbf{q}$ для каждого $q \in \mathcal{Q}$
- функциональный символ, обозначающий операцию конкатенации ленточных слов: $\cdot^{(2)}$
  (*ассоциативную вправо в инфиксной записи*)
- предикатный символ, обозначающий отношение достижимости конфигурации из начальной: $\mathrm{Re}^{(3)}$

Компоненты формулы $\varphi_{M,w}$*:*

- терм, обозначающий ленточное слово $a_1 \dots a_p$

$$\widetilde{a_1 \dots a_p} = \mathbf{a_1} \cdot \dots \cdot \mathbf{a_p}$$

- атом “конфигурация $u\ q\ v$ достижима” $\left((a_1 \dots a_p)^- = a_p \dots a_1\right)$

$$\mathrm{Re}(\widetilde{u^-}, \mathbf{q}, \widetilde{v})$$

Теорема Чёрча: доказательство

Компоненты формулы $\varphi_{M,w}$:

- атом “начальная конфигурация достижима”

$$\varphi_{start}\colon \mathrm{Re}(\mathbf{\Lambda}, \mathbf{q_0}, \widetilde{w})$$

- подформулы “если текущая конфигурация достижима, то конфигурация после применения команды C будет достижима”

  - $C = (q, a, b, R, q')$

$$\varphi_C\colon \forall \mathrm{x}\, \forall \mathrm{y}\, (\mathrm{Re}(\mathrm{x}, \mathbf{q}, \mathbf{a}{\cdot}\mathrm{y}) \to \mathrm{Re}(\mathbf{b}{\cdot}\mathrm{x}, \mathbf{q'}, \mathrm{y}))$$

$$\psi_C\colon \forall \mathrm{x}\, (\mathrm{Re}(\mathrm{x}, \mathbf{q}, \mathbf{a}) \to \mathrm{Re}(\mathbf{b}{\cdot}\mathrm{x}, \mathbf{q'}, \mathbf{\Lambda}))$$

  - $C = (q, a, b, L, q')$

$$\varphi_C\colon \forall \mathrm{x}\, \forall \mathrm{y}\, \forall \mathrm{z}\, (\mathrm{Re}(\mathrm{z}{\cdot}\mathrm{x}, \mathbf{q}, \mathbf{a}{\cdot}\mathrm{y}) \to \mathrm{Re}(\mathrm{x}, \mathbf{q'}, \mathrm{z}{\cdot}\mathbf{b}{\cdot}\mathrm{y}))$$

$$\psi_C\colon \forall \mathrm{x}\, \forall \mathrm{y}\, (\mathrm{Re}(\mathrm{x}, \mathbf{q}, \mathbf{a}{\cdot}\mathrm{y}) \to \mathrm{Re}(\mathbf{\Lambda}, \mathbf{q'}, \mathrm{x}{\cdot}\mathbf{b}{\cdot}\mathrm{y}))$$

- подформула
  “конфигурация, следующая за достижимой, также достижима”

$$\varphi_{step}\colon \mathop{\&}_{C \in M} (\varphi_C \,\&\, \psi_C)$$

Теорема Чёрча: доказательство

Компоненты формулы $\varphi_{M,w}$:

- $\mathcal{G} \subseteq \mathcal{Q} \times \mathcal{A}$ — множество пар (q, a), таких что в M
  нет команд, начинающихся с q, a,
  но есть команды, начинающиеся с q
- подформула
  "хотя бы одна заключительная конфигурация достижима"

$$\varphi_{finish}\colon \exists \mathrm{x}\ \exists \mathrm{y}\ \Big(\bigvee_{(q,a)\in\mathcal{G}} \mathrm{Re}(\mathrm{x}, \mathbf{q}, \mathbf{a}\cdot \mathrm{y})\Big)$$

Возвращаемся к тому, что нужно доказать:

HALT(M, w): МТ M останавливается на слове w

$\varphi_{M,w}$: $\varphi_{start} \,\&\, \varphi_{step} \to \varphi_{finish}$

$$\mathbf{HALT}(M, w) \quad \Leftrightarrow \quad \models \varphi_{M,w}$$

Теорема Чёрча: доказательство

$$\mathbf{HALT}(M, w) \quad \Leftrightarrow \quad \models \varphi_{M,w}$$

($\Leftarrow$): если формула $\varphi_{M,w}$ истинна в любой интерпретации, то она истинна и в такой интерпретации $\mathcal{I}$:

$\overline{\mathrm{Re}}(\widetilde{u^-}, \mathbf{q}, \widetilde{v}) =$ "конфигурация $u\ q\ v$ достижима из $q_0\ w$ для M"

($\Rightarrow$): предположим от противного, что $\mathbf{HALT}(M, w)$ верно, но формула $\varphi_{M,w}$ необщезначима

Тогда существует интерпретация $\mathcal{I}$, такая что $\mathcal{I} \not\models \varphi_{M,w}$:

$$\mathcal{I} \models \varphi_{start}, \qquad \mathcal{I} \models \varphi_{step}, \qquad \mathcal{I} \not\models \varphi_{finish}$$

Рассмотрим работу МТ M на слове w:

$$q_0\ w \to_M u_1\ q_1\ v_1 \to_M u_2\ q_2\ v_2 \to_M \dots \to_M u_k\ q_k\ v_k,$$

где $u_k\ q_k\ v_k$ — заключительная конфигурация

Используя эту последовательность конфигураций, докажем, что

$$\mathcal{I} \models \varphi_{finish}$$

(*это противоречие, из которого будет следовать общезначимость формулы* $\varphi_{M,w}$)

Теорема Чёрча: доказательство, ($\Rightarrow$):

$$q_0\ w \to_M u_1\ q_1\ v_1 \to_M u_2\ q_2\ v_2 \to_M \cdots \to_M u_k\ q_k\ v_k$$

Исходное предположение: формула $\varphi_{M,w}$ необщезначима

$$\mathcal{I} \models \varphi_{start}, \qquad \mathcal{I} \models \varphi_{step}, \qquad \mathcal{I} \not\models \varphi_{finish}$$

$$\varphi_{start}\colon \mathrm{Re}(\mathbf{\Lambda}, \mathbf{q_0}, \mathbf{w}) \qquad \varphi_{finish}\colon \exists \mathrm{x}\ \exists \mathrm{y}\ \Big(\bigvee_{(q,a)\in\mathcal{G}} \mathrm{Re}(\mathrm{x}, \mathbf{q}, \mathbf{a}\cdot\mathrm{y})\Big)$$

$\mathcal{I} \models \varphi_{start}$ по рассматриваемому случаю

$\mathcal{I} \models \mathrm{Re}(\widetilde{u_1^-}, \mathbf{q_1}, \widetilde{v_1})$, так как $\varphi_{start}, \varphi_{step} \models \mathrm{Re}(\widetilde{u_1^-}, \mathbf{q_1}, \widetilde{v_1})$

$\dots$

$\mathcal{I} \models \mathrm{Re}(\widetilde{u_k^-}, \mathbf{q_k}, \widetilde{v_k})$, так как

$$\mathrm{Re}(\widetilde{u_{k-1}^-}, \mathbf{q_{k-1}}, \widetilde{v_{k-1}}), \varphi_{step} \models \mathrm{Re}(\widetilde{u_k^-}, \mathbf{q_k}, \widetilde{v_k})$$

$\mathcal{I} \models \varphi_{finish}$, так как $\mathrm{Re}(\widetilde{u_k^-}, \mathbf{q_k}, \widetilde{v_k}) \models \varphi_{finish}$

Но согласно *исходному предположению*, верно $\mathcal{I} \not\models \varphi_{finish}$

Значит, *исходное предположение* неверно:
формула $\varphi_{M,w}$ общезначима ▼

Автоматическое доказательство теорем: практический взгляд

С точки зрения практики, неразрешимость проблемы общезначимости означает, что любой прувер будет либо содержать неполную стратегию вывода, либо в некоторых случаях будет зацикливаться, и избежать этого никак нельзя

Но если мы **абсолютно уверены**, что формула φ, подаваемая на вход, общезначима, и хотим предоставить **доказательство** её общезначимости, то это сделать можно

Например, с помощью *метода семантических таблиц*

Но будет ли доказательство общезначимости вычисляться за разумное время?

- К какой формуле применять правило табличного вывода?
- При применении правил $L\forall$, $R\exists$ какие термы подставлять?

Автоматическое доказательство теорем: практический взгляд

Выбор формулы

Как избежать перебора всех формул таблицы?

База знаний	Запрос
В огороде бузина $\text{Растёт}(\textbf{бузина}, \textbf{огород})$ Всё в огороде посадил дядька $\forall x\ (\text{Растёт}(x, \textbf{огород}) \to$ $\quad \exists y\ (\text{Посадил}(y, x)\ \&\ \text{Дядька}(y)))$ Бузину сажают только Киевляне $\forall x\ (\text{Посадил}(x, \textbf{бузина})$ $\quad \to \text{Живёт}(x, \textbf{Киев}))$	В Киеве дядька $\exists y\ (\text{Дядька}(y)$ $\quad \&\ \text{Живёт}(y, \textbf{Киев}))$

Автоматическое доказательство теорем: практический взгляд

Выбор терма

$L\forall\ \dfrac{\langle \Gamma,\ \forall \mathtt{x}\ \varphi(\mathtt{x}) | \Delta\rangle}{\langle \Gamma,\ \forall \mathtt{x}\ \varphi(\mathtt{x}),\ \varphi(\mathtt{x})\{\mathtt{x}/t\} | \Delta\rangle}$ $\qquad$ $R\exists\ \dfrac{\langle \Gamma | \Delta,\ \exists \mathtt{x}\ \varphi(\mathtt{x})\rangle}{\langle \Gamma | \Delta,\ \exists \mathtt{x}\ \varphi(\mathtt{x}),\ \varphi(\mathtt{x})\{\mathtt{x}/t\}\rangle}$

Может быть, достаточно подставлять только "неглубокие" термы, построенные из содержащихся в таблице?

Из **одного** функционального символа $\mathbf{f}^{(2)}$, использующегося 10 раз, и **двух** констант c_1, c_2 можно построить более 10^{300} термов

Гугол — это 10^{100},

и это больше числа атомов в наблюдаемой вселенной

Можно ли как-то сократить перебор подставляемых термов?

В некоторой степени — да, можно[1,2]

[1] J.A. Robinson: метод резолюций — о нём будут следующие лекции

[2] С.Ю. Маслов: обратный вывод