Математическая логика

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

Лекция 10

Полнота резолютивного вывода
Задачи и проблемы
Алгоритмы
Разрешимость
М-сводимость

Лектор:
Подымов Владислав Васильевич

E-mail:
valdus@yandex.ru

ВМК МГУ, 2020, весенний семестр

Напоминание

Система *дизъюнктов*: $S = \{\mathrm{P}(\mathbf{f}(\mathrm{x})),\ \neg\mathrm{Q}(\mathbf{c},\mathrm{x}),\ \mathrm{Q}(\mathrm{x},\mathrm{y}) \vee \neg\mathrm{P}(\mathrm{y})\}$

Резолютивный вывод пустого дизъюнкта $\square$ из S:

$$\begin{array}{rl}
\text{вариант} & \mathrm{P}(\mathbf{f}(\mathrm{x}_1)) \\
\text{вариант} & \mathrm{Q}(\mathrm{x}_2,\mathrm{y}_2) \vee \neg\mathrm{P}(\mathrm{y}_2) \\
\text{резольвента} & \mathrm{Q}(\mathrm{x}_3,\mathbf{f}(\mathrm{x}_1)) \\
\text{вариант} & \mathrm{P}(\mathbf{f}(\mathrm{x}_1)) \\
\text{резольвента} & \square
\end{array}$$

Корректность вывода: если $\square$ резолютивно выводим из S, то $\not\models S$

Полнота вывода: если $\not\models S$, то $\square$ резолютивно выводим из S

Полнота резолютивного вывода

Теорема(*о полноте резолютивного вывода*)
Из любой противоречивой системы дизъюнктов резолютивно выводим пустой дизъюнкт

Схема доказательства:

1. Рассмотрим противоречивую систему дизъюнктов S
2. По *теореме Эрбрана*, существует конечное противоречивое множество $\mathcal{G}$ основных примеров дизъюнктов из S
3. Покажем, что $\square$ резолютивно выводим из $\mathcal{G}$
   (*лемма об основных дизъюнктах*)
4. По выводу $\square$ из $\mathcal{G}$ построим вывод $\square$ из S
   (две *леммы о подъёме*)

(*Полное доказательство приводится дальше*)

Полнота резолютивного вывода

Лемма(*об основных дизъюнктах*). Из любой конечной противоречивой системы основных дизъюнктов резолютивно выводим пустой дизъюнкт

Доказательство.

Рассмотрим произвольную конечную противоречивую систему основных дизъюнктов S

Докажем лемму индукцией
по числу $\|S\|$ различных атомов, содержащихся в S

База: $\|S\| = 0$

$\not\models S \quad \Rightarrow \quad S \neq \emptyset$

$S \neq \emptyset$ *и* $\|S\| = 0 \quad \Rightarrow \quad S = \{\square\} \quad \Rightarrow \quad \square$ выводим из S

Полнота резолютивного вывода

Доказательство (леммы). Переход: $\not\models S$, $\|S\| = N > 0$; $\quad S \overset{?}{\rightsquigarrow} \square$?

Индуктивное предположение: $\not\models \widetilde{S}$ и $\|\widetilde{S}\| < N \quad \Rightarrow \quad \widetilde{S} \rightsquigarrow \square$

Перейдём от S к системе дизъюнктов S',
удалив все дизъюнкты вида $D \vee A \vee \neg A$

$\not\models S$*, и все удаляемые дизъюнкты общезначимы*
$\Rightarrow \quad \not\models S'$, и достаточно предложить вывод $\square$ из S'

Перейдём от S' к системе S'' так: пока это возможно,
будем заменять дизъюнкты вида $D \vee L \vee L$ на их склейки $D \vee L$

$\not\models S'$*, и дизъюнкты заменяются на равносильные выводимые*
$\Rightarrow \quad \not\models S''$, и достаточно предложить вывод $\square$ из S''

Если $\|S''\| < N$, то обоснование завершено

Предположим теперь, что $\|S''\| = N$

Полнота резолютивного вывода

Доказательство (леммы). *Переход:* $\not\models S''$, $\|S''\| = N > 0$,

и в S'' нет дизъюнктов вида $D \vee L \vee \neg L$ и $D \vee L \vee L$; $\quad S'' \overset{?}{\rightsquigarrow} \square$

Индуктивное предположение: $\not\models \widetilde{S}$, $\|\widetilde{S}\| < N \quad \Rightarrow \quad \widetilde{S} \rightsquigarrow \square$

Произвольно выберем атом A,
содержащийся хотя бы в одном дизъюнкте из S''

Разобьём S'' на три множества:

- S_+ — все дизъюнкты из S'', содержащие A
- S_- — все дизъюнкты из S'', содержащие $\neg A$
- $S_\times$ — все дизъюнкты из S'', не содержащие атом A

Построим все резольвенты по контрарной паре A, $\neg A$:

$$S_r = \{D_1 \vee D_2 \mid D_1 \vee A \in S_+,\ D_2 \vee \neg A \in S_-\}$$

Достаточно показать, что $\square$ выводим из системы $S''' = S_r \cup S_\times$

$\|S'''\| = \|S''\| - 1 = N - 1 < N$, а значит, по предположению индукции, достаточно обосновать соотношение $\not\models S'''$

Полнота резолютивного вывода

Доказательство (леммы). Переход:

$\not\models S''$: $S_+ \boxed{\dots\ D_+ \vee A \dots}$ $S_- \boxed{\dots\ D_- \vee \neg A \dots}$ $S_\times \boxed{\text{дизъ. без } A}$

$\not\models ?\ S'''$: $S_r \boxed{\dots\ D_+ \vee D_-\ \dots}$ $S_\times \boxed{\text{дизъ. без } A}$

Рассмотрим произвольную $\mathcal{H}$-интерпретацию $\mathcal{I}$

По *теореме об эрбрановских интерпретациях*,
достаточно обосновать соотношение $\mathcal{I} \not\models S'''$

$\not\models S'' \Rightarrow \mathcal{I} \not\models S''$

Случай 1: $\mathcal{I} \not\models S_\times$. $S_\times \subseteq S''' \Rightarrow \mathcal{I} \not\models S'''$

Случай 2: $\mathcal{I} \models S_\times$, $A \in \mathcal{I}$

$A \in \mathcal{I} \Rightarrow \mathcal{I} \models S_+$

$\mathcal{I} \models S_+ \cup S_\times$ и $\mathcal{I} \not\models S_+ \cup S_\times \cup S_- \Rightarrow \mathcal{I} \not\models S_-$
$\Rightarrow$ в S_- содержится дизъюнкт $D_- \vee \neg A$, такой что $\mathcal{I} \not\models D_- \vee \neg A$
$\Rightarrow \mathcal{I} \not\models D_-$

Полнота резолютивного вывода

Доказательство (леммы). *Переход:*

$$\not\models S'': S_+ \boxed{\dots\ D_+ \vee A \dots} \qquad S_- \boxed{\dots\ D_- \vee \neg A \dots} \qquad S_\times \boxed{\text{дизъ. без } A}$$

$$\mathcal{I} \not\models ?\ S''': \qquad S_r \boxed{\dots\ D_+ \vee D_-\ \dots} \qquad S_\times \boxed{\text{дизъ. без } A}$$

Случай 2: $\mathcal{I} \models S_\times$, $A \in \mathcal{I}$; получено: $\mathcal{I} \not\models D_-$, $D_- \vee \neg A \in S_-$

Рассмотрим $\mathcal{H}$-интерпретацию $\mathcal{J} = \mathcal{I} \setminus \{A\}$

$\mathcal{I} \models S_\times$, *и в дизъюнктах из* $S_\times$ *не содержится атом* $A \Rightarrow \mathcal{J} \models S_\times$

$\not\models S'' \Rightarrow \mathcal{J} \not\models S''$

$A \notin \mathcal{J}$, *и дизъюнкты из* S_- *имеют вид* $D \vee \neg A \Rightarrow \mathcal{J} \models S_-$

$\mathcal{J} \models S_- \cup S_\times$ *и* $\mathcal{J} \not\models S_- \cup S_\times \cup S_+ \Rightarrow \mathcal{J} \not\models S_+ \Rightarrow$ в S_+ содержится дизъюнкт $D_+ \vee \neg A$, такой что $\mathcal{J} \not\models D_+ \vee \neg A \Rightarrow \mathcal{J} \not\models D_+$

$\mathcal{J} \not\models D_+$, *и в* D_+ *не содержится атом* $A \Rightarrow \mathcal{I} \not\models D_+$

$\mathcal{I} \not\models D_+, \mathcal{I} \not\models D_- \Rightarrow \mathcal{I} \not\models D_+ \vee D_-$

$\mathcal{I} \not\models D_+ \vee D_-$, $D_+ \vee D_- \in S_r \Rightarrow \mathcal{I} \not\models S_r \Rightarrow \mathcal{I} \not\models S'''$

Случай 3: $\mathcal{I} \models S_\times$, $A \notin \mathcal{I}$ — аналогичен случаю 2 ▼

Полнота резолютивного вывода

Лемма(*о подъёме для правила резолюции*)

Пусть:

- D_1, D_2 — дизъюнкты, и $\mathrm{Var}_{D_1} \cap \mathrm{Var}_{D_2} = \emptyset$;
- D'_1, D'_2 — основные примеры дизъюнктов D_1, D_2 соответственно;
- D' — резольвента дизъюнктов D'_1, D'_2.

Тогда существует резольвента D дизъюнктов D_1, D_2, примером которой является D'.

$$
\begin{tikzcd}
D_1 \arrow[dr] \arrow[dd, "\theta_1"'] & & D_2 \arrow[dl] \arrow[dd, "\theta_2"] \\
& D \arrow[dd, "\theta"] & \\
D'_1 \arrow[dr] & & D'_2 \arrow[dl] \\
& D' &
\end{tikzcd}
$$

Доказательство леммы о подъёме

$$\begin{tikzcd}
D_1 \arrow[d] & & D_2 \arrow[d] \\
D_1' \arrow[dr] & & D_2' \arrow[dl] \\
& D' &
\end{tikzcd}$$

Доказательство леммы о подъёме

$$
\begin{tikzcd}
D_1 \arrow[d] & & D_2 \arrow[d] \\
D_1'' \vee A \arrow[dr] & & D_2'' \vee \neg A \arrow[dl] \\
& D_1'' \vee D_2'' &
\end{tikzcd}
$$

Выделим в D_1', D_2' контрарную пару A, $\neg A$ для резольвенты D'

Доказательство леммы о подъёме

$$\begin{tikzcd}
D_1 \arrow[d, "\theta_1"'] & & D_2 \arrow[d, "\theta_2"] \\
D_1'' \vee A \arrow[dr] & & D_2'' \vee \neg A \arrow[dl] \\
& D_1'' \vee D_2'' &
\end{tikzcd}$$

Выделим в D_1', D_2' контрарную пару A, $\neg A$ для резольвенты D'

Пусть, для ясности, $D_1' = D_1\theta_1$ и $D_2' = D_2\theta_2$

Доказательство леммы о подъёме

$$
\begin{array}{ccccc}
D_1''' \lor B_1 & & & & D_2''' \lor \neg B_2 \\
\theta_1 \big\downarrow & & & & \big\downarrow \theta_2 \\
(D_1''' \lor B_1)\theta_1 & & & & (D_2''' \lor \neg B_2)\theta_2 \\
& \longrightarrow & D_1'''\theta_1 \lor D_2'''\theta_2 & \longleftarrow &
\end{array}
$$

Выделим в D_1', D_2' контрарную пару A, $\neg A$ для резольвенты D'

Пусть, для ясности, $D_1' = D_1\theta_1$ и $D_2' = D_2\theta_2$

Выделим в D_1, D_2 литеры B_1, $\neg B_2$, породившие контрарную пару

Доказательство леммы о подъёме

$$\begin{tikzcd}
D_1''' \vee B_1 \arrow[d, "\eta"'] & & D_2''' \vee \neg B_2 \arrow[d, "\eta"] \\
(D_1''' \vee B_1)\eta \arrow[dr] & & (D_2''' \vee \neg B_2)\eta \arrow[dl] \\
& (D_1''' \vee D_2''')\eta &
\end{tikzcd}$$

Выделим в D_1', D_2' контрарную пару A, $\neg A$ для резольвенты D'

Пусть, для ясности, $D_1' = D_1\theta_1$ и $D_2' = D_2\theta_2$

Выделим в D_1, D_2 литеры B_1, $\neg B_2$, породившие контрарную пару

Без ограничения общности положим, что $\mathrm{D}_{\theta_1} \cap \mathrm{D}_{\theta_2} = \emptyset$

Тогда для подстановки $\eta = \theta_1 \cup \theta_2$ верно $D_1' = D_1\eta$ и $D_2' = D_2\eta$

Доказательство леммы о подъёме

$$
\begin{tikzcd}
D_1''' \vee B_1 \arrow[d, "\eta"'] \arrow[r] & (D_1''' \vee D_2''')\mu & D_2''' \vee \neg B_2 \arrow[d, "\eta"] \arrow[l] \\
(D_1''' \vee B_1)\eta \arrow[r] & (D_1''' \vee D_2''')\eta & (D_2''' \vee \neg B_2)\eta \arrow[l]
\end{tikzcd}
$$

Выделим в D_1', D_2' контрарную пару A, $\neg A$ для резольвенты D'

Пусть, для ясности, $D_1' = D_1\theta_1$ и $D_2' = D_2\theta_2$

Выделим в D_1, D_2 литеры B_1, $\neg B_2$, породившие контрарную пару

Без ограничения общности положим, что $\mathrm{D}_{\theta_1} \cap \mathrm{D}_{\theta_2} = \emptyset$

Тогда для подстановки $\eta = \theta_1 \cup \theta_2$ верно $D_1' = D_1\eta$ и $D_2' = D_2\eta$

По *теореме об унификации*,

существует наиболее общий унификатор μ атомов B_1, B_2

Значит, $(D_1''' \vee D_2''')\mu$ — резольвента дизъюнктов D_1, D_2

Доказательство леммы о подъёме

$$
\begin{tikzcd}
D_1''' \lor B_1 \arrow[d, "\mu\theta"'] \arrow[r] & (D_1''' \lor D_2''')\mu & D_2''' \lor \neg B_2 \arrow[l] \arrow[d, "\mu\theta"] \\
(D_1''' \lor B_1)\mu\theta \arrow[dr] & & (D_2''' \lor \neg B_2)\mu\theta \arrow[dl] \\
& (D_1''' \lor D_2''')\mu\theta &
\end{tikzcd}
$$

Выделим в D_1', D_2' контрарную пару A, $\neg A$ для резольвенты D'

Пусть, для ясности, $D_1' = D_1\theta_1$ и $D_2' = D_2\theta_2$

Выделим в D_1, D_2 литеры B_1, $\neg B_2$, породившие контрарную пару

Без ограничения общности положим, что $\mathrm{D}_{\theta_1} \cap \mathrm{D}_{\theta_2} = \emptyset$

Тогда для подстановки $\eta = \theta_1 \cup \theta_2$ верно $D_1' = D_1\eta$ и $D_2' = D_2\eta$

По *теореме об унификации*,

существует наиболее общий унификатор μ атомов B_1, B_2

Значит, $(D_1''' \lor D_2''')\mu$ — резольвента дизъюнктов D_1, D_2

По *определению наиболее общего унификатора*,

существует подстановка θ, такая что $\eta = \mu\theta$

Доказательство леммы о подъёме

$$\begin{tikzcd}
D_1''' \vee B_1 \arrow[dr] \arrow[dd, "\mu\theta"'] & & D_2''' \vee \neg B_2 \arrow[dl] \arrow[dd, "\mu\theta"] \\
& (D_1''' \vee D_2''')\mu \arrow[dd, "\theta"] & \\
(D_1''' \vee B_1)\mu\theta \arrow[dr] & & (D_2''' \vee \neg B_2)\mu\theta \arrow[dl] \\
& (D_1''' \vee D_2''')\mu\theta &
\end{tikzcd}$$

Выделим в D_1', D_2' контрарную пару A, $\neg A$ для резольвенты D'

Пусть, для ясности, $D_1' = D_1\theta_1$ и $D_2' = D_2\theta_2$

Выделим в D_1, D_2 литеры B_1, $\neg B_2$, породившие контрарную пару

Без ограничения общности положим, что $\mathrm{D}_{\theta_1} \cap \mathrm{D}_{\theta_2} = \emptyset$

Тогда для подстановки $\eta = \theta_1 \cup \theta_2$ верно $D_1' = D_1\eta$ и $D_2' = D_2\eta$

По *теореме об унификации*,

существует наиболее общий унификатор μ атомов B_1, B_2

Значит, $(D_1''' \vee D_2''')\mu$ — резольвента дизъюнктов D_1, D_2

По *определению наиболее общего унификатора*,

существует подстановка θ, такая что $\eta = \mu\theta$, и $D' = D\theta$ ▼

Полнота резолютивного вывода

Лемма(*о подъёме для правила склейки*)
Пусть:

- D_1, D_1' — дизъюнкт и его основной пример;
- D' — склейка дизъюнкта D_1'.

Тогда существует склейка D дизъюнкта D_1, примером которой является D'.

$$\begin{tikzcd}
D_1 \arrow[d, "\theta_1"'] \arrow[dr] & \\
D_1' \arrow[dr] & D \arrow[d, "\theta"] \\
 & D'
\end{tikzcd}$$

Доказательство. Аналогично доказательству леммы о подъёме для правила резолюции ▼

Теорема о полноте резолютивного вывода

Из любой противоречивой системы дизъюнктов резолютивно выводим пустой дизъюнкт

Доказательство.

Рассмотрим произвольную противоречивую систему дизъюнктов S

По *теореме Эрбрана*, существует конечное противоречивое множество $\mathcal{G}$ основных примеров дизъюнктов из S

По *лемме об основных дизъюнктах*,
существует вывод $D_1', \ldots, D_n', \Box$ из $\mathcal{G}$

Теорема о полноте резолютивного вывода

Из любой противоречивой системы дизъюнктов резолютивно выводим пустой дизъюнкт

Доказательство. ($D'_1, \ldots, D'_n, \square$ — вывод из $\mathcal{G}$)

Рассмотрим такую последовательность дизъюнктов $\mathfrak{S} = (D_1, \ldots, D_n, \square)$:

- если D'_i — **пример** дизъюнкта D из S, то D_i — вариант D
- если D'_i — **резольвента** D'_j и D'_k ($j < i$, $k < i$), то D_i — резольвента D_j и D_k, примером которой является D'_j
- если D'_i — **склейка** D'_j ($j < i$), то D_i — склейка D_j, примером которой является D'_j
- подстановки (переименования и унификаторы) выберем так, чтобы множества Var_{D_i} попарно непересекались

Корректность задания $\mathfrak{S}$ обеспечивается *леммами о подъёме*

По *определению резолютивного вывода*, $\mathfrak{S}$ — вывод $\square$ из S ▼

Теорема о полноте резолютивного вывода

В доказательстве *теоремы о полноте табличного вывода* приводился свод правил, которых достаточно придерживаться, чтобы получить успешный вывод для **любой** невыполнимой таблицы

В доказательстве *теоремы о полноте резолютивного вывода* не было ничего похожего на такой свод правил

Для самостоятельного размышления:
Каких правил достаточно придерживаться при построении резолютивного вывода, чтобы гарантированно вывести $\square$ из **любой** противоречивой системы дизъюнктов?

Метод резолюций: заключительный пример

Метод резолюций оказался хорошим средством проверки общезначимости формул логики предикатов:

- он корректен (*доказано*)
- он полон (*доказано*)
- он эффективен
  (*всего два правила,*
  и они применяются практически однозначно)

Напоследок обсудим на простом показательном примере, как можно использовать этот метод для решения практических задач

Метод резолюций: заключительный пример

Известно, что:

1. Даша любит Сашу
2. Саша любит пиво
3. Паша любит пиво и всех тех, кто любит то же, что и он

Вопрос 1. Любит ли кто-нибудь Дашу?

Вопрос 2. Если кто-то любит Дашу, то кто?

Запишем задачу на языке логики предикатов:

- *предикатный символ* — $\mathrm{L}^{(2)}$: "$\mathrm{L}(\mathrm{x}, \mathrm{y})$" = "икс любит игрека"
- *константы*: **Даша**, **Саша**, **Паша**, **пиво**

1. $\varphi_1 = \mathrm{L}(\textbf{Даша}, \textbf{Саша})$
2. $\varphi_2 = \mathrm{L}(\textbf{Саша}, \textbf{пиво})$
3. $\varphi_3 = \mathrm{L}(\textbf{Паша}, \textbf{пиво})$,
   $\varphi_4 = \forall \mathrm{x}\ (\exists \mathrm{y}\ (\mathrm{L}(\textbf{Паша}, \mathrm{y})\ \&\ \mathrm{L}(\mathrm{x}, \mathrm{y})) \to \mathrm{L}(\textbf{Паша}, \mathrm{x}))$

Вопрос 1: $\varphi_1, \varphi_2, \varphi_3, \varphi_4 \models \varphi$? $(\varphi = \exists \mathrm{z}\ \mathrm{L}(\mathrm{z}, \textbf{Даша}))$

Метод резолюций: заключительный пример

Теорема о логическом следствии:

$\varphi_1, \varphi_2, \varphi_3, \varphi_4 \models \varphi \quad \Leftrightarrow \quad \models \varphi_1 \,\&\, \varphi_2 \,\&\, \varphi_3 \,\&\, \varphi_4 \to \varphi$

Этап 1: ставим отрицание над формулой

$$\neg(\varphi_1 \,\&\, \varphi_2 \,\&\, \varphi_3 \,\&\, \varphi_4 \to \varphi)$$

Этап 2: строим равносильную ПНФ

$$\forall \mathrm{x}\, \forall \mathrm{y}\, \forall \mathrm{z} \left(\begin{array}{c} \mathrm{L}(\textbf{Даша}, \textbf{Саша}) \,\&\, \mathrm{L}(\textbf{Саша}, \textbf{пиво}) \,\&\, \mathrm{L}(\textbf{Паша}, \textbf{пиво}) \\ \&(\neg \mathrm{L}(\textbf{Паша}, \mathrm{y}) \vee \neg \mathrm{L}(\mathrm{x}, \mathrm{y}) \vee \mathrm{L}(\textbf{Паша}, \mathrm{x})) \\ \& \neg \mathrm{L}(\mathrm{z}, \textbf{Даша}) \end{array} \right)$$

Этап 3: строим равновыполнимую ССФ

Формула выше — ССФ

Этап 4: переходим к системе дизъюнктов:

$$S = \left\{ \begin{array}{c} \mathrm{L}(\textbf{Даша}, \textbf{Саша}),\ \mathrm{L}(\textbf{Саша}, \textbf{пиво}),\ \mathrm{L}(\textbf{Паша}, \textbf{пиво}), \\ \neg \mathrm{L}(\textbf{Паша}, \mathrm{y}) \vee \neg \mathrm{L}(\mathrm{x}, \mathrm{y}) \vee \mathrm{L}(\textbf{Паша}, \mathrm{x}), \\ \neg \mathrm{L}(\mathrm{z}, \textbf{Даша}) \end{array} \right\}$$

Метод резолюций: заключительный пример

Этап 5: пытаемся вывести пустой дизъюнкт

$$
\begin{array}{rcl}
 & \neg \mathrm{L}(z, \textbf{Даша}) & \\
\{z/\textbf{Паша}, x'/\textbf{Даша}, y'/y\} & \downarrow & \neg \mathrm{L}(\textbf{Паша}, y') \lor \neg \mathrm{L}(x', y') \lor \mathrm{L}(\textbf{Паша}, x') \\
 & \neg \mathrm{L}(\textbf{Паша}, y) \lor \neg \mathrm{L}(\textbf{Даша}, y) \leftarrow & \\
\{y/\textbf{Саша}\} & \downarrow & \mathrm{L}(\textbf{Даша}, \textbf{Саша}) \\
 & \neg \mathrm{L}(\textbf{Паша}, \textbf{Саша}) \leftarrow & \\
\{x'/\textbf{Саша}, y'/y\} & \downarrow & \neg \mathrm{L}(\textbf{Паша}, y') \lor \neg \mathrm{L}(x', y') \lor \mathrm{L}(\textbf{Паша}, x') \\
 & \neg \mathrm{L}(\textbf{Паша}, y) \lor \neg \mathrm{L}(\textbf{Саша}, y) \leftarrow & \\
\{y/\textbf{пиво}\} & \downarrow & \mathrm{L}(\textbf{Паша}, \textbf{пиво}) \\
 & \neg \mathrm{L}(\textbf{Саша}, \textbf{пиво}) \leftarrow & \\
\varepsilon & \downarrow & \mathrm{L}(\textbf{Саша}, \textbf{пиво}) \\
 & \square \leftarrow &
\end{array}
$$

Ответ 1: $\varphi_1, \varphi_2, \varphi_3, \varphi_4 \models \varphi$ — кто-то действительно любит Дашу

Вопрос 2: а кто?

Метод резолюций: заключительный пример

$\theta_1 = \{z/\textbf{Паша}, x'/\textbf{Даша}, y'/y\}$

$\theta_2 = \{y/\textbf{Саша}\}$

$\theta_3 = \{x'/\textbf{Саша}, y'/y\}$

$\theta_4 = \{y/\textbf{пиво}\}$

$\theta_5 = \varepsilon$

$$\begin{array}{c}
\neg L(z, \textbf{Даша}) \\
\downarrow \\
\neg L(\textbf{Паша}, y) \vee \neg L(\textbf{Даша}, y) \\
\downarrow \\
\neg L(\textbf{Паша}, \textbf{Саша}) \\
\downarrow \\
\neg L(\textbf{Паша}, y) \vee \neg L(\textbf{Саша}, y) \\
\downarrow \\
\neg L(\textbf{Саша}, \textbf{пиво}) \\
\downarrow \\
\square
\end{array}$$

Тайный поклонник Даши в выводе обозначен переменной z

Посмотрим, как эта переменная изменялась унификаторами:

$$z \xrightarrow{\theta_1} \textbf{Паша} \xrightarrow{\theta_2\theta_3\theta_4\theta_5} \textbf{Паша}$$

Ответ 2: Паша любит Дашу (*но могут быть и другие поклонники*)

А как **строго** сформулировать и обосновать утверждение о том, что в такой композиции подстановок обязательно записан ответ к задаче, и для каких выводов это утверждение справедливо?

Интерлюдия

Корректность и полнота метода семантических таблиц:
$\models \varphi \Leftrightarrow$ для таблицы $\langle \ \mid \varphi \ \rangle$ **существует** успешный вывод

Корректность и полнота метода резолюций:
$\models \varphi \Leftrightarrow$ для соответствующей системы дизъюнктов **существует** успешный вывод

А можно ли написать программу, которая автоматически проверяет общезначимость **любой** формулы φ?
(*например, строит соответствующий вывод, если* $\models \varphi$,
и выдаёт ответ "такого вывода нет", если $\not\models \varphi$)

Оказывается, что написать такую программу **невозможно**,
и далее строго формулируется и обосновывается этот факт

Аналогичные утверждения для других задач, как и бо́льшая часть сопутствующих определений, известны вам из других курсов,
но всё же полезно будет всё это повторить ещё раз

Задачи и проблемы

У Васи есть 5 яблок. 2 яблока он отдал Коле.
Сколько яблок осталось у Васи?

Это пример того, что принято называть задачей

Более точно, это индивидуальная задача:
ответ к этой задаче — конкретный предмет (число)

У васи есть N яблок. K яблок ($K \leq N$) он отдал Коле.
Сколько яблок осталось у Васи?

Это также пример того, что принято называть задачей

Ответ к этой задаче определяется
значениями параметров (входными данными) N и K

Такие (*параметризованные*) задачи принято называть
массовыми задачами, или, по-другому, проблемами

Задачи и проблемы

Массовую задачу $\mathfrak{T}$
можно понимать как отображение $\mathfrak{T} : \mathfrak{I} \to \mathfrak{O}$, где

- $\mathfrak{I}$ — множество всевозможных входных данных (входов)
- $\mathfrak{O}$ — множество всевозможных
выходных данных (выходов; ответов)
- значение $\mathfrak{T}(\mathfrak{i})$ — правильный ответ для входа $\mathfrak{i}$

Например, последняя задача о яблоках — это отображение
$\mathfrak{T} : \{(n, k) \mid n, k \in \mathbb{N}_0,\ k \leq n\} \to \mathbb{N}_0$, где

- $\mathbb{N}_0$ — множество всех неотрицательных целых чисел
- $\mathfrak{T}(n, k) = n - k$

Алгоритмы и разрешимость

Алгоритм — это особая совокупность действий,[1] согласно которой *входы* заданного множества $\mathfrak{I}$ преобразуются в *ответы* заданного множества $\mathfrak{O}$ (или не преобразуются, если к данным применяется бесконечно много действий)[2]

Алгоритмом $\mathcal{A}$ реализуется *частично определённое* отображение $\overline{\mathcal{A}} : \mathfrak{I} \to \mathfrak{O}$ следующего вида:

- если к входу $\mathfrak{i}$ применяется конечное число действий, то $\overline{\mathcal{A}}(\mathfrak{i})$ — ответ, вычисляемый алгоритмом
  - и алгоритм останавливается (завершается) на входе $\mathfrak{i}$
- иначе значение $\overline{\mathcal{A}}(\mathfrak{i})$ не определено
  - и алгоритм не останавливается (не завершается) на входе $\mathfrak{i}$

[1] Вспоминайте из других курсов, какая именно совокупность каких действий

[2] На самом деле бывают и другие алгоритмы, согласно которым выходные данные получаются многократно, или постоянно, или понятие выходных данных отсутствует — но не будем всё переусложнять

Алгоритмы и разрешимость

Алгоритмы[1] придумываются для того,
чтобы **решать** *массовые задачи*

Алгоритм $\mathcal{A}$ решает задачу $\mathfrak{T} : \mathfrak{I} \to \mathfrak{O}$, если $\overline{\mathcal{A}} = \mathfrak{T}$, то есть

- $\mathcal{A}$ и $\mathfrak{T}$ определены
  для одинаковых множеств входных и выходных данных, и
- $\mathcal{A}$ завершается на любом входе
  и всегда вычисляет правильный ответ к задаче $\mathfrak{T}$

Массовая задача (алгоритмически) разрешима,
если существует алгоритм, решающий эту задачу,
и неразрешима, если такого алгоритма не существует

[1] Как минимум такие алгоритмы, как на предыдущем слайде

M-сводимость

Задача распознавания — это массовая задача
с множеством ответов $\{\textbf{да}, \textbf{нет}\}$ (оно же $\{1, 0\}$, оно же $\{\mathbf{t}, \mathbf{f}\}$)

Задача распознавания $\mathfrak{T}_1 : \mathfrak{I}_1 \to \{1, 0\}$ m-сводится[1]
к задаче распознавания $\mathfrak{T}_2 : \mathfrak{I}_2 \to \{1, 0\}$,
если существует алгоритм $\mathcal{A}$, такой что

- $\overline{\mathcal{A}} : \mathfrak{I}_1 \to \mathfrak{I}_2$ — всюду определённое отображение и
- для любого входа $\mathfrak{i}$ задачи $\mathfrak{T}_1$ верно $\mathfrak{T}_1(\mathfrak{i}) = \mathfrak{T}_2(\mathcal{A}(\mathfrak{i}))$

Обозначенный алгоритм $\mathcal{A}$ m-сводит задачу $\mathfrak{T}_1$ к задаче $\mathfrak{T}_2$

---

[1] Many-one reducible: разным входным данным $\mathfrak{T}_1$ могут соответствовать одинаковые входные данные $\mathfrak{T}_2$. Этот вид сводимости (*должен быть*) вам известен из доказательства неразрешимости проблемы останова машин Тьюринга: эта проблема m-сводилась к проблеме самоприменимости

М-сводимость

Теорема(*об m-сводимости*). Если задача $\mathfrak{T}_1$ m-сводима к разрешимой задаче $\mathfrak{T}_2$, то задача $\mathfrak{T}_1$ также разрешима

Доказательство.[1]

$\mathfrak{T}_2$ разрешима $\Rightarrow$ существует алгоритм $\mathcal{A}$, решающий $\mathfrak{T}_2$

$\mathfrak{T}_1$ m-сводима к $\mathfrak{T}_2$ $\Rightarrow$ существует алгоритм $\mathcal{B}$, m-сводящий $\mathfrak{T}_1$ к $\mathfrak{T}_2$

Тогда существует и алгоритм решения задачи $\mathfrak{T}_1$:

последовательно примéним $\mathcal{B}$ и $\mathcal{A}$ к входу $\mathfrak{i}$ задачи $\mathfrak{T}_1$ $(\mathfrak{i} \xrightarrow{\mathcal{B}} \mathfrak{j} \xrightarrow{\mathcal{A}} \mathfrak{o})$

По выбору алгоритма $\mathcal{A}$, $\overline{\mathcal{A}}(\overline{\mathcal{B}}(\mathfrak{i})) = \mathfrak{T}_2(\mathcal{B}(\mathfrak{i}))$

По выбору алгоритма $\mathcal{B}$, $\mathfrak{T}_2(\mathcal{B}(\mathfrak{i})) = \mathfrak{T}_1(\mathfrak{i})$ ▼

Следствие. Если неразрешимая задача $\mathfrak{T}_1$ m-сводима к задаче $\mathfrak{T}_2$, то задача $\mathfrak{T}_2$ также неразрешима

[1] Это доказательство (*должно быть*) вам известно из курса, посвящённого алгоритмам. Повторим его “для профилактики”.

М-сводимость

Поясняющий пример

Представьте себе пекарню с двумя работниками:

- **Хозяин** пекарни хочет, чтобы его работники умели определять
  - по ингредиентам — можно ли из них испечь вкусный торт ($\mathfrak{T}_1$)
  - по торту — вкусный ли он ($\mathfrak{T}_2$)
- **Кондитер** $\mathcal{B}$ знает, для каких ингредиентов какой торт лучший

Положительный случай (теорема): в пекарню устроился эксперт $\mathcal{A}$, способный оценить вкус любого торта

При помощи $\mathcal{A}$ и $\mathcal{B}$ можно оценить и пригодность ингредиентов:

- Показать $\mathcal{B}$ ингредиенты ($\mathfrak{i}$) и узнать, какой торт ($\mathfrak{j}$) лучший
- Спросить у $\mathcal{A}$, вкусный ли этот торт $\mathfrak{j}$

Отрицательный случай (следствие): хозяин узнал, что пригодность ингредиентов достоверно оценить, вообще говоря, нельзя

Тогда и про оценку вкуса тортов можно забыть