Коллоквиум по Дискретной Математике-2

Алиса Вернигор Telegram
Валерий Березовский Telegram
Василий Шнышко Telegram
Денис Козлов Telegram
Ира Голобородько Telegram
Марк Рофин Telegram
Никита Насонков Telegram
Оля Козлова Telegram

Версия от 13.12.2020 04:47

Спасибо команде hse-tex и в частности Сергею Пилипенко за конспекты лекций.

Спасибо Демиду Васильеву за предоставленные материалы по вычислимости.

Содержание

1 Обозначения в разделе вычислимости

- Алгоритмы и машины Тьюринга обозначаются рукописными буквами, например, $\mathcal{M}$ (читается как «М-красивое» по Дашкову).
- $\operatorname{dom} f$ и $\operatorname{rng} f$ — области определения и значений функции f соответственно.
- Мы не пользуемся записью вида $f : A \xrightarrow{p} B$ для частичных функций, а явно указываем, если рассматриваемая функция тотальна.
- Привычно равенство функций обозначать как $f = g$, но так как в данном курсе рассматриваются и не всюду определенные функции, то $f(x) \simeq g(x) \iff$ в точке x функции совпадают по значению либо обе не определены.
- Функции ξ и $\mathrm{id}_{\mathbb{N}}$ — нигде не определенная и тождественная соответственно.

2 Вопросы по вычислимости

2.1 Вычислимые функции (при интуитивном понимании алгоритма). Разрешимые и перечислимые множества. Связь конечности, разрешимости и перечислимости. Разрешимые множества под действием операций алгебры множеств и декартова произведения. [R, с. 3–4]

Алгоритмом в его интуитивном понимании считается конечная последовательность инструкций, которая исполняется по шагам. Алгоритм может принимать на вход аргументы и выдавать какой-то результат.

Определение 1. Функция f вычислима, если существует алгоритм $\mathcal{A}$, вычисляющий ее. Это значит, что для любого входа $x \in \operatorname{dom} f$ $\mathcal{A}$ выдает результат $f(x)$ за конечное число шагов, а при $x \notin \operatorname{dom} f$ зацикливается (причем неважно, естественным или искусственным образом).

Определение 2. Множество A разрешимо, если вычислима его характеристическая функция

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

Определение 3. Множество A перечислимо, если существует алгоритм-«перечислитель» $\mathcal{A}$ без входа, печатающий каждый элемент A за конечное число шагов, и только элементы A. Также A перечислимо тогда и только тогда, когда вычислима его полухаракетристическая функция

$$\omega_A(x) = \begin{cases} 1, & x \in A \\ \text{не опр.}, & x \notin A \end{cases}.$$

Эквивалентность этих определений доказана в билете 4.

Утверждение 2.1. *Из конечности множества следует его разрешимость, а из разрешимости — перечислимость.*

Если $A = \{a_1, a_2, \ldots, a_n\}$ конечно, то приведенный ниже код вычисляет характеристическую функцию:

function $\chi_A(x)$
  if $x = a_1$ **or** $x = a_2$ **or** $\ldots$ **or** $x = a_n$ **then**
    return 1
  else
    return 0

Для бесконечного множества такой трюк невалиден, так как код должен быть **конечной** последовательностью байт.

Если A разрешимо, то его характеристическая функция χ_A вычислима, поэтому данный алгоритм рано или поздно обработает каждое натуральное число, не зациклившись:

procedure $\textsc{print}_A()$
  for all $x \in \mathbb{N}$ **do**

if $\chi_A(x)$ **then**
  print x

Утверждение 2.2. *Из разрешимости A и B следует разрешимость $A \cap B,\ A \cup B,\ \bar{A},\ A \times B$.*

Доказательство. Достаточно предъявить характеристические функции данных множеств:

- $\chi_{A\cap B}(x) = \chi_A(x) \cdot \chi_B(x)$
- $\chi_{A\cup B}(x) = \chi_A(x) + \chi_B(x) - \chi_{A\cap B}(x)$
- $\chi_{\bar{A}}(x) = 1 - \chi_A(x)$
- $\chi_{A\times B}((x,y)) = \chi_A(x) \cdot \chi_B(y)$

Понятно, что эти функции вычислимы как композиции вычислимых. ■

2.2 Перечислимые множества под действием операций алгебры множеств, декартова произведения и проекции. Теорема Поста. [R, 3–4]

Утверждение 2.3. *Из перечислимости A и B следует перечислимость $A \cap B,\ A \cup B,\ A \times B,\ \mathrm{pr}^i A$.*

Доказательство. Предложим алгоритмы перечисления этих множеств, подразумевая, что $\mathcal{A}$ и $\mathcal{B}$ — перечислители A и B соответственно:

$A \cap B$ Будем параллельно исполнять $\mathcal{A}$ и $\mathcal{B}$ по шагам и сохранять вывод каждого в два буфера. Время от времени (скажем, после каждых 2020 шагов) за конечное время просматриваем оба буфера и выводим элементы, оказавшиеся в обоих. Перечислимость можно также вывести как $\omega_{A\cap B}(x) = \omega_A(x) \cdot \omega_B(x)$.

$A \cup B$ Достаточно подать вывод как $\mathcal{A}$, так и $\mathcal{B}$ на выход перечислителя $A \cup B$.

$A \times B$ Аналогично случаю $A \cap B$, только выводить нужно все пары $(a,b) \in A' \times B'$, где A' и B' — буферы в текущий момент исполнения $\mathcal{A}$ и $\mathcal{B}$. Перечислимость можно также вывести как $\omega_{A\times B}((x,y)) = \omega_A(x) \cdot \omega_B(y)$.

$\mathrm{pr}^i A$ Проекцией $\mathrm{pr}^i A$ называется множество $\{b \in \mathbb{N} \mid \exists a_1, \ldots, a_k : (a_1, \ldots, a_{i-1}, b, a_{i+1}, \ldots, a_k) \in A\}$ при $A \subseteq \mathbb{N}^k$ и $1 \leqslant i \leqslant k$. Чтобы перечислить проекцию, запустим $\mathcal{A}$ и будем выводить каждую i-тую координату всех полученных элементов множества. ■

Заметим, что перечислимость A не гарантирует перечислимость $\bar{A}$ из-за проблемы «остановки»: на любом конечном количестве шагов работы перечислителя непонятно, по какой причине он не вывел конкретное число.

Теорема 2.4 (Поста)**.** *Множество A разрешимо тогда и только тогда, когда A и $\bar{A}$ перечислимы.*

Доказательство. Из билета 1: A разрешимо $\implies$ $\bar{A}$ разрешимо. Из разрешимости следует перечислимость, следовательно A и $\bar{A}$ перечислимы.

В обратную сторону. Хотим узнать истинность $x \in A$. Для этого будем по очереди исполнять по шагам перечислитель то A, то $\bar{A}$. Так как $x \in \mathbb{N} = A \cup \bar{A}$, то x будет напечатан перечислителем ровно одного из двух множеств за конечное число шагов. Если это был перечислитель A, то $x \in A$, иначе $x \notin A$. Иными словами,

$$\chi_A(x) = \begin{cases} 1, & \omega_A(x) = 1 \\ 0, & \omega_{\bar{A}}(x) = 1 \end{cases}.$$

■

2.3 Теорема о графике вычислимой функции. Перечислимость образа и прообраза множества под действием вычислимой функции. [R, 14]

Определение 4. Графиком функции $f : \mathbb{N} \to \mathbb{N}$ называется множество его точек $\Gamma_f = \{(x, y) \in \mathbb{N}^2 \mid f(x) = y\}$.

Теорема 2.5 (о графике)**.** *Функция f вычислима $\iff$ Γ_f перечислим.*

Доказательство.

$\Longrightarrow$ Перечислим все пары $(x, k) \in \mathbb{N}^2$, и для каждой запустим алгоритм, вычисляющий $f(x)$. Если спустя k шагов был возвращен результат y, то даем на выход точку (x, y) графика. Иначе переходим к следующей паре (x', k'). Заметим, что если f не определена в какой-то точке, то никакие конечные k шагов не выдадут значение функции, поэтому алгоритм корректен.

$\Longleftarrow$ Запустим перечислитель $\mathcal{G}$ графика Γ_f. Если $f(x)$ определено, то спустя конечное число шагов $\mathcal{G}$ напечатает пару вида (x, y), и тогда верно $f(x) = y$. Иначе $x \notin \mathrm{pr}^1 \Gamma_f$, и в таком случае $\mathcal{G}$ будет работать бесконечно, что и требуется при неопределенном значении f в точке x. ■

Утверждение 2.6. *Функция f вычислима и тотальна $\Longrightarrow$ Γ_f разрешим.*

Доказательство.

$\Longrightarrow$

$$\chi_{\Gamma_f}((x, y)) = \begin{cases} 1, & (x, y) \in \Gamma_f \\ 0, & (x, y) \notin \Gamma_f \end{cases} = \begin{cases} 1, & f(x) = y \\ 0, & f(x) \neq y \end{cases} \text{ — вычислима.}$$

■

Утверждение 2.7. *Если $f : \mathbb{N} \to \mathbb{N}$ вычислима и A перечислимо, то $f(A)$ и $f^{-1}(A)$ перечислимы.*

Доказательство. Заметим, что $f(A) = \mathrm{pr}^2\big(\Gamma_f \cap (A \times \mathbb{N})\big)$ и $f^{-1}(A) = \mathrm{pr}^1\big(\Gamma_f \cap (\mathbb{N} \times A)\big)$. Оба перечислимы, так как проекция, пересечение и декартово произведение перечислимых множеств перечислимы (билет 2). ■

Следствие. Если $f : \mathbb{N} \to \mathbb{N}$ вычислима, то $\mathrm{dom}\, f = f^{-1}(\mathbb{N})$ и $\mathrm{rng}\, f = f(\mathbb{N})$ перечислимы.

2.4 Перечислимые множества суть, в точности, области определения вычислимых функций. [R, 10]

См. утверждение (1) $\iff$ (3) из теоремы ниже.

Теорема 2.8 (равносильные определения перечислимости)**.** *Следующие утверждения о произвольном множестве $A \subseteq \mathbb{N}$ эквивалентны:*

(1) A перечислимо;

(2) полухарактеристическая функция $\omega_A(x) \simeq \begin{cases} 1, & x \in A \\ \text{не опр.}, & x \notin A \end{cases}$ вычислима;

(3) существует вычислимая функция $f : \mathbb{N} \to \mathbb{N}$, такая что $A = \mathrm{dom}\, f$;

(4) существует вычислимая функция $f : \mathbb{N} \to \mathbb{N}$, такая что $A = \mathrm{rng}\, f$;

(5) $A = \varnothing$ или существует вычислимая тотальная функция $f : \mathbb{N} \to \mathbb{N}$, такая что $A = \mathrm{rng}\, f$;

(6) существует разрешимое $B \subseteq \mathbb{N}^2$, такое что $A = \mathrm{pr}^i B$.

Доказательство.

(1) $\iff$ (2) Запустим перечислитель $\mathcal{A}$. Если в выводе встречается x, то $\omega_A(x) = 1$, иначе алгоритм зациклится на входе $x \notin A$. В обратную сторону: $\operatorname{dom}\omega_A = A \implies A$ перечислимо (см. билет 3).

(1) $\iff$ (3) $\operatorname{dom} f = A \implies A$ перечислимо; если A перечислимо, то за f можно взять ω_A.

(1) $\iff$ (5) Пусть $A \neq \varnothing$ перечислимо и $\mathcal{A}$ напечатал первое число ровно после k шагов. Тогда зададим $f(n)$ как последнее выведенное перечислителем число ровно после $n + k$-того шага алгоритма. Обратно: $\mathcal{A}$ по очереди перечисляет пары $(x, k) \in \mathbb{N}^2$ и эмулирует вычисление k шагов значения $f(x)$. $\mathcal{A}$ печатает результат y, если он есть, и переходит к следующей паре (x', k').

(1) $\iff$ (4) Если $A = \varnothing$, то подойдет $f = \xi$, иначе достаточно взять функцию, описанную в предыдущем пункте. Обратно: аналогично предыдущему пункту.

(1) $\iff$ (6) Если $A = \varnothing$, то подойдет $B = \varnothing$, иначе достаточно взять функцию f, описанную в пункте (1) $\iff$ (5), и задать $B = \Gamma_f$, тогда $A = \operatorname{pr}^2 B$. Обратно: B разрешимо $\implies$ B перечислимо $\implies$ $\operatorname{pr}^1 B = A$ перечислимо. ■

2.5 Непустые перечислимые множества суть, в точности, области значений вычислимых тотальных функций. [R, 10, с. 4]

См. утверждение (1) $\iff$ (5) из билета 4.

2.6 Перечислимые множества суть, в точности, проекции разрешимых. [R, 10]

См. утверждение (1) $\iff$ (6) из билета 4.

2.7 Универсальная вычислимая функция (в классе вычислимых функций $\mathbb{N} \to \mathbb{N}$). T-Предикат. [R, 7–8]

Определение 5. Отображение $U : \mathbb{N}^2 \to \mathbb{N}$ — универсальная вычислимая функция (УВФ), если (а) U вычислима и (б) для любой вычислимой $f : \mathbb{N} \to \mathbb{N}$ найдется $n \in \mathbb{N}$, такое что $\forall x \in \mathbb{N}\ \ U(n, x) \simeq f(x)$. Иными словами, сечение U_n совпадает с f.

Функция $d : \mathbb{N} \to \mathbb{N}$ называется диагональю функции $V : \mathbb{N}^2 \to \mathbb{N}$, если $\forall x \in \mathbb{N}\ \ d(x) \simeq V(x, x)$.

Неформально: алгоритмы можно рассматривать как конечные последовательности байт, поэтому их счетно и каждому тексту программы можно сопоставить его номер из $\mathbb{N}$. Он и есть первый аргумент U, а второй — аргумент функции, которую вычисляет алгоритм. Получается, УВФ эмулирует вычисление всех вычислимых функций одного аргумента.

Пусть U — УВФ, а $\mathcal{U}$ — алгоритм, вычисляющий ее.

Определение 6. T-предикат — подмножество $\mathbb{N}^3$, такое что $(n, x, k) \in T$ тогда и только тогда, когда $\mathcal{U}$ останавливается на входе (n, x) за k шагов. T'-предикат — подмножество $\mathbb{N}^4$, такое что $(n, x, y, k) \in T$ тогда и только тогда, когда $\mathcal{U}$ останавливается на входе (n, x) за k шагов и возвращает y. Ясно, что оба отношения разрешимы, так как можно исполнить k шагов вычисляющего алгоритма и проверить, остановился ли он и вывел ли что-то.

2.8 Неразрешимость проблем самоприменимости и остановки. Примеры перечислимого неразрешимого и неперечислимого множеств. [R, 23]

Утверждение 2.9. *Существует перечислимое неразрешимое множество.*

Доказательство. Пусть U — УВФ. Рассмотрим $K_U = \{n \in \mathbb{N} \mid U(n, n) \text{ определено}\} = \operatorname{dom} d_U$. d_U вычислима $\implies K_U = \operatorname{dom} d_U$ перечислимо.

Предположим, что K_U разрешимо, тогда по теореме Поста $\bar{K}_U$ перечислимо. Тогда вычислима функция

$$r(x) \simeq \omega_{\bar{K}_U}(x) \simeq \begin{cases} 1, & x \notin K_U \\ \text{не опр.}, & x \in K_U \end{cases}.$$

Тогда $\exists n \in \mathbb{N} :\ U_n = r \implies U(n,n) \simeq r(n)$. Приходим к двум случаям:

- $U(n,n)$ определено $\implies n \in \operatorname{dom} d_U \implies n \in K_U \implies r(n)$ не определено, но $U(n,n)$ определено.
- $U(n,n)$ не определено $\implies n \notin \operatorname{dom} d_U \implies n \notin K_U \implies r(n) = 1$, но $U(n,n)$ не определено.

Пришли к противоречию, следовательно r невычислима $\implies \bar{K}_U$ неперечислимо $\implies K_U$ неразрешимо по теореме Поста.

Итак, $K_U = \operatorname{dom} d_U$ — искомое перечислимое неразрешимое множество. ■

Заметим, что найденное K_U — множество всех программ, останавливающихся на входе из своего текста, поэтому теорема называется также проблемой самоприменимости, которая, как оказалось, неразрешима, то есть невозможно за конечное число шагов узнать, остановится ли программа на входе, совпадающим с ее текстом.

Эта проблема связана также с проблемой остановки. Рассмотрим $S_U = \operatorname{dom} U \subseteq \mathbb{N}^2$ — перечислимое из вычислимости U. Сведем S_U к K_U, заметив, что $n \in K_U \iff U(n,n)$ определено $\iff (n,n) \in S_U$. Отсюда сразу можем заключить, что S_U неразрешимо $\implies$ проблема остановки неразрешима.

Таким образом, не существует программы, которая бы за конечное число шагов определяла, остановится ли произвольная программа на любом входе либо входе, совпадающим с ее текстом.

2.9 Пример вычислимой функции, не имеющей вычислимого тотального продолжения. [R, 29]

Утверждение 2.10. *Пусть U — УВФ и d — ее диагональ. Тогда для любой вычислимой функции $f : \mathbb{N} \to \mathbb{N}$ существует $n \in \mathbb{N} :\ f(n) \simeq d(n)$.*

Доказательство. Ввиду универсальности U найдется номер $n \in \mathbb{N} :\ U_n = f$. Тогда $f(n) \simeq U(n,n) \simeq d(n)$. ■

Следствие. Функция f невычислима, если $\forall n \in \mathbb{N}\ \ f(n) \not\simeq d(n)$.

Определение 7. Функция $g : \mathbb{N} \to \mathbb{N}$ называется продолжением $f : \mathbb{N} \to \mathbb{N}$, если $\forall x \in \operatorname{dom} f\ \ g(x) = f(x)$. Иными словами, $\Gamma_f \subseteq \Gamma_g$.

Пусть d — диагональ произвольной УВФ U, а d' — ее тотальное вычислимое продолжение, тогда функция $g(x) = d'(x) + 42$ тотальна и вычислима как композиция вычислимых тотальных функций. Но g не совпадает с d ни в одной точке, следовательно она не может быть вычислимой — противоречие.

Таким образом, диагональная функция произвольной УВФ не имеет тотального вычислимого продолжения.

2.10 Область определения вычислимой функции, не имеющей вычислимого тотального продолжения, перечислима, но не разрешима. [R, 32]

Утверждение 2.11. *Если функция f вычислима, но не имеет вычислимого тотального продолжения, то* $\operatorname{dom} f$ *— неразрешимое перечислимое множество.*

Доказательство. Предположим противное: пусть $\operatorname{dom} f$ разрешимо (при этом оно всегда перечислимо — см. билет 3). Рассмотрим

$$g(x) = \begin{cases} f(x), & x \in \operatorname{dom} f \\ 42, & x \notin \operatorname{dom} f \end{cases} = \chi_{\operatorname{dom} f}(x) \cdot f(x) + (1 - \chi_{\operatorname{dom} f}(x)) \cdot 42.$$

Ясно, что g — вычислимое тотальное продолжение f — противоречие. Значит, $\operatorname{dom} f$ неразрешимо и перечислимо. ■

2.11 Теорема о рекурсии как следствие теоремы Клини. Пример применения теоремы о рекурсии. [R, 37]

Подробнее о теореме Клини — в 16-м билете.

Теорема 2.12 (о рекурсии)**.** *Пусть U — ГУВФ и $V : \mathbb{N}^2 \to \mathbb{N}$ вычислима. Тогда $\exists n \in \mathbb{N} :\ U_n = V_n$.*

Доказательство. Ввиду главности U существует вычислимая тотальная $s :\ \forall k \in \mathbb{N}\ \ U_{s(k)} = V_k$, а по теореме Клини $\exists n \in \mathbb{N} :\ U_{s(n)} = U_n$. Следовательно, $U_n = V_n$. ■

Но причем здесь рекурсия? Дело в том, что V можно задать как функцию, зависящую от U:

- *Пример.* Существование квайнов (программ, выводящих свой текст): $\exists n \in \mathbb{N} :\ \forall x\ U(n, x) = n$.

  Доказательство. Функция $V(k, x) = k$ вычислима. По теореме о рекурсии $\exists n \in \mathbb{N} :\ U(n, x) \simeq V(n, x) = n$. ■

- *Пример.* Рассмотрим вычислимую функцию

  $$V(k, x) \simeq \begin{cases} 1, & x = 0 \\ x \cdot U(k, x - 1), & x > 0 \end{cases}.$$

  По теореме о рекурсии $\exists n :\ U_n = V_n \implies U(n, 0) = 1$ и $U(n, x) \simeq x \cdot U(n, x - 1)$ при $x > 0$, при этом тотальность U_n доказывается по индукции по x. Таким образом, $U(n, x)$ рекурсивно вычисляет факториал второго аргумента.

Неформально о смысле теоремы: в главных языках программирования программа может иметь доступ к своему коду, что приводит нас к понятию рекурсии, существование алгоритма для которой гарантирует теорема Клини.

2.12 m-Сводимость и ее свойства. [R, 52–56]

Определение 8. Пусть $A, B \subseteq \mathbb{N}$. A m-сводится к B тогда и только тогда, когда существует вычислимая тотальная $f : \mathbb{N} \to \mathbb{N} :\ \forall n\ [n \in A \iff f(n) \in B]$. Обозначается как $A \leqslant_m B$ или $A \leqslant_m^f B$ (если необходимо уточнить функцию сведения). Это определение обобщается на $A \subseteq \mathbb{N}^n$, $B \subseteq \mathbb{N}^m$ и $f : \mathbb{N}^n \to \mathbb{N}^m$.

Перечислим свойства m-сводимости:

- Рефлексивность: $A \leqslant_m^{\mathrm{id}_{\mathbb{N}}} A$
- Транзитивность: $A \leqslant_m^f B \wedge B \leqslant_m^g C \implies A \leqslant_m^{g \circ f} C$

- $A \leqslant_m^f B \implies \bar{A} \leqslant_m^f \bar{B}$: $n \in \bar{A} \iff n \notin A \iff f(n) \notin B \iff f(n) \in \bar{B}$ ■
- *Сравнение множеств по алгоритмической сложности:* если $A \leqslant_m B$ и B разрешимо (перечислимо), то разрешимо (перечислимо) и A.

  Доказательство. $\forall n \left[n \in A \iff \chi_A(n) = 1 \iff \chi_B(f(n)) = 1 \iff f(n) \in B \right] \implies \chi_A = \chi_B \circ f$ — вычислима $\implies$ A разрешимо (аналогично $\omega_A = \omega_B \circ f$). ■
- **Следствие.** Если $A \leqslant_m B$ и A неразрешимо (неперечислимо), то и B неразрешимо (неперечислимо).
- Если A разрешимо и B нетривиально ($\varnothing \neq B \neq \mathbb{N}$), то $A \leqslant_m B$.

  Доказательство. Пусть $b \in B$, $a \in \bar{B}$, зададим вычислимую $f(n) := \begin{cases} b, & n \in A \\ a, & n \notin A \end{cases} \implies A \leqslant_m^f B$. ■
- $\exists A:\ A \not\leqslant_m \bar{A}$. Возьмем $A := \bar{K} = \mathbb{N} \setminus \operatorname{dom} d$ — неперечислимое, но $\bar{A}$ перечислимо — противоречие сравнению по алгоритмической сложности. ■
- $\nexists A:\ \forall B \subseteq \mathbb{N}\ B \leqslant_m A$. Одна функция может m-сводить к A лишь одно множество, но вычислимых функций счетно, а подмножеств $\mathbb{N}$ — несчетно много. ■

2.13 Машины Тьюринга (допустимо неформальное определение с лентой и головкой). Сложение натуральных чисел (при унарном и бинарном кодировании) вычислимо по Тьюрингу. [ВШ-3, 9.2]

Машина Тьюринга — устройство, представляющее собой бесконечную ленту, разделенную на ячейки с записанными в них символами, головку, которая движется по ленте и перезаписывает символы в ячейки, и инструкции, оперирующие головкой и задающие некоторый алгоритм.

Задаются множества Γ — алфавит, символы которого можно использовать при записи в ячейки (в том числе символ пробела «#»); $\Sigma \subseteq \Gamma$ — алфавит, в символах которого записан вход (причем $\# \in \Gamma \setminus \Sigma$); Q — множество состояний, которые принимает головка. Все эти множества обязательно **конечны**.

Головка имеет начальное и конечное состояние (обычно они обозначаются как q_1 и q_0), а также промежуточные состояния, с помощью которых задается алгоритм. Для всех элементов $Q \times \Gamma$ существуют инструкции вида $qc \mapsto q'c'S$. Она означает, что если головка находится в состоянии q и в текущей ячейке записан символ c, то головка переходит в состояние q', записывает в текущую ячейку символ c' и сдвигается влево, вправо либо остается на месте ($S \in \{L = \text{«Left»}, R = \text{«Right»}, N = \text{«Neutral»}\}$). Таким образом, должна быть определена функция инструкций $\delta : Q \times \Gamma \to Q \times \Gamma \times \{N, L, R\}$.

Для понимания работы машины Тьюринга вводится понятие конфигурации машины — это строка вида $AqcB$, означающая, что в данный момент на ленте подряд записаны слово $A \in \Gamma^*$, символ $c \in \Gamma$, слово $B \in \Gamma^*$, причем головка находится в состоянии q и указывает на ячейку с символом c. Отметим, что, например, `42`q`195` и `###42`q`195#` — одна и та же конфигурация. На множестве всевозможных конфигураций машины Тьюринга $\mathcal{M}$ задаются отношения $AqcB \underset{\mathcal{M}}{\to} A'q'c'B'$ и $AqcB \underset{\mathcal{M}}{\twoheadrightarrow} A'q'c'B'$, означающие достижимость за один и за сколько угодно шагов работы машины соответственно.

Рассмотрим задачу сложения натуральных чисел. Пусть на вход даны числа n и m в унарном виде, тогда лента будет иметь такой вид:

$$\texttt{\#\#\#\#\#}\underset{\uparrow\, q_1}{\#}\underbrace{11\ldots11}_{n}\texttt{\#}\underbrace{11\ldots11}_{m}\texttt{\#\#\#\#\#\#}$$

Тогда для получения суммы $n + m$ достаточно «склеить» две последовательности. Поэтому стартуем из начального состояния до пробела, заменяем его на единицу, после чего переходим в новое состояние, доходим до конца записи m

и останавливаемся на пробеле. Необходимо перейти в еще одно состояние, чтобы удалить последнюю единицу, после чего дойти до начала входных данных и остановиться.

Заметим, что если $m = 0$, то добавленная единица будет стерта. При $n = 0$ замена на единицу произойдет также в правильной ячейке ленты.

В итоге получили такую конфигурацию:

$$\#\#\#\#\#\#\underbrace{11\ldots1}_{n}1\underbrace{11\ldots\#}_{m}\#\#\#\#\#\#$$

Важно, что кодирование чисел не имеет значения, так как перевод числа в новую кодировку вычислим по Тьюрингу. Вот как двоичная запись превращается в унарную:

- Приходим к концу числа, чтобы вычесть из него единицу;
- При вычитании находимся в состоянии «нужно из разряда слева попросить единицу, в текущем разряде сейчас поменяю 0 на 1 и сдвинусь влево»;
- Так сдвигаемся, пока либо не получили корректный результат (находясь хоть в середине числа), либо до конца числа (это будет значить, что все нули превратились в единицы, то есть произошло переполнение и пора заканчивать алгоритм);
- Теперь необходимо добавить единичку в унарное представление числа, для чего идем в правый конец и на место второго пробела записываем единицу (первый же пробел служит разделителем входа и выхода алгоритма);
- Снова ищем первый пробел, чтобы вернуться в состояние вычитания;
- Завершение алгоритма: когда получили некорректное вычитание, головка окажется слева от входа и выхода. Переходим в новое состояние, чтобы пройтись до первого пробела и стереть на своем пути символы измененного входа. Так перейдем в конечное состояние и получим корректный вывод.

Таким образом, сложение в унарном и бинарном кодировании вычислимо по Тьюрингу.

2.14 Главная универсальная вычислимая функция. Вычислимое биективное кодирование пар натуральных чисел. Построение главной у.в.ф. с помощью произвольной у. в. ф. [R, 22, с. 9–10]

Определение 9. Отображение $U : \mathbb{N}^2 \to \mathbb{N}$ — главная универсальная вычислимая функция (ГУВФ), если (а) она вычислима и (б) для любой вычислимой $V : \mathbb{N}^2 \to \mathbb{N}$ найдется вычислимая тотальная $s : \mathbb{N} \to \mathbb{N}$, такая что $\forall n \in \mathbb{N}\ V_n = U_{s(n)}$.

Неформально: можем рассматривать V как другой язык программирования (от которого не требуется универсальность), а s — как функцию, преобразующую корректную программу в языке V в эквивалентную в языке U.

Утверждение 2.13. *Если U — ГУВФ, то U — УВФ.*

Доказательство. Рассмотрим произвольную вычислимую функцию f, для которой хотим найти номер n ее сечения в U. Введем $V : \mathbb{N}^2 \to \mathbb{N}$, такую что каждое ее сечение совпадает с f. Ввиду главности U существует вычислимая тотальная $s : \forall k \in \mathbb{N}\ U_{s(k)} = V_k$. Тогда за n можно взять любой элемент из $\operatorname{rng} s$, например, $n := s(42) \implies f = V_{42} = U_{s(42)} = U_n$. Следовательно, U обладает свойством универсальности. ■

Утверждение 2.14. *Если существует УВФ, то существует и ГУВФ.*

Доказательство. Зафиксируем УВФ U и введем кодирование пар, для этого рассмотрев любую вычислимую биекцию $h : \mathbb{N}^2 \to \mathbb{N}$ $\left(\text{например, } h(n,m) = \dfrac{(n+m)(n+m+1)}{2} + n\right)$. Пусть код пары — функция $\langle n, m\rangle := h(n,m)$, а также $\pi^1(\langle n,m\rangle) = n$ и $\pi^2(\langle n,m\rangle) = m$ (они вычислимы, так как можем перечислить $\mathbb{N}^2$ и найти единственную подходящую пару).

Рассмотрим $W : \mathbb{N}^2 \to \mathbb{N}$, такую что $\forall n \forall x \;\; W(n,x) \simeq U(\pi^1(n), \langle \pi^2(n), x\rangle)$ — вычислима как композиция вычислимых функций. Установим свойство главности для W.

Пусть $V : \mathbb{N}^2 \to \mathbb{N}$ — произвольная вычислимая функция, а $V' : \mathbb{N} \to \mathbb{N}$, такая что $V'(x) \simeq V(\pi^1(x), \pi^2(x))$ — тоже вычислима. Тогда $\exists\, m \in \mathbb{N} : \; U_m = V'$. Положим $s(n) := \langle m, n\rangle$ — вычислимая тотальная.

Далее,

$$\forall n \forall x \;\; W\big(s(n),\, x\big) \simeq W\big(\langle m,n\rangle,\, x\big) \simeq U\big(\pi^1(\langle m,n\rangle),\, \langle \pi^2(\langle m,n\rangle),\, x\rangle\big) \simeq U\big(m,\, \langle n,x\rangle\big) \simeq U_m\big(\langle n,x\rangle\big) \simeq$$

$$\simeq V'\big(\langle n,x\rangle\big) \simeq V\big(\pi^1(\langle n,x\rangle),\, \pi^2(\langle n,x\rangle)\big) \simeq V(n,x) \implies \forall n \in \mathbb{N} \;\; W_{s(n)} = V_n \implies W - \text{ГУВФ}$$

■

При этом УВФ, не являющаяся главной — «объект в некотором роде экзотический», хотя ее существование доказывается в билете 21.

2.15 Невозможность универсальной вычислимой тотальной функции. [?, 9.15], [ВШ-3, 2.2, т. 8]

Утверждение 2.15. *Не существует универсальной вычислимой тотальной функции W.*

Парадокс самоприменимости. Пусть $d : \mathbb{N} \to \mathbb{N}$ — диагональная функция $W : \;\; d(x) = W(x,x)$. Заметим, что d вычислима и тотальна из существования этих свойств у W. Введем также $g(x) = d(x)+1$, которая по тем же причинам вычислима и тотальна.

W универсальна, следовательно $\exists m \in \mathbb{N} : W_m = g \implies W(m,x) = g(x) \;\forall x \in \mathbb{N}$. Возьмем $x = m$ и тогда получим $W(m,m) = g(m) = d(m) + 1 = W(m,m) + 1 \implies 0 = 1$ — противоречие $\implies$ УВТФ не существует. ■

Заметим, что так же «доказать» несуществование УВФ U не получится, так как запись $U(m,m) \simeq U(m,m) + 1$ как раз имеет место, если на этих аргументах функция не определена.

2.16 Теорема Клини о неподвижной точке. [R, 36]

Теорема 2.16 (Клини о неподвижной точке)**.** *Пусть U — ГУВФ. Тогда для любой вычислимой тотальной $f : \mathbb{N} \to \mathbb{N}$ $\exists n \in \mathbb{N} : \; U_{f(n)} = U_n$.*

Неформально: в главном языке программирования U никакое алгоритмическое преобразование программ f не меняет смысл всех программ разом.

Доказательство. Рассмотрим $V : \mathbb{N}^2 \to \mathbb{N}$, такую что $\forall k \forall x \;\; V(k,x) \simeq U\big(U(k,k),\, x\big)$ — вычислима как композиция вычислимых, откуда из главности U существует вычислимая тотальная $s : \mathbb{N} \to \mathbb{N}$, такая что $U_{s(k)} = V_k = U_{U(k,k)} \;\forall k \in \mathbb{N}$.

Теперь берем произвольную f из формулировки теоремы. $f \circ s$ вычислима тотальна $\implies \exists t : U_t = f \circ s \implies U(t,t) = f(s(t))$, тогда $U_{s(t)} = U_{U(t,t)} = U_{f(s(t))}$. Тогда для f найдется $n = s(t)$, такое что $U_{f(n)} = U_n$. ■

«Более интуитивное» доказательство есть в учебнике Верещагина.

2.17 Индексные множества. Теорема Райса-Успенского: вывод из теоремы Клини. [R, 48] Пример применения.

Пусть $\mathcal{F}$ — семейство вычислимых функций одного аргумента. Назовем его индексным множеством относительно ГУВФ U множество $F = \{n \in \mathbb{N} \mid U_n \in \mathcal{F}\}$.

Теорема 2.17 (Райса-Успенского)**.** *Если семейство $\mathcal{F}$ вычислимых функций нетривиально (то есть $\varnothing \neq F \neq \mathbb{N}$), то его индексное множество F относительно любой ГУВФ неразрешимо.*

Неформально: множество программ, которые вычисляют функцию с каким-то нетривиальным свойством, неразрешимо. **Еще проще:** по номеру программы нельзя наперед узнать, обладает ли она нетривиальным свойством. Например, где-то определена или монотонно возрастает на своей области определения.

Доказательство (Есенина-Вольнина). Пусть $f \in \mathcal{F}$ и $g \notin \mathcal{F}$ вычислимы. Ввиду универсальности U $\exists n \exists m : \ f = U_n$ и $g = U_m$.

Предположим противное: пусть F разрешимо, тогда вычислима тотальная функция

$$h(k) = \begin{cases} m, & k \in F \\ n, & k \notin F \end{cases}.$$

В таком случае можно применить теорему Клини: $\exists\, t : \ U_t = U_{h(t)}$. Рассмотрим два случая:

- $t \in F \implies U_t = U_{h(t)} \in \mathcal{F} \implies h(t) = m \implies U_m = g \in \mathcal{F}$ — противоречие.
- $t \notin F \implies U_t = U_{h(t)} \notin \mathcal{F} \implies h(t) = n \implies U_n = f \notin \mathcal{F}$ — противоречие.

Следовательно, множество F неразрешимо. ■

2.18 Индексные множества. Теорема Райса-Успенского: доказательство с помощью сведения. [R, 47] Пример применения.

Все формулировки в предыдущем билете.

Доказательство (Райса). Пусть $\xi \notin \mathcal{F} \implies \exists f \in \mathcal{F} : \ f \neq \xi$. Рассмотрим любое перечислимое неразрешимое K и вычислимую $V(n, x) \simeq f(x) \cdot \omega_K(n)$. Из главности U следует существование вычислимой тотальной $s : \ U_{s(n)} = V_n$. Рассмотрим два случая:

- $n \in K \implies V_n = f \in \mathcal{F} \implies U_{s(n)} \in \mathcal{F} \implies s(n) \in F$
- $n \notin K \implies V_n = \xi \notin \mathcal{F} \implies U_{s(n)} \notin \mathcal{F} \implies s(n) \notin F$

Получили, что $n \in K \iff s(n) \in F \implies K \leqslant_m^s F$, причем K неразрешимо, поэтому неразрешимо и F (по свойствам m-сводимости, билет 12).

Пусть теперь $\xi \in \mathcal{F}$. Тогда просто применим такое же доказательство к множеству $\bar{F}$ и получим тот же результат. ■

2.19 Пример неперечислимого множества с неперечислимым дополнением. [R, 61 или 64]

Пусть U — ГУВФ. Докажем, что множество $Z = \{n \in \mathbb{N} \mid \operatorname{dom} U_n = 2\mathbb{N}\}$ и $\bar{Z}$ неперечислимы (задача 4с домашнего задания №3).

Пусть K — неразрешимое перечислимое множество, откуда $\bar{K}$ неперечислимо по теореме Поста (билет 2). Введем две функции:

$$V(n,x) \simeq \begin{cases} 1, & n \in K \cap x \vdots 2 \\ \text{не опр.}, & \text{иначе} \end{cases} \text{ — вычислима как } \omega_K(n) \text{ с дополнительной проверкой четности } x$$

$$\text{Тогда из главности } U \ \ \exists s: \ \forall n \in \mathbb{N} \ \ U_{s(n)} = V_n \implies$$

$$\implies \Big[\ n \in K \iff \operatorname{dom} V_n = 2\mathbb{N} \iff \operatorname{dom} U_{s(n)} = 2\mathbb{N} \iff s(n) \in Z \ \Big] \implies$$

$$\implies K \leqslant_m^s Z \implies \bar{K} \leqslant_m \bar{Z} \implies \bar{Z} \text{ неперечислимо по свойствам } m\text{-сводимости.}$$

$$V'(n,x) \simeq \begin{cases} 1, & n \in K \cup x \vdots 2 \\ \text{не опр.}, & \text{иначе} \end{cases}, \ \text{аналогично } \exists s': \ \forall n \in \mathbb{N} \ \ U_{s'(n)} = V'_n \implies$$

$$\implies \Big[\ n \in K \iff \operatorname{dom} V'_n \neq 2\mathbb{N} \iff \operatorname{dom} U_{s'(n)} \neq 2\mathbb{N} \iff s'(n) \notin Z \iff s'(n) \in \bar{Z} \ \Big] \implies$$

$$\implies K \leqslant_m^{s'} \bar{Z} \implies \bar{K} \leqslant_m Z \implies Z \text{ неперечислимо по свойствам } m\text{-сводимости.}$$

2.20 Пример непересекающихся перечислимых множеств, не отделимых никаким разрешимым множеством. [R, 34], [G, с. 21–22]

Пусть $A, B \subseteq \mathbb{N}$. Множество $C \subseteq \mathbb{N}$ отделяет A от B, если $A \subseteq C$ и $B \subseteq \bar{C}$.

Утверждение 2.18. *Существуют перечислимые множества A и B, не отделимые никаким разрешимым множеством.*

Доказательство. Зафиксируем УВФ U и ее диагональ d. Зададим вычислимую функцию

$$f(x) \simeq \begin{cases} 0, & x \in \operatorname{dom} d \ \wedge \ d(x) > 0 \\ 1, & x \in \operatorname{dom} d \ \wedge \ d(x) = 0 \\ \text{не опр.}, & x \notin \operatorname{dom} d \end{cases}.$$

Заметим, что у f не существует вычислимого тотального продолжения, так как $\Gamma_f \cap \Gamma_d = \varnothing$ (см. билет 9).

Положим $A = f^{-1}(1)$, $B = f^{-1}(0)$ — перечислимы как прообразы перечислимых множеств под действием вычислимой функции f (билет 3). Пусть также C разрешимо и отделяет A от B. Тогда $x \in A \implies \chi_C(x) = 1 = f(x)$, $\quad x \in B \implies \chi_C(x) = 0 = f(x)$, при этом $A \cup B = \operatorname{dom} f$, следовательно $\forall x \in \operatorname{dom} f \ \ f(x) = \chi_C(x) \implies \chi_C$ — тотальное продолжение $f \implies \chi_C$ невычислима $\implies C$ неразрешимо. ■

2.21 Существование неглавной у. в. ф. [R, 49]

Утверждение 2.19. *Существует **не**главная УВФ.*

Доказательство. Пусть U — ГУВФ, а множество $Z = \{n \in \mathbb{N} \mid U_n = \xi\}$. Тогда его дополнение

$$\bar{Z} = \{n \in \mathbb{N} \mid U_n \neq \xi\} = \{n \in \mathbb{N} \mid \exists x: \ U_n(x) \text{ определено}\} = \{n \in \mathbb{N} \mid \exists x \, \exists k: \ T(n,x,k)\}$$

перечислимо как проекция разрешимого T, откуда существует вычислимая $f : \mathbb{N} \to \mathbb{N}$, такая что $\operatorname{rng} f = \bar{Z}$ (эквивалентное определение перечислимости, см. билет 4). При этом Z неперечислимо, иначе по теореме Поста Z было бы разрешимым (билет 2), что невозможно по теореме Райса-Успенского (билет 17).

Зададим функцию двух аргументов

$$W(n,x) \simeq \begin{cases} \text{не опр.}, & n = 0 \\ U(f(n-1),x), & n \neq 0 \end{cases}.$$

W вычислима как композиция вычислимых функций, а также универсальна: если вычислимая g равна ξ, то ее номер в W — ноль, иначе $g = W_{f^{-1}(k)+1}$, где $g = U_k$. Получили $Z' = \{n \in \mathbb{N} \mid W_n = \xi\} = \{0\}$, то есть в языке программирования W у нигде не определенной функции есть только одна вычисляющая ее программа с номером 0. Z' — разрешимое индексное множество нетривиального семейства вычислимых функций, поэтому W — неглавная УВФ, иначе не выполняется теорема Райса-Успенского (билет 17). ■

2.22 Бесконечность множества неподвижных точек в смысле теоремы Клини. [R, 45]

Утверждение 2.20 (семинарская задача 3.7)**.** *Пусть U — ГУВФ и $f : \mathbb{N} \to \mathbb{N}$ вычислима. Тогда множество неподвижных точек $X = \{n \in \mathbb{N} \mid U_n = U_{f(n)}\}$ бесконечно.*

Доказательство. Предположим противное: пусть X конечно, а значит и разрешимо. Так как вычислимых функций бесконечно много, то найдется такая $g : \mathbb{N} \to \mathbb{N}$, что ее индексное множество $\{n \in \mathbb{N} \mid U_n = g\}$ не пересекается с X. Пусть $U_m = g$. Введем функцию

$$h(n) = \begin{cases} m, & n \in X \\ f(n), & n \notin X \end{cases}$$

Она вычислима и тотальна в силу этих свойств у f и χ_X. Тогда по теореме Клини $\exists n \in \mathbb{N} :\ U_n = U_{h(n)}$.

- $n \in X$: тогда $h(n) = m \neq n$, так как $m \notin X$. Получаем, что $U_n = U_m = g \implies n \notin X$ — противоречие.
- $n \notin X$: тогда $U_n = U_{f(n)} \implies n \in X$ — противоречие.

Получаем, что множество неподвижных точек для произвольных УВФ и ВФ бесконечно. ■

2.23 Вычислимость индекса композиции вычислимых функций. [R, 42] Совместная рекурсия: решение «систем уравнений». [R, 43]

Утверждение 2.21. *Если U — ГУВФ, то существует вычислимая тотальная c, такая что $\forall p, q \in \mathbb{N}\ \ U_{c(p,q)} = U_p \circ U_q$.*

Неформально: зная тексты программ p и q, можно автоматически сгенерировать программу, вычисляющую их композицию.

Доказательство. Достаточно ввести функцию $V(n,x) \simeq U\big(\pi^1(n), U\big(\pi^2(n), x\big)\big)$, вычислимую как композицию вычислимых. Ввиду главности U существует вычислимая тотальная $s :\ \forall n \in \mathbb{N}\ \ U_{s(n)} = V_n$. Зададим $c(x,y) := s(\langle x, y\rangle)$. Тогда имеем

$$\forall p \forall q \forall x\ \ U_{c(p,q)}(x) \simeq U_{s(\langle p,q\rangle)}(x) \simeq V_{\langle p,q\rangle}(x) \simeq U\big(\pi^1(\langle p,q\rangle), U\big(\pi^2(\langle p,q\rangle), x\big)\big) \simeq U\big(p, U(q,x)\big) \simeq \big(U_p \circ U_q\big)(x)$$

■

Теорема 2.22 (о совместной рекурсии)**.** *Пусть U — ГУВФ, а $V_1, V_2 : \mathbb{N}^3 \to \mathbb{N}$ вычислимы. Тогда*

$$\exists a,\, \exists b :\ \forall x \begin{cases} U(a,x) \simeq V_1(a,b,x) \\ U(b,x) \simeq V_2(a,b,x) \end{cases}$$

3 Вопросы по логике

3.1 Структуры и сигнатуры. Нормальные структуры. Изоморфизм структур. [MD]

Определение 10. Сигнатурой называется тройка множеств $\sigma = (\mathrm{Rel}, \mathrm{Func}, \mathrm{Const})$, где Rel — символы отношений (предикаты), Func — функциональные символы, Const — символы констант. Также мы считаем, что каждому $R \in \mathrm{Rel}$ приписано число $n \in \mathbb{N}$ — валентность символа (арность, местность). Используется как $R^{(n)}$. Эта запись означает, что символ отношения принимает n аргументов. Аналогично вводится валентность для функциональных символов.

Давайте теперь отдельно отметим, что у нас есть общее для всех сигнатур:

- алфавит переменных: счётное множество $\mathrm{Var} = \{v_0, v_1, v_2, \dots\}$. *Соглашение:* по умолчанию, разные буквы x, y, z и т.д. обозначают разные v_i.
- символы связок: $\wedge, \vee, \implies, \neg, \iff$
- кванторы: $\exists, \forall$
- скобки: (,)

И что теперь со всем этим делать?

Например в какой-нибудь сигнатуре $\sigma = (=^{(2)}; +^{(2)}; 2)$ мы можем записать выражение типа $2 + x = 2$. Но что такое 2? И что подставлять вместо x? Допустим, что в переменные подставляются элементы некого множества M. Но тогда нам надо уметь сложить 2 и элемент из M, а значит и сама 2 должна быть элементом этого множества, знак "+" надо понимать как функцию на множестве M, а "=" как отношение на нём. Но тогда надо вообще все константы понимать как элементы множества M, символы отношений как отношения на нём, а фукциональные символы как функции. Но какие? Ответом является **структура сигнатуры**.

Чтобы понять, как именно нам надо работать с нашей сигнатурой, нам надо придать смысл всем её элементам: символам констант, отношений и функций, ведь сами по себе смысла они не несут (кроме, разве что, валентности).

Придачей смысла сигнатуре занимается

Определение 11. Интепретация сигнатуры σ — это пара $\mathcal{M} = (M, I_{\mathcal{M}})$, где $M \neq$, а $I_{\mathcal{M}}$ — это такое отображение, что

1. $\forall R^{(n)} \in \mathrm{Rel}_\sigma \quad I_{\mathcal{M}}(R) \subseteq M^n$, то есть $I_{\mathcal{M}}(R)$ — это n-арное отношение на M;
2. $\forall f^{(m)} \in \mathrm{Func}_\sigma \quad I_{\mathcal{M}}(f) \colon M^m \to M$;
3. $\forall c \in \mathrm{Const}_\sigma \quad I_{\mathcal{M}}(c) \in M$.

Множество M называется *носителем интерпретации* $\mathcal{M}$.

К примеру такая структура, как поле вещественных чисел $\mathcal{R}$ является интерпретацией сигнатуры $(=^{(2)}; \cdot^{(2)}, +; 0, 1)$.

Также существует понятие *нормальной* структуры. Под ним понимается структура, в которой знак "=" ознаает именно равенство элементов в нашем обыденном понимании, то есть $\mathrm{id}_M = \{(a,a) \mid a \in M\}$

Теперь поговорим об уже знакомом нам понятии изоморфизма.

Определение 12. Будем говорить, что α — *изоморфизм* между $\mathcal{M}$ и $\mathcal{N}$, если

1. $\alpha\colon M \to N$ — биекция;
2. Сохраняются все отношения, то есть $\forall R^{(n)} \in \mathrm{Rel}_\sigma$, $\forall \vec{a} \in M^n$ $R^{\mathcal{M}}(\vec{a}) \iff R^{\mathcal{N}}(\alpha\vec{a})$;
3. "Уважаются" все функции, то есть $\forall f^{(n)} \in \mathrm{Func}_\sigma$, $\forall \vec{a} \in M^n$ $\alpha f^{\mathcal{M}}(\vec{a}) = f^{\mathcal{N}}(\alpha\vec{a})$;
4. $\forall c \in \mathrm{Const}_\sigma$, $\alpha c^{\mathcal{M}} = c^{\mathcal{N}}$;

Определение 13. Будем говорить, что структуры $\mathcal{M}$ и $\mathcal{N}$ изоморфны (обозн. $\mathcal{M} \cong \mathcal{N}$), если существует изоморфизм $\alpha\colon \mathcal{M} \to \mathcal{N}$.

Утверждение 3.1. *1.* $\mathcal{M} \overset{Id_{\mathcal{M}}}{\cong} \mathcal{M}$.

2. $\mathcal{M} \overset{\alpha}{\cong} \mathcal{N} \implies \mathcal{N} \overset{\alpha^{-1}}{\cong} \mathcal{M}$.

3. $\mathcal{M} \overset{\alpha}{\cong} \mathcal{N}$ *и* $\mathcal{N} \overset{\beta}{\cong} \mathcal{L} \implies \mathcal{M} \overset{\beta\circ\alpha}{\cong} \mathcal{L}$.

Пример. Рассмотрим конкретный пример, который является классическим. Положим $\mathcal{M} = \Big(\mathbb{R}; =; +^{(2)}; 0\Big)$ и $\mathcal{N} = \Big(R_+; =; \cdot^{(2)}; 1\Big)$. Естественно, это интерпретация одной сигнатуры $\sigma = \Big(=; \circ^{(2)}; e\Big)$.

3.2 Формулы первого порядка данной сигнатуры. Параметры (свободные переменные) формулы. Предложения. [F, с. 1–2]

Мы навводили всяких сигнатур и структур, но вопрос что нам с ними делать. Писать в них математические формулы, конечно! Но для начала разберёмся с термами, из которых строятся формулы.

Определение 14. Терм в сигнатуре σ. Tm_σ — множество термов в σ

- $x \in \mathrm{Var} \implies x \in \mathrm{Tm}_\sigma$
- $c \in \mathrm{Const} \implies c \in \mathrm{Tm}_\sigma$
- $f^{(m)} \in \mathrm{Func}_\sigma, t_1, \ldots, t_m \in \mathrm{Tm}_\sigma \implies ft_1 \ldots f_m \in \mathrm{Tm}_\sigma$. (Тут мы воспользовались префиксной польской записью).

Пример. **Термы в арифметике**

2 — терм, x — терм, значит $(2 + x)$ — терм, значит $(2 + x) + +$ — терм.

3 — терм, z — терм, значит $(3 \cdot z)$ — терм, значит $(y + (3 \cdot z))$ — терм.

Термы готовы, определим формулы.

Определение 15. Формулы в сигнатуре σ Fm_σ — множество формул.

- $R^{(n)} \in \mathrm{Rel}, t_1, \ldots, t_n \in \mathrm{Tm} \implies \in \mathrm{Fm}$
- $\varphi, \psi \in \mathrm{Fm} \implies (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \implies \psi), (\varphi \iff \psi), \neg\varphi \in \mathrm{Fm}$
- $x \in \mathrm{Var}, \varphi \in \mathrm{Fm} \implies \exists x\varphi, \forall x\varphi \in \mathrm{Fm}$

Пример. **Формулы в арифметике**

$(2 + x) + +$ — терм, $(y + 3 \cdot z)$ — терм, а значит $(2 + x) + + < y + 3 \cdot z$ — формула. А значит $\neg((2 + x) + + < y + 3 \cdot z)$ — формула, а значит $\forall w\neg((2 + x) + + < y + 3 \cdot z)$ — формула, а значит $\forall w\neg((2 + x) + + < y + 3 \cdot z) \implies (x + 3)$ — формула, т.к. $(x + 3)$ — терм, и так далее.

В данном случае мы получили формулы первого порядка, по той причине что мы оперируем лишь конкретными элементами. Если бы мы работали с подмножествами, то это были бы уже формулы второго порядка, чем мы тут пока не занимаемся.

Определение 16 (свободная переменная)**.** Зафиксируем функцию $\mathrm{FV}\colon \mathrm{Fm}_\sigma \to \mathrm{Var}$, которая каждой формуле ставит в соответствие множество *свободных* переменных в ней, следующим образом:

1. $\mathrm{FV}(Rt_1 \dots t_n) = V(t_1) \cup \dots \cup V(t_n)$.
2. $\mathrm{FV}(\varphi \wedge \psi) = \mathrm{FV}(\varphi \vee \psi) = \dots = \mathrm{FV}(\varphi) \cup \mathrm{FV}(\psi)$.
3. $\mathrm{FV}(\forall x\ \varphi) = \mathrm{FV}(\exists x\ \varphi) = \mathrm{FV}(\varphi) \setminus \{x\}$.

Человеческим языком: под свободной переменной (или параметром) формулы понимается та переменная(ые), не связанные квантором. Важно понимать, что в одну и ту же формулу x может иметь как свободное вхождение, так и связанное, например

$$x = 3 \quad \vee \quad \exists x\ x + 2 = 1.$$

Здесь первый x имеет свободное вхождение, а второй x — связанное. Получается, что хоть обозначение и одно, вхождения разные, ведь в первом случае что-то говорится про конкретный объект x, конкретное число, а во втором случае что-то говорится про всю область наших чисел (что среди них имеется решение нашего уравнения). То есть это, по сути дела, разные x, и их возможное совпадение может считаться случайным.

Определение 17. Предложением называется формула, которая не содержит свободных переменных.

3.3 Оценка переменных. Значение терма и формулы в данной структуре при данной оценке. [F, с. 2–3] Независимость значения формулы от значений переменных, не являющихся ее параметрами. [F, 5]

Напоминание: Переменные – это какие-то символы (различимые) $Var = \{v_0, v_1, \dots, v_n, \dots\} \sim \mathbb{N}$ (то есть, их счётно много).

Определение 18 (Оценка переменных)**.** Оценка переменных в интерпретации $\mathcal{M}$ – это любая функция $\pi : Var \to M$.

Пример. Всем переменным с чётными номерами поставим в соответствие 5, а всем переменным с нечётными – их номер. Получится оценка переменных в любой интерпретации, где носителем выступают натуральные числа.

Обозначения: Значение терма $t \in Tm_\sigma$ в интерпретации $\mathcal{M}$ при оценке π : $[t]_\mathcal{M}(\pi) \in M$ (иногда $\mathcal{M}$ можно опускать, если и так понятно, какая интерпретация).

Определение 19 (Значение терма $t \in Tm_\sigma$ в интерпретации $\mathcal{M}$ при оценке π)**.**
Индукция по построению:

(1) $t = x \in Var \Rightarrow [x]_\mathcal{M}(\pi) = \pi(x)$

(2) $c \in Const \Rightarrow [c]_\mathcal{M}(\pi) = c^\mathcal{M}$ (константе в интерпретации уже приписано некое значение)

(3) $[ft_1 \dots t_m]_\mathcal{M}(\pi) = f^\mathcal{M}([t_1]_\mathcal{M}(\pi), \dots, [t_m]_\mathcal{M}(\pi))$

Пример. Вернёмся к нашей интерпретации $\mathcal{N}$ из предыдущих билетов.

$[f(\#x)x]_\mathcal{N}(\pi) = f^\mathcal{N}([\#x]_\mathcal{N}(\pi), [x]_\mathcal{N}(\pi)) = f^\mathcal{N}(\#^\mathcal{N}([x]_\mathcal{N}(\pi)), [x]_\mathcal{N}(\pi)) = f^\mathcal{N}(\#^\mathcal{N}(\pi(x)), \pi(x))$

Допустим наша оценка оценила x числом 9 ($\pi(x) = 9$). Тогда $[f(\#x)x]_\mathcal{N}(\pi) = ((9+7)\cdot 9)^2 = (16 \cdot 9)^2 \in \mathbb{N}$

Лемма 3.2. Если $\forall x \in V(t) \pi_1(x) = \pi_2(x)$, то $[t]_\mathcal{M}(\pi_1) = [t]_\mathcal{M}(\pi_2)$.
Доказательство в билете не просят, но доказывается индукцией по построению.

Обозначения: Значение формулы $\varphi \in Fm_\sigma$ в интерпретации $\mathcal{M}$ при оценке π : $[\varphi]_\mathcal{M}(\pi) \in \{0, 1\}$ (ложь/истина)

Определение 20 (Модифицированная оценка)**.**
Пусть $\pi : Var \to M$
Пусть $y \in Var$ и $m \in M$
$(\pi + (y \mapsto m)) : Var \to M$ (альтернативное обозначение: π_y^m) называется модифицированной оценкой

$$\pi_y^m(x) = \begin{cases} m, x = y (\text{x то же самое, что и y, алфавитно}) \\ \pi(x), x \neq y \end{cases}$$

Определение 21 (Значение формулы $\varphi \in Fm_\sigma$ в интерпретации $\mathcal{M}$ при оценке π)**.**
Индукция по построению:

(1) (атомарная формула) $[Rt_1, \ldots, [t_n]_{\mathcal{M}}(\pi) = \begin{cases} 1, ([t_1]_{\mathcal{M}}(\pi), \ldots, [t_n]_{\mathcal{M}}(\pi) \in R^{\mathcal{M}} \\ 0, \text{ иначе} \end{cases}$

(2) (логические связки) $[\varphi \wedge \psi]_{\mathcal{M}}(\pi) = \text{И}([\varphi]_{\mathcal{M}}(\pi), [\psi]_{\mathcal{M}}(\pi))$. Аналогично для ИЛИ, СЛЕДОВАНИЯ, ЭКВИВАЛЕНТНОСТИ и НЕ

(3) $[\forall x \varphi](\pi) = \begin{cases} 1, \text{для всех } m \in M [\varphi](\pi_x^m) = 1 \\ 0, \text{иначе} \end{cases}$

$[\exists x \varphi](\pi) = \begin{cases} 1, \text{существует } m \in M [\varphi](\pi_x^m) = 1 \\ 0, \text{иначе} \end{cases}$

Пример. Вернёмся к нашей интерпретации $\mathcal{N}$ из предыдущих билетов.

$\varphi = \exists x \forall y Q x y y$ (это замкнутая формула – в ней нет свободных переменных)

$[\exists x \forall y Q x y y](\pi) = 1 \Leftrightarrow \exists a \in \mathbb{N} [\forall y Q x y y](\pi_x^a) = 1 \Leftrightarrow \exists a \in \mathbb{N}, \forall b \in \mathbb{N} [Q x y y](\pi_{xy}^{ab}) \Leftrightarrow [x](\pi_{xy}^{ab}) + [y](\pi_{xy}^{ab}) = [y](\pi_{xy}^{ab}) \Leftrightarrow$

$\pi_x^a(x) + \pi_y^b(y) = \pi_y^b(y)$ (этот шаг по лемме) $\Leftrightarrow a + b = b$

В нашей интерпретации значение формулы действительно истина (a возьмём нулём)

Лемма 3.3. Если $\forall y \in FV(\varphi) \pi_1(y) = \pi_2(y)$, то $[\varphi]_{\mathcal{M}}(\pi_1) = [\varphi]_{\mathcal{M}}(\pi_2)$

Доказательство. Индукция по построению:

(1) $\varphi = Rt_1, \ldots, t_n$
$FV(Rt_1, \ldots, t_n) = V(t_1) \cup \ldots \cup V(t_n) \Rightarrow V(t_i) \subseteq FV(Rt_1, \ldots, t_n)$
$[\varphi](\pi_1) = 1 \Leftrightarrow R^m([t_1](\pi_1), \ldots, [t_n](\pi_1))$
$\Leftrightarrow$ (по лемме выше) $R^m([t_1](\pi_2), \ldots, [t_n](\pi_2)) \Leftrightarrow [\varphi](\pi_2) = 1$

(2) $FV(\varphi \wedge \psi) = FV(\varphi) \cup FV(\psi)$
$[\varphi \wedge \psi](\pi_1) = \text{И}([\varphi](\pi_1), [\psi](\pi_1))$ (по предположению индукции) $= \text{И}([\varphi](\pi_2), [\psi](\pi_2)) = [\varphi \wedge \psi](\pi_2)$

(3) $FV(\forall z \psi) = FV(\forall z) \backslash \{z\}$
$\varphi = \forall z \psi \Rightarrow FV(\psi) = FV(\varphi) \cup \{z\}$

Утверждение: $\forall y \in FV(\psi) \Rightarrow \pi_{1z}^m(y) = \pi_{2z}^m(y)$

Доказательство.

1. $y \in FV(\varphi)$, тогда y точно отличен от z. Значит, $\pi_{1z}^m(y) = \pi_1(y) = \pi_2(y) = \pi_{2z}^m(y)$
2. y совпадает с z, тогда $\pi_{1z}^m(y) = m = \pi_{2z}^m(y)$

■

$\Rightarrow$ (по предположению индукции) $[\psi](\pi_{1z}^m(y)) = [\psi](\pi_{2z}^m(y))$

$[\forall z \psi](\pi_1) = 1 \Leftrightarrow \forall m \in M [\psi](\pi_{1z}^m) = 1 \Leftrightarrow \forall m \in M [\psi](\pi_{2z}^m) = 1 \Leftrightarrow [\forall z \psi](\pi_1) = 1$

■

3.4 Значение терма и формулы на наборе элементов структуры. Выразимые в структуре множества (отношения, функции, элементы). Примеры выразимых множеств. [MD] [F, с. 4]

Утверждение 3.4 (значение формулы на наборе элементов структуры). *Зафиксируем* $(x_1, x_2, ..., x_n) \in Var^n$, $x_1, ..., x_n$ *попарно различны. Если* $FV(\varphi) \subseteq \{x_1, ..., x_n\}$, *то в качестве упрощённой записи будем писать* $\varphi(x_1, ..., x_n)$. *Пусть* $\overrightarrow{a} = (a_1, ..., a_n) \in M^n$, *тогда*

$$\forall \varphi(x_1, ..., x_n)\ \forall \overrightarrow{a}\ \forall \pi\ \mathcal{M} \vDash \varphi(\overrightarrow{a}) \Leftrightarrow [\varphi]_{\mathcal{M}}(\pi^{a_1\ a_2\ \dots\ a_n}_{x_1\ x_2\ \dots\ x_n}) = 1$$

Определение 22. Формула $\varphi(x_1, ..., x_n) \in Fm_\sigma$ выражает отношение $X \subseteq M^n$ в интерпретации $\mathcal{M}$ сигнатуры $\sigma \Leftrightarrow \forall \overrightarrow{a} \in M^n\ (\mathcal{M} \vDash \varphi(\overrightarrow{a}) \Leftrightarrow \overrightarrow{a} \in X)$. (Тогда пишут ещё $\varphi^{\mathcal{M}} = X$).

Примеры выразимых множеств:

1) Пусть есть $\mathcal{M} = (\mathbb{N}; =^{(2)}; +^{(2)})$. В $\mathcal{M}$ выразимы ($\Leftrightarrow \exists \varphi$, которая выражает) $\{0\} \subseteq \mathbb{N}'$; ЧЁТНОЕ $\subseteq \mathbb{N}; \leqslant, < \subseteq \mathbb{N}^2$

   - $\varphi_0(x) \rightleftharpoons \forall y\ (x + y = y)$
     $\mathcal{M} \vDash \varphi_0(a) \Leftrightarrow a = 0 \Leftrightarrow a \in \{0\}$
   - $\varphi_{\text{чётн.}}(x) \rightleftharpoons \forall y\ (x = y + y)$
     $\mathcal{M} \vDash \varphi_{\text{чётн.}}(a) \Leftrightarrow a$ чётно $\Leftrightarrow a \in$ ЧЁТНОЕ
   - $\varphi_{\leqslant}(x, y) \rightleftharpoons \forall z\ (x + z = y)$
     $\forall (a, b) \in \mathbb{N}^2\ \mathcal{M} \vDash \varphi_{\leqslant}(a, b) \Leftrightarrow a \leqslant b$
   - $\varphi_{<}(x, y) \rightleftharpoons \varphi_{\leqslant}(x, y) \wedge \neg(x = y)$

2) В поле $\mathcal{R}$ выразимо отношение $\mathbb{R}_{\geqslant 0}$

   - $\varphi_{\geqslant 0}(x) = \exists y\ (y \cdot y = x)$
     $\forall a \in \mathbb{R}\ \mathcal{R} \vDash \varphi_{\geqslant 0}(a) \Leftrightarrow a \geqslant 0 \Leftrightarrow a \in \mathbb{R}_{\geqslant 0}$

3.5 Значение формулы при изоморфизме структур. Элементарная эквивалентность структур. Изоморфные структуры элементарно эквивалентны. [MD, 10.5]

Теорема (о значении формулы при изоморфизме).

Пусть M, N – какие-то интерпретации *одной* сигнатуры σ; $\varphi(x_1, \dots, x_n) \in Fm_\sigma$.

Тогда если $M \overset{\alpha}{\cong} N$, то $\forall \overrightarrow{a} \in M^n$ верно $M \vDash \varphi(\overrightarrow{a}) \iff N \vDash \varphi(\alpha \overrightarrow{a})$.

Лемма. Пусть $t(x_1, \dots x_n) \in Tm_\sigma$. Если $M \overset{\alpha}{\cong} N$, то $\forall \overrightarrow{a} \in M^n\ \ \alpha(t^M(\overrightarrow{a})) = t^N(\alpha \overrightarrow{a})$.

Доказательство. Индукция по построению терма.

$$(I)\ t = x_i \implies \begin{cases} t^M(a_1, \dots, a_n) = a_i \\ t^N(b_1, \dots, b_n) = b_i \end{cases} \implies \begin{cases} \alpha(t^M(\overrightarrow{a})) = \alpha\, a_i; \\ t^N(\alpha\, \overrightarrow{a}) = t^N(\alpha\, a_1, \dots, \alpha\, a_n) = a_i. \end{cases}$$

Как видим, получили одинаковое значение.

$(II)\ t = c \implies \begin{cases} t^M(a_1, \dots a_n) = c^M; \\ t^N(b_1, \dots b_n) = c^N. \end{cases}$

$\forall \pi\ [c]_M(\pi) = c^M \implies \alpha(t^M(\vec{a})) = \alpha\, c^M = c^N = t^N(\alpha\, \vec{a})$ из определения изоморфизма.

$(III)\ t = f\, t_1 \dots t_m \implies t^M(\vec{a}) = f^M\left(t_1^M(\vec{a}), \dots, t_m^M(\vec{a})\right) \implies \alpha\left(t^M(\vec{a})\right) = \alpha\left(f^M\left(t_1^M(\vec{a}), \dots, t_m^M(\vec{a})\right)\right).$

По определению изоморфизма, $\cdots = f^N\left(\alpha\left(t_1^M(\vec{a})\right), \dots, \alpha\left(t_m^M(\vec{a})\right)\right).$

Внутри уже более простые термы, для них воспользуемся предположением индукции:

$\cdots = f^N\left(t_1^N(\alpha\, \vec{a}), \dots, t_m^N(\alpha\, \vec{a})\right) = t^N(\alpha\, \vec{a}).$

■

Доказательство. (Теоремы о значении формулы)

Индукция по построению φ.

$(I)\ \varphi = R\, t_1 \dots t_m.$

По лемме, $t_i^N\,(\alpha\, \vec{a}) = \alpha\,(t_i^M\,(\vec{a}))$

$\begin{cases} M \vDash \varphi(\vec{a}) \iff \left(t_1^M(\vec{a}), \dots, t_m^M(\vec{a})\right) \in R^M; \circledast \\ N \vDash \varphi(\alpha\, \vec{a}) \iff \left(t_1^N(\alpha\, \vec{a}), \dots, t_m^N(\alpha\, \vec{a})\right) \in R^N \iff \left(\alpha\,(t_1^M\,(\vec{a})), \dots, \alpha\,(t_m^M\,(\vec{a}))\right) \in R^N \iff \circledast \text{ по определению.} \end{cases}$

(II) Булевы связки. Приведём док-во для конъюнкции и отрицания.

$\varphi = (\Theta \wedge \psi)(\vec{a}) \iff M \vDash \Theta(\vec{a})$ и $M \vDash \psi(\vec{a}) \iff$ (по пред. инд.) $N \vDash \Theta(\alpha\, \vec{a})$ и $N \vDash \psi(\alpha\, \vec{a}) \iff N \vDash (\Theta \wedge \psi)(\alpha\, \vec{a}).$

$M \vDash (\neg\psi)(\vec{a}) \iff M \nvDash \psi(\vec{a}) \iff N \nvDash \psi(\alpha\, \vec{a}) \iff N \vDash (\neg\psi)(\alpha\, \vec{a}).$

(III) Кванторы.

Пусть $\varphi = \exists\, x\ \psi.$

$M \vDash (\exists\, x\ \psi)(\vec{a}) \iff$ сущ. $b \in M$, т.ч. $M \vDash \psi(\vec{a}, b) \iff$ (по предположению индукции) $N \vDash \psi(\alpha\, \vec{a}, \alpha\, b).$

$N \vDash (\exists\, x\ \psi)(\alpha\, \vec{a}) \iff$ сущ. $c \in N$, т.ч. $N \vDash \psi(\alpha\, \vec{a}, c).$

В силу биективности α, существование таких $b \in M$ и $c \in N$ равнозначны ($\forall\, c \in N\ \exists\, b \in M\ \ c = \alpha\, b$). Ч.т.д.

Теперь пусть $\varphi = \forall\, x\ \psi.$

$M \vDash (\forall\, x\ \psi)(\vec{a}) \iff$ для всех $b \in M$ верно $M \vDash \psi(\vec{a}, b) \iff$ (по предположению индукции) $N \vDash \psi(\alpha\, \vec{a}, \alpha\, b).$

$N \vDash (\forall\, x\ \psi)(\alpha\, \vec{a}) \iff$ для всех $c \in N$ верно $N \vDash \psi(\alpha\, \vec{a}, c).$

В силу биективности α утверждения выше равнозначны ($\forall\, c \in N$ имеет вид $\alpha\, b$ для всех $b \in M$). Ч.т.д.

■

St_σ – *множество предложений.*

Пусть M, N – какие-то интерпретации *одной* сигнатуры σ.

N и M называются элементарно эквивалентными, если $\forall \varphi \in St_\sigma$ верно $M \vDash \varphi \iff N \vDash \varphi$. Обозначение – $M \equiv N$.

Иначе говоря, две интерпретации неразличимы ни одним предложением в St_σ.

Утверждение. $N \cong M \implies M \equiv N$.

Доказательство. Пусть $\varphi \in St_\sigma$.

Известно, что $M \vDash \varphi(\vec{a}) \iff N \vDash \varphi(\alpha\,\vec{a})\ \ \forall \vec{a}$ (теорема о значении формулы при изоморфизме).

Пусть $\vec{a}$ – пустой набор. Тогда, так как φ не имеет свободных переменных,

$$M \vDash \varphi \iff M \vDash \varphi(\vec{a}) \iff N \vDash \varphi(\alpha\,\vec{a}) \iff M \vDash \varphi$$

ведь $\alpha\,\vec{a}$ – пустой набор, если $\vec{a}$ – пустой набор.

■

3.6 Значение формулы при изоморфизме структур. Сохранение выразимых множеств автоморфизмами структуры. Примеры невыразимых множеств. [MD, 10.5]

Теорема о значении формулы при изоморфизме структур точно такая же, что и в предыдущем билете (см. формулировки билетов).
Теорема (о значении формулы при изоморфизме).

Пусть M, N – какие-то интерпретации *одной* сигнатуры σ; $\varphi(x_1, \ldots, x_n) \in Fm_\sigma$.

Тогда если $M \overset{\alpha}{\cong} N$, то $\forall \vec{a} \in M^n$ верно $M \vDash \varphi(\vec{a}) \iff N \vDash \varphi(\alpha\,\vec{a})$.

Лемма. Пусть $t(x_1, \ldots x_n) \in Tm_\sigma$. Если $M \overset{\alpha}{\cong} N$, то $\forall \vec{a} \in M^n\ \ \alpha(t^M(\vec{a})) = t^N(\alpha\,\vec{a})$.

Доказательство. Индукция по построению терма.

$$(I)\ t = x_i \implies \begin{cases} t^M(a_1, \ldots, a_n) = a_i \\ t^N(b_1, \ldots, b_n) = b_i \end{cases} \implies \begin{cases} \alpha(t^M(\vec{a})) = \alpha\, a_i; \\ t^N(\alpha\,\vec{a}) = t^N(\alpha\, a_1, \ldots, \alpha\, a_n) = a_i. \end{cases}$$

Как видим, получили одинаковое значение.

$$(II)\ t = c \implies \begin{cases} t^M(a_1, \ldots a_n) = c^M; \\ t^N(b_1, \ldots b_n) = c^N. \end{cases}$$

$\forall \pi\ [c]_M(\pi) = c^M \implies \alpha(t^M(\vec{a})) = \alpha\, c^M = c^N = t^N(\alpha\,\vec{a})$ из определения изоморфизма.

$$(III)\ t = f\, t_1 \ldots t_m \implies t^M(\vec{a}) = f^M\left(t_1^M(\vec{a}), \ldots, t_m^M(\vec{a})\right) \implies \alpha\left(t^M(\vec{a})\right) = \alpha\left(f^M\left(t_1^M(\vec{a}), \ldots, t_m^M(\vec{a})\right)\right).$$

По определению изоморфизма, $\cdots = f^N\left(\alpha\left(t_1^M(\overrightarrow{a})\right),\ldots,\alpha\left(t_m^M(\overrightarrow{a})\right)\right)$.

Внутри уже более простые термы, для них воспользуемся предположением индукции:

$\cdots = f^N\left(t_1^N(\alpha\,\overrightarrow{a}),\ldots,t_m^N(\alpha\,\overrightarrow{a})\right) = t^N(\alpha\,\overrightarrow{a})$.

■

Доказательство. (Теоремы о значении формулы)

Индукция по построению φ.

(I) $\varphi = R\,t_1\ldots t_m$.

По лемме, $t_i^N\,(\alpha\,\overrightarrow{a}) = \alpha\,(t_i^M\,(\overrightarrow{a}))$

$\begin{cases} M \vDash \varphi(\overrightarrow{a}) \iff \left(t_1^M(\overrightarrow{a}),\ldots,\,t_m^M(\overrightarrow{a})\right) \in R^M;\ \circledast \\ N \vDash \varphi(\alpha\,\overrightarrow{a}) \iff \left(t_1^N(\alpha\,\overrightarrow{a}),\ldots,\,t_m^N(\alpha\,\overrightarrow{a})\right) \in R^N \iff \left(\alpha\,(t_1^M\,(\overrightarrow{a})),\ldots,\,\alpha\,(t_m^M\,(\overrightarrow{a}))\right) \in R^N \iff \circledast \text{ по определению.} \end{cases}$

(II) Булевы связки. Приведём док-во для конъюнкции и отрицания.

$\varphi = (\Theta \wedge \psi)(\overrightarrow{a}) \iff M \vDash \Theta(\overrightarrow{a})$ и $M \vDash \psi(\overrightarrow{a}) \iff$ (по пред. инд.) $N \vDash \Theta(\alpha\,\overrightarrow{a})$ и $N \vDash \psi(\alpha\,\overrightarrow{a}) \iff N \vDash (\Theta \wedge \psi)(\alpha\,\overrightarrow{a})$.

$M \vDash (\neg\psi)(\overrightarrow{a}) \iff M \nvDash \psi(\overrightarrow{a}) \iff N \nvDash \psi(\alpha\,\overrightarrow{a}) \iff N \vDash (\neg\psi)(\alpha\,\overrightarrow{a})$.

(III) Кванторы.

Пусть $\varphi = \exists\, x\ \psi$.

$M \vDash (\exists\, x\ \psi)(\overrightarrow{a}) \iff$ сущ. $b \in M$, т.ч. $M \vDash \psi(\overrightarrow{a}, b) \iff$ (по предположению индукции) $N \vDash \psi(\alpha\,\overrightarrow{a},\,\alpha\,b)$.

$N \vDash (\exists\, x\ \psi)(\alpha\,\overrightarrow{a}) \iff$ сущ. $c \in N$, т.ч. $N \vDash \psi(\alpha\,\overrightarrow{a}, c)$.

В силу биективности α, существование таких $b \in M$ и $c \in N$ равнозначны $(\forall\, c \in N\ \exists\, b \in M\ \ c = \alpha\, b)$. Ч.т.д.

Теперь пусть $\varphi = \forall\, x\ \psi$.

$M \vDash (\forall\, x\ \psi)(\overrightarrow{a}) \iff$ для всех $b \in M$ верно $M \vDash \psi(\overrightarrow{a}, b) \iff$ (по предположению индукции) $N \vDash \psi(\alpha\,\overrightarrow{a},\,\alpha\,b)$.

$N \vDash (\forall\, x\ \psi)(\alpha\,\overrightarrow{a}) \iff$ для всех $c \in N$ верно $N \vDash \psi(\alpha\,\overrightarrow{a}, c)$.

В силу биективности α утверждения выше равнозначны ($\forall\, c \in N$ имеет вид $\alpha\, b$ для всех $b \in M$). Ч.т.д.

■

Теорема 3.5 (Выразимые отношения сохраняются всеми автоморфизмами структуры)**.** *Если X выразимо в $\mathcal{M}$, то $\forall\overrightarrow{a} \in M^n\ \ \overrightarrow{a} \in X \Leftrightarrow \alpha\overrightarrow{a} \in X$.*

Доказательство. X выразимо $\implies$ по определению $\exists\varphi(x_1,...,x_n)\ \forall\overrightarrow{a} \in M^n\ \ \overrightarrow{a} \in X \Leftrightarrow \mathcal{M} \vDash \varphi(\overrightarrow{a})$

$\mathcal{M} \overset{\alpha}{\cong} \mathcal{M} \implies \overrightarrow{a} \in X \Leftrightarrow \mathcal{M} \vDash \varphi(\overrightarrow{a}) \Leftrightarrow$ [по теореме о значении формулы при изоморфизме] $\Leftrightarrow \mathcal{M} \vDash \varphi(\alpha\overrightarrow{a}) \Leftrightarrow \alpha\overrightarrow{a} \in X$.
■ ■

Утверждение 3.6. *Пусть $\mathcal{M} = (\mathbb{Z}; <); \mathcal{M} \overset{\alpha}{\cong} \mathcal{M}; \alpha(x) = x + 1$. Тогда множество $\mathbb{Z}_+ = \{n \in \mathbb{Z} \mid n > 0\}$ не выразимо в $\mathcal{M}$.*

Доказательство. $\alpha \in Aut(\mathcal{M})$
$0 \notin \mathbb{Z}_+$, но $\alpha(0) = 1 \in \mathbb{Z}_+$, таким образом $\exists a \in \mathbb{Z} : \ a \in \mathbb{Z}_+ \not\Leftrightarrow \alpha a \in \mathbb{Z}_+$.
Значит $\mathbb{Z}_+$ не выразимо в $\mathcal{M}$. ■

3.7 Общезначимые и выполнимые формулы. [F, 12] Эквивалентность формул первого порядка. [F, с. 4] Лемма о фиктивном кванторе. [F, 10] Квантор всеобщности и общезначимость. [F, 12]

3.7.1 Общезначимые и выполнимые формулы.

Пусть фиксирована сигнатура σ.

Определение 23. Формула φ *общезначима*, если для любой интерпретации $\mathcal{M}$, для любой оценки переменных π в этой самой интерпретации: $\mathrm{Var} \to M$

$$[\varphi]_{\mathcal{M}}(\pi) = 1.$$

(Как ее ни интерпретируй, что с ней ни делай, будет принимать значение 1, которое всегда истинно.)

Пример.

$$\psi = Px \implies (\neg Px \implies Qyz)$$

Если Px ложь, то ψ истинна, иначе получаем ψ: $1 \implies (0 \implies *)$ — тоже истина (запись варварская, ну и что?) $\implies \psi$ общезначима.

Пример. Рассмотрим формулу

$$\varphi = Px \vee \neg Qy.$$

Положим $M = \mathbb{N}$, $P^{\mathcal{M}} = Q^{\mathcal{M}} =$ "равно 0", $\pi(x) = 2020$, $\pi(y) = 0$. Тогда значение φ ложно $\implies \varphi$ не общезначима.

Определение 24. Формула φ *выполнима*, если существует интерпретация $\mathcal{M}$ и оценка π такая, что

$$[\varphi]_{\mathcal{M}}(\pi) = 1.$$

Общезначимая формула истинна всегда, выполнимая истинна в каком-то случае.

Пример. Рассмотрим формулу

$$\varphi = (x - 3 > 1)$$

При $M = \mathbb{N}$ и π такой, что $\pi(x) = 5$

$$[\varphi]_{\mathcal{M}}(\pi) = 1$$

$\implies \varphi$ выполнима.

Лемма 3.7. Формула φ общезначима $\iff \neg\varphi$ не выполнима.

Лемма 3.8. Формула φ выполнима $\iff \neg\varphi$ не общезначима.

3.7.2 Эквивалентность формул первого порядка.

Формулы первого порядка — формулы, в которых кванторы берутся только по элементам носителя.

Пример. первый порядок: $\forall x \in M$, не первый порядок: $\forall y \subseteq M$

Определение 25. Формулы φ и ψ (логически) эквивалентны, если для любой интерпретации $\mathcal{M}$, для любой оценки π

$$[\varphi]_{\mathcal{M}}(\pi) = [\psi]_{\mathcal{M}}(\pi).$$

Лемма 3.9. Определенная выше эквивалентность является отношением эквивалентности:

1. $\varphi \equiv \varphi$;

2. $\varphi \equiv \psi \implies \psi \equiv \varphi$;

3. $\varphi \equiv \psi \wedge \psi \equiv \theta \implies \psi \equiv \theta$.

Лемма 3.10 (О конгруэнции отношения эквивалентности)**.** Если $\varphi \equiv \varphi'$, то

- $\neg\varphi \equiv \neg\varphi'$;
- $\varphi \wedge \psi \equiv \varphi' \wedge \psi$.
- $\varphi \vee \psi \equiv \varphi' \vee \psi$.
- $\varphi \implies \psi \equiv \varphi' \implies \psi$.
- $\psi \implies \varphi \equiv \psi \implies \varphi'$.
- $\forall x\varphi \equiv \forall x\varphi'$.
- $\exists x\varphi \equiv \exists x\varphi'$.

Так как значение сложной формулы определяется через значения ее подформул и для любой интерпретации $\mathcal{M}$, для любой оценки π значение φ можно заменить на значение φ'.

Доказательство. Докажем одно из утверждений.

$[\forall x\varphi]_{\mathcal{M}}(\pi) = 1 \iff \forall m \in M\ [\varphi]\,(\pi_x^m) = 1$, но $[\varphi]\,(\pi_x^m) = [\varphi']\,(\pi_x^m)$, тогда $[\varphi']\,(\pi_x^m) = 1$. ■

Лемма 3.11. $\varphi \equiv \psi \iff$ общезначима формула

$$(\varphi \implies \psi) \wedge (\psi \implies \varphi).$$

Импликация истинна $\iff$ значение посылки не больше значения заключения, а в лемме сказано, что они одинаковы.

Лемма 3.12. Формула φ общезначима тогда и только тогда, когда

$\varphi \equiv \top$ ("заведомая истина").

Следствие. Все общезначимые формулы эквивалентны друг другу.

3.7.3 Лемма о фиктивном кванторе.

Лемма 3.13 (О фиктивном кванторе.)**.** Если $x \notin \mathrm{FV}(\varphi)$, то $\forall x\varphi \equiv \varphi$. Аналогично, $\exists\varphi \equiv \varphi$.

Доказательство. Рассмотрим произвольную интерпретацию $\mathcal{M}$ и оценку π. По определению:

$$[\forall x\varphi]_{\mathcal{M}}(\pi) = 1 \iff \forall m \in M\ [\varphi](\pi_x^m) = 1.$$

где

$$\pi_x^m(z) = \begin{cases} m, & y = x, \\ \pi(y), & y \neq x. \end{cases}$$

Вспомним лемму о том, что $\forall z \in \mathrm{FV}(\psi)\colon \pi_1(z) = \pi_2(z)$, то $[\psi]_{\mathcal{M}}(\pi_1) = [\psi]_{\mathcal{M}}(\pi_2)$.

Оценки π_x^m и π подходят под эту лемму, так как отличаются только в x, а $x \notin \mathrm{FV}(\varphi)$.

Тогда

$$[\forall x\varphi]_{\mathcal{M}}(\pi) = 1 \iff \forall m \in M\ [\varphi](\pi_x^m) = 1 \iff \forall m \in M\ [\varphi](\pi) = 1 \iff [\varphi](\pi) = 1$$

Последний переход верен, так как значение $[\varphi](\pi)$ не зависит от m. ■

Следствие. $\forall x\exists x\varphi \equiv \exists x\varphi$. (Так как $x \notin \mathrm{FV}(\exists x\varphi)$.)

3.7.4 Квантор всеобщности и общезначимость.

Лемма 3.14. Формула φ общезначима $\iff$ $\forall x\varphi$ общезначима.

Доказательство.

$\Longrightarrow$ Дано: $\forall\mathcal{M}$, $\forall\pi\colon [\varphi]_{\mathcal{M}}(\pi) = 1$. Хотим доказать: $\forall\mathcal{M}$, $\forall\rho\colon [\forall x\varphi]_{\mathcal{M}}(\rho) = 1$. Зафиксируем какие-то $\mathcal{M}$ и ρ, тогда

$$[\forall x\varphi](\rho) = 1 \iff \forall m \in M\ [\varphi]\left(\rho_x^m\right) = 1.$$

Последнее — то, что мы хотим получить. Однако

$$\forall\pi\colon [\varphi]_{\mathcal{M}}(\pi) = 1 \implies \forall\pi\colon \forall m \in M [\varphi]_{\mathcal{M}}(\pi) = 1 \implies \forall m \in M [\varphi]_{\mathcal{M}}(\rho_x^m) = 1$$

(Добавили квантор, который ничего не меняет и подставили $\pi = \rho_x^m$, получили то, что хотели для выбранной ρ.)

$\Longleftarrow$ Дано: $\forall\mathcal{M}$, $\forall\pi\colon [\forall\varphi]_{\mathcal{M}}(\pi) = 1$. Хотим доказать: $\forall\mathcal{M}$, $\forall\rho\colon [\varphi]_{\mathcal{M}}(\rho) = 1$.
Зафиксируем какие-то $\mathcal{M}$ и ρ, тогда

$$\forall\pi\colon [\forall\varphi]_{\mathcal{M}}(\pi) = 1 \iff \forall\pi\colon \forall m \in M\colon [\varphi]_{\mathcal{M}}\left(\pi_x^m\right) = 1$$

Возьмем $\pi = \rho$, $m = \rho(x)$, тогда $\pi_x^m = \rho_x^{\rho(x)} = \rho$. Получаем $[\varphi]_{\mathcal{M}}(\rho) = 1$.

■

3.8 Основные эквивалентности логики первого порядка [F, 24]. Замена подформулы на эквивалентную. [F, 26, 30]

3.8.1 Основные эквивалентности логики первого порядка

Эквивалентности алгебры логики:

$$\begin{aligned}
\varphi &\implies \psi \equiv \neg\varphi \vee \psi,\\
\neg\varphi &\implies \neg\psi \equiv \psi \implies \varphi,\\
\neg(\varphi &\implies \psi) \equiv \varphi \wedge \neg\psi,\\
\neg\neg\varphi &\equiv \varphi,\\
\neg(\varphi \wedge \psi) &\equiv \neg\varphi \vee \neg\psi,\\
\neg(\varphi \vee \psi) &\equiv \neg\varphi \wedge \neg\psi,\\
\varphi \wedge (\psi \vee \theta) &\equiv (\varphi \wedge \psi) \vee (\varphi \wedge \theta),\\
\varphi \vee (\psi \wedge \theta) &\equiv (\varphi \vee \psi) \wedge (\varphi \wedge \theta),\\
\varphi \wedge (\varphi \vee \psi) &\equiv \varphi,\\
\varphi \vee (\varphi \wedge \psi) &\equiv \varphi,\\
\varphi \wedge \psi &\equiv \psi \wedge \varphi,\\
\varphi \wedge \varphi &\equiv \varphi,\\
(\varphi \wedge \psi) \wedge \theta &\equiv \varphi \wedge (\psi \wedge \theta).
\end{aligned}$$

Последние три эквивалентности также верны, если $\wedge$ заменить на $\vee$. Все эквивалентности доказываются по таблице истинности.

Теорема 3.15 (Основные эквивалентности с кванторами)**.**

1.

$$\begin{aligned}
\forall x(\varphi \wedge \psi) &\equiv \forall x\varphi \wedge \forall x\psi,\\
\exists x(\varphi \vee \psi) &\equiv \exists x\varphi \vee \exists x\psi.
\end{aligned}$$

2. *Пусть* $x \notin FV(\psi)$, *тогда*

$$\forall x(\varphi \wedge \psi) \equiv \forall x\varphi \wedge \psi,$$
$$\exists x(\varphi \wedge \psi) \equiv \exists x\varphi \wedge \psi,$$
$$\forall x(\varphi \vee \psi) \equiv \forall x\varphi \vee \psi,$$
$$\exists x(\varphi \vee \psi) \equiv \exists x\varphi \vee \psi.$$

3.

$$\neg\forall x\varphi \equiv \exists x\neg\varphi,$$
$$\neg\exists x\varphi \equiv \forall x\neg\varphi.$$

Доказательство проводится за счет определения: постепенно превращаем это утверждение в утверждение про неформальные кванторы. Проверим одно из них.

Доказательство. (2.2) Зафиксируем $\mathcal{M}$ и π.

$$[\exists x(\varphi \wedge \psi)](\pi) = 1 \iff \exists m \in M\ [\varphi \wedge \psi](\pi_x^m) = 1 \iff$$
$$\iff \exists m \in M\ \text{И}([\varphi](\pi_x^m) = 1, [\psi](\pi_x^m) = 1) \iff \exists m \in M\ \text{И}([\varphi](\pi_x^m) = 1, [\psi](\pi) = 1) \iff$$
$$(\exists m \in M\ [\varphi](\pi_x^m) = 1)\ \text{И}\ [\psi](\pi) = 1 \iff [\exists x\varphi](\pi) = 1\ \text{И}\ [\psi](\pi) = 1 \iff [\exists x\varphi \wedge \psi](\pi) = 1$$

Сначала делаем переход по определению. Потом заменяем $\wedge$ на функцию И(). Затем заменяем для ψ оценку с π_x^m на π, так как их значения не отличаются на свободных переменных (была теорема, что в этом случае замена равносильна). Далее выносим $[\psi](\pi)$, не зависящую от m. Оставшиеся переходы по определениям. ■

Следствие (Выразимость одного квантора через другой)**.**

1. $\forall x\varphi \equiv \forall x\neg\neg\varphi \equiv \neg\exists x\neg\varphi$.
2. $\exists x\varphi \equiv \neg\forall x\neg\varphi$.

Следствие. Пусть $x \notin \mathrm{FV}(\psi)$, тогда

$$\forall x(\varphi \implies \psi) \equiv \exists x\varphi \implies \psi,$$
$$\exists x(\varphi \implies \psi) \equiv \forall x\varphi \implies \psi,$$
$$\forall x(\psi \implies \varphi) \equiv \psi \implies \forall\varphi,$$
$$\exists x(\psi \implies \varphi) \equiv \psi \implies \exists\varphi.$$

При вынесении квантора из посылки, он меняется на противоположный. При вынесении квантора из заключения, он остается тем же.

Доказательство. $\forall x(\varphi \implies \psi) \equiv \forall x(\neg\varphi \vee \psi)$. Так как $x \notin \mathrm{FV}(\psi)$, то

$$\forall x(\neg\varphi \vee \psi) \equiv \forall x\neg\varphi \vee \psi \equiv \neg\exists x\varphi \vee \psi \equiv \exists x\varphi \implies \psi.$$

■

3.8.2 Замена подформулы на эквивалентную.

Если в формуле заменить какое-либо вхождение некоторой подформулы на эквивалентную этой подформуле формулу, мы получим формулу, эквивалентную исходной. (На лекции было только это.)

То же самое другими словами из конспекта first_order:

Лемма 3.16. Пусть $\psi \equiv \psi'$ и формула φ' получена из φ заменой некоторых вхождений ψ на ψ'. Тогда $\varphi \equiv \varphi'$.

3.9 Булевы комбинации формул. Булева функция, соответствующая булевой комбинации. Теорема о приведении булевой комбинации к дизъюнктивной нормальной форме и к конъюнктивной нормальной форме.

3.9.1 Булевы комбинации формул.

Пусть фиксирован набор попарно различных формул (атомарных или вида $\forall x\varphi$, $\exists x\varphi$) $(F_1, \ldots, F_n)$ в сигнатуре σ.

Определение 26. Определим множество $\mathcal{B}(F_1, \ldots, F_n)$ *булевых комбинаций* формул из $(F_1, \ldots, F_n)$ следующим образом:

1. $\forall i\ F_i \in \mathcal{B}(F_1, \ldots, F_n)$;
2. $\varphi, \psi \in \mathcal{B}(F_1, \ldots, F_n) \implies \neg\varphi, (\varphi \wedge \psi), (\varphi \vee \psi), (\varphi \implies \psi), (\varphi \iff \psi) \in \mathcal{B}(F_1, \ldots, F_n)$.

Хотим понять, как определяется истинность булевой комбинации. Каждой $\varphi \in \mathcal{B}(F_1, \ldots, F_n)$ поставим в соответствие булеву функцию $f_\varphi \colon \{0,1\}^n \to \{0,1\}$ таким образом, что (дальше рекурсией по построению)

1. $\varphi = F_i \implies f_\varphi(x_1, \ldots, x_n) = x_i$;
2. (a) $\varphi = \neg\psi \implies f_\varphi(\vec{x}) = \text{НЕ}(f_\psi(\vec{x}))$;
   (b) $\varphi = \psi \vee \theta \implies f_\varphi(\vec{x}) = \text{ИЛИ}(f_\psi(\vec{x}), f_\theta(\vec{x}))$;
   (c) Аналогично для других связок.

Лемма 3.17. Для любой формулы $\varphi \in \mathcal{B}(F_1, \ldots, F_n)$, $\forall M$, $\forall \pi$

$$[\varphi]_{\mathcal{M}}(\pi) = f_\varphi\left([F_1]_{\mathcal{M}}(\pi), \ldots, [F_n]_{\mathcal{M}}(\pi)\right).$$

Доказательство. Индукцией по построению φ. ■

Определение 27. Формула $\varphi \in \mathcal{B}(F_1, \ldots, F_n)$ называется *тавтологией*, если $\forall \vec{x}\ f_\varphi(\vec{x}) = 1$.

Предложение. Если φ тавтология, то φ общезначима. (Следует из леммы что была недавно.)

Не всякая общезначимая формула является тавтологией. Например, формула $\varphi = \forall x P x \implies \exists x P x$ не является тавтологией, потому что, если представить ее в виде булевой комбинации, она будет иметь вид $F_1 \implies F_2$, и ей будет соответствовать функция $\text{ИМП}(x_1, x_2)$, которая не всегда истинна.

3.9.2 Булева функция, соответствующая булевой комбинации.

Определение 28 (ДНФ над набором формул)**.** Пусть фиксирован набор формул $(F_1, \ldots, F_n)$ (как прежде). Определим дизъюнктивную нормальную форму следующим образом:

1. F_i или $\neg F_i$ — *литералы*;
2. Если $l_1, \ldots, l_k$ — литералы, то $l_1 \wedge \ldots \wedge l_k$ — *элементарная конъюнкция*;
3. Если $c_1, \ldots, c_m$ — элементарные конъюнкции, то $c_1 \vee \ldots \vee c_m$ — ДНФ над набором $(F_1, \ldots, F_n)$.

Определение 29 (КНФ над набором формул)**.** Пусть фиксирован набор формул $(F_1, \ldots, F_n)$ (как прежде). Определим конъюнктивную нормальную форму следующим образом:

1. F_i или $\neg F_i$ — *литералы*;
2. Если $l_1, \ldots, l_k$ — литералы, то $l_1 \vee \ldots \vee l_k$ — *элементарная дизъюнкция*;
3. Если $d_1, \ldots, d_m$ — элементарные дизъюнкции, то $d_1 \wedge \ldots \wedge d_m$ — КНФ над набором $(F_1, \ldots, F_n)$.

ДНФ и КНФ, вообще говоря, являются разными объектами. Например,

$$(F_1 \wedge \neg F_2 \wedge F_1) \vee (\neg F_3) \vee (F_1 \wedge F_4)$$

является ДНФ, но не является КНФ, потому что в дереве разбора формулы ниже дизъюнкции стоит конъюнкции.

Однако, существуют формулы, которые являются одновременно КНФ и ДНФ, например

$$F_1 \wedge \neg F_2; \quad F_3 \wedge \neg F_4 \wedge F_5.$$

На самом деле, одновременно КНФ и ДНФ являются литералы и элементарные конъюнкции (дизъюнкции).

Следствие. $\mathrm{CNF}\left(\vec{F}\right) \cup \mathrm{DNF}\left(\vec{F}\right) \subseteq \mathcal{B}\left(\vec{F}\right)$.

3.9.3 Теорема о приведении булевой комбинации к дизъюнктивной нормальной форме и к конъюнктивной нормальной форме.

Теорема 3.18. *Любую булеву комбинацию $\varphi \in \mathcal{B}(F_1, \ldots, F_n)$ существуют $\varphi_1 \in DNF(F_1, \ldots, F_n)$ и $\varphi_2 \in CNF(F_1, \ldots, F_n)$ такие, что*

$$\varphi \equiv \varphi_1 \wedge \varphi \equiv \varphi_2.$$

Доказательство. Все доказательство будет строиться вокруг рассмотрения функции $f_\varphi \colon \{0,1\}^n \to \{0,1\}$, которая истиностные значения формул $F_1, \ldots, F_n$ превращает в истиностное значение формулы φ. В любой интерпретации и при любой оценке переменных

$$[\varphi](\pi) = f_\varphi([F_1](\pi), \ldots, [F_n](\pi)) = f_\varphi([\vec{F}](\pi)).$$

Теперь давайте исследуем функцию f_φ. Рассмотрим $U = \{\sigma \in \{0,1\}^n \mid f_\varphi(\vec{\sigma}) = 1\}$. Надо рассмотреть несколько случаев:

1. $U = \varnothing$. Тогда для любого π $[\varphi](\pi) = f_\varphi([\vec{F}](\pi)) = 0$. Положим $\varphi_1 = F_1 \wedge \neg F_1$, тогда $\varphi_1 \equiv \varphi$.
2. $U \neq \varnothing$. Пусть $A \in \mathrm{Fm}$, а $\sigma \in \{0,1\}$, тогда положим

$$A^\sigma = \begin{cases} A, & \sigma = 1, \\ \neg A, & \sigma = 0. \end{cases}$$

Предложение. $[A^\sigma](\pi) = 1 \iff \sigma = [A](\pi)$.

Доказательство. Действительно, если $\sigma = 1$, то $[A^1](\pi) = [A](\pi)$, то есть $[A^1](\pi) = 1 \iff [A](\pi) = 1$. Если же $\sigma = 0$, то $[A^0](\pi) = 1 \iff [\neg A](\pi) = 1 \iff [A](\pi) = 0 = \sigma$. ■

Следствие. $\Phi_{\vec{\sigma}} = [F_1^{\sigma_1} \wedge \ldots \wedge F_n^{\sigma_n}](\pi) = 1 \iff \forall i [F_i^{\sigma_i}](\pi) = 1 \iff \forall i\ \sigma_i = [F_i](\pi) \iff \vec{\sigma} = [\vec{F}]$.

$[\varphi](\pi) = 1$ тогда и только тогда, когда $f_\varphi([\vec{F}](\pi)) = 1 \iff [\vec{F}](\pi) \in U \iff \exists \vec{\sigma} \in U\ [\vec{F}](\pi) = \vec{\sigma}$. Получилось тоже самое, что и в следствии последнем, поэтому это все равносильно тому, что $\exists \vec{\sigma} \in U\ [\Phi_{\vec{\sigma}}](\pi) = 1 \iff [\bigvee\limits_{\vec{\sigma} \in U} \Phi_{\vec{\sigma}}](\pi) =$

1. Но если φ и $\bigvee\limits_{\vec{\sigma} \in U} \Phi_{\vec{\sigma}}$ принимают значение 1 одновременно, то и значение 0 они принимают одновременно

(поскольку возможных значений всего два), тогда $\varphi \equiv \bigvee\limits_{\vec{\sigma} \in U} \Phi_{\vec{\sigma}} \equiv \bigvee\limits_{\vec{\sigma} \in U} F_1^{\sigma_1} \wedge \ldots \wedge F_n^{\sigma_n} \in \mathrm{DNF}(F_1, \ldots, F_n)$.

Построим теперь КНФ. На этот раз проанализируем множество $Z = \{\vec{\sigma} \mid f_\varphi(\vec{\sigma}) = 0\}$. Рассмотрим несколько случаев:

1. $Z = \varnothing$. Тогда для любого π $[\varphi](\pi) = 1$. Положим $\varphi_2 = F_1 \vee \neg F_1 \equiv \varphi$.

2. Делаем все тоже самое, что и для ДНФ, только наоборот. Рассмотрим формулу $\psi_{\vec{\sigma}} = F_1^{\overline{\sigma_1}} \vee \ldots \vee F_n^{\overline{\sigma_n}}$, где $\overline{\sigma_i}$ значит отрицание σ_i, тогда

$$\left[F_1^{\overline{\sigma_1}} \vee \ldots \vee F_n^{\overline{\sigma_n}}\right](\pi) = 0 \iff \forall i\ [F_i^{\overline{\sigma_i}}](\pi) = 0 \iff \forall i\ \overline{\sigma_i} \neq [F_i](\pi) \iff \forall i\ \sigma_i = [F_i](\pi) \iff \vec{\sigma} = [\vec{F}](\pi).$$

Что же мы делаем дальше? Дальше мы смотрим, когда $[\varphi](\pi) = 0 \iff f_\varphi([\vec{F}](\pi)) = 0 \iff [\vec{F}](\pi) \in Z \iff \exists \vec{\sigma} \in Z\ [\vec{F}](\pi) = \sigma$. Это равносильно тому, что $\exists \vec{\sigma} \in Z\ [\psi_{\vec{\sigma}}](\pi) = 0 \iff [\bigwedge\limits_{\vec{\sigma} \in Z} \psi_{\vec{\sigma}}](\pi) = 0$, отсюда $\varphi \equiv \bigwedge\limits_{\vec{\sigma} \in Z} \psi_{\vec{\sigma}} \in \mathrm{CNF}(F_1, \ldots, F_n)$.

■

Если мы хотим использовать это на практике, то надо, прежде всего, найти функцию f_φ (то есть, построить таблицу истинности). Такая таблица будет являться таблицей зависимости значений формулы φ от значений образующих ее формул. Дальше, если строим ДНФ, то мы берем наборы, где наша функция принимает значение 1. Каждый такой набор мы кодируем элементарной конъюнкцией $F_1^{\sigma_1} \wedge \ldots \wedge F_n^{\sigma_n}$ и берем их дизъюнкцию.

Также, можно не пускать каждый раз в ход этот алгоритм, а просто пользоваться элементарными эквивалентностями, и, раскрывая скобки, получить ДНФ (КНФ).

3.10 Лемма о корректной подстановке. [F, 73]

Лемма 3.19. В любой интерпретации при любой оценке π дл всех $\varphi \in \mathrm{Fm}_\sigma$, $t, s \in \mathrm{Tm}_\sigma$ и $x \in \mathrm{Var}$, если $t - x - \varphi$, то

$$[s(t/x)](\pi) = [s](\pi + (x \mapsto [t](\pi))) \text{ и } [\varphi(t/x)](\pi) = [\varphi](\pi + (x \mapsto [t](\pi)).$$

Доказательство. Подобно лемме F18 (являющейся частным случаем данной) доказывается индукцией по построению:

Пусть $s = z \neq x$. Имеем $[s(t/x)](\pi) = \pi(z) = [s](\pi + (x \mapsto [t](\pi)))$. Если же $s = x$, то $[s(t/x)](\pi) = [t](\pi) = [s](\pi + (x \mapsto [t](\pi)))$. Случай $s = \mathbb{f}_i$ тривиален (значение константы не меняется).

Если $s = \mathbb{f}_j(t_1, t_2, \ldots, t_{a_j})$, то по предположению индукции:

$$[s(t/x)](\pi) = \mathbb{f}_j([t_1(t/x)](\pi), \ldots, [t_{a_j}(t/x)](\pi)) = \\ = \mathbb{f}([t_1](\pi + (x \mapsto [t](\pi))), \ldots, [t_{a_j}](\pi + (x \mapsto [t](\pi)))) = [s](\pi + (x \mapsto [t](\pi))).$$

Случай $\varphi = \mathbb{P}_i$ тривиален (константа). Если $\varphi = \mathbb{P}_j(t_1, t_2, \ldots, t_{a_j})$, то по предположению индукции:

$$[\varphi(t/x)](\pi) = \mathbb{P}_j([t_1(t/x)](\pi), \ldots, [t_{a_j}(t/x)](\pi)) = \\ = \mathbb{P}([t_1](\pi + (x \mapsto [t](\pi))), \ldots, [t_{a_j}](\pi + (x \mapsto [t](\pi)))) = [\varphi](\pi + (x \mapsto [t](\pi))).$$

«Принципиальный» случай, когда $\varphi = \forall z\, \psi$ и $z \neq x$. Из условия $t - x - \varphi$ вытекает $z \notin V(t)$ (z — связанная в φ) и $t - x - \psi$ или $x \notin FV(\varphi)$. В первом случае, в силу предположения индукции и леммы 5,

$$[\varphi(t/x)](\pi) = [\forall z \psi(t/x)](\pi) = \\ = \min_{m \in M} [\psi(t/x)](\pi + (z \mapsto m)) = \min_{m \in M} [\psi](\pi + (z \mapsto m) + (x \mapsto [t](\pi + (z \mapsto m)))) = \\ = \min_{m \in M} [\psi](\pi + (z \mapsto m) + (x \mapsto [t](\pi))) = \min_{m \in M} [\psi](\pi + (x \mapsto [t](\pi)) + (z \mapsto m)) = \\ = [\forall z \psi](\pi + (x \mapsto [t](\pi)) = [\varphi](\pi + (x \mapsto [t](\pi)).$$

В случае $x \notin FV(\varphi)$ верно также, что $x \notin FV(\psi)$ (откуда и $t - x - \psi$), записанные равенства выполняются: применяем предположение индукции, а для всех оценок π' и элементов $k, l \in M$ по лемме F5 $[\psi](\pi' + (x \mapsto k)) = [\psi](\pi' + (x \mapsto l))$. ■

Сказанное позволяет объявить аксиомами ИП все формулы из Fm_σ вида

(A12) $\forall x\,\varphi \to \varphi(t/x)$, если $t - x - \varphi$;

(A13) $\varphi(t/x) \to \exists x\,\varphi$, если $t - x - \varphi$.

3.11 Понятие корректной подстановки («терм свободен для переменной в формуле»). Пример некорректной подстановки. Лемма о корректной подстановке (без доказательства). [F, 73] Переименование связанной переменной. [F, 16, 18]. Общезначимость формул вида $\forall x\ \varphi \to \varphi(t/x)$ и $\varphi(t/x) \to \exists x\ \varphi$ в случае корректной подстановки. [F, 74]

3.12 Переименование связанной переменной (без доказательства). [F, 16] Теорема о предваренной нормальной форме. [F, 36]

Утверждение 3.20 (Переименование связанных переменных). *Если* $y \notin V(\varphi)$, *то* $\begin{cases}\forall x\ \varphi \equiv \forall y\ \varphi(y/x)\\ \exists x\ \varphi \equiv \exists y\ \varphi(y/x)\end{cases}$

Определение 30. Формула φ называется *предварённой* или *пренексной*, если $\varphi = Q_1y_1...Q_ny_n\ \psi$, где $Q_1,..Q_n$ — некоторые кванторы, а ψ — бескванторная формула.

Теорема 3.21. *$\forall\varphi \in Fm$ $\exists$(не обязательно единственная) предварённая φ'такая, что $\varphi \equiv \varphi'$. Такая φ' называется предварённой нормальной формой формулы φ.*

Неформально: в абсолютно любой формуле можно вынести кванторы наружу.

Доказательство. Воспользуемся индукцией по построению φ.

База: Если $\varphi = R(t_1..t_n)$ (то есть φ атомарная), то $\varphi' = \varphi$ (сама уже предварённая).

Шаг:

- Если $\varphi = \forall x\psi$, то по предположению индукции $\exists$ предварённая ψ' такая, что $\psi \equiv \psi'$, тогда $\varphi = \forall x\psi \equiv \forall x\psi' = \varphi'$.
- Если $\varphi = \exists x\psi$, то по предположению индукции $\exists$ предварённая ψ' такая, что $\psi \equiv \psi'$, тогда $\varphi = \exists x\psi \equiv \exists x\psi' = \varphi'$.
- Если $\varphi = \neg\psi$, то по предположению индукции $\exists$ предварённая ψ' такая, что $\psi \equiv \psi'$. Заметим, что ψ' имеет вид $Q_1x_1..Q_nx_n\ \psi_0$, где $Q_1,..,Q_n$ — кванторы, а ψ_0 бескванторная.
  $\varphi = \neg\psi \equiv \neg\psi' = \neg Q_1x_1..Q_nx_n\ \psi_0 = \overline{Q_1}x_1..\overline{Q_n}x_n\ \neg\psi_0 = \varphi'$ (здесь $\overline{\forall} = \exists, \overline{\exists} = \forall$).
- $\varphi = \psi \wedge \theta$. По предположению индукции $\psi \equiv Q_1x_1..Q_nx_n\ \psi_0$, $\theta \equiv Q'_1y_1..Q'_my_m\ \theta_0$
  $\varphi = Q_1x_1..Q_nx_n\ \psi_0 \wedge Q'_1y_1..Q'_my_m\ \theta_0$. Пусть $z_1,..,z_n,w_1,..,w_m$ — "свежие" ($\notin V(\varphi)$) и различные между собой переменные.
  Тогда по теореме о переименовании связанных переменных $\varphi \equiv Q_1z_1..Q_nz_n\ \psi_0(z/x) \wedge Q'_1w_1..Q'_mw_m\ \theta_0(w/y) \equiv$
  $\equiv Q_1z_1..Q_nz_nQ'_1w_1..Q'_mw_m\ \psi_0(z/x) \wedge \theta_0(w/y) = \varphi'$.
  Аналогичные рассуждения можно применить для остальных логических связок.

■

Пример. Приведем формулу $\neg\forall xPxy \vee \exists yQzxy$ к предварённой нормальной форме.

$\neg\forall xPxy \vee \exists yQzxy \implies \exists x\neg Pxy \vee \exists yQzxy \implies \exists x'\neg Px'y \vee \exists yQzxy \implies$
$\implies \exists x'(\neg Px'y \vee \exists yQzxy) \implies \exists x'(\neg Px'y \vee \exists y'Qzxy') \implies \exists x'\exists y'(\neg Px'y \vee Qzxy')$

3.13 Понятие теории первого порядка. Примеры содержательных теорий. Модель теории. Семантическое (логическое) следование (для замкнутых формул) [ВШ-2, с. 187]

Определение 31. Теория(в сигнатуре σ) - любое множество предложений этой сигнатуры.

Определение 32. $M \vDash T \iff \forall \varphi \in T : M \vDash \varphi$, то есть если каждое предложение в нашей интерпретации истинно, то и вся теория. Множество M будет моделью нашей теории.

Определение 33. Теория T выполнима(или совместна) $\iff \exists M : M \vDash T$

Определение 34. Предложение φ следует из теории T, если $\forall M : M \vDash T \Rightarrow M \vDash \varphi$

В примерах мы работаем в нормальных моделях(то есть равно - это привычное нам равно)

Пример. T_{ord} - частичный порядок, $T = \begin{cases} \forall x : \neg(x < x), \text{антирефлексивность} \\ \forall x : \forall y : \forall x : (x < y) \wedge \ (y < z) \Rightarrow (x < z), \text{транзитивность} \end{cases}$

Работаем в структуре $M = (A, =, <)$

Утверждение 3.22. $\forall M : M \vDash T \Rightarrow M \vDash \forall x : \forall y : (x < y \wedge y < x \Rightarrow (x = y))$, *то есть антисимметричность следует из транзитивности и антирефлексивности*

Доказательство. Предположим, что наша посылка($x < y \wedge y < x$) истинна. Воспользуемся транзитивностью: $(x < y \wedge y < x) \Rightarrow (x < x)$. Получили противоречие, так как в нашей теории есть антирефлексифность, которая говорит, что $x < x$ никогда не верно. Значит, посылка всегда ложная, а интерпетация всегда истинна. ■

Пример. $G = (A, =, +, -, 0)$ - структура, это группа, когда в ней выполняется теория T = теория групп, $T =$

$$\begin{cases} \forall x : \forall y : \forall z : (x + y) + z = x + (y + z), \text{ассоциативность} \\ \forall x : (x + (-x) = 0) \wedge ((-x) + x = 0), \text{обратный элемент} \\ \forall x : (x + 0 = x) \wedge (0 + x = x), \text{нейтральный элемент} \end{cases}.$$

3.14 Сколемизация предварённой формулы. Сколемовская нормальная форма. Теорема о равновыполнимости.

Определение 35. *Сколемизацией* предварённой формулы называется преобразование следующего вида:

$$\forall \overrightarrow{x}\ \exists y\, \varphi \to_S \forall \overrightarrow{x}\ \varphi\,(f(\overrightarrow{x})/y)$$

Неформально: мы заменяем одну переменную под квантором существования на функцию от переменных под кванторами всеобщности.

Определение 36. Предварённая формула φ' — *сколемовская нормальная форма* предварённой формулы φ, если:

1. в φ' нет кванторов существования;
2. $\varphi \to_S \varphi_1 \to_S ... \to_S \varphi_n \to_S \varphi'$ (обозначается $\varphi \twoheadrightarrow_S \varphi'$), то есть φ' получается из φ цепочкой сколемизаций.

Очевидный факт. Если $\varphi \twoheadrightarrow_S \varphi'$, то φ выполнима $\iff$ φ' выполнима.

Определение 37. Γ выполнимо $\iff \exists \mathcal{M} \exists \pi\ [\Gamma]_{\mathcal{M}}(\pi) = 1$.

Определение 38. Множества формул Γ и Δ *равновыполнимы* $\iff$ (Γ выполнимо $\iff$ Δ выполнимо).

Предложение. Для любой предварённой формулы φ такой, что она не содержит фиктивных кванторов, существует сколемовская нормальная форма ψ такая, что $\varphi \twoheadrightarrow_S \psi$.

Доказательство. Применим алгоритм сколемизации и заметим, что кванторов у нас конечное число, поэтому алгоритм точно остановится.

■

Теорема 3.23 (о сколемизации). *Пусть* $\Gamma \subseteq Fm$ *и* $\varphi \to_S \psi$. *Тогда* $\Gamma \cup \{\varphi\}$ *и* $\Gamma \cup \{\psi\}$ *равновыполнимы.*

Что это означает? Это означает, что у нас было какое-то множество формул (хочется сказать теорий, но в нашем множестве могут быть свободные переменные), мы взяли оттуда одну формулу и подвергли ее сколемизации. Тогда то, что получилось, равновыполнимо с исходным множеством.

Доказательство. Раз у нас была сколемизация, то $\varphi = \forall \vec{x} \exists y \theta$, а $\psi = \forall \vec{x}\ \theta(f\vec{x}/y)$, где f «свежая», то есть, в частности, f не встречается в Γ. Сделаем несколько наблюдений:

1. В формуле $\exists y \theta$ нет кванторов по $\vec{x}$ (иначе в φ есть фиктивный квантор) $\implies$ $f\vec{x}$-y-θ, ну а раз подстановка корректная, то формула $\theta(f\vec{x}/y) \implies \exists y \theta$ общезначима. Поскольку формула общезначима, то, по факту с семинара, формула $\forall \vec{x} \theta(f\vec{x}/y) \implies \forall \vec{x} \exists y \theta$ также общезначима. Вспомним про определение φ и ψ, и заметим, что $\psi \implies \varphi$, то есть, в любой структуре, где верно ψ, верно и φ. Тогда если $\exists \mathcal{M}\ \exists \pi$ такие, что $[\Gamma \cup \{\psi\}]_{\mathcal{M}}(\pi) = 1$, то $[\Gamma \cup \{\varphi\}]_{\mathcal{M}}(\pi) = 1$. Значит, если $\Gamma \cup \{\psi\}$ выполнима, то $\Gamma \cup \{\varphi\}$ выполнима.
2. Допустим, что $\Gamma \cup \{\forall \vec{x} \exists y \theta\}$ выполнима. Тогда $\exists \mathcal{M}\ \exists \pi$ ($[\Gamma]_{\mathcal{M}}(\pi) = 1$ и $[\forall \vec{x} \exists y \theta]_{\mathcal{M}}(\pi) = 1$). Заметим, что
$$[\forall \vec{x} \exists y \theta]_{\mathcal{M}}(\pi) = 1 \iff \forall \vec{a} \in M\ \exists b \in M\ [\theta]_{\mathcal{M}}(\pi^{\vec{a}\ b}_{x\ y}) = 1.$$
Теперь рассмотрим $\mathcal{M}' = (\mathcal{M}, f^{\mathcal{M}})$ (мы расширили структуру, добавив[1] в нее интерпертацию символа f). Как мы можем ее расширить? Для этого нам нужно определить значение $f^{\mathcal{M}}(\vec{a})$. Положим его равным $b \in M$ такому, что $\forall \vec{a} [\theta]_{\mathcal{M}}(\pi^{\vec{a}\ b}_{x\ y}) = 1$, то есть, $\forall \vec{a} \in M^n\ [\theta]_{\mathcal{M}}(\pi^{\vec{a}\ f^{\mathcal{M}}(\vec{a})}_{x\ y}) = 1$. Такая $f^{\mathcal{M}}$ существует в силу аксиомы выбора. Ну вот мы взяли такую интерпретацию, дальше мы хотим посмотреть, что же будет с ψ и ее значением
$$[\forall \vec{x} \theta(f\vec{x}/y)]_{\mathcal{M}'}(\pi).$$
В старой структуре у нее вообще не было значения, потому что там у нас не интерпретировался символ f. В новой же структуре
$$[\forall \vec{x} \theta(f\vec{x}/y)]_{\mathcal{M}'}(\pi) = 1 \iff \forall \vec{a} \in M\ [\theta(f\vec{x}/y)]_{\mathcal{M}'}(\pi^{\vec{a}}_{\vec{x}}) = 1.$$
Докажем последнее равенство. Мы можем воспользоваться леммой о корректной подстановке и получится, что
$$[\theta(f\vec{x}/y)]_{\mathcal{M}'}(\pi^{\vec{a}}_{\vec{x}}) = [\theta]_{\mathcal{M}'}\left(\pi^{\vec{a}\ [f\vec{x}]_{\mathcal{M}'}(\pi^{\vec{a}}_{x})}_{\vec{x}\ y}\right) = [\theta]_{\mathcal{M}'}\left(\pi^{\vec{a}\ f^{\mathcal{M}}(\vec{a})}_{\vec{x}\ y}\right) \overset{f\ -\ \text{свежая}}{=} [\theta]_{\mathcal{M}}\left(\pi^{\vec{a}\ f^{\mathcal{M}}(\vec{a})}_{x\ y}\right) = 1$$
Итак, $[\varphi]_{\mathcal{M}'}(\pi) = 1$. А что с Γ? В Γ ничего не изменится, поскольку f не встречается в Γ, поэтому
$$[\Gamma]_{\mathcal{M}'}(\pi) = [\Gamma]_{\mathcal{M}}(\pi) = 1.$$
Таким образом, $[\Gamma \cup \{\varphi\}]_{\mathcal{M}'}(\pi) = 1$, то есть $\Gamma \cup \{\psi\}$ выполнима. ■

3.15 Исчисление резолюций для произвольных множеств формул. Теорема о корректности. Теорема о полноте (без доказательства).

В исчислении резолюций есть 2 правила.

Правило вывода (резолюции). $\boxed{\dfrac{\neg A \vee B \quad A \vee C}{B \vee C}}$

Частный случай ПР – вывод пустой дизъюнкции (лжи): $\dfrac{A \quad \neg A}{\bot}$.

Правило подстановки. $\boxed{\dfrac{\forall y A}{A(t/y)}}$, где t – произвольный терм, A – универсальна.

Говорят, что формула φ выводится из множества формул Γ в исчислении резолюций, если φ возможно получить из формул в Γ, применяя к ним правило резолюции и правило подстановки какое-то конечное число раз.

[1] Такая операция называется *обогащением* структуры $\mathcal{M}$.

Обозначение: $\Gamma \vdash \varphi$.

Корректность ПР. $\forall M\ \forall \pi$ если $[\neg A \vee B]_M(\pi) = 1$ и $[A \vee C]_M(\pi) = 1$, то $[B \vee C]_M(\pi) = 1$.

Другими словами, импликация $((\neg A \vee B) \wedge (A \vee C) \to (B \vee C))$ общезначима.

Доказательство. По контрапозиции.

$[B \vee C]_M(\pi) = 0 \implies ([B]_M(\pi) = 0) \wedge ([C]_M(\pi) = 0) \implies [\neg A \vee B]_M(\pi) = 0 \vee [A \vee C]_M(\pi) = 0 \implies$

$\neg([\neg A \vee B]_M(\pi) = 1 \wedge [A \vee C]_M(\pi) = 1)$. ■

Корректность ПП. Пусть A – универсальна.

$\forall M\ \forall \pi$ если $[\,\forall y\, A\,]_M(\pi) = 1$, то $[\,A(t/y)\,]_M(\pi) = 1$.

Доказательство. Допустим, $A = \forall \overrightarrow{x} A_0$, где A_0 – бескванторная формула.

$[\forall y \forall \overrightarrow{x}\, A_0]_M(\pi) = 1 \iff \forall a \in M \forall \overrightarrow{b} \in M^n\ \ [A_0]\left(\pi_y^a\ {}^{\overrightarrow{b}}_{\overrightarrow{x}}\right) = 1 \iff \forall \overrightarrow{b} \in M^n \forall a \in M\ \ [A_0]\left(\pi_{\overrightarrow{x}}^{\overrightarrow{b}}\ {}^{a}_{y}\right) = 1.$

Теперь положим $a := [\,t\,]\left(\pi_{\overrightarrow{x}}^{\overrightarrow{b}}\right) \implies \forall \overrightarrow{b} \in M^n\ [A_0]\begin{pmatrix} \overrightarrow{b} & [\,t\,]\left(\pi_{\overrightarrow{x}}^{\overrightarrow{b}}\right) \\ \pi_{\overrightarrow{x}} & y \end{pmatrix} = 1.\ \circledast$

С другой стороны $[A(t/y)]_M(\pi) = 1 \iff [\forall \overrightarrow{x}\ A_0(t/y)\,]_M(\pi) = 1 \iff \forall \overrightarrow{b} \in M^n\ [\,A_0(t/y)\,]_M\left(\pi_{\overrightarrow{x}}^{\overrightarrow{b}}\right) = 1.$

Так как в A_0 нет кванторов, $t - y - A_0$. Тогда по лемме о корректной подстановке

$\forall \overrightarrow{b} \in M^n\ [\,A_0(t/y)\,]_M\left(\pi_{\overrightarrow{x}}^{\overrightarrow{b}}\right) = 1 \iff \forall \overrightarrow{b} \in M^n\ [A_0]\begin{pmatrix} \overrightarrow{b} & [\,t\,]\left(\pi_{\overrightarrow{x}}^{\overrightarrow{b}}\right) \\ \pi_{\overrightarrow{x}} & y \end{pmatrix} = 1$, что совпадает с $\circledast$. Равносильность доказана.

■

Теорема о корректности. Если $\Gamma \vdash \varphi$, то $\Gamma \vDash \varphi$.

Доказательство. Индукция по построению вывода в ИР.

Применяем утверждения о корректности ПП и ПР, доказанные выше. ■

Теорема о полноте. Δ – набор формул в сигнатуре σ. Если $\Delta \nvdash \bot$, то $\exists M\ \exists \pi\ [\Delta]_M(\pi) = 1$, причём $|M| \leqslant max(|\mathbb{N}|, |\sigma|)$.

3.16 Исчисление резолюций для произвольных множеств формул. Теоремы о корректности и о полноте (обе без доказательства). Доказывание общезначимости и логического следования в теории с помощью исчисления резолюций. Пример применения исчисления резолюций (должны присутствовать формулы, не являющиеся универсальными дизъюнктами).

В исчислении резолюций есть 2 правила.

Правило вывода (резолюции). $\boxed{\dfrac{\neg A \vee B \quad A \vee C}{B \vee C}}$

Частный случай ПР – вывод пустой дизъюнкции (лжи): $\dfrac{A \quad \neg A}{\bot}$.

Правило подстановки. $\boxed{\dfrac{\forall y A}{A(t/y)}}$, где t – произвольный терм, A – универсальна.

Говорят, что формула φ выводится из множества формул Γ в исчислении резолюций, если φ возможно получить из формул в Γ, применяя к ним правило резолюции и правило подстановки какое-то конечное число раз.

Обозначение: $\Gamma \vdash \varphi$.

Теорема о корректности. Если $\Gamma \vdash \varphi$, то $\Gamma \vDash \varphi$.

Теорема о полноте. Δ – набор формул в сигнатуре σ. Если $\Delta \nvdash \bot$, то $\exists M\, \exists \pi\ [\Delta]_M(\pi) = 1$, причём $|M| \leqslant max(|\mathbb{N}|, |\sigma|)$.

Как доказать общезначимость формулы φ? Знаем, что

φ общезначима $\iff$ $\neg\,\varphi$ не выполнима $\iff$ $\{\neg\,\varphi\}$ не выполнима.

Так что достаточно вывести из теории $\{\neg\,\varphi\}$ ложь (с помощью ИР).

Пример: $\varphi = \forall x\, \exists y\, \forall z\, Pxyz \to \exists y\, \forall z\, \exists x\, Pxyz$. Доказать, что она общезначима.

$\neg\,\varphi \equiv \forall x\, \exists y\, \forall z\, Pxyz \wedge \neg\, \exists y\, \forall z\, \exists x\, Pxyz \equiv \forall x\, \exists y\, \forall z\, Pxyz \wedge\ \forall y\, \exists z\, \forall x\, \neg\, Pxyz \equiv \forall x\, \exists y\, \forall z\, Pxyz \wedge\ \forall v\, \exists w\, \forall u\, \neg\, Puvw \equiv$

$\forall x\, \exists y\, \forall z\, \forall v\, \exists w\, \forall u\, (Pxyz \wedge \neg\, Puvw)$.

Сколемизируем, $y \rightsquigarrow f(x)$ $\implies$ $\cdots \equiv \forall x\, \forall z\, \forall v\, \exists w\, \forall u\, (Px\,(fx)\,z \wedge \neg\, Puvw)$.

Второй шаг сколемизации, $w \rightsquigarrow g(x,z,v)$ $\implies$ $\cdots \equiv \forall x\, \forall z\, \forall v\, \forall u\, (Px\,(fx)\,z \wedge \neg\, Puv\,(g\,xzv))$.

Делаем из получившейся штуковины теорию. Заметим, что она не является универсальным дизъюнктом. Поэтому мы имеем право разбить её на несколько УД. Наша теория, в итоге, выглядит так:

$\{\forall x\, \forall z\, \forall v\, \forall u\, (Px\,(fx)\,z),\ \ \forall x\, \forall z\, \forall v\, \forall u\, \neg\, Puv\,(g\,xzv)\}$

Выведем из неё ложь:

$\dfrac{\forall x\, \forall z\, \forall v\, \forall u\, (Px\,(fx)\,z)}{Pu\,f(u)\,(g\,uz\,(fu))}$ – правило подстановки, сделали $\begin{cases} x := u; \\ z := g\,uz\,(fu) \end{cases}$

$\dfrac{\forall x\, \forall z\, \forall v\, \forall u\, \neg\, Puv\,(g\,xzv)}{\neg Pu\,f(u)\,(g\,uz\,(fu))}$ – правило подстановки, сделали $\begin{cases} x := u; \\ v := fu; \\ z := z; \\ u := u \end{cases}$

$\dfrac{Pu\,f(u)\,(g\,uz\,(fu)) \quad \neg Pu\,f(u)\,(g\,uz\,(fu))}{\bot}$ – правило резолюций.

Всё – УРА, доказали, что исходная φ общезначима.

3.17 Теорема компактности (в двух формах: про выполнимость и про логическое следование). Вариант для нормальных моделей (без доказательства). Любой пример применения.

Теорема о компактности-1.

Если каждое конечное подмножество Γ выполнимо ($\iff$ Γ "конечно выполнимо"), то Γ выполнимо.

Доказательство. Контрапозиция. Пусть Γ не выполнимо $\implies \Gamma^* \vdash \bot$ по теореме о полноте.

Любой вывод в ИР – конечное дерево $\implies \exists$ конечное $\Delta \subseteq \Gamma^*$ $\Delta \vdash \bot \implies \exists$ конечное $\Gamma_1 \subseteq \Gamma$, т.ч. $\Delta \subseteq \Gamma_1^*$ и $\Gamma_1^* \vdash \bot$.

По теореме о корректности Γ_1^* невыполнимо $\implies \Gamma_1$ невыполнимо.

Т.е. нашлось конечное невыполнимое подмножество Γ.

■

Теорема о компактности-2. Если $\Gamma \vDash \varphi$, то $\exists$ конечное $\Gamma' \subseteq \Gamma$ $\Gamma' \vDash \varphi$.

Доказательство. $\Gamma \vDash \varphi \iff$ невыполнима $\Gamma \cup \{\neg\varphi\} \implies \exists$ конечное $\Gamma' \subseteq \Gamma$ $\Gamma' \cup \{\neg\varphi\}$ невыполнима $\iff \Gamma' \vDash \varphi$.

■

Определим $Ax_{=}^{\sigma}$ (аксиомы равенства).

$Ax_{=}^{\sigma} : \{\, \forall x\,(x = x)\,,\ \ \forall x\,\forall y\,(x = y \to y = x)\,,\quad \forall x\,\forall y\,\forall z\,(x = y \wedge y = z \to x = z)\,\} \cup$

$\{(x_1 = y_1 \wedge \cdots \wedge x_n = y_n) \to (R_{x_1 \ldots x_n} = R_{y_1 \ldots y_n}) \mid R^{(n)} \in Rel_\sigma\} \cup$

$\{(x_1 = y_1 \wedge \cdots \wedge x_n = y_n) \to (f_{x_1 \ldots x_n} = f_{y_1 \ldots y_n}) \mid f^{(n)} \in Fnc_\sigma\}.$

Утверждение. Пусть в σ есть равенство. У Γ есть нормальная модель ($\leqslant max(|\mathbb{N}|, |\sigma|)$) $\iff$ выполнима $\Gamma \cup Ax_{=}^{\sigma}$.

Доказательство. $\boxed{\Rightarrow}$ В нормальной модели выполняются аксиомы равенства.

$\boxed{\Leftarrow}$ В каком случае модель, в которой выполнена теория $Ax_{=}^{\sigma} \cup \Gamma$, может оказаться не нормальной?

Только если у каких-то элементов есть "двойники".

В этом случае модифицируем модель и склеим все дублирующиеся элементы. $Ax_{=}^{\sigma} \cup \Gamma$ всё ещё выполнима, так как наличие или отсутствие двойников ничего не меняет, но модель уже является нормальной, чего мы и хотели.

■

Компактность для нормальных моделей. Если у каждого конечного подмножества Γ есть нормальная модель, то у Γ есть нормальная модель (мощности $\leqslant max(|\mathbb{N}|, |\sigma|)$).

Доказательство. По утверждению выше, $\forall$ конечного $\Gamma_1 \subseteq \Gamma$ выполнима $\Gamma_1 \cup Ax_{=}^{\sigma} \implies$

$\forall$ конечное подмножество $\Gamma' \subseteq \Gamma \cup Ax_{=}^{\sigma}$ выполнимо $\implies$

$\Gamma \cup Ax_{=}^{\sigma}$ выполнимо (по обычной компактности) $\implies$ у Γ есть нормальная модель из утверждения выше.

■

Игра Эренфойхта. Формулировка основной теоремы и примеры применения: когда побеждает Новатор, и когда побеждает Консерватор.

• Чтобы доказать, что 2 структуры не являются элементарно эквивалентными, достаточно привести контрпример. Но для доказательства элементарной эквивалентности необходимо пользоваться игрой Эренфойхта.

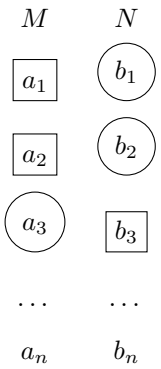
Пусть σ – сигнатура, где (I) нет функциональных и константных символов (т.е. сигнатура состоит лишь из предикатных символов); (II) σ конечна.

Пусть N, M – две σ-структуры. Два игрока, называемые Новатором (Н) и Консерватором (К), играют в такую игру:

Н объявляет продолжительность игры в $n \in \mathbb{N}$ ходов.

Н делает первых ход и выбирает в одной из структур элемент a_1. В ответ на это консерватор выбирает в другой структуре элемент b_1, который является "аналогом" a_1. Затем Н делает очередной шаг, и всё повторяется n раз.

Пример игры. Н – квадратик, К – кружок



В результате получилось какое-то конечное соответствие между элементами M и N.

Кто выигрывает?

K выигрывает $\iff$ {ни один предикат из σ не отличает $a_1 \dots a_n$ от $b_1 \dots b_n$} $\iff$
$\forall R^k \in Rel_\sigma \; \forall \; 1 \leqslant i_1, \dots i_k \leqslant n \quad (a_{i_1} \dots a_{i_k}) \in R^M \iff (b_{i_1} \dots b_{i_k}) \in R^N$.

Иначе выигрывает новатор.

Суть: консерватор пытается доказать, что структуры нельзя различить. Новатор же ищет различия.

Пример 1. $(\mathbb{N}, <)$ и $(\mathbb{Z}, <)$.

Новатор выигрывает при любой игре консерватора (т.е. у Н есть выигрышная стратегия).

Новатор: $n = 2$.

$(\mathbb{N}, <)$	$(\mathbb{Z}, <)$
$\boxed{0}$	(n)
(m)	$\boxed{n-1}$

$n,\ m$ – произвольные числа, которые выбрал К (мы пытаемся доказать, что выигрыш не зависит от игры К).

Новатор победил, ведь $(m \not<_{\mathbb{N}} 0)$, но $(n-1 <_{\mathbb{Z}} n)$.

Теорема. $M \equiv N \iff$ в игре Эренфойхта для M и N у консерватора есть выигрышная стратегия ($\iff$ различие найти нельзя ни за какое конечное число шагов).

Пример 2.

Новатор: $n = 3$.

$(\mathbb{Z}, <)$	$(\mathbb{Q}, <)$
$a_1 = \boxed{0}$	$(q_1) = b_1$
$a_2 = \boxed{1}$	$\boxed{q_2} = b_2$
$a_3 = (n)$	$\boxed{\frac{q_1+q_2}{2}} = b_3$

К проиграл, ведь $b_1 <_{\mathbb{Q}} b_2 <_{\mathbb{Q}} b_3$, однако $\forall\, n \neg (a_1 <_{\mathbb{Z}} a_2 <_{\mathbb{Z}} a_3)$, так как неверно $0 <_{\mathbb{Z}} n <_{\mathbb{Z}} 1$.

Пример 3. Докажем через игру Эренфойхта, что $(\mathbb{Q}, <) \equiv (\mathbb{R}, <)$.

Доказательство. Достаточно доказать, что у К есть выигрышная стратегия.

К должен уметь для $\forall\, n \in \mathbb{N}$ продержаться n ходов, чтобы не возникло отличия между структурами.

Индукция по n.

База. $n = 1 \implies$ Н не сможет выиграть, ведь предикат у нас бинарный.

Точнее, если $a_1,\ b_1$ – соответствующие ходы, то в обеих структурах всегда верно $a_1 \not< a_1;\ b_1 \not< b_1$.

Переход. Пусть К не проигрывает за n ходов. Докажем, что он может продержаться ещё один ход.

Игра сейчас имеет вид:

$$
\begin{array}{ccc}
(\mathbb{Q}, <) & & (\mathbb{R}, <) \\
a_1 & \xrightarrow{\alpha} & b_1 \\
a_2 & \xrightarrow{\alpha} & b_2 \\
\dots & \xrightarrow{\alpha} & \dots \\
a_n & \xrightarrow{\alpha} & b_n
\end{array}
$$

Мы задали по данной партии отображение $\alpha(a_i) = b_i$.

К не проиграл $\iff$ α – изоморфизм, т.е. $\forall\, i, j \;\; a_i < a_j \iff b_i < b_j$.

Упорядочим a_i по возрастанию: $a_{(1)} < a_{(2)} < \dots < a_{(n)}$. Упорядочим b_i аналогично.

Тогда $\alpha(a_{(i)}) = b_{(i)}$ в силу $\forall\, i, j \;\; a_i < a_j \iff b_i < b_j$.

Замечание. Если вдруг $a_i = a_j \implies \neg\,(a_i < a_j) \wedge \neg\,(a_j < a_i) \implies \neg\,(b_i < b_j) \wedge \neg\,(b_j < b_i) \implies b_i = b_j$. *В силу этого мы имеем право игнорировать повторы (если найдутся равные элементы, то в неравенстве выше просто будут фигурировать* $l < n$ *элементов, его суть же от этого не изменится).*

Теперь пусть Н сделал какой-то ход, условно, он выбрал b в $\mathbb{R}$ (для $\mathbb{Q}$ аналогично).

Случай 1. $b < b_{(1)} \implies$ К отвечает каким-то a, т.ч. $a < a_{(1)}$. Это возможно, ведь в $(Q, <)$ нет минимального.

Случай 2. $b_{(l)} < b \implies$ К отвечает каким-то a, т.ч. $a_{(l)} < a$. Это возможно, ведь в $(Q, <)$ нет максимального.

Случай 3. $b_{(i)} < b < b_{(i+1)} \implies$ К отвечает каким-то a, т.ч. $a_{(i)} < a < a_{(i+1)}$. Это возможно, ведь $(Q, <)$ – плотный.

Итого – в любом кейсе К не проиграл. Ч.т.д.

■

Как следствие получим, что если M и N – плотные лин. порядки без наибольшего и наименьшего элемента, то $M \equiv N$. (Все рассуждения выше применимы к любому DLO без наименьшего и наибольшего элемента).