Математическая логика

Лектор:

Подымов Владислав Васильевич

e-mail:
valdus@yandex.ru

2018, весенний семестр

Лекция 5

Полнота табличного вывода

Теорема Лёвенгейма-Сколема

Теорема компактности Мальцева

Теорема Чёрча

Автоматическое доказательство теорем

Напоминание

Корректность табличного вывода в логике предикатов:

$$
\begin{tikzcd}
 & & T_0\colon \langle\ \mathrm{A}(\mathbf{c})\,\&\,\mathrm{A}(\mathbf{d}) \to \neg\mathrm{A}(\mathbf{e}) \mid \exists \mathrm{x}\ \neg\mathrm{A}(\mathrm{x})\ \rangle \arrow[dl] \arrow[drr, "L\to"] & & & \\
 & T_1 \arrow[dl, "R\exists"'] & & & T_2 \arrow[dl, "R\vee"] \arrow[dr] & \\
\begin{array}{c}\langle\ \neg\mathrm{A}(\mathbf{e}) \mid \exists \mathrm{x}\ \neg\mathrm{A}(\mathrm{x}), \neg\mathrm{A}(\mathbf{e})\ \rangle \\ \text{закр.таб.}\end{array} & & & T_3 \arrow[dll, "R\exists"] & & T_4 \arrow[d, "R\exists"] \\
 & T_5 \arrow[dl, "R\neg"'] & & & & T_6 \arrow[d, "R\neg"] \\
\begin{array}{c}\langle\ \mathrm{A}(\mathbf{c}) \mid \mathrm{A}(\mathbf{c}), \exists \mathrm{x}\ \neg\mathrm{A}(\mathrm{x})\ \rangle \\ \text{закр.таб.}\end{array} & & & & & \begin{array}{c}\langle\ \mathrm{A}(\mathbf{d}) \mid \mathrm{A}(\mathbf{d}), \exists \mathrm{x}\ \neg\mathrm{A}(\mathrm{x})\ \rangle \\ \text{закр.таб.}\end{array}
\end{tikzcd}
$$

Если для таблицы T_0 существует **успешный** табличный вывод,

то T_0 невыполнима

Полнота табличного вывода

А для любой ли

невыполнимой семантической таблицы
можно построить успешный табличный вывод?

В частности,

всегда ли мы можем убедиться в общезначимости формулы, используя только метод семантических таблиц?

Это и есть полнота табличного вывода

Теорема полноты табличного вывода
Если семантическая таблица невыполнима, то для неё существует успешный табличный вывод

Полнота табличного вывода: доказательство

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

Для простоты считаем, что

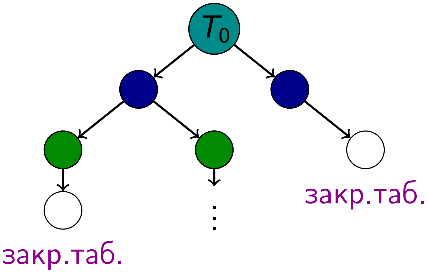
- множества Γ_0, Δ_0 конечны
- все формулы из Γ_0, Δ_0 замкнуты
- формулы из Γ_0, Δ_0 не содержат функциональных символов

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

Полнота табличного вывода: доказательство

При построении табличного вывода для T_0 будем придерживаться следующих правил:

1. Незакрытые неатомарные таблицы обрабатываются в порядке появления при построении вывода



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

Полнота табличного вывода: доказательство

При построении табличного вывода для T_0 будем придерживаться следующих правил:

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

$$\langle\ 1{:}\forall \mathtt{x}\ \varphi,\ 3{:}\psi_1 \to \psi_2 \mid 2{:}\chi_1 \vee \chi_2\ \rangle$$

$$\downarrow$$

$$\langle\ 2{:}\psi_1 \to \psi_2,\ 3{:}\forall \mathtt{x}\ \varphi,\ 4{:}\varphi' \mid 1{:}\chi_1 \vee \chi_2\ \rangle$$

$$\downarrow$$

$$\langle\ 1{:}\psi_1 \to \psi_2,\ 2{:}\forall \mathtt{x}\ \varphi,\ 3{:}\varphi' \mid 4{:}\chi_1,\ 5{:}\chi_2\ \rangle$$

$$\swarrow \qquad \searrow$$

$$\langle 1{:}\forall \mathtt{x}\ \varphi, 2{:}\varphi', 5{:}\psi_2 \mid 3{:}\chi_1, 4{:}\chi_2 \rangle \qquad \langle 1{:}\forall \mathtt{x}\ \varphi, 2{:}\varphi' \mid 3{:}\chi_1, 4{:}\chi_2, 5{:}\psi_1 \rangle$$

$$\cdots \qquad\qquad\qquad \cdots$$

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

Полнота табличного вывода: доказательство

При построении табличного вывода для T_0 будем придерживаться следующих правил:

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

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

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

Полнота табличного вывода: доказательство

Стратегия построения табличного вывода описана

Покажем, что вывод $\mathfrak{D}$, построенный по этой стратегии для невыполнимой таблицы $T_0 = \langle\ \Gamma_0 \mid \Delta_0\ \rangle$, успешен

Предположим, что это не так: вывод $\mathfrak{D}$ неуспешен

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

Тогда в полученном выводе обязательно найдётся бесконечная ветвь, состоящая только из незакрытых таблиц:

$$T_0 \to T_1 \to T_2 \to \dots$$

По имеющейся бесконечной ветви построим интерпретацию $\mathcal{I}$:

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

Полнота табличного вывода: доказательство

Имеем ветвь $T_0 \to T_1 \to T_2 \to \dots$, $T_i = \langle\ \Gamma_i \mid \Delta_i\ \rangle$

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

- предметная область D — это все константы во всех T_i:
  $$\mathrm{D} = \bigcup_{i \geq 0} \mathrm{Const}_i = \mathrm{Const}_\omega \qquad (\mathrm{Const}_i \text{ — все константы в } T_i)$$
- значение каждой константы — это её изображение:
  $$\overline{\mathbf{c}} = \mathbf{c}$$
- значение предиката = есть ли он хотя бы в одном Γ_i:
  $$\overline{\mathrm{P}}(\mathbf{c_1}, \dots, \mathbf{c_k}) = \mathbf{t} \qquad \Leftrightarrow \qquad \mathrm{P}(\mathbf{c_1}, \dots, \mathbf{c_k}) \in \bigcup_{i \geq 0} \Gamma_i = \Gamma_\omega$$

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 $\mathcal{I}$

Полнота табличного вывода: доказательство

База индукции: рассмотрим атом $\varphi \in \Gamma_\omega \cup \Delta_\omega$

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

- Пусть $\mathrm{P}(\mathbf{c_1}, \dots, \mathbf{c_k}) \in \Gamma_\omega$

  Тогда $\overline{\mathrm{P}}(\mathbf{c_1}, \dots, \mathbf{c_k}) = \mathbf{t}$, а значит, $\mathcal{I} \models \varphi$

- Пусть $\mathrm{P}(\mathbf{c_1}, \dots, \mathbf{c_k}) \in \Delta_\omega$

  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 $\mathcal{I} \not\models \varphi$

Полнота табличного вывода: доказательство

Индуктивный переход

Утверждение: если $\chi \in \Gamma_\omega$, то $\mathcal{I} \models \chi$; если $\chi \in \Delta_\omega$, то $\mathcal{I} \not\models \chi$

Предположение: если χ содержит менее N *логических операций* (связок и кванторов), то утверждение верно

Рассматриваемый случай: χ содержит N логических операций

Пусть $\chi = \varphi \to \psi \in \Gamma_\omega$

В ветви $T_0 \to T_1 \to \dots$ существует таблица T_i, такая что правило вывода применяется к χ в левой части (почему?)

Тогда верно хотя бы одно из двух:

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

Полнота табличного вывода: доказательство

Индуктивный переход

Утверждение: если $\chi \in \Gamma_\omega$, то $\mathcal{I} \models \chi$; если $\chi \in \Delta_\omega$, то $\mathcal{I} \not\models \chi$

Предположение: если χ содержит менее N *логических операций* (связок и кванторов), то утверждение верно

Рассматриваемый случай: χ содержит N логических операций

Пусть $\chi = \varphi \to \psi \in \Gamma_\omega$ $\quad \chi = \varphi \to \psi \in \Delta_\omega$

$\chi = \varphi \,\&\, \psi \in \Gamma_\omega$ $\quad \chi = \varphi \,\&\, \psi \in \Delta_\omega$

$\chi = \varphi \vee \psi \in \Gamma_\omega$ $\quad \chi = \varphi \vee \psi \in \Delta_\omega$

$\chi = \neg\varphi \in \Gamma_\omega$ $\quad \chi = \neg\varphi \in \Delta_\omega$

Во всех этих случаях рассуждения аналогичны

Полнота табличного вывода: доказательство

Индуктивный переход
Утверждение: если $\chi \in \Gamma_\omega$, то $\mathcal{I} \models \chi$; если $\chi \in \Delta_\omega$, то $\mathcal{I} \not\models \chi$
Предположение: если χ содержит менее N *логических операций* (связок и кванторов), то утверждение верно
Рассматриваемый случай: χ содержит N логических операций

Пусть $\chi = \forall \mathtt{x}\, \varphi \in \Gamma_\omega$

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

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

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

Пусть $\psi = \exists \mathtt{x}\, \varphi \in \Delta_\omega$
Рассуждения в этом случае аналогичны

Полнота табличного вывода: доказательство

Индуктивный переход
Утверждение: если $\chi \in \Gamma_\omega$, то $\mathcal{I} \models \chi$; если $\chi \in \Delta_\omega$, то $\mathcal{I} \not\models \chi$
Предположение: если χ содержит менее N *логических операций* (связок и кванторов), то утверждение верно
Рассматриваемый случай: χ содержит N логических операций

Пусть $\chi = \forall \mathtt{x}\, \varphi \in \Delta_\omega$

В одной из таблиц T_i к формуле χ в правой части **обязательно** применится правило $R\exists$

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

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

Пусть $\chi = \exists \mathtt{x}\, \varphi \in \Gamma_\omega$
Рассуждения в этом случае аналогичны

Полнота табличного вывода: доказательство

Имеем ветвь $T_0 \to T_1 \to T_2 \to \dots$, $T_i = \langle\, \Gamma_i \mid \Delta_i \,\rangle$

Итог: $\mathcal{I} \models \psi$ для всех $\psi \in \Gamma_\omega$, $\mathcal{I} \not\models \chi$ для всех $\chi \in \Delta_\omega$

Резюме доказательства: “*предположим*, что вывод, построенный для произвольной невыполнимой таблицы T_0 по особой стратегии, неуспешен; тогда в этом выводе существует ветвь, для которой верен *итог*”

Имеем: $\Gamma_0 \subseteq \Gamma_\omega$, $\Delta_0 \subseteq \Delta_\omega$

Значит, $\mathcal{I} \models \psi$ для всех $\psi \in \Gamma_0$ и $\mathcal{I} \not\models \chi$ для всех $\chi \in \Delta_0$

Из этого следует, что таблица T_0 **выполнима**

Значит, *предположение* о том, что построенный вывод неуспешен, неверно

Таким образом, описанная стратегия позволяет построить успешный вывод для **любой** невыполнимой таблицы ▼

Полнота табличного вывода: доказательство

А что изменится в доказательстве для общего случая?

То есть:

- какой порядок обработки формул позволит “справедливо” обращаться с бесконечными множествами формул?
- какие термы подставлять, если в сигнатуре алфавита есть функциональные символы?
- как работать с интерпретацией $\mathcal{I}$, если в таблицах встречаются незамкнутые формулы?

Полнота табличного вывода

Теорема Гёделя о полноте
(вариант для *исчисления* семантических таблиц)

$\models \varphi \quad \Leftrightarrow$ **для семантической таблицы** $\langle \quad \mid \varphi \ \rangle$
существует успешный табличный вывод

Доказательство.
Следует из корректности и полноты табличного вывода
(*и утверждения о связи общезначимости формулы и выполнимости соответствующей таблицы*)

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

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

Теорема Лёвенгейма-Сколема

Предложение φ выполнимо $\Leftrightarrow$ φ имеет модель с конечной или счётно-бесконечной 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

$\Gamma \models \varphi \quad \Leftrightarrow$ **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

В выводе $\mathfrak{D}$ правила применяются лишь к <u>конечному</u> подмножеству формул Γ' множества Γ (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

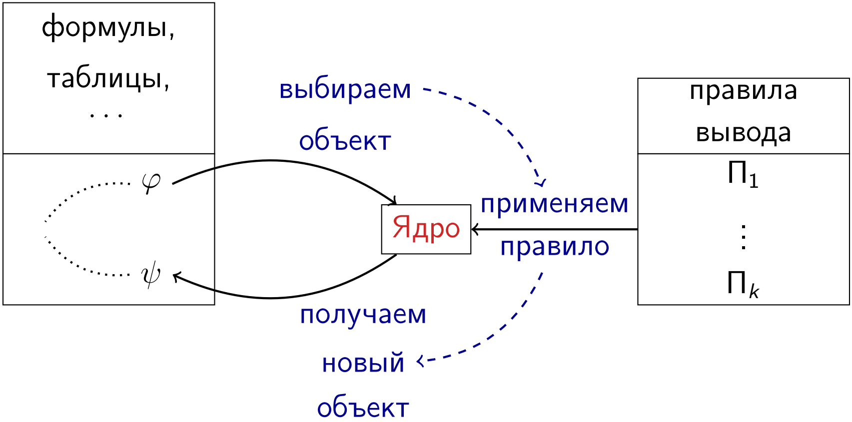
А может, все пруверы бесполезны — зачем их упоминать?

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, простоты и при этом “неоспоримой полезности” формулировки результата

Автоматическое доказательство теорем

Как выглядят 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)

Значит, проблема "$\models \varphi$?" полуразрешима, или

частично разрешима

Автоматическое доказательство теорем: теоретический взгляд

Неразрешимость проблемы общезначимости можно доказать обычным способом: взять известную неразрешимую проблему и **свести** её к “$\models \varphi$?”

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

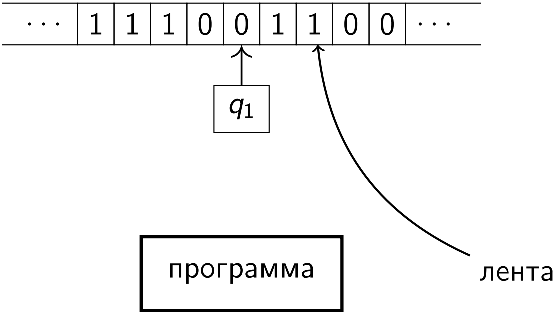
Что такое “свести”?

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

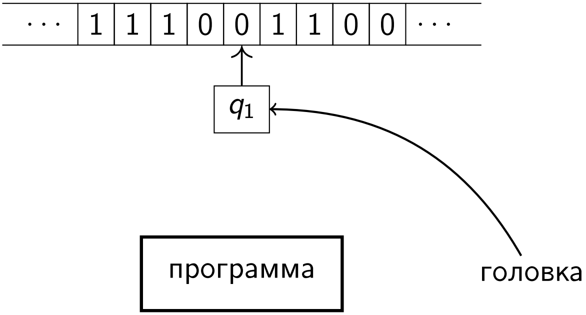
$$\mathbf{HALT}(M, w) \qquad \Leftrightarrow \qquad \models \varphi_{M,w}$$

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

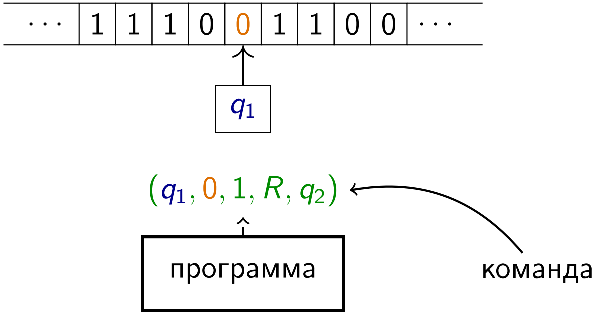
Машины Тьюринга (МТ)



Машины Тьюринга (МТ)



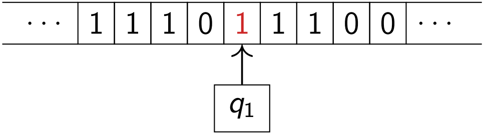
Машины Тьюринга (МТ)



Шаг вычисления выглядит так:

- по текущему состоянию и обозреваемому символу выбираем команду

Машины Тьюринга (МТ)



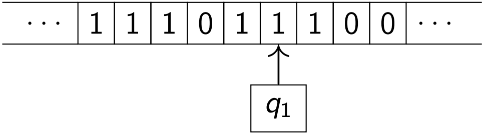
$$(q_1, 0, 1, R, q_2)$$

программа

Шаг вычисления выглядит так:

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

Машины Тьюринга (МТ)



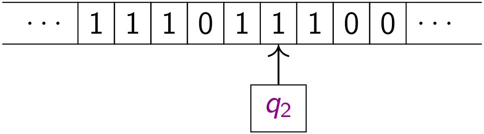
$$(q_1, 0, 1, R, q_2)$$

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)

Теперь 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

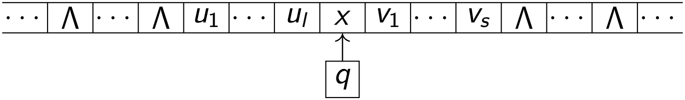
$\mathcal{Q}$ — конечный алфавит состояний, q_0 — начальное состояние

$(q_0 \in \mathcal{Q})$

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



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: из состояния q, обозревая символ a, записать в 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, задаваемое МТ M на множестве ленточных конфигураций, определяется так:

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

α — заключительная конфигурация МТ M, 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 C_{fin} **достижима** из начальной конфигурации $q_0\ w$:

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

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 $\varphi_{M,w}$:

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

Что будет записано в формуле:

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

$$\mathit{Start} \mathbin{\&} \mathit{Step} \to \mathit{Finish}$$

Теорема Чёрча: доказательство

Какие символы понадобятся в формуле:

- константа $\mathbf{a}$ для каждого $a \in \mathcal{A}$
- константа $\mathbf{q}$ для каждого $q \in \mathcal{Q}$
- операция конкатенации: $\cdot^{(2)}$

  (*ассоциативная вправо в инфиксной записи*)
- отношение достижимости конфигурации из начальной: $\mathrm{Re}^{(3)}$

Компоненты формулы $\varphi_{M,w}$:

- ленточное слово $a_1 \dots a_p$

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

- "конфигурация $u\ q\ v$ достижима" $\quad ((a_1 \dots a_p)^- = a_p \dots a_1)$

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

Теорема Чёрча: доказательство

Компоненты формулы $\varphi_{M,w}$:

- "начальная конфигурация достижима"

$$\mathit{Start}\colon \mathrm{Re}(\mathbf{\Lambda}, \mathbf{q_0}, \widetilde{w})$$

- "если текущая конфигурация достижима, то конфигурация после применения команды C будет достижима"

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

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

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

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

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

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

- "конфигурация, следующая за достижимой, также достижима"

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

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
- "хотя бы одна заключительная конфигурация достижима"

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

Возвращаемся к тому, что нужно доказать:

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

$\varphi_{M,w}$: $\textit{Start} \;\&\; \textit{Step} \to \textit{Finish}$

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

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, что $\mathbf{HALT}(M, w)$, но $\not\models \varphi_{M,w}$

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

$$\mathcal{I} \models \mathit{Start}, \qquad \mathcal{I} \models \mathit{Step}, \qquad \mathcal{I} \not\models \mathit{Finish}$$

Рассмотрим работу МТ M на слове w:

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

где $u_k\ q_k\ v_k$ — заключительная конфигурация

Используя эту последовательность конфигураций, докажем, что

$$\mathcal{I} \models \mathit{Finish}$$

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

Теорема Чёрча: доказательство, $\Rightarrow$

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

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

$$\mathcal{I} \models \mathit{Start}, \qquad \mathcal{I} \models \mathit{Step}, \qquad \mathcal{I} \not\models \mathit{Finish}$$

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

$\mathcal{I} \models \mathit{Start}$ по рассматриваемому случаю

$\mathcal{I} \models \mathrm{Re}(\widetilde{u_1^-}, \mathbf{q_1}, \widetilde{v_1})$, так как $\mathit{Start}, \mathit{Step} \models \mathrm{Re}(\widetilde{u_1^-}, \mathbf{q_1}, \widetilde{v_1})$

...

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

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

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

Но согласно *исходному предположению*, верно $\mathcal{I} \not\models \mathit{Finish}$

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 эффективно?

- 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 $\text{Растёт}(\textbf{бузина}, \textbf{огород})$	В Киеве дядька $\exists y\ (\text{Дядька}(y)$ $\quad \& \text{ Живёт}(y, \textbf{Киев}))$
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 $\forall x\ (\text{Посадил}(x, \textbf{бузина})$ $\quad \to \text{Живёт}(x, \textbf{Киев}))$	

Автоматическое доказательство теорем: практический взгляд

Выбор терма

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

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

Из **одного** функционального символа $\mathbf{f}^{(2)}$ и **двух** констант c_1, c_2 можно построить более 10^{300} термов с 10-ю вложенными парами скобок

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

Конец лекции 5