Коллоквиум по Дискретной математике, 2 курс

Залялов Александр, @bcategorytheory,
Солодовников Никита, @applied_memes,
Шморгунов Александр, @Owlus
Виноградова Дарья, @orange_to_the_wall

Содержание

1 Определение вычислимой частичной функции из $\mathbb{N}$ в $\mathbb{N}$. Счётность семейства частичных вычислимых функций, и существование невычислимых функций. Разрешимые и перечислимые подмножества $\mathbb{N}$. Счётность семейства перечислимых множеств, существование неперечислимых множеств.

Здесь не даётся формального определения алгоритма. В нашем случае "алгоритм" — некоторый чёрный ящик, принимающий на вход конструктивный объект (натуральное число или же объект, который можно закодировать как натуральное число), производящий некоторый результат (также конструктивный объект), а также работающий по шагам (некоторые атомарные действия вроде сложения).

Rule of thumb для вопроса "Алгоритм ли это?" — можно написать как программу на каком-нибудь языке программирования.

Определение. Функция $f : \mathbb{N} \to \mathbb{N}$ называется *частичной*, если $\mathrm{Dom}\, f \subseteq \mathbb{N}$.

Определение. Функция $f : \mathbb{N} \to \mathbb{N}$ называется *тотальной*, если $\mathrm{Dom}\, f = \mathbb{N}$.

Определение. Алгоритм $\mathcal{A}$ *вычисляет* частичную функцию $f : \mathbb{N} \to \mathbb{N}$, если

$$\begin{cases} \mathcal{A}(x) = f(x), & \text{если } x \in \mathrm{Dom}\, f, \\ \mathcal{A}(x) \text{ не определено} & \text{иначе.} \end{cases}$$

Определение. Частичная функция $f : \mathbb{N} \to \mathbb{N}$ называется *вычислимой*, если существует алгоритм, её вычисляющий.

Утверждение. *Множество частичных вычислимых функций не более, чем счётно.*

Доказательство. Действительно, всякой вычислимой функции можно поставить в соответствие некоторый алгоритм, причём различные функции вычисляются различными алгоритмами. Алгоритм — это программа, то есть конечная строка. Конечных строк (а следовательно, алгоритмов) всего лишь счётное число. Существует инъекция из множества вычислимых функций в множество алгоритмов, значит, количество вычислимых функций не более, чем счётно. □

Теорема. *Существуют невычислимые функции $f : \mathbb{N} \to \mathbb{N}$.*

Доказательство. Мощность множества вычислимых функций меньше мощности множества всех функций из $\mathbb{N} \to \mathbb{N}$, а значит, его дополнение не пусто. □

Определение. Множество $A \subseteq \mathbb{N}$ называется *разрешимым*, если существует алгоритм, вычисляющий его характеристическую функцию $\chi_A(x)$, то есть функцию такую, что

$$\chi_A(x) = \begin{cases} 1, & \text{если } x \in A, \\ 0 & \text{иначе.} \end{cases}$$

Определение. Множество $A \subseteq \mathbb{N}$ называется *перечислимым*, если существует алгоритм (не принимающий никаких входных данных), который выводит последовательность a_n такую, что множество всех элементов этой последовательности равно A.

Утверждение. *Множество перечислимых подмножеств $\mathbb{N}$ не более, чем счётно.*

Доказательство. Всякому перечислимому множеству соответствует алгоритм, его перечисляющий, причём различные множества перечисляются различными алгоритмами. Отсюда следует, что мощность множества перечислимых множеств не превосходит мощности множества алгоритмов, которое, в свою очередь, является счётным. □

Теорема. *Существуют неперечислимые множества $A \subseteq \mathbb{N}$.*

Доказательство. Множество перечислимых множеств имеет мощность меньшую, чем $2^{\mathbb{N}}$. Значит, его дополнение не пусто. □

2 Эквивалентные определения перечислимости: полуразрешимость, область определения вычислимой функции, множество значений вычислимой функции.

Определение. Множество $A \subseteq \mathbb{N}$ называется *полуразрешимым*, если существует алгоритм, вычисляющий его полухарактеристическую функцию $\xi_A(x)$, то есть функцию такую, что

$$\xi_A(x) = \begin{cases} 1, & \text{если } x \in A, \\ \text{не определено} & \text{иначе.} \end{cases}$$

Теорема. *Следующие утверждения эквивалентны:*

1. *Множество A перечислимо.*
2. *Множество A полуразрешимо.*
3. *Существует частичная вычислимая функция $f : \mathbb{N} \to \mathbb{N}$ такая, что $A = \operatorname{Dom} f$.*
4. *Существует частичная вычислимая функция $f : \mathbb{N} \to \mathbb{N}$ такая, что $A = \operatorname{Ran} f$.*

Доказательство. Чтобы показать эквивалентность всех этих утверждений, докажем несколько импликаций.

(1) $\implies$ (2)

Множество A перечислимо, докажем его полуразрешимость.

Модифицируем алгоритм $\mathcal{A}$ перечисления множества A следующим образом: если для входа x при перечислении мы встретили x, вернём ответ 1, иначе продолжим работу, ничего не возвращая. Так как в последовательности, получаемой алгоритмом, рано или поздно встретится каждый из элементов A, положительный ответ будет дан за конечное число шагов. В случае, если $x \notin A$, алгоритм зациклится без вывода, что вполне устраивает нас в рамках нашей задачи.

(2) $\implies$ (3)

Множество A полуразрешимо, докажем, что найдётся вычислимая функция, для которой A — область значений.

Этой частичной вычислимой функцией был ~~Альберт Эйнштейн~~ $\xi_A(x)$. Действительно, знаем, что $\xi_A(x)$ вычислима, а $\operatorname{Dom} \xi_A = A$. Значит, мы нашли искомую функцию.

(3) $\implies$ (4)

Множество A является областью определения некоторой вычислимой функции f, докажем, что оно также является областью значений некоторой другой вычислимой функции.

Определим функцию $g(x)$:

$$g(x) = \begin{cases} x, & \text{если } x \in \operatorname{Dom} f, \\ \text{не определено} & \text{иначе.} \end{cases}$$

Эта функция вычислима. Алгоритм, её вычисляющий, должен попытаться вычислить $f(x)$ и затем просто вывести x. Кроме того, $\operatorname{Ran} g = \operatorname{Dom} f$, а значит, мы нашли искомую функцию.

(4) $\implies$ (1)

Множество A является областью значений некоторой вычислимой функции, докажем его перечислимость.

Известно, что существует алгоритм $\mathcal{F}$, вычисляющий функцию f, область значений которой совпадает с A. Чтобы перечислить элементы множества A, будем бесконечно производить итерации следующего вида: на n-той итерации запустим по очереди на n шагов $\mathcal{F}(i)$ для каждого $0 \leqslant i \leqslant n$. Таким образом, для всех i алгоритм $\mathcal{F}(i)$ будет рано или поздно запущен на число шагов, необходимое для завершения. Значит, на всех x из $\operatorname{Dom} f$ мы вычислим (и выведем) $f(x)$. Таким образом будут выведены все элементы $\operatorname{Ran} f$, равного A.

Из каждого утверждения следуют все остальные. Значит, утверждения эквивалентны. □

3 Теорема Поста. Теорема о графике.

Теорема Поста. Множества A и $\mathbb{N} \setminus A$ перечислимы тогда и только тогда, когда A разрешимо.

Доказательство.

$\implies$

Перечислимость множества эквивалентна его полуразрешимости. Будем использовать алгоритмы $\mathcal{A}$ и $\mathcal{B}$, вычисляющие $\xi_A(x)$ и $\xi_{\mathbb{N}\setminus A}(x)$ соответственно.

Алгоритм $\mathcal{C}$, находящий $\chi_A(x)$, будет по очереди запускать $\mathcal{A}(x)$ и $\mathcal{B}(x)$ на некоторое число шагов. Как только один из этих алгоритмов завершится, можно будет дать ответ: если $x \in A$, вернуть 1, в противном случае вернуть 0.

Докажем корректность построенного алгоритма. Во-первых, он действительно даёт правильный ответ на всех $x \in \mathbb{N}$, а во-вторых, всегда завершается, так как всякое натуральное число лежит либо в множестве A, либо в его дополнении. Оба вспомогательных алгоритма могут при необходимости отработать бесконечное число шагов, значит, если какой-то из них завершается на данном входе, он завершится.

$\Longleftarrow$

Если множество разрешимо, его дополнение также разрешимо. Разрешимость влечёт перечислимость. □

Определение. Пусть задана функция f. Множество $\Gamma_f = \{(x, f(x)) \mid x \in \operatorname{Dom} f\}$ называется *графиком* функции f.

Теорема о графике. Функция f вычислима тогда и только тогда, когда Γ_f перечислимо.

Доказательство.

$\Longrightarrow$

Умея вычислять функцию f, хотим перечислить Γ_f.

Будем бесконечно производить итерации следующего вида: на n-той итерации попытаемся вычислить $f(x)$ для всех $0 \leqslant x \leqslant n$ не более, чем за n шагов. Если удастся, выведем пару $(x, f(x))$ в противном случае остановим вычисление $f(x)$ и перейдём к следующему i. Для каждого $x \in \operatorname{Dom} f$ рано или поздно мы произведём достаточное число шагов, чтобы вычислить $f(x)$, так как алгоритм, вычисляющий $f(x)$, должен завершаться за конечное число шагов. Значит, Γ_f таким образом действительно будет перечислено.

$\Longleftarrow$

Умея перечислять Γ_f, хотим вычислить $f(x)$.

Будем перечислять Γ_f, пока не найдём пару, в которой первый элемент равен x. Действительно, если функция определена на x, то такая пара найдётся в Γ_f, а значит, будет выведена алгоритмом его перечисления за конечное число шагов. Далее просто выведем второй элемент этой пары и завершим работу.

□

4 Универсальные вычислимые функции (нумерации) для семейства частичных вычислимых функций натурального аргумента. Несуществование универсальной вычислимой функции для семейства тотальных вычислимых функций натурального аргумента (диагональное рассуждение). Главные универсальные функции.

Известно, что множество частичных вычислимых функций счётно. Значит, все эти функции можно каким-то способом занумеровать.

Определение. Пусть φ_n — последовательность вычислимых частичных функций. Такая последовательность называется *универсальной нумерацией*. Функция $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ такая, что $f(n, x) = \varphi_n(x)$, называется *универсальной функцией*.

Теорема. *Существует вычислимая нумерация (универсальная функция).*

Доказательство. Определим следующий порядок на двоичных словах: если слово a короче слова b, $a \prec b$, если наоборот — $b \prec a$, в случае же равной длины будем сравнивать слова лексикографически. Последовательность двоичных слов в таком порядке будет выглядеть как $\{\bot, 0, 1, 00, 01, 10, 11, \ldots\}$. Таким образом множество окажется вполне упорядоченным. Теперь каждому натуральному числу можно поставить в соответствие некоторое двоичное слово.

Без ограничения общности будем считать, что алгоритм можно записать некоторым двоичным словом.

Определим теперь функцию $f(n, x)$ следующим образом: интерпретируем двоичное слово с номером n (в нашем порядке $\prec$) как код (запись машины Тьюринга, программу на C, whatever) для алгоритма $\mathcal{A}$, и положим $f(n, x) = \mathcal{A}(x)$. Если двоичное слово с номером n не является корректной записью алгоритма, будем считать, что $f(n, x)$ не определена для всех x.

Описанная функция вычислима. Она также является универсальной, так как пробегает по всем возможным алгоритмам (и, как следствие, всем возможным вычислимым функциям). Значит, мы построили вычислимую универсальную функцию. □

Может показаться, что универсальная функция может существовать и для семейства тотальных вычислимых функций. Однако, это неверно.

Теорема. *Не существует вычислимой нумерации (универсальной функции) для семейства тотальных вычислимых функций.*

Доказательство. Допустим, что существует вычислимая нумерация ψ_n тотальных вычислимых функций. Значит, будет тотальной и вычислимой функция следующего вида

$$f(x) = \psi_x(x) + 1.$$

Так как функция f тотальна и вычислима, должно найтись n такое, что $\psi_n(x) = f(x)$. Однако, если поставить $x = n$:

$$\psi_n(n) = f(n) = \psi_n(n) + 1.$$

Произошло противоречие [1]...

□

Определение. Нумерация φ называется *главной*, если для любой вычислимой частичной функции $V(n, x)$ существует тотальная вычислимая функция $s(n)$ такая, что $V(n, x) = \varphi_{s(n)}(x)$.

Теорема. *Существует главная нумерация (универсальная функция).*

Доказательство. Рассмотрим построенную выше нумерацию. Для функции $V(n, x)$ построим алгоритм $\mathcal{S}(m)$, который "вшивает" в алгоритм $\mathcal{V}(n, x)$, вычисляющий $V(n, x)$, константу m вместо переменной n. Такой алгоритм, очевидно, всегда будет завершаться. Значит, он вычисляет некоторую тотальную функцию $s(n)$. □

5 Вычислимая функция, не имеющая тотального вычислимого продолжения. Перечислимое неразрешимое множество. Неразрешимость проблемы применимости.

Определение. Функция g является *продолжением* функции f, если $\mathrm{Dom}\, f \subset \mathrm{Dom}\, g$ и $\forall x \in \mathrm{Dom}\, f\ g(x) = f(x)$.

Теорема. *Существует вычислимая частичная функция, не имеющая всюду определённого продолжения.*

Доказательство. Определим функцию f:

$$f(x) = \varphi_x(x) + 1.$$

Пусть мы вычислимо продолжили функцию f функцией φ_n (продолжение вычислимо, а потому будет присутствовать в главной нумерации). Запишем уравнение:

$$\varphi_x(x) + 1 = \varphi_n(x).$$

Это уравнение, вообще говоря, неверно, так как левая часть может быть не определена, но при этом при подстановке $x = n$ получаем слева вполне определённое выражение (напомню, φ_n всюду определена), а вместе с ним и противоречие:

$$\varphi_n(n) + 1 = \varphi_n(n).$$

Значит, для функции f не существует всюду определённого вычислимого продолжения. □

Теорема. *Множество $A = \{x \mid \varphi_x(x)$ определено$\}$ неразрешимо.*

[1] Такая конструкция не будет приводить к противоречию, если говорить о частичных функциях, а не тотальных. Действительно, построенная нами функция $f = \varphi_n$ просто не будет определена в точке n.

Доказательство. Вернёмся вновь к нашей любимой функции f:

$$f(x) = \varphi_x(x) + 1.$$

Продолжим эту функцию самым простым способом — везде вне её области определения её продолжение будет равно нулю. Нетрудно было бы реализовать это продолжение, умея разрешать множество A: просто вычислим $\varphi_x(x) + 1$, если это значение определено, и вернём ноль иначе.

Однако мы уже знаем, что продолжение функции f не может быть вычислимым. Значит, вычислимость χ_A приводит к противоречию. □

Определение. Задача разрешения множества $\{(n, x) \mid \varphi_n(x) \text{ определено}\}$ называется *проблемой остановки (применимости).*

Теорема. *Проблема остановки неразрешима.*

Доказательство. Пусть χ_A вычисляется алгоритмом $\mathcal{A}$. Запустив $\mathcal{A}(x, x)$, можно разрешить множество $\{x \mid \varphi_x(x) \text{ определено}\}$, для которого уже доказана неразрешимость. □

6 Теорема Поста. Существование перечислимого множества, дополнение которого неперечислимо. Перечислимые неотделимые множества.

Теорема Поста была доказана здесь.

Теорема. *Существует перечислимое множество с неперечислимым дополнением.*

Доказательство. Уже знакомое нам множество $\{x \mid \varphi_x(x) \text{ определено}\}$ является неразрешимым. Однако же, это множество очевидно полуразрешимо, а значит, и перечислимо.

Предположим теперь, что дополнение данного множества перечислимо. В таком случае, согласно теореме Поста, само множество разрешимо. Противоречие. □

Определение. Множества A, B называются *отделимыми*, если существует множество C такое, что $A \subseteq C$ и $B \cap C = \varnothing$.

Теорема. *Существуют непересекающиеся перечислимые множества, которые нельзя отделить разрешимым множеством.*

Доказательство. Рассмотрим множества $A = \{x \mid \varphi_x(x) = 0\}$ и $B = \{x \mid \varphi_x(x) = 42\}$. Они, очевидно, перечислимы и не пересекаются.

Допустим, существует разрешимое C, отделяющее A и B. Пусть оно содержит в себе множество A. Тогда:

$$\chi_C(x) = \begin{cases} 1, & \text{если } \varphi_x(x) = 0, \\ 0, & \text{если } \varphi_x(x) = 42, \\ \text{и что-то ещё на других числах.} \end{cases}$$

χ_C вычислима. Значит, $\exists n\ \chi_C(x) = \varphi_n(x)$ Но пусть тогда $x = n$. Получаем:

$$\varphi_n(n) = \begin{cases} 1, & \text{если } \varphi_n(n) = 0, \\ 0, & \text{если } \varphi_x(n) = 42, \\ \text{и что-то ещё на других числах.} \end{cases}$$

Получили противоречие. □

7 Сводимости: m-сводимость и Тьюрингова сводимость. Свойства. Полные перечислимые множества.

Определение. Множество A *m-сводится* к множеству B, если существует тотальная вычислимая функция f такая, что $\forall x\ x \in A \iff f(x) \in B$. Обозначается как $A \leqslant_m B$.

m-сводимость позволяет построить алгоритм разрешения множества A, если есть алгоритм разрешения множества B. Строго говоря, $\chi_A(x) = \chi_B(f(x))$.

Свойства m-сводимости:

- $A \leqslant_m A$ (рефлексивность),
- $A \leqslant_m B \wedge B \leqslant_m C \implies A \leqslant_m C$ (транзитивность),
- $\left.\begin{array}{l} B \text{ разрешимо} \\ A \leqslant_m B \end{array}\right\} \implies A$ разрешимо,
- $\left.\begin{array}{l} A \text{ неразрешимо} \\ A \leqslant_m B \end{array}\right\} \implies B$ неразрешимо.

Определение. Множество A *T-сводится* (сводится по Тьюрингу) к множеству B, если при помощи алгоритма вычисления χ_B (не обязательно существующего) можно вычислить χ_A. Обозначается как $A \leqslant_T B$ [2].

Тьюринова сводимость обладает теми же свойствами, что и m-сводимость. Однако же, $A \leqslant_m B \implies A \leqslant_T B$, а обратное утверждение неверно.

Тьюрингова сводимость обладает ещё одним свойством: $A \leqslant_T \mathbb{N} \setminus A$. Однако же данное утверждение не будет верно для m-сводимости. К примеру, множество $\mathbb{N}$ не может быть m-сведено к своему дополнению.

Определение. Перечислимое множество, к которому m-сводится любое другое перечислимое множество, называется *полным перечислимым множеством.*

Теорема. *Существует полное перечислимое множество.*

Доказательство. Рассмотрим множество $A = \{(n, x) \mid \varphi_n(x) \text{ определено}\}$. Заметим, что оно перечислимо.

Пусть мы хотим свести некоторое перечислимое множество B к множеству A. Знаем, что в силу перечислимости существует вычислимая частичная функция f такая, что $B = \operatorname{Dom} f$. Эта функция должна присутствовать в универсальной нумерации. Пусть это φ_n. Тогда для того, чтобы проверить принадлежность $x \in B$, достаточно проверить принадлежность $(n, x) \in A$. Сводящая функция в данном случае выглядит как $m(x) = (n, x)$. □

8 Теорема Клини о неподвижной точке.

Теорема. *Для всякой тотальной вычислимой функции f и главной нумерации φ_n найдётся n такое, что $\varphi_n = \varphi_{f(n)}$* [3].

Доказательство. Педагогический трюк для лучшего запоминания: сначала попытаемся доказать ложное утверждение о том, что у всякой тотальной вычислимой функции есть неподвижная точка, то есть число n такое, что $n = f(n)$.

Функция f вычислима, функция $\varphi_x(x)$ вычислима, значит, вычислима их композиция. То есть, существует m такое, что

$$f(\varphi_x(x)) = \varphi_m(x).$$

Подставляя $x = m$, получаем

$$f(\varphi_m(m)) = \varphi_m(m),$$

то есть $n = \varphi_m(m)$.

И всё бы было хорошо, если бы $\varphi_m(m)$ было всегда определено. Но вернёмся в суровую реальность и докажем истинное утверждение теоремы Клини.

Вместо равенства чисел нужно рассматривать эквивалентность следующего вида: $n \sim m$, если $\varphi_n = \varphi_m$.

Рассмотрим вычислимую функцию

$$V(m, x) = \varphi_{f(\varphi_m(m))}(x).$$

По свойству главности нумерации φ найдётся тотальная вычислимая функция s такая, что

$$V(m, x) = \varphi_{s(m)}(x).$$

[2] Это — старая добрая сводимость из курса алгоритмов. Классы задач P и NP машут ручкой.

[3] Неформально: существует программа, которая может напечатать свой код.

Значит, можем записать, что

$$f(\varphi_m(m)) \sim s(m).$$

Важно отметить, что $s(m)$ тотальна. Какое бы значение m мы не подставили, наше утверждение сохранит истинность в силу того, что правая часть уравнения определена.

Теперь, зная, что $s(m)$ вычислима, запишем её как $\varphi_k(m)$

$$f(\varphi_m(m)) \sim \varphi_k(m),$$

и подставим $m = k$

$$f(\varphi_k(k)) \sim \varphi_k(k).$$

Чудесным образом получили слева и справа вполне определённые значения, так как и f, и φ_k являются тотальными функциями. То есть, неподвижной точкой (в смысле определённой нами эквивалентности, а не обычного равенства) функции f является $\varphi_k(k)$, совершенно точно определённое значение. □

9 Теорема Райса-Успенского.

Теорема. *Пусть множество F является собственным подмножеством множества частичных вычислимых функций (то есть, F не пусто и не совпадает с множеством всех частичных вычислимых функций). Тогда множество $\{i \mid \varphi_i \in F\}$ неразрешимо* [4].

Доказательство. Обозначим нигде не определённую функцию как $\zeta(x)$. Рассмотрим два случая.

- $\zeta \notin F, f \in F$

  Пусть A — перечислимое неразрешимое множество. Хотим m-свести A к F. Для этого определим функцию $V(n, x)$ следующим образом:

  $$V(n,x) = \begin{cases} f(x), & n \in A, \\ \zeta(x), & \text{иначе.} \end{cases}$$

  Так как полухарактеристическая функция A вычислима, $V(n, x)$ также вычислима. Кроме того, в главной нумерации φ найдётся тотальная вычислимая функция s такая, что $V(n, x) = \varphi_{s(n)}(x)$. Запишем:

  $$\varphi_{s(n)}(x) = \begin{cases} f(x), & n \in A, \\ \zeta(x), & \text{иначе.} \end{cases}$$

  Но теперь мы получили, что $n \in A \iff s(n) \in F$. Значит, неразрешимое множество A m-сводится к нашему множеству F. Значит, и F является неразрешимым.

- $\zeta \in F, f \notin F$

  Построив всё аналогично предыдущему пункту, мы получаем, что $n \in A \iff s(n) \notin F$. Это значит, что дополнение F неразрешимо. Само F в таком случае также неразрешимо.

□

10 Определение машин Тьюринга и вычислимых на машинах Тьюринга функций. Тезис Чёрча-Тьюринга. Неразрешимость проблемы остановки машины Тьюринга.

Машина Тьюринга задаётся[5]

[4] Неформально эту теорему можно понимать так: по алгоритму вычисления функции нельзя понять (алгоритмически), обладает ли она каким-либо свойством. То есть, к примеру, нельзя написать алгоритм, решающий, монотонна ли функция, по коду, её вычисляющему.

[5] Здесь машина Тьюринга определяется в соответсвии с лекцией. Следует понимать, что это определение не является общепринятым. Вариаций масса: кто-то запрещает головке оставаться на месте, кто-то выделяет выходной алфавит, отличный от входного и т. д.

- непустым конечным алфавитом Σ, среди которого выделен пробельный символ ␣ и не содержащее пробела подмножество Γ — входной алфавит;
- непустым конечным множеством состояний Q, среди которых выделено начальное состояние s_0 и множество терминальных состояний F;
- функцией переходов $\delta : (Q \setminus F) \times \Sigma \to Q \times \Sigma \times \{-1, 0, +1\}$.

Машина Тьюринга состоит из бесконечной ленты, разбитой на ячейки, головки, в любой момент времени указывающей на одну ячейку и одной ячейки памяти, в которой хранится текущее состояние. В начальный момент времени на ленте записано некоторое слово, составленное из букв входного алфавита, головка смотрит на первый символ этого слова, во всех остальных ячейках пробелы. Затем в каждый момент времени вычисляется $\delta(q, c) = (q', c', \Delta)$, где q — текущее состояние, c — символ записанный в ячейке, на которую сейчас смотрит головка. Состояние меняется на q', символ в текущей ячейке на c', головка остаётся на месте или передвигается на один влево или вправо в соответствии со значением Δ. Если q' оказалось терминальным, на этом работа машины заканчивается, иначе этот процесс продолжается.

Машины Тьюринга естественным образом отождествляются с частичными функциями $f : \Gamma^* \to \Gamma^*$ — аргументом функции является входное слово, а возвращает функция слово, записанное на ленте после завершения работы машины(то есть всё, что написано на ленте, кроме бесконечного числа пробелов слева и справа). Функции будут частичными, поскольку машина Тьюринга может продолжать работать бесконечно или в данной конструкции может оказаться, что на выходе есть символ, не содержащийся в Γ. Функции, которые можно таким образом получить по некоторой машине Тьюринга, называются вычислимыми на машине Тьюринга.

Тезис Чёрча-Тьюринга. *Любая вычислимая функция вычислима на машине Тьюринга.*

Здесь понятие "вычислимая функция"используется в неформальном смысле, под ним понимается функция, вычислимая в любой разумной модели, которая может прийти вам в голову. Тезис не является формальным утверждением, он никак не доказывается и принимается нами на веру.

Теорема. *Не существует вычислимой функции, определяющей по машине Тьюринга и входному слову, остановится ли эта машина.*

Теперь, когда мы отождествили вычислимые и вычислимые на машине Тьюринга функции, эта теорема непосредственно следует из доказательства теоремы о существовании полного перечислимого множества из 7 билета.

11 Неразрешимость проблемы достижимости в односторонних ассоциативных исчислениях. Полугруппы, заданные порождающими и соотношениями. Теорема Маркова–Поста: неразрешимость проблемы равенства слов в некоторой конечно определенной полугруппе (без доказательства).

Определение. *Односторонним ассоциативным исчислением* называется множество из всех слов над некоторым конечным алфавитом и конечный набор подстановок. Каждая подстановка представляет собой пару слов (s, t) и позволяет в любом слове содержащем s как подстроку заменить её на t (но не наоборот).

Теорема. *Существует одностороннее ассоциатвиное исчисление, в котором не разрешима задача проверить по паре слов, можно ли некоторой последовательностью подстановок перейти от первого ко второму.*

Доказательство. Возьмём некоторую машину Тьюринга M, для которой неразрешима проблема остановки, при чём если такую, что если она останавливается, то на ленте записано пустое слово. Построим по ней одностороннее ассоциативное исчисление, в котором из $[X]$ можно получить Y, если и только если M преобразует X в Y. В качестве алфавита для исчисления возьмём объединение алфавита M и её множества состояний (а также квадратные скобки и символы $\triangleleft, \triangleright$). Будем сопоставлять конфигурациям машины слова исчисления. Если машина находится в состоянии s, на ленте записано слово PQ(конкатенация слов P и Q) и головка указывает на первый символ слова Q, сопоставим такой конфигурации слово $[PsQ]$ в нашем исчислении. Тут важно, что мы считаем, что у машины не пересекаются алфавит и множество состояний. Построим по переходам машины подстановки для исчисления.

Переход МТ	Подстановка одностороннего ассоциативного исчисления
$(s,c)\mapsto(s',c',0)$	$sc\to s'c'$
$(s,c)\mapsto(s',c',+1)$	$sc\to cs'$
$(s,c)\mapsto(s',c',-1)$	$xsc\to s'xc'$ — для каждого символа x из алфавита машины, а также $[sc\to[s'\_c'$
$(s,\_)\mapsto(s',c',0)$	$s]\to s'c']$
$(s,\_)\mapsto(s',c',+1)$	$s]\to cs']$
$(s,\_)\mapsto(s',c',-1)$	$xs]\to s'xc']$

Дополнительно к этому введём подстановки, позволяющие получить пустое слово, если машина остановится.

- $f\to\triangleleft$, f — терминальное состояние;
- $c\triangleleft\to\triangleleft, c\neq[$;
- $[\triangleleft\to\triangleright$;
- $\triangleright c\to\triangleright, c\neq]$;
- $\triangleright]\to\varepsilon$(пустое слово).

Это можно было бы реализовать проще без двух дополнительных символов, но так мы получаем, что всегда существует ровно одна последовательностей подстановок, моделирующих работу машины Тьюринга. Осталась одна деталь — мы пообщеали, что мы начнём с $[X]$, а не с $[s_0X]$. Она решается просто — добавлением подстановки $[x\to[s_0x$ для всех символом x из алфавита машины.

Итак, мы свели задачу остановки машины Тьюринга (про которую было известно, что она неразрешима) к задаче достижимости в одностороннем ассоциативном исчислении и показали этим, что эта задача тоже неразрешима. □

Теорема Маркова-Поста гласит, что если потребовать, чтобы все подстановки были двухсторонними, то задача останется неразрешимой, но доказывать этот факт от нас не требуют. При чём такую задачу можно сформулировать на языке алгебры:

Пусть про некоторую полугруппу известно, что она содержит[6] элементы $a_1,\dots,a_n$ и в ней выполняются некоторые (конечное количество) равенства вида $a_{i_1}a_{i_2}\dots a_{i_k}=a_{j_1}a_{j_2}\dots a_{j_m}$. Обязательно ли в ней выполняется заданное равенство такого же вида?

12 Исчисление высказываний (аксиомы и правила вывода), понятие вывода. Теорема корректности исчисления высказываний

Высказываниями мы называем утверждения, которые либо истинны, либо ложны. При этом если A,B являются высказываниями, то $\neg A, A\vee B, A\wedge B, A\to B$ — тоже высказывания. Из такого определения никак не следует, что высказывания вообще существуют, так что в любом применении исчисления высказываний также описывают некоторые атомарные высказывания. Но нам для доказательства общих фактов это никак не потребуется. Исчисление высказываний задаётся аксиомами и правилами вывода. У нас имеется 11 аксиом:

1. $(A\to(B\to C))\to((A\to B)\to(A\to C))$
2. $A\to(B\to A)$
3. $A\wedge B\to A$
4. $A\wedge B\to B$
5. $A\to(B\to A\wedge B)$
6. $A\to A\vee B$
7. $B\to A\vee B$
8. $(A\to C)\to((B\to C)\to((A\vee B)\to C))$

[6]Можно потребовать, чтобы в полугруппе были только элементы, порождённые заданными. Это никак не меняет задачу.

9. $\neg A \to (A \to B)$
10. $(A \to B) \to ((A \to \neg B) \to \neg A)$
11. $A \vee \neg A$

и 1 правило вывода(modus ponens)

$$\frac{A \to B,\ A}{B}$$

Вывод в исчислении высказываний — это последовательность из операций двух видов

- Подстановка в некоторую аксиому любых высказываний вместо A, B, C.
- Применение правила вывода. Если уже выведены $A \to B$ и A, можно вывести B

Теорема. *(Корректность исчисления резолюций) Любая формула, которую можно вывести в исчислении высказываний, истинна(тавтологична).*

Здесь мы называем формулу истинной(тавтологичной), если она как булева формула верна при всех значениях входящих в неё переменных. Отметим, что только в этом контексте мы понимаем $\neg, \vee, \wedge$ как привычные логические операции. С точки зрения исчисления высказываний, это просто какие-то символы, всё что мы про них знаем — это аксиомы и правило.

Доказательство. Достаточно убедиться, что все действия, который мы можем производить в ходе вывода не позволяют получить ложное выражение. Во-первых, все аксиомы истинны при любых значениях входящих в них переменных. Во-вторых, если $A \to B$ истинно и A истинно, то B истинно. □

13 Вывод из гипотез. Лемма о дедукции. Полезные производные правила.

Пусть Γ — некоторое множество высказываний(гипотез). Тогда говорят, что формула A выводится из Γ, если её можно вывести, разрешая пользоваться не только аксиомами и правилом вывода, но и высказываниями из Γ. Можно сказать, что у нас появилась третья операция: бесплатно получить формулу из Γ. Обозначение: $\Gamma \vdash A$. В таких терминах можно сказать, что формула, которую можно вывести в исчислении высказываний, выводится из пустого множества гипотез, обозначение: $\vdash A$.

Лемма. $\vdash A \to A$

Доказательство.
1. $A \to (A \to A)$(2 аксиома)
2. $\neg A \to (A \to A)$ (9 аксиома)
3. $A \vee \neg A$ (11 аксиома)
4. $(A \to (A \to A)) \to ((\neg A \to (A \to A)) \to ((A \vee \neg A) \to (A \to A)))$ (8 аксиома, подставлены $A, \neg A, A \to A$)
5. $(\neg A \to (A \to A)) \to (A \vee \neg A) \to (A \to A)$ (modus ponens)
6. $(A \vee \neg A) \to (A \to A)$ (modus ponens)
7. $A \to A$ (modus ponens)

□

Теорема. *(Лемма о дедукции)* $\Gamma \cup \{A\} \vdash B \implies \Gamma \vdash (A \to B)$

Доказательство. Пусть с набором гипотез $\Gamma \cup \{A\}$ мы могли вывести формулу B, последовательно выводя формулы $B_1, B_2, \ldots, B_n, B_n = B$. По индукции докажем, что с набором гипотез Γ можно доказать последовательность $A \to B_1, \ldots, A \to B_n$. Разберём для этого все способы, которыми мы умеем выводить

1. B_i получено как гипотеза. Если $B_i = A$, то по лемме мы сможем вывести $A \to A$. Иначе нам доступен такой вывод: $B_i, B_i \to (A \to B_i), A \to B_i$.
2. B_i получено подставлением формул в аксиому. Работает последовательность из предыдущего пункта.

3. B_i получено по modus ponens из B_j и $B_k (j < i, k < i)$. Тогда без потери общности считаем, что $B_j = B_k \to B_i$. По предположению индукции мы уже вывели $A \to B_k$ и $A \to (B_k \to B_i)$. По первой аксиоме выведем $A \to (B_k \to B_i) \to ((A \to B_k) \to (A \to B_i))$. Дважды применив к этому modus ponens, получим $A \to B_i$.

□

Некоторые производные правила — следствия из леммы о дедукции:

- Из A и B можно вывести $A \wedge B$.
- Если из $\Gamma \cup \{A\}$ можно вывести B и $\neg B$, то из Γ можно вывести $\neg A$ (производное правило доказательства от противного).
- Если из $\Gamma \cup \{A\}$ можно вывести B и из $\Gamma \cup \{\neg A\}$ можно вывести B, то из Γ можно вывести B (производное правило разбора случаев).
- Из $A, \neg A$ можно вывести что угодно.

14 Теорема полноты исчисления высказываний.

Лемма. *Пусть формула A зависит от переменных $p_1, \ldots, p_n$. При этом при $(p_1, \ldots, p_n) = (\varepsilon_1, \ldots, \varepsilon_n)$ формула выдаёт значение ε. Тогда $\{p_1^{\varepsilon_1}, \ldots, p_n^{\varepsilon_n}\} \vdash A^\varepsilon$, где*

$$P^\varepsilon = \begin{cases} \neg P, & \varepsilon = 0 \\ P & \varepsilon = 1 \end{cases}$$

Доказательство. Доказательство индукцией по построению формулы A. Разбираем все способы, которыми она была построена, а для них все значения её составных частей.

1. $A = p$. Очевидно, $p \vdash p$ и $\neg p \vdash \neg p$.
2. $A = B \wedge C$.
   (a) Пусть B и C истинны. Тогда по предположению индукции мы можем вывести B и C и требуется показать, что мы можем вывести $B \wedge C$. Мы умеем это делать по производному правилу.
   (b) Пусть B истинно, а C ложно. Тогда по предположению индукции мы можем вывести B и $\neg C$, и хотим вывести $\neg(B \wedge C)$. Воспользуемся правилом доказательства от противного и добавим себе в гипотезы $B \wedge C$. Из $B \wedge C$ нетрудно вывести C, и мы умеем выводить $\not C$, противоречие достигнуто.

   Оставшиеся два случая аналогичны второму.
3. $A = B \vee C$. Если хотя бы одно из B или C истинно, то ясно, что можно вывести $B \vee C$. Пусть теперь мы умеем выводить $\neg B, \neg C$ и нужно вывести $\neg(B \vee C)$. Снова будем выводить от противного и предположим $B \vee C$. Заметим, что из $\neg B, \neg C, B$ можно вывести всё что угодно, и из $\neg B, \neg C, C$ можно вывести всё что угодно. Тогда всё что угодно можно вывести и из $\neg B, \neg C, B \vee C$, в том числе и противоречие.
4. $A = B \to C$. Для случаев с истинным B или ложным C вывод простой — достаточно воспользоваться 2 или 9 аксиомой (и modus ponens). Пусть мы умеем выводить $B, \neg C$ и нужно вывести $\neg(B \to C)$. Опять докажем от противного и по modus ponens из $B, B \to C$ выведем C. Это даст противоречие, поскольку у нас есть $\neg C$.
5. $A = \neg B$. Ясно, что $\neg B \vdash \neg B$. Нужно доказать, что $B \vdash \neg\neg B$. Для этого нужно в очередной раз доказать от противного и вывести из $B, \neg B$ какое-нибудь противоречие. Но $B, \neg B$ уже противоречие.

□

Теорема. *(Полнота исчисления высказываний) Любую тавтологию можно вывести в исчислении высказываний.*

Доказательство. Пусть тавтология A зависит от переменных $p_1, \ldots, p_n$. Тогда по лемме $p_1, \ldots, p_n \vdash A$. И $p_1, \ldots, \neg p_n \vdash A$. И вообще как угодно можно расставить отрицания, потому что A — тавтология. Из двух приведённых фактов по производному правилу $p_1, \ldots, p_{n-1}, p_n \vee \neg p_n \vdash A$. Но $p_n \vee \neg p_n$ можно получить из аксиомы, значит это можно выкинуть из списка гипотез и получить $p_1, \ldots, p_{n-1} \vdash A$. Аналогично начав с $p_1, \ldots, \neg p_{n-1}, p_n \vdash A$ и $p_1, \ldots, \neg p_{n-1}, \neg p_n \vdash A$, мы получим $p_1, \ldots, \neg p_{n-1} \vdash A$. Из этих двух результатов мы сможем избавиться от p_{n-1} и получить $p_1, \ldots, p_{n-2} \vdash A$. Долго повторяя этот процесс, мы избавимся от всех переменных и получим $\vdash A$, а это то, что требовалось. □

15 Исчисление резолюций для опровержения пропозициональных формул в конъюнктивной нормальной форме (КНФ): дизъюнкты, правило резолюции, опровержение КНФ в исчислении резолюций. Теорема корректности исчисления резолюций (для пропозициональных формул в КНФ)

Если исчисление высказываний работало с произвольными формулами, построенными с помощью отрицания, конъюнкции, дизъюнкции и импликации, исчисление резолюций работает только с дизъюнктами.

Определение. *Литерал* — переменная или отрицание переменной

Определение. *Дизъюнкт* — это дизъюнкция по некоторому конечному множеству литералов

Обратите внимание, что в этом определении речь про множество. Хотя мы записываем дизъюнкты как формулы $\lambda_1 \vee \lambda_2 \vee \ldots \vee \lambda_n$, мы считаем, что, к примеру, $\lambda_1 \vee \lambda_2, \lambda_2 \vee \lambda_1, \lambda_1 \vee \lambda_2 \vee \lambda_1$ — это всё один и тот же дизъюнкт.

У исчисления резолюций нет аксиом и есть одно правило — правило резолюции

$$\frac{A \vee p,\ B \vee \neg p}{A \vee B}$$

Отметим, что при применении правила к p и $\neg p$ результатом будет пустой дизъюнкт, который обозначается как $\bot$(или как $\square$).

На записанные в КНФ пропозиональные формулы можно смотреть как на множества дизъюнктов в исчислении резолюций. Будем говорить, что множество дизъюнктов совместно, если есть набор значений переменных, при котором каждый дизъюнкт возвращает истину. Утверждается, что из множества дизъюнктов можно вывести в исчислени пустой дизъюнкт, если и только если множество несовместно.

Теорема. *(Корректность исчисления резолюций) Если множества дизъюнктов можно вывести пустой дизъюнкт, то оно несовместно.*

Доказательство. Можно убедиться, что из истинных (при каких-то значениях переменных) формул можно вывести только истинные (при тех же значениях). Но пустой дизъюнкт всегда ложен.

Если вам по каким-либо причинам не нравятся слова о ложности пустого дизъюнкта, можно сказать, что пустой дизъюнкт можно вывести только из $p, \neg p$, а они не могут быть истинны одновременно. $\square$

16 Теорема полноты исчисления резолюций (для пропозициональных формул в КНФ). Доказательство только для конечных и счетных множеств формул.

Теорема. *(Полнота исчисления резолюций) Если множество дизъюнктов S несовместно, то из него можно вывести пустой дизъюнкт.*

Докажем для случая, когда S не более чем счётно.

Доказательство. Применим контрапозицию и докажем, что если из S нельзя вывести пустой дизъюнкт, то оно совместно. Обозначим за S' множество всех формул, которые можно вывести из S. Поскольку множество дизъюнктов не более чем счётно, а сами дизъюнкты конечны, множество используемых переменных тоже будет не более чем счётно. Занумеруем их $x_1, x_2, \ldots$. Докажем, что можно так выбрать значения переменным, что для любого n все дизъюнкты из S', содержащие только переменные с номерами не больше n, истинны. Ясно, что это и означает совместность. Доказывать будем индукцией по n.

База индукции. Это могло бы быть неверно для $n = 1$, только если бы в S' содержались x_1 и $\neg x_1$. Но такого быть не может, ведь тогда мы могли бы вывести пустой дизъюнкт.

Шаг индукции. По предположению индукции мы уже как-то умеем выбирать значения для переменных $x_1, \ldots, x_n$. Предположим, выбрать значение для x_{n+1} нельзя.

- $x_{n+1} = 0$ не подходит $\implies A \vee x_{n+1} \in S'$, где A содержит только $x_1, \ldots, x_n$ и ложно при выбранных для них значениях.
- $x_{n+1} = 1$ не подходит $\implies B \vee \neg x_{n+1} \in S'$, где B содержит только $x_1, \ldots, x_n$ и ложно при выбранных для них значениях.

Но тогда можно вывести $A \vee B$. Поскольку $A \vee B$ содержит только $x_1, \ldots, x_n$, по предположению индукции оно верно при выбранных значениях. А значит не может быть, что и A, и B ложны, противоречие. □

На самом деле аналогичным образом можно было бы доказать корректность и для несчётных множеств формул (для корректности индукции пришлось бы прибегнуть к теореме Цермело), но несчётное число переменных — это крайне нетипичная ситуация и этим мы тут не занимаемся.

17 Полиномиальный алгоритм сведения задачи распознавания совместности конечных множеств произвольных формул к задаче распознавания совместности конечных множеств дизъюнктов.

Перейти от формулы к конечному множеству дизъюнктов — то же самое, что привести её к КНФ. Ясно, что формулу длины l, зависящую от m переменных, можно за $O(2^m \cdot l)$ — построить таблицу истинности и взять дизъюнкты, соответствующие строкам, в которых формула ложна, но этот метод не полиномиальный.

Пусть наша формула имеет вид $f(A, B)$ — где A, B — некоторые формулы, а f — операция, выполняющаяся в нашей формуле последней. Тогда введём новые переменные x', x'' и заменим нашу формулу на $f(x', x'') \wedge (x' \equiv A) \wedge (x'' \equiv B)$. Длина формулы $f(x', x'')$ —константа, следовательно экспоненциальный метод сведёт её к КНФ за $O(1)$. Повторим процедуру для формул $x' \equiv A$ и $x'' \equiv B$, если A и B – это не просто переменные. За каждый запуск наивного алгоритма мы избавляемся от одной операции в исходной формуле, поэтому время работы можно оценить как $O(l)$.

Мы дали описание для бинарных операций, но ясно, что тот же самый подход замены выражений на переменные применим и для отрицания, и для каких-то экзотических операций.

18 Определение формулы первого порядка в данной сигнатуре. Свободные и связанные вхождения переменных. Интерпретации данной сигнатуры. Общезначимые и выполнимые формулы. Равносильные формулы.

Определение. *Сигнатура* языка — набор функциональных и предикатных символов определённых валентностей.

Формулы первого порядка состоят из кванторов, индвидных переменных, функциональных и предикатных символов. Но для того, чтобы дать корректное определение формуле первого порядка, нам потребуется ввести ещё несколько вспомогательных понятий. Во-первых, *терм*.

1. Любая индвидная переменная является термом.
2. Если f — функциональный символ валентности n, а $t_1, \ldots, t_n$ — термы, то $f(t_1, \ldots, t_n)$ — терм.

Во-вторых, будем называть *атомарной формулой* выражение вида $P(t_1, \ldots, t_n)$, где P — предикатный символ валентности n, а $t_1, \ldots, t_n$ — термы. Теперь мы готовы дать определение формуле первого порядка (далее — просто формуле).

Определение.
1. Атомарные формулы являются формулами.
2. Если a, b — формулы, то $(a \wedge b), (a \vee b), (a \to b), \neg a$ также являются формулами.
3. Если a — формула, то $(\exists x\ a)$ и $(\forall x\ a)$ также являются формулами.

Скобки в определении нужны для того, чтобы можно было однозначно определять приоритет операций. Для удобства мы (как и любой разумный человек) не будем ставить все из этих скобок.

Если перед каждым появлением переменной в формуле в составе терма эта переменная появляется под квантором, говорят что она *связана* в этой формуле. Иначе говорят, что она входит в формулу *свободно*. Формула без свободных вхождений переменных называется *замкнутой*.

Определение. *Интерпретация* данной сигнатуры состоит из непустого множества M (*носителя*) и функций, сопоставленных каждому символу. Функциональному символу f валентности n сопоставляется функция $\hat{f} : M^n \to M$, а предикатному символу p валентности m — функция $\hat{p} : M^m \to \{0, 1\}$.

Ясно, что после выбора интерпретации любой замкнутой формуле данной сигнатуры можно однозначно сопоставить значение. При этом формула называется *общезначимой*, если она верна в любой интерпретации и *выполнимой*, если верна хотя бы в какой-то. Обычно эти термины применяют только к замкнутым формулам, но если формула содержит свободные переменные, то считается, что она верна, если она верна при любых их значениях. Формулы A и B называются равносильными, если формула $(A \to B) \wedge (B \to A)$ общезначима.

19 Теории и их модели. Семантическое следование. Теорема Черча об алгоритмической неразрешимости отношения семантического следования и общезначимости формул (в доказательстве теоремы можно использовать существование конечно определенной полугруппы с неразрешимой проблемой равенства).

Определение. *Теория* — некоторое множество замкнутых формул

Определение. Интерпретация M соответствующей сигнатуры, в которой верны все формулы теории T, называется *моделью* T. Обозначение: $M \vDash T$.

Определение. Формула A называется *семантическим следствием* теории T, если в любой модели T истинна A. Обозначение: $T \vDash A$

Теорема. *(Чёрч) Множество общезначимых формул неразрешимо*

Доказательство. Будем говорить, что теория T разрешима, если множество формул $\{A | T \vDash A\}$ разрешимо. Тогда если найдётся неразрешимая теория с конечным числом формул, теорема будет доказана. Действительно, пусть $T = \{A_1, \ldots, A_n\}$. Тогда проверить, следует ли из неё формула A — то же самое, что проверить, общезначима ли формула $(A_1 \wedge \ldots \wedge A_n) \to A$. Значит если мы не умеем проверять на следование из теории, то не умеем и проверять на общезначимость.

Построим неразрешимую теорию, пользуясь теоремой Маркова-Поста. Выберем некоторую полугруппу, порождённую $a_1, \ldots, a_n$ с неразрешимой проблемой равенства. В качестве сигнатуры возьмём функциональные символы $\cdot, =$ валентности 2 и $a_1, \ldots, a_n$ валентности 0. В качестве аксиом возьмём аксиому полугруппы $\forall x \forall y \forall z\ x \cdot (y \cdot z) = (x \cdot y) \cdot z$ и все имеющиеся у нас равенства. Теперь проблема равенства превращается в проверку на семантическое следование из этой теории, значит оно тоже неразрешимо. □

20 Дизъюнкты, универсальные дизъюнкты. Исчисление резолюций (ИР) для доказательства несовместности множеств универсальных дизъюнктов. Теорема корректности ИР.

Определение. *Дизъюнктом* называется дизъюнкция атомарных формул и их отрицаний.
Пример: $P(x) \vee \overline{Q}(y, f(x)) \vee s$ (в данном случае $P(x), \overline{Q}(y, f(x)), s$ — атомарные формулы, а $\vee$ — операция дизъюнкции)

Определение. *Универсальным дизъюнктом* называется формула, полученная из дизъюнкта приписыванием кванторов всеобщности. Пример: $\forall x \forall y [P(x) \vee \overline{Q}(y, f(x)) \vee s]$

Для того, чтобы доказывать несовместность множеств универсальных дизъюнктов (несовместность конъюнкции всех универсальных дизъюнктов этого множества) мы пользуемся правилами в исчислении резолюций

Правил в исчислении резолюций два:

- $\frac{A \vee p,\ B \vee \overline{p}}{A \vee B}$ (правило резолюций)
- $\forall x D(x) \vDash D(t)$ для некоторого t

Теорема. *(Теорема корректности исчисления резолюций) Если из набора универсальных дизъюнктов можно вывести пустой дизъюнкт, то этот набор несовместен.*

Доказательство. Идем методом от противного. Пускай существует модель M, в которой все данные дизъюнкы истинны. Заметим, что оба правила исчисления резолюций сохраняют истинность.

Действительно, если в правиле резолюций для $\frac{A \vee p,\ B \vee \overline{p}}{A \vee B}$ мы получим, что $A \vee B$ ложно, то это значит, что и A, и B ложно, однако если это так, то ложно либо $A \vee p$, либо $B \vee \overline{p}$

В правиле резолюций для $\forall x D(x) \vDash D(t)$, если выражение $D(x)$ истинно для любого x, то оно будет истинно для и для некоторого t [7]

Если мы вывели пустой дизъюнкт, то по истинности правил исчисления резолюций получаем, что пустой дизъюнкт является истинным. Противоречие. □

21 Непротиворечивые теории. Теорема полноты ИР (для множеств универсальных дизъюнктов).

Определение. *Непротиворечивой теорией* называется теория такая, что в ней утверждение не может быть одновременно доказано и опровергнуто

Теорема. *(Теорема полноты исчисления резолюций) Если набор универсальных дизъюнктов несовместен, то из него можно вывести пустой дизъюнкт*

Доказательство. Пускай есть счётное множество универсальных дизъюнктов S. Заметим, что если мы подставим вместо терм конкретные значения в этом множестве, то можем заменить все атомарные формулы пропозициональными переменными (константа 0 исчезает, так как дизъюнкция; константу 1 заменяем на дизъюнкцию переменных $p \vee \overline{p}$, p в данном случае — новая переменная, которую мы ввели). Назовём это новое множество из пропозициональных переменных S'.

Так как S несовместно, то S' тоже несовместно, так как существует набор терм, при котором из S мы получаем S'. Значит, мы свели теорему к случаю для дизъюнктов из пропозициональных переменных. Теорема полноты для такого случая доказывалась в билете 16. А раз для любого набора терм вывести пустой дизъюнкт нельзя, то и для S тоже. □

22 Исчисление резолюций для теорий, состоящих из формул общего вида (приведение к предваренной нормальной форме и сколемизация). Доказательства общезначимости с помощью ИР. Выводимость формулы в теории с помощью ИР. Теорема компактности.

Для того, чтобы применить правила исчислений резолюций для теорий, состоящих из формул общего вида необходимо для начала привести их к форме, состоящей из конъюнкций, дизъюнкций, отрицаний атомарных формул и кванторов всеобщности. Поэтому каждую формулу приводят сначала к *предваренной нормальной форме*, а затем к *сколемовской нормальной форме*

Определение. *Нормальной формой* называется формула, состоящая только из конъюнкций, дизъюнкций, отрицаний атомарных формул и кванторов

Определение. *Предваренной нормальной формой* называется нормальная форма формулы, кванторы которой стоят в начале

Определение. *Сколемовской нормальной формой* называется предваренная нормальная форма формулы, кванторы которой являются кванторами всеобщности

[7] В случае $\forall x \exists y, x < y$ не выполняется, если мы поставим $x = y$. Однако наши универсальные дизъюнкты не допускают квантора существования, поэтому такая формула невозможна

Для приведения к нормальной форме нужно преобразовывать нестандартные операции в вид конъюнкций, дизъюнкций и отрицаний (Пример: $A \to B \equiv \overline{A} \vee B$), а также пользоваться следующими правилами:

- $\overline{\exists x A(x)} \equiv \forall x \overline{A(x)}$
- $\overline{A \vee B} \equiv \overline{A} \wedge \overline{B}$

Для приведения к предваренной нормальной форме нужно вынести кванторы. Делается это при помощи следующих правил:

- $C \vee \forall x A(x) \equiv \forall x [C \vee A(x)]$, C не зависит от x, операции между A(x) и C могут быть любые ($\vee$ или $\wedge$), квантор для x тоже любой ($\forall$ или $\exists$)
- $\forall x A(x) \vee \forall x B(x) \equiv \forall x \forall y [A(x) \vee B(y)]$, тоже для любых операций и кванторов
- $\forall x A(x) \vee \forall x B(x) \vdash \forall x [A(x) \vee B(x)]$, для любых операций
- $\exists x [A(x) \vee B(x)] \vdash \exists x A(x) \vee \exists B(x)$, для любых операций

Для приведения к сколемовской нормальной форме будем использовать следующую операцию:

- Убираем самый левый квантор существования. Заменяем его в атомарных формулах на функцию от всех предыдущих кванторов всеобщности.

  Пример: $\forall x \exists y \forall z \exists w [A(x,w) \vee B(y,z)] \vdash \forall x \forall z \exists w [A(x,w) \vee B(f_y(x),z)] \vdash \forall x \forall z [A(x, f_w(x,z)) \vee B(f_y(x),z)]$

  Функции f_y, f_w называются *сколемовскими функциями*

Общезначимость формулы можно доказывать с помощью исчисления резолюций. Для этого возьмём отрицание этой формулы. Общезначимасть формулы $\Leftrightarrow$ несовместности отрицания. А несовместность доказываем с помощью исчисления резолюций, выводя пустой дизъюнкт.

Выводимость формулы в теории можно доказывать с помощью исчисления резолюций. Для этого (пусть формулы — A и B) заметим, что выводимость равносильна несовместности формулы $A \wedge \overline{B}$ (если есть хоть один набор терм, что эта формула истинна, то для него, слеедовательно, из A не выводима формула, истинная при всех значениях, при которых истинна B)

Пусть T — множество формул (может быть как конечным, так и счётным)

Теорема. *(Теорема компактности) Если T несовместно, то у него существует несовместное конечное подмножество T'*

Доказательство. Для конечного множества очевидно (берём в качестве подмножества само множество)

Для счётного множества: так как T несовместно, то из него можно вывести пустой дизъюнкт (теорема полноты ИР, билет 21). Причём этот пустой дизъюнкт выводится из конечного числа исходных формул (так как сами формулы конечные и число операций конечно). Поэтому возьмём в качестве T' эти формулы. Из них выводится пустой дизъюнкт (теорема корректности ИР, билет 20), а значит T' несовместна □

23 Гомоморфизмы, эпиморфизмы (сюръективные гомоморфизмы), изоморфизмы. Теорема о сохранении истинности при эпиморфизме. Изоморфные модели. Элементарно эквивалентные модели, элементарная эквивалентность изоморфных моделей.

Γ — сигнатура
M_1, M_2 — интерпретации Γ

Определение. *Гомоморфизмом* $h : M_1 \to M_2$ называется отображение, сохраняющее все предикаты и формулы в сигнатуре.

Для предиката $P^n \in \Gamma$, его интерпретаций $P_1 \in M_1, P_2 \in M_2$ действует
$\forall a_1, a_2, ..., a_n [P_1(a_1, a_2, ..., a_n) = P_2(h(a_1), h(a_2), ..., h(a_n))]$

Для формулы $f^n \in \Gamma$, его интерпретаций $f_1 \in M_1, f_2 \in M_2$ действует
$\forall a_1, a_2, ..., a_n [h(f_1(a_1, a_2, ..., a_n)) = f_2(h(a_1), h(a_2), ..., h(a_n))]$

Определение. *Эпиморфизмом (сюръективным гомоморфизмом)* $h : M_1 \to M_2$ называется, если h - гомоморфизм и является сюръекцией

Определение. *Изоморфизмом* $h : M_1 \to M_2$ называется, если h - гомоморфизм и является биекцией

Определение. M_1 *элементарно эквивалентно* M_2 *(*$M_1 \cong M_2$*)*, если для любой замкнутой формулы A сигнатуры Γ $M_1 \vDash A \Leftrightarrow M_2 \vDash A$ (формула истинна в M_1 т. и т.т, когда она истинна в M_2)

Пусть $h : M_1 \to M_2$ — эпиморфизм
$A(x_1,...,x_n)$ — произвольная формула

Теорема. *(Теорема о сохранении истинности при эпиморфизме) Для всех элементов* $a_1,...,a_n \in M_1, M_1 \vDash A(a_1,...,a_n) \leftrightarrow M_2 \vDash A(h(a_1),...,h(a_2))$

Доказательство.

Лемма. *для терма* t *верно, что* $h(|t(a_1,...,a_n)|_1) = |t(h(a_1),...,h(a_n))|_2$ *(*$|t(...)|_1$ *- терм в интерпретации* M_1*)*

Доказательство. Пусть $t = f(x, g(y))$. Тогда $|t(a,b)|_1 = f_1(a, g_1(b))$
$h(f_1(a, g_1(b))) = f_2(h(a), h(g_1(b))) = f_2(h(a), g_2(h(b)))$, мы пользуемся тем, что при гомоморфизме функции и предикаты сохраняются □

Пользуемся идукцией по построению A

1. База индукции: $A = P(t_1,...,t_m)$
   $M_1 \vDash A(a_1,...,a_m) \leftrightarrow P_1(|t_1(a_1,...,a_m)|_1,...) = 1 \Leftrightarrow P_2(h(t_1(a_1,...,a_m)),...) = 1$
   $\Leftrightarrow P_2(|t_1(h(a_1),...,h(a_m))|_2)$ (по лемме) $\leftrightarrow M_2 \vDash A(h(a_1),...,h(a_m))$
2. Индуктивный переход: разбиваем на случаи:
   - $A = B \vee C$
     $M_1 \vDash (B(a,...) \vee C(a,...)) \Leftrightarrow M_1 \vDash B$ или $M_1 \vDash C \Leftrightarrow M_2 \vDash B(h(a),...)$ или $M_2 \vDash C(h(a),...) \Leftrightarrow M_2 \vDash (B \vee C)(h(a),...)$ (аналогично доказывается для остальных операций)
   - $A = \exists x B(x, y)$
     $M_1 \vDash \exists x B(x, a) \leftrightarrow \exists b \in M_1, M_1 \vDash B(b, a) \leftrightarrow \exists b \in M_1, M_2 \vDash B(h(b), h(a)) \leftrightarrow \exists c \in M_2, M_2 \vDash B(c, h(a)) \leftrightarrow M_2 \vDash \exists x B(x, h(a))$ (предпоследняя эквивалентность верна именно потому, что у нас эпиморфизм), квантор всеобщности доказывается аналогично

□

Теорема. *(Элементарная эквивалентность изоморфных моделей) Если модели* M_1 *и* M_2 *изоморфны, то они элементарно эквивалентны* [8]

Доказательство. Рассматриваем только замкнутые формулы A. Из предыдущей теоремы следует, что формула A сохраняет свою истинность при изоморфизме, а это значит, что M_1 и M_2 будут элементарно эквивалентны по определению. □

26 Игры Эренфойхта

Цель: сформулировать общий критерий элементарной эквивалентности двух интерпретаций некоторой сигнатуры (считаем, что сигнатура содержит только предикатные символы).

Критерий будет сформулирован в терминах некоторой игры, называемой игрой Эренфойхта. В ней участвуют два игрока, называемые Новатором (Н) и Консерватором (К). Игра определяется выбранной парой интерпретаций.

В начале игры Новатор объявляет натуральное число k. Далее они ходят по очереди, начиная с Н; каждый из игроков делает k ходов, после чего определяется победитель.

На i-м ходу Н выбирает элемент в одной из интерпретаций (в любой из двух) и помечает его числом i. В ответ К выбирает некоторый элемент из другой интерпретации и также помечает его числом i.

После k ходов игра заканчивается. При этом в каждой интерпретации k элементов оказываются помеченными числами от 1 до k (мы не учитываем, кто именно из игроков их пометил). Обозначим эти элементы $a_1, a_2, \cdots, a_k$

[8] Для элементарной эквивалентности достаточно даже просто эпиморфизма, но мы используем более частую формулировку теоремы

(для первой интерпретации) и b_1, b_2, $\cdots$, b_k (для второй). Элементы a_i и b_i (с одним и тем же i) будем называть соответствующими друг другу.

Посмотрим, найдётся ли предикат сигнатуры, который различает помеченные элементы первой и второй интерпретации (то есть истинен на некотором наборе помеченных элементов в одной интерпретации, но ложен на соответствующих элементах другой). Если такой предикат найдётся, то выигрывает Новатор, в противном случае — Консерватор.

Теорема. *Интерпретации не элементарно эквивалентны* $\iff$ *Н имеет выигрышную стратегию в этой игре.*

Доказательство. Докажем, что если Новатор имеет выигрышную стратегию, то интерпретации не элементарно эквивалентны.

Пусть есть различающая формула. Приведем ее к предваренной форме. Будем последовательно смотреть на кванторы в ее начале. Пусть текущий квантор - это $\exists$. Значит, есть элемент в M_1, для которого верна оставшаяся часть формулы, в то время как в M_2 такого нет. Этот элемент и должен выбрать Новатор очередным ходом.

Пусть текущий квантор - это $\forall$. В таком случае мы можем перейти к отрицанию и поступить аналогично шагу с $\exists$, только выбирая элемент в M_2.

Таким образом, за количество шагов, равное количеству кванторов в различающей формуле, Новатор может построить различающие наборы.

□

27 Семантически полные теории. Критерий семантической полноты теории в терминах эле- ментарной эквивалентности моделей. Аксиоматизация элементарной теории упорядоченного множества целых чисел.

Определение. *Аксиоматическая теория* T - множество замкнутых формул.

T *семантически полна*, если для любой замкнутой формулы A выполнено одно из двух:

1. из T семантически следует A (A истинно во всех моделях теории)
2. из T семантически следует $\neg A$

Лемма. *Теория семантически полна* $\iff$ *любые 2 ее модели элементарно эквивалентны.*

Доказательство. $\Rightarrow$ Элементарная эквивалентность значит, что в обоих моделях любая формула или истинна, или ложна. Тогда если ϕ следует из A, то она истинна для всех моделей, следовательно, для каждой пары. Аналогично для $\neg\phi$

$\Leftarrow$ От противного: какая-то формула сама не следует и ее отрицание не следует. Значит, есть модели, в одной из которых A истинно, в другой - ложно. Противоречие с элементарной эквивалентностью.

□

Аксиоматизация множества рациональных чисел

$M = (\mathbb{Q}, =, <)$

- аксиомы равенства
  1. $\forall x\ x = x$
  2. $\forall x \forall y\ x = y \to y = x$
  3. $\forall x \forall y \forall z\ \ x = y \wedge y = z \to x = z$
  4. $\forall x_1 \forall x_2 \forall y_1 \forall y_2\ \ x_1 = x_2 \wedge y_1 = y_2 \to (x_1 = x_2 \to y_1 = y_2)$
- аксиомы линейного порядка
  1. $x < y \wedge y < z \to x < z$
  2. $\neg\,(x < x)$
  3. $\forall x \forall y\ x < y \vee x > y \vee x = y$

- отсутствие наибольшего и наименьшего элемента
- плотность множества $\forall x, y\ (x < y \to \exists z\ \ x < z \wedge z < y)$

Теорема. *T - совместная и семантически полная.*

Доказательство. Доказательство аналогично игре Эренфойхта с $\mathbb{R}$ и$\mathbb{Q}$. Все выбранные в одной модели элементы идут в том же порядке, что и элементы второй модели. Консерватору достаточно возможности выбрать элемент между любыми двумя и отсутствие наибольшего и наименьшего элемента. □

28 Аксиоматизация множества целых чисел.

$M = (\mathbb{Z}, =, <)$

- аксиомы равенства
- аксиомы линейного порядка
- отсутствие наибольшего и наименьшего элемента
- $\forall x \exists y (x < y \wedge \neg(\exists z\ \ x < z \wedge z < y))$
- $\forall x \exists y (x > y \wedge \neg(\exists z\ \ x > z \wedge z > y))$

Теорема. *T - совместная и семантически полная.*

Доказательство. Как устроены модели T? Это $\mathbb{Z}$, $\mathbb{Z}+\mathbb{Z}$ или любое множество вида AZ (A - линейно упорядоченное множество, в каждом элементе которого лежит множество целых чисел). Скажем, что элементы эквивалентны, если мы можем получить один из другого за конечное число шагов. Факторизуем по этому отношению эквивалентности. □

Лемма. *Для любого линейно упорядоченного A $A\mathbb{Z} \cong \mathbb{Z}$*

Доказательство. Доказывается аналогично случаю с $\mathbb{Z} + \mathbb{Z}$. □