Курс математической логики по Штукенбергу Д. Г.

Daniyar Itegulov, Aleksei Latyshev, Ignat Loskutov

12 февраля 2015 г.

Содержание

лан, всё не книжку верстаем))))000

некто Игнат Лоскутов о качестве вёрстки

данияр лолка пиздос)))))

аноним о всяких там хех латехерах

Mykhail Volkhov, 2538, 2014Sep-2015Jan
Я не отвечаю за верность написанного - много информации я придумал сам, много достал из недостоверных источников.

I. Базовые понятия

I.1. Формальные системы и модели

Сделано мной для меня самого, be careful

Мы работаем с формальными системами. Формальная система определяется сигнатурой, грамматикой, набором аксиом и набором правил вывода.

1. Сигнатура ФС – это (Pr, F, C, Links, Misc, arity):
   - Pr – описывает предикаты (число + заглавная буква латинского алфавита)
   - F – множество функций (заглавные буквы латинского алфавита)
   - C – описывает константы
   - Links – множество связок ({«→», «∪», «пробел»})
   - Misc – дополнительные элементы ({«(», «)», «пробел»})
   - $\mathtt{arity}\colon \mathsf{Foo} \cup \mathsf{Pr} \cup \mathsf{C} \to \mathbb{N}$ возвращает арность
2. Грамматика описывает то, как мы можем строить выражения в соответствии с нашей сигнатурой.
3. Аксиомы – выражения в нашей грамматике.
4. Правила вывода – пары вида (List, List), где List – список утверждений. Первый элемент – посылки, второй – то, что из них следует.

Иногда нам хочется что-то посчитать и мы прикручиваем к формальной системе модель – корректную структуру с оценкой. Структура – это сигнатура с интерпретацией и носителем.

1. Сигнатура структуры – (R, F, C, arity):
   - Pr – множество символов для предикатов
   - F – функциональных символов
   - C – символов констант
   - $\mathtt{arity}$ – функция, определяющая арность $\mathsf{Pr} \cup \mathsf{F} \to \mathbb{N}$.
2. Интерпретация – это приписывание символам значения и правил действия (отображения из $\mathsf{Pr} \cup \mathsf{F} \cup \mathsf{C}$ в носитель)
3. Носитель – это объединение множеств, в котором обязательно присутствует V – множество истинностных значений. Если же мы рассматриваем только нульместные предикаты, на этом можно остановиться, otherwise часто вводится P – предметное множество, в которое отображаются элементы из F, C.

TODO Эта реализация структуры не определяет ничего в районе аксиоматики, но аксиоматически заданные структуры существуют – например в ФА есть Пеано.

Если все аксиомы тавтологии, то структура корректна. В таком случае она называется моделью.

Оценку иногда определяют раньше/позже чем модель, мне удобно думать о ней, как об отдельной сущности, потому что она связывает модель с ФС.

Оценка – это функция оценки и функция тавтологии.

1. Функция оценки – отображение из (множества всех формул, сгенеренных грамматикой) x (какие-нибудь допаргументы) в V модели. Дополнительные аргументы – например оценки элементов связки.

2. Функция тавтологии – отображение из множества формул грамматики в $\{0, 1\}$ – является ли формула тавтологией. Тавтология использует функцию оценки. Например, тавтология – это выражение, оценка которого на любых аргументах возвращает $\sigma \in V$ – какой-то элемент V.

Когда говорится «сигнатура модели» – имеется в виду ровно она. Когда говорится «сигнатура ФС» – имеется в виду скорее всего объединение сигнатур, а может только сигнатура самой ФС. Первый вариант тут предпочтительней.

II. Определения (нужно знать идеально)

Определения тут зачастую дублируют то, что написано в самом конспекте, поэтому удаление этого блока сэкономит бумагу при печати.

II.1. ИВ

Формальная система с алгеброй Яськовского J_0 в качестве модели, множество истинностных значений $\{0, 1\}$. Формальная теория нулевого порядка, кванторов нету, предикаты – это пропозициональные переменные. Аксиомы:

1. $\alpha \to \beta \to \alpha$
2. $(\alpha \to \beta) \to (\alpha \to \beta \to \gamma) \to (\alpha \to \gamma)$
3. $\alpha \to \beta \to \alpha \& \beta$
4. $\alpha \& \beta \to \alpha$
5. $\alpha \& \beta \to \beta$
6. $\alpha \to \alpha \vee \beta$
7. $\beta \to \alpha \vee \beta$
8. $(\alpha \to \beta) \to (\gamma \to \beta) \to (\alpha \vee \gamma \to \beta)$
9. $(\alpha \to \beta) \to (\alpha \to \neg\beta) \to \neg\alpha$
10. $\neg\neg\alpha \to \alpha$

II.2. Общезначимость, доказуемость, выводимость

- Общезначимость формулы – ее свойство в теории с моделью. Общезначимость можно определить как угодно, в принципе. Например в ИВ общезначимость – это что оценка формулы на любых значениях свободных переменных отображает в 1. В модели крипке – существование формулы во всех мирах и т.д.
- Доказуемость – свойство формулы в теории, значащее, что существует доказательство для этой формулы. Доказательство для теории тоже определяется по разному (последовательность утверждений, каждое из которых есть аксиома или следует по правилу вывода из предыдущих в ИВ, дерево с выводами в S_∞)
- Выводимость – в общем случае часто используется как аналог доказуемости, в ИВ это доказуемость из всего, что и ранее + из посылок.

II.3. Теорема о дедукции для ИВ

Теорема, утверждающая, что из $\Gamma, \alpha \vdash \beta$ следует $\Gamma \vdash \alpha \to \beta$ и наоборот.
Доказывается вправо поформульным преобразованием, влево добавлением 1 формулы. Работает в ИВ, ИИВ, предикатах.

II.4. Теорема о полноте исчисления высказываний

Теорема II.1 (о полноте исчисления высказываний)**.** Исчисление предикатов полно.
Общий ход д-ва: строим док-ва для конкретных наборов перменных, 2^n, где n – количество возможных переменных. Потом их мерджим.

II.5. ИИВ

Берем ИВ, выкидываем 10 аксиому, добавляем $\alpha \to \neg\alpha \to \beta$.
Она доказывается и в ИВ:

Лемма II.2. $\alpha, \alpha \vee \neg\alpha, \neg\alpha \vdash \beta$

(1)	α	Допущение
(2)	$\neg\alpha$	Допущение
(3)	$\alpha \to \neg\beta \to \alpha$	Сх. акс. 1
(4)	$\neg\beta \to \alpha$	М.Р. 1,3
(5)	$\neg\alpha \to \neg\beta \to \neg\alpha$	Сх. акс. 1
(6)	$\neg\beta \to \neg\alpha$	М.Р. 2,5
(7)	$(\neg\beta \to \alpha) \to (\neg\beta \to \neg\alpha) \to (\neg\neg\beta)$	Сх. акс. 9
(8)	$(\neg\beta \to \neg\alpha) \to (\neg\neg\beta)$	М.Р. 4,7
(9)	$\neg\neg\beta$	М.Р. 6,8
(10)	$\neg\neg\beta \to \beta$	Сх. акс. 10
(11)	β	М.Р. 9,10

А еще в ИИВ главная фишка – недоказуемо $\alpha \vee \neg\alpha$ (можно подобрать такую модель).

II.6. Теорема Гливенко

Теорема II.3 (Гливенко)**.** Если в ИВ доказуемо α, то в ИИВ доказуемо $\neg\neg\alpha$

Общий ход д-ва: говорим, что если в ИИВ доказуема δ_i, то в ней же доказуема $\neg\neg\delta_i$. Доказываем руками двойное отрицание 10 аксиомы и то же самое для МР.

II.7. Порядки

Определение. Частичный порядок – рефлексивное, антисимметричное, транзитивное отношение.

Определение. Частично упор. мн-во – множество с частичным порядком на элементах.

Определение. Линейно упорядоч. мн-во – множество с частичным порядком, в котором два любых элемента сравнимы.

Определение. Фундированное мн-во – частично упорядоч. множество, в котором каждое непустое подмножество имеет минимальный элемент.

Определение. Вполне упорядоченное множество – фундированное множество с линейным порядком.

II.8. Решетки (все свойства)

Определение. Решетка – это $(L, +, *)$ в алгебраическом смысле и $(L, \leqslant)$ в порядковом.

Решетку можно определить как алгебраическую структуру через аксиомы: коммутативность, ассоциативность, поглощение.

Решетку можно определить как упорядоченное множество через множество с частичным порядком на нем, тогда операции $+$, $*$ определяются как sup и inf:

$$
\begin{aligned}
\sup p &= \min\{u \mid u \geqslant all\ s \in p\} \\
\inf p &= \max\{u \mid u \leqslant all\ s \in p\} \\
a + b &= \sup\{a, b\} \\
a * b &= \inf\{a, b\}
\end{aligned}
$$

Если для двух элементов всегда можно определить $a+b$ и $a*b$, то такое множество назывется решеткой.

Определение. Дистрибутивная решетка – решетка, в которой работает дистрибутивность: $a * (b + c) = (a * b) + (a * c)$

Определение. Импликативная решетка – всегда существует псевдодополнение b ($b \to a$) $a \to b = \max\{c \mid c \times a \leqslant b\}$

Имеет свойства, что в ней всегда есть максимальный элемент $a \to a$ и что она дистрибутивна.

II.9. Булевы/псевдобулевы алгебры

- Булеву алгебру можно определить так:

  1. $(L, +, *, -, 0, 1)$ с выполненными аксиомами – коммутативность, ассоциативность, поглощение, две дистрибутивности и $a * -a = 0$, $a + -a = 1$.
  2. Импликативная решетка над фундированным множеством.

     Тогда мы в ней определим 1 как $a \to a$ (традиционно для импликативной), отрицание как $-a = a \to 0$, и тогда последняя аксиома из предыдущего определения будет свойством:

     $$a * -a = a * (a \to 0) = a * (\max c : c * a \leqslant 0) = a * 0 = 0$$

     Насчет второй аксиомы – должно быть 1. То есть лучше как-то через аксиомы определять, видимо.

     $$a + -a = a + (a \to 0) = a + (\max c : c * a \leqslant 0) = a + 0 = a$$

     // не 1

- Псевдобулева алгебра – это импликативная решетка над фундированным множеством с $\neg a = (a \to 0)$

II.10. Топологическая интерпретация ИИВ

Булеву алгебру и алгебру Гейтинга можно интерпретировать на множестве $\mathbb{R}^n$. Тогда заключения о общезначимости формулы можно делать более наглядно. Давайте возьмем в качестве множества алгебры все открытые подмножества $\mathbb{R}^n$. Определим операции следующим образом:

1. $a + b \coloneqq a \cup b$
2. $a * b \coloneqq a \cap b$
3. $a \to b \coloneqq \mathrm{Int}(a^c \cup b)$
4. $-a \coloneqq \mathrm{Int}(a^c)$
5. $0 \coloneqq \emptyset$
6. $1 \coloneqq \bigcup\{\text{всех мн-в в } L\}$

II.11. Модель Крипке

$Var = \{P, Q, \dots\}$ Модель Крипке – это $\langle W, \leqslant, \nu \rangle$, где

- W – множество «миров»
- $\leqslant$ – частичный порядок на W (отношение достижимости)
- $\nu\colon W \times Var \to \{0, 1, \_\}$ – оценка перменных на W, монотонна (если $\nu(x, P) = 1$, $x \leqslant y$, то $\nu(y, P) = 1$ – формулу нельзя un'вынудить)

  Правила:

- $W, x \vDash P \Leftrightarrow \nu(x, P) = 1$, если $P \in Var$
- $W, x \vDash (A\&B) \Leftrightarrow W, x \vDash A \& W, x \vDash B$
- $W, x \vDash (A \vee B) \Leftrightarrow W, x \vDash A \vee W, x \vDash B$
- $W, x \vDash (A \to B) \Leftrightarrow \forall y \geqslant x (W, y \vDash A \circledcirc W, y \vDash B)$
- $W, x \vDash \neg A \Leftrightarrow \forall y \in x (W, x \neg \vDash A)$

  В мире разрешается быть не вынужденной переменной и ее отрицанию одновремемен-но. Формула называется тавтологией в ИИВ с моделью Крипке, если она истинна (вынуждена) в любом мире любой модели Крипке.

II.12. Вложение Крипке в алгебры Гейтинга

Возьмем модель Крипке, возьмем какое-то объединение поддеревьев со всеми потомками, каждое такое объединение пусть будет входить в алгебру Гейтинга. $\leqslant$ – отношение «быть подмножеством». Определим 0 как $\emptyset$ (пустое объединение поддеревьев); Определим операции:

$$\begin{aligned} + &= \cup, \\ * &= \cap, \\ a \to b &= \bigcup\{z \in H \mid z \leqslant x^c \cup y\} \end{aligned}$$

Так созданное множество с операциями является импликативной решеткой, в которой мы определим $-a = a \to 0$, получим булеву алгебру.

II.13. Полнота ИИВ в алгебрах Гейтинга и моделях Крипке

ИИВ полно относительно алгебр Гейтинга и моделей Крипке.

Общий ход доказательства первого сводится к вложению в Гейтинга алгебры Линденбаума-Тарского, а второго - к построению дизъюнктивного множества всех доказуемых формул, являющегося миром Крипке.

II.14. Нетабличность ИИВ

Не существует полной модели, которая может быть выражена таблицей (конечной – алгебра Гейтинга и Крипке не табличны, так как и там и там связки определяются иначе).

От противного соорудим табличную модель и покажем, что она не полна, приведя пример большой дизъюнкции из импликаций, для которой можно построить модель Крипке в которой она не общезначима.

II.15. Предикаты

Теория первого порядка, расширяющая исчисление высказываний. Добавляются две новые аксиомы $\forall x.A \to A[x := \eta]$, где η свободна для подстановки в A $A[x := \eta] \to \exists x.A$, $-//-$

Правила вывода:

$$\frac{A \to B}{A \to \forall x.B}$$

x не входит сводобно в A

$$\frac{A \to B}{\exists x.A \to B}$$

x не входит свободно в B

II.16. Теорема о дедукции в предикатах

Аналогично 1 теореме о дедукции в ИВ, но в доказательстве должны отсутствовать применения правил для кванторов по переменным входящих свободно в выражение γ

$$\Gamma, \gamma \vdash \alpha \Rightarrow \Gamma \vdash \gamma \to \alpha$$

II.17. Теорема о полноте исчисления предикатов

Исчисление предикатов полно (заметим, что относительно любой модели). Суть в том, что если предикаты непротиворечивы, то у них есть модель. Если у них есть модель, то типа там можно по контрпозиции показать $\models \alpha$.

II.18. Теории первого порядка, определение структуры и модели

Теория первого порядка – это формальная система с кванторами по функциональным символам, но не по предикатам. Рукомахательное определение – это фс с логикой первого порядка в основе, в которой абстрактные предикаты и функциональные символы определяются точно (а может такое определение даже лучше).

Структура по ДГ:
Структурой теории первого порядка мы назовем упорядоченную тройку $\langle D, F, P\rangle$, где F — списки оценок для 0-местных, 1-местных и т.д. функций, и $P = P_0, P_1 \ldots$ — списки оценок для 0-местных, 1-местных и т.д. предикатов, D — предметное множество.

Понятие структуры — развитие понятия оценки из исчисления предикатов. Но оно касается только нелогических составляющих теории; истинностные значения и оценки для связок по-прежнему определяются исчислением предикатов, лежащим в основе теории. Для получения оценки формулы нам нужно задать структуру, значения всех свободных индивидных переменных, и (естественным образом) вычислить результат.

Структура по-моему:
Все то же самое определение из ИВ. Мы просто забиваем на предикаты в ИВ (не определям их), расширяем нашу сигнатуру (добавляя конкретные предикаты и функциональные символы), определяем для нее интерпретацию.

И как всегда,..
Модель – это корректная структура (любое доказуемое утверждение должно быть в ней общезначимо).

II.19. Аксиоматика Пеано

Множество N удовлетворяет аксиоматике Пеано, если:

1. $0 \in N$
2. $x \in N, succ(x) \in N$
3. $\nexists x \in N : (succ(x) = 0)$
4. $(succ(a) = c \& succ(b) = c) \to a = b$
5. $P(0) \& \forall n.(P(n) \to P(succ(n))) \to \forall n.P(n)$

II.20. Формальная арифметика – аксиомы

Формальная арифметика – это теория первого порядка, у которой сигнатура определена как: (циферки, логические связки, алгебр. связки, $'$), а интерпретацию сейчас будем определять. Интерпретация определяет два множества – V, P – истинностные и предметные значения. Пусть множество $V = \{0, 1\}$ по-прежнему. P = {всякие штуки, которые мы можем получать из логических связок и 0}

Определим оценки логических связок естественным образом.

Определим алгебраические связки так:

$$\begin{aligned} +(a, 0) &= a \\ +(a, b') &= (a + b)' \\ *(a, 0) &= 0 \\ *(a, b') &= a * b + a \end{aligned}$$

II.20.1. Аксиомы

1. $a = b \rightarrow a' = b'$
2. $a = b \rightarrow a = c \rightarrow b = c$
3. $a' = b' \rightarrow a = b$
4. $\neg(a' = 0)$
5. $a + b' = (a + b)'$
6. $a + 0 = a$
7. $a * 0 = 0$
8. $a * b' = a * b + a$
9. $\varphi[x := 0] \& \forall x.(\varphi \rightarrow \varphi[x := x']) \rightarrow \varphi$ // φ содержит св.п x

II.21. Рекурсивные функции

$Z(x) = 0$
$N(x) = x + 1$
$U_i^n(x_1, \ldots, x_n) = x_i$
$S\langle f, g_1, \ldots, g_n\rangle(x_1, \ldots, x_m) = f(g_1(x_1 \ldots x_m), \ldots g_n(x_1, \ldots, x_m))$

$$R\langle f, g\rangle(x_1 \ldots x_n, n) = \begin{cases} f(x_1 \ldots x_n) & n = 0 \\ g(x_1 \ldots x_n, n, R\langle f, g\rangle(x_1 \ldots x_n, n-1)) & n > 0 \end{cases}$$

$\mu\langle f\rangle(x_1, \ldots, x_n)$ – минимальное k, такое что $f(x_1 \ldots x_n, k) = 0$

II.22. Функция Аккермана

$$\begin{aligned} A(0,n) &= n+1 \\ A(m,0) &= A(m-1,1) \\ A(m,n) &= A(m-1, A(m,n-1)) \end{aligned}$$

II.23. Существование рек.ф-й не явл. ф-ей Аккермана (определение конечной леммы)

Пусть $f(n_1, \ldots, n_k)$ – примитивная рекурсинвная функция, $k \geqslant 0$.

$$\exists J : f(n_1 \ldots n_k) < A(J, \sum(n_1, \ldots n_k))$$

Доказывается индукцией по рекурсивным функциям.

II.24. Представимость

Функция $f : N^n \to N$ называется представимой в формальной арифметике, если существует отношение $a(x_1 \ldots x_{n+1})$, ее представляющее, причем выполнено следующее:

1. $f(a, b, \ldots) = x \Leftrightarrow \vdash a(\overline{a}, \overline{b}, \ldots, \overline{x})$
2. $\exists! x. f(a, b, \ldots x)$ (вот это свойство вроде бы не обязательно, но ДГ его писал).

II.25. Выразимость

Отношение n называется выразимым, если существует предикат N его выражающий, такой что

1. $n(x_1, \ldots, x_n)$истинно $\Rightarrow \vdash N(\overline{x_1}, \ldots, \overline{x_n})$
2. $n(x_1, \ldots, x_n)$ложно $\Rightarrow \vdash \neg N(\overline{x_1}, \ldots, \overline{x_n})$

II.26. Лемма о связи представимости и выразимости

Если n выразимо, то C_n представимо. $C_n = 1$ если n, и нулю если $!n$

II.27. Бета-функция Гёделя, Г-последовательность

$$\beta(b, c, i) = k_i$$

Функция, отображающая конечную последовательность из $N(a_i)$ в k_i. Работает через магию, математику, простые числа и Гёделеву последовательность, которая подходит под условия китайской теоремы об остатках.

$$\beta(b, c, i) = b\%((i+1) * c + 1)$$

II.28. Представимость рек.ф-й в ФА (знать формулы для самых простых)

Рекурсивные функции представимы в ФА

1. $z(a, b) = (a = a)\&(b = 0)$
2. $n(a, b) = (a = b')$
3. $u_i^n = (x_1 = x_1)\&\ldots\&(x_n = x_n)\&(x_{n+1} = x_i)$
4. $s(a_1 \ldots a_m, b) = \exists b_1 \ldots \exists b_n(G_1(a_1 \ldots a_n, b_1)\&\ldots\&Gn(a_1 \ldots a_m, b_n)$
5. $r(x_1, \ldots, x_n, k, a) =$
$$\begin{aligned}&\exists b\exists c(\exists k(\beta(b, c, 0, k)\&\varphi(x_1, \ldots, x_n, k))\&\\&\quad B(b, c, x_{n+1}, a)\&\\&\quad \forall k(k < x_{n+1} \to \exists d\exists e(B(b, c, k, d)\&B(b, c, k', e)\&G(x_1 \ldots x_n, k, d, e))))\end{aligned}$$
6. $m\langle F\rangle(x_1, \ldots, x_{n+1}) = F(x_1, \ldots, x_n, x_{n+1}, 0)\&\forall y((y < x_{n+1}) \to \neg F(x_1, \ldots, x_n, y, 0))$

II.29. Гёделева нумерация (точно)

a	$\ulcorner a \urcorner$	описание
(	3	
)	5	
,	7	
$\neg$	9	
$\to$	11	
$\vee$	13	
&	15	
$\forall$	17	
$\exists$	19	
x_k	$21 + 6 \cdot k$	переменные
f_k^n	$23 + 6 \cdot 2^k \cdot 3^n$	n-местные функцион. символы (′, +, *)
P_k^n	$25 + 6 \cdot 2^k \cdot 3^n$	n-местные предикаты (=)

II.30. Выводимость и рекурсивные функции (че там с Тьюрингом)

Основные тезисы по вопросу:

- Emulate(input, prog) = plog($R\langle f, g\rangle(\langle\langle S$, input, $0\rangle$, , pb, pc, tb, tc, steps($-//-$)), 1) == F
- Proof(term, proof) = Emulate(proof, MY_PROOFCHECKER)
  &&(plog(proof, len(proof)) = term)
- *Любая представимая в ФА ф-я является рекурсивной*

$$f(x_1, \ldots, x_n) =$$
$$\text{plog}(\langle S\langle G_\varphi, U_{n+1,1}, \ldots, U_{n+1,n}, \text{plog}(U_{n+1,n+1}, 1), \text{plog}(U_{n+1,n+1}, 2)\rangle\rangle(x_1, \ldots, x_n), 1)$$

G_φ тут принимает $n+2$ аргумента: $x_1 \dots x_n, p, b$ и возвращает 0 если p – доказательство $\varphi(x_1 \dots x, p)$, представляющего f.

II.31. Непротиворечивость

Теория непротиворечива, если в ней нельзя одновременно вывести a и $\neg a$. Одновременная выводимость $\neg a$ и a эквивалентна выводимости $a \& \neg a$

II.32. ω-непротиворечивость

Теория ω-непротиворечива, если из $\forall \varphi(x) \vdash \varphi(\overline{x})$ следует $\nvdash \exists p \neg \varphi(p)$. Проще говоря, если мы взяли формулу, то невозможно вывести одновременно $\exists x \neg A(x)$ и $A(0), A(1), \dots$

II.33. Первая теорема Гёделя о неполноте

1. Если формальная арифметика непротиворечива, то недоказуемо $\sigma(\ulcorner \overline{\sigma} \urcorner)$

2. Если формальная арифметика ω-непротиворечива, то недоказуемо $\neg\sigma(\ulcorner \overline{\sigma} \urcorner)$

II.34. Первая теорема Гёделя о неполноте в форме Россера

Если формальная арифметика непротиворечива, то в ней найдется такая формула φ, что $\nvdash \varphi$ и $\nvdash \neg\varphi$

II.35. Consis

Consis – утверждение, формально доказывающее непротиворечивость ФА

То есть $\vdash Consis =>$ непротиворечива

II.36. Условия Г-Б (наизусть)

Пусть $\pi g(x, p)$ выражает $\text{Proof}(x, p)$. $\pi(x) = \exists t.\pi g(x, t)$ действительно показывает, что выражение доказуемо, если

1. $\vdash a => \vdash \pi(\ulcorner \overline{a} \urcorner)$

2. $\vdash \pi(\ulcorner \overline{a} \urcorner) \to \pi\left(\ulcorner \overline{\pi(\ulcorner \overline{a} \urcorner)} \urcorner\right)$

3. $\vdash \pi(\ulcorner \overline{a} \urcorner) \to \pi\left(\ulcorner \overline{(a \to b)} \urcorner\right) \to \pi\left(\ulcorner \overline{b} \urcorner\right)$

II.37. Лемма о самоприменении

$\alpha(x)$ – формула, тогда $\exists b$ такой что

1. $\vdash \alpha\left(\ulcorner\overline{b}\urcorner\right) \to b$

2. $\vdash \beta \to \alpha\left(\ulcorner\overline{b}\urcorner\right)$

II.38. Вторая теорема Гёделя о неполноте ФА

Если теория непротиворечива, в ней $\nvdash \mathrm{Consis}$

II.39. Теория множеств

Теория множеств – теория первого порядка, в которой есть единственный предикат $\in$ (в ФА был =), есть связка $\leftrightarrow$, есть пустое множество, операции пересечения и объединения. $x \cap y = z$, тогда $\forall t(t \in z \leftrightarrow t \in x \& t \in y)$ $x \cup y = z$, тогда $\forall t(t \in z \leftrightarrow t \in x \vee t \in y)$ $D_j(x) \forall a \forall b(a \in x \& b \in x \& a \neq b \to a \cap b = \emptyset)$

II.40. ZFC

II.40.1. Аксиома равенства

$\forall x \forall y \forall z((x = y \& y \in z) \to x \in z)$ Если два множества равны, то любой элемент лежащий в первом, лежит и во втором

II.40.2. Аксиома пары

$\forall x \forall y(\neg(x = y) \to \exists p(x \in p \& y \in p \& \forall z(z \in p \to (x = z \vee y = z))))$ $x \neq y$, тогда сущ. $\{x, y\}$

II.40.3. Аксиома объединений

$\forall x(\exists y(y \in x) \to \exists p \forall y(y \in p \leftrightarrow \exists s(y \in s \& s \in x)))$ Если x не пусто, то из любого семейства множеств можно образовать «кучу-малу», то есть такое множество p, каждый элемент y которого принадлежит по меньшей мере одному множеству s данного семейства s x

II.40.4. Аксиома степени

$\forall x \exists p \forall y(y \in p \leftrightarrow y \in x)$ P(x) – множество степени x (не путать с 2◎ – булеаном) Это типа мы взяли наш x, и из его элементов объединением и пересечением например понаобразовывали кучу множеств, а потом положили их в p.

II.40.5. Схема аксиом выделения

$\forall x \exists b \forall y(y \in b \leftrightarrow (y \in x \& \varphi(y)))$ Для нашего множества x мы можем подобрать множество побольше, на котором для всех элементов, являющихся подмножеством x выполняется предикат.

II.40.6. Аксиома выбора (не входит в ZF по дефолту)

Если $a = Dj(x)$ и $a \neq 0$, то $x \in a \neq 0$

II.40.7. Аксиома бесконечности

$\exists N(\emptyset \in N \& \forall x(x \in N \to x \cup \{x\} \in N))$

II.40.8. Аксиома фундирования

$\forall x(x = \emptyset \vee \exists y(y \in x \& y \cap x = \emptyset))$ $\forall x(x \neq \emptyset \to \exists y(y \in x \& y \cap x = \emptyset))$ Равноценные формулы.

Я бы сказал, что это звучит как-то типа «не существует бесконечно вложенных множеств»

II.40.9. Схема аксиом подстановки

$\forall x \exists ! y.\varphi(x, y) \to \forall a \exists b \forall c(c \in b \leftrightarrow (\exists d.(d \in a \& \varphi(d, c))))$ Пусть формула φ такова, что для при любом x найдется единственный y такой, чтобы она была истинна на x, y, тогда для любого a найдется множество b, каждому элементу которого c можно сопоставить подмножество a и наша функция будет верна на нем и на c Типа для хороших функций мы можем найти множество с отображением из его элементов в подмножество нашего по предикату.

II.41. Ординальные числа, операции

- Определение вполне упорядоченного множества (фундированное с линейный порядком).
- Определение транзитивного множества Множество X транзитивно, если $\forall a \forall b((a \in b \& b \in x) \to a \in x)$
- Ординал – транзитивное вполне упорядоченное отношением $\in$ мн-во
- Верхняя грань множества ординалов S $C|\{C = min(X) \& C \in X \mid X = \{z \mid \forall(y \in S)(z \geqslant y)\}\}$ $C = Upb(S)$ $Upb(\{\emptyset\}) = \{\emptyset\}$
- Successor ordinal (сакцессорный ординал?) Это $b = a' = a \cup \{a\}$
- Предельны ординал Ординал, не являющийся ни 0 ни successor’ом.
- Недостижимый ординал ε – такой ординал, что $\varepsilon = w^{\varepsilon}$

  $\varepsilon_0 = Upb(w, w^w, w^{w^w}, w^{w^{w^w}}, \dots)$ – минимальный из ε
- Канторова форма – форма вида $\sum(a*w^b+c)$, где b – ординал, последовательность строго убывает по b. Есть слабая канторова форма, где вместо $a(a \in N)$ пишут a раз w^b. В канторовой форме приятно заниматься сложениями и прочим, потому что всякие upb – слишком ниочем.

$$
\begin{aligned}
x + 0 &= x \\
x + c' &= (x + c)' \\
x + \lim(a) &= \mathrm{Upb}\{x + c \mid c < a\} \\
x * 0 &= 0 \\
x * c' &= x * c + x \\
x * \lim(a) &= \mathrm{Upb}\{x * c \mid c < a\} \\
x^0 &= 1 \\
x^{c'} &= (x^c) * x \\
x^{\lim(a)} &= \mathrm{Upb}\{x^c \mid c < a\}
\end{aligned}
$$

II.42. Кардинальные числа, операции

Определение. Будем называть множества равномощными, если найдется биекция.

Определение. Будем называть A не превышающим по мощности B, если найдется инъекция $A \to B(|A| \leqslant |B|)$

Определение. Будем называть меньше по мощности, чем B, если $|A| \leqslant |B| \& |A| \neq |B|$

Определение. Кардинальное число – число, оценивающее мощность множества.

Определение. Кардинальное число $\aleph$ – это ординальное число a, такое что $\forall x \leqslant a |x| \leqslant |a|$
$\aleph_0 = w$ по определению; $\aleph_1 =$ минимальный кардинал, следующий за $\aleph_0$

Определение. Кардинальное число $\beth$ – это ординальное число a, такое что $\beth_i = P(\beth_{i-1})$
$\beth_0 = \aleph_0$
$+ : |A| + |B| = \max(|A|, |B|)(\text{если нет общих элементов}) = |A \cup B|$

II.43. Диагональный метод, теорема Лёвенгейма-Скулема

Диагональный метод – метод доказательства $|2^X| > |X|$

II.44. Парадокс Скулема

Мнимый парадокс, базирующийся на теореме Лёвенгейма-Скулема и том факте, что в формальной арифметике существуют несчетные множества. Заковырка в том, что «существует счетное мн-во» выражается в ФА «не существует биекции». И тогда прийти к противоречию нельзя.

II.45. Теорема Генцена о непротиворечивости ФА

Ну типа мы можем обернуть ФА в теорию покруче, доказать что в ней невозможно доказать $0 = 1$, а потом доказать, что если S_∞ непротиворечива, то и S непротиворечива.

1. Ticket 1: ИВ

1.1. Определения (исчисление, высказывание, оценка...)

Формальная система с алгеброй Яськовского J_0 в качестве модели, множество истинностных значений $\{0, 1\}$. Формальная теория нулевого порядка, кванторов нету, предикаты - это пропозициональные переменные.

1.2. Общезначимость, доказуемость, выводимость

- Общезначимость формулы – ее свойство в теории с моделью. Общезначимость можно определить как угодно, в принципе. Например в ИВ общезначимость – это что оценка формулы на любых значениях свободных переменных отображает в 1. В модели крипке - существование формулы во всех мирах и т.д.
- Доказуемость - свойство формулы в теории, значащее, что существует доказательство для этой формулы. Доказательство для теории тоже определяется по разному (последовательность утверждений, каждое из которых есть аксиома или следует по правилу вывода из предыдущих в ИВ, дерево с выводами в $S\infty$)
- Выводимость - в общем случае часто используется как аналог доказуемости, в ИВ это доказуемость из всего, что и ранее + из посылок.

1.3. Схемы аксиом и правило вывода

Аксиомы:

1. $\alpha \to \beta \to \alpha$
2. $(\alpha \to \beta) \to (\alpha \to \beta \to \gamma) \to (\alpha \to \gamma)$
3. $\alpha \to \beta \to \alpha \& \beta$
4. $\alpha \& \beta \to \alpha$
5. $\alpha \& \beta \to \beta$
6. $\alpha \to \alpha \vee \beta$
7. $\beta \to \alpha \vee \beta$
8. $(\alpha \to \beta) \to (\gamma \to \beta) \to (\alpha \vee \gamma \to \beta)$
9. $(\alpha \to \beta) \to (\alpha \to \neg \beta) \to \neg \alpha$
10. $\neg \neg \alpha \to \alpha$

Правило вывода М.Р.:

$$\frac{\alpha \quad (\alpha \to \beta)}{\beta}$$

1.4. Теорема о дедукции

Теорема 1.1. $\Gamma, \alpha \vdash \beta \Leftrightarrow \Gamma \vdash \alpha \to \beta$

Доказательство. $\Rightarrow$ Если нужно переместить последнее предположение вправо, то рассматриваем случаи – аксиома или предположение, МР, это самое выражение.

1. A
   $A \to \alpha \to A$
   $\alpha \to A$

2. (там где-то сзади уже было $\alpha \to A$, $\alpha \to A \to B$)
   $(\alpha \to A) \to (\alpha \to A \to B) \to (\alpha \to B)$
   $(\alpha \to A \to B) \to (a \to B)$
   $\alpha \to B$

3. $\alpha \to \alpha$ умеем доказывать

$\Leftarrow$ Если нужно переместить влево, то перемещаем, добавляем
$A \to B$ (последнее)
A (перемещенное)
B $\square$

1.5. Корректность исчисления высказываний относительно алгебры Яськовского

- Индукцией по доказательству – если аксиома, то она тавтология, все ок. Если модус поненс, то таблица истинности для импликации и все ок

2. Ticket 2: полнота ИВ

2.1. Полнота исчисления высказываний относительно алгебры Яськовского

Кстати полноту можно доказывать маханием руками как для предикатов, и я не могу утверждать, что при таком подходе ИВ не будет полно относительно любой модели.

2.1.1. Контрапозиция

Лемма 2.1. $(\alpha \to \beta) \to (\neg\beta \to \neg\alpha)$

Доказательство. Докажем, что $(\alpha \to \beta), \neg\beta \vdash \neg\alpha$:

(1)	$\alpha \to \beta$	Допущение
(2)	$(\alpha \to \beta) \to (\alpha \to \neg\beta) \to \neg\alpha$	Сх. акс. 9
(3)	$(\alpha \to \neg\beta) \to \neg\alpha$	М.Р. 1,2
(4)	$\neg\beta \to \alpha \to \neg\beta$	Сх. акс. 1
(5)	$\neg\beta$	Допущение
(6)	$\alpha \to \neg\beta$	М.Р. 5,4
(7)	$\neg\alpha$	М.Р. 6,3

После применения теоремы о дедукции 2 раза получим как раз то, что нужно □

2.1.2. Правило исключененного третьего

С помощью контрапозиции доказываем два утверждения:
$\neg(A|\neg A) \to \neg A$ (один раз контрапозицию от этого обратную, там $A \to (A|\neg A)$ акс)
$\neg(A|\neg A) \to \neg\neg A$ Потом девятую аксиому и снимаем двойное отрицание

2.1.3. Всякие очевидные вещи типа если выводится из А и из Б то из А и Б тоже

2.1.4. Правило со звездочкой (14 доказательств)

1. $\alpha, \beta \vdash \alpha \vee \beta$
   α
   $\alpha \to \alpha \vee \beta$
   $\alpha \vee \beta$

2. $\alpha, \neg\beta \vdash \alpha \vee \beta$
   α
   $\alpha \to \alpha \vee \beta$
   $\alpha \vee \beta$

3. $\neg\alpha, \beta \vdash \alpha \vee \beta$
   β
   $\beta \to \alpha \vee \beta$
   $\alpha \vee \beta$

4. $\neg\alpha, \neg\beta \vdash \neg(\alpha \vee \beta)$
   $\neg\alpha$
   $\neg\beta$
   $(\alpha \vee \beta \to \alpha) \to (\alpha \vee \beta \to \neg\alpha) \to \neg(\alpha \vee \beta)$
   $\neg\alpha \to \alpha \vee \beta \to \neg\alpha$
   $\alpha \vee \beta \to \neg\alpha$
   $\neg\alpha, \neg\beta, \alpha \vee \beta \vdash \alpha$
   $\neg\alpha$
   $\neg\beta$
   $\alpha \vee \beta$
   $\alpha \to \alpha$
   … //д-во $\neg\beta, \neg\alpha \vdash \beta \to \alpha$
   $\beta \to \alpha$
   $(\alpha \to \alpha) \to ((\beta \to \alpha) \to (\alpha \vee \beta \to \alpha))$
   $(\beta \to \alpha) \to (\alpha \vee \beta \to \alpha)$
   $\alpha \vee \beta \to \alpha$
   α
   $\alpha \vee \beta \to \alpha$
   $(\alpha \vee \beta \to \neg\alpha) \to \neg(\alpha \vee \beta)$
   $\neg(\alpha \vee \beta)$

5. $\alpha, \beta \vdash \alpha\&\beta$
   α
   β
   $\alpha \to \beta \to \alpha\&\beta$
   $\beta \to \alpha\&\beta$
   $\alpha\&\beta$

6. $\alpha, \neg\beta \vdash \neg(\alpha\&\beta)$
   $\neg\beta$
   $((\alpha\&\beta) \to \beta) \to ((\alpha\&\beta) \to \neg\beta) \to \neg(\alpha\&\beta)$
   $\alpha\&\beta \to \beta$
   $(\alpha\&\beta \to \neg\beta) \to \neg(\alpha\&\beta)$
   $\neg\beta \to \alpha\&\beta \to \neg\beta$
   $\alpha\&\beta \to \neg\beta$
   $\neg(\alpha\&\beta)$

7. $\neg\alpha, \beta \vdash \neg(\alpha\&\beta)$
   аналогично

8. $\neg\alpha, \neg\beta \vdash \neg(\alpha\&\beta)$
   аналогично

9. $\alpha, \beta \vdash \alpha \to \beta$
   β
   $\beta \to \alpha \to \beta$
   $\alpha \to \beta$

10. $\alpha, \neg\beta \vdash \neg(\alpha \to \beta)$
    α
    $\neg\beta$
    $\neg\beta \to ((\alpha \to \beta) \to \neg\beta)$
    $(\alpha \to \beta) \to \neg\beta$
    $\alpha, \neg\beta, \alpha \to \beta \vdash \beta$
    α
    $\alpha \to \beta$
    β
    $(\alpha \to \beta) \to \beta$
    $((\alpha \to \beta) \to \beta) \to ((\alpha \to \beta) \to \neg\beta) \to \neg(\alpha \to \beta)$
    $((\alpha \to \beta) \to \neg\beta) \to \neg(\alpha \to \beta)$
    $\neg\beta \to (\alpha \to \beta) \to \neg\beta$
    $(\alpha \to \beta) \to \neg\beta$
    $\neg(\alpha \to \beta)$

11. $\neg\alpha, \beta \vdash \alpha \to \beta$
    β
    $\beta \to \alpha \to \beta$
    $\alpha \to \beta$

12. $\neg\alpha, \neg\beta \vdash \alpha \to \beta$
    Ну тут типо очевидно (на самом деле тут боль и страдания)

13. $\alpha \vdash \neg\neg\alpha$
    Схема аксиом 9

14. $\neg\alpha \vdash \neg\alpha$
    $\neg\alpha$

3. Ticket 3: ИИВ

3.1. ИИВ, структура, модель

Сигнатура – (R, F, C, r): R – множество символов для предикатов, F – функциональных символов, C – символов констант, r – функция, определяющая арность $x \in R \cup F$.

Интерпретация – это приписывание символам значения и правил действия.

Структура – это носитель M (множество истинностных значений), сигнатура и интерпретация над носителем.

Если все аксиомы верны, то структура корректна. В таком случае она называется моделью.

Выкидываем 10 аксиому, добавляем $\alpha \to \neg\alpha \to \beta$.

Она доказывается и в ИВ.

Лемма 3.1. $\alpha, \alpha \vee \neg\alpha, \neg\alpha \vdash \beta$

(1)	α	Допущение
(2)	$\neg\alpha$	Допущение
(3)	$\alpha \to \neg\beta \to \alpha$	Сх. акс. 1
(4)	$\neg\beta \to \alpha$	М.Р. 1,3
(5)	$\neg\alpha \to \neg\beta \to \neg\alpha$	Сх. акс. 1
(6)	$\neg\beta \to \neg\alpha$	М.Р. 2,5
(7)	$(\neg\beta \to \alpha) \to (\neg\beta \to \neg\alpha) \to (\neg\neg\beta)$	Сх. акс. 9
(8)	$(\neg\beta \to \neg\alpha) \to (\neg\neg\beta)$	М.Р. 4,7
(9)	$\neg\neg\beta$	М.Р. 6,8
(10)	$\neg\neg\beta \to \beta$	Сх. акс. 10
(11)	β	М.Р. 9,10

Таким образом мы умеем доказывать $\alpha \to \alpha \vee \neg\alpha \to \neg\alpha \to \beta$ применив 3 раза теорему о дедукции

Лемма 3.2. $\alpha \to \alpha \vee \neg\alpha \to \neg\alpha \to \beta, \alpha \vee \neg\alpha \vdash \alpha \to \neg\alpha \to \beta$

(1)	$(\alpha \to \alpha \vee \neg\alpha) \to (\alpha \to \alpha \vee \neg\alpha \to (\neg\alpha \to \beta)) \to (\alpha \to (\neg\alpha \to \beta))$	Сх. акс. 2
(2)	$\alpha \vee \neg\alpha \to \alpha \to \alpha \vee \neg\alpha$	Сх. акс. 1
(3)	$\alpha \vee \neg\alpha$	Допущение
(4)	$\alpha \to \alpha \vee \neg\alpha$	М.Р. 3,2
(5)	$(\alpha \to \alpha \vee \neg\alpha \to (\neg\alpha \to \beta)) \to (\alpha \to (\neg\alpha \to \beta))$	М.Р. 4,1
(6)	$\alpha \to \alpha \vee \neg\alpha \to \neg\alpha \to \beta$	Допущение
(7)	$\alpha \to \neg\alpha \to \beta$	М.Р. 6,5

3.2. Опровергаемость исключенного третьего

Вводим в наше множество *истинностных значений* дополнительный элемент $\mathsf{Н}$ (сокращение от слова «Неизвестно»). Отождествим $\mathsf{Н}$ с $\frac{1}{2}$, так что $\mathsf{Л} < \mathsf{Н} < \mathsf{И}$. Определим операции на этом множестве *истинностных значений*:

- конъюнкция: минимум из двух значений (например $\mathsf{И}\&\mathsf{Н} = \mathsf{Н}$).
- дизъюнкция: максимум из двух значений (например $\mathsf{И} \vee \mathsf{Н} = \mathsf{И}$).

- импликация: $\text{И} \to \alpha = \alpha$, $\text{Л} \to \alpha = \text{И}$, $\text{Н} \to \text{Л} = \text{Л}$, $\text{Н} \to \text{Н} = \text{И}$, $\text{Н} \to \text{И} = \text{И}$.

- отрицание: $\neg\text{Н} = \text{Л}$, а для остальных элементов все так же.

Назовем формулу *3-тавтологией*, если она принимает значение И при любых значениях переменных из множества $\{\text{И}, \text{Л}\,\text{Н}\}$. Теперь нужно всего-лишь проверить, что все аксиомы являются 3-тавтологиями и, что если посылка импликации является тавтологией, то и заключение является тавтологией. Второе очевидно по определению тавтологии, а аксиомы просто проверяются вручную.

Значит любая интуиционистски выводимая формула 3-тавтология. Теперь заметим, что формула $\alpha \vee \neg\alpha$ принимает значение Н при $\alpha = \text{Н}$. Следовательно она не 3-тавтология, а значит невыводима.

3.3. Решетки

Просто *решетка* – это $(L, +, *)$ в алгебраическом смысле и $(L, \leqslant)$ в порядковом. Решетку можно определить как алгебраическую структуру через аксиомы:

- Аксиомы идемпотентность
  $\alpha + \alpha = \alpha$
  $\alpha * \alpha = \alpha$

- Аксиомы коммутативности
  $\alpha + \beta = \beta + \alpha$
  $\alpha * \beta = \beta * \alpha$

- Аксиомы ассоциативности
  $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$
  $(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$

- Аксиомы поглощения
  $\alpha + (\alpha * \beta) = \alpha$
  $\alpha * (\alpha + \beta) = \alpha$

Также решетку можно определить как упорядоченное множество с частичным порядком на нем. Тогда операции $+, *$ определяются как sup и inf

$$\sup(\varphi) = \min\{u \mid u \geqslant \forall x \in \varphi\}$$
$$\inf(\varphi) = \max\{u \mid u \leqslant \forall x \in \varphi\}$$
$$\alpha + \beta = \sup(\{\alpha, \beta\})$$
$$\alpha * \beta = \inf(\{\alpha, \beta\})$$

Если для любых двух элементов из множества S можно определить эти две операции, то S называется решеткой.

Дистрибутивная решетка – *решетка*, в которой добавляется дистрибутивность:

$$\alpha * (\beta + \gamma) = \alpha * \beta + \alpha * \gamma$$

Импликативная решетка – *решетка*, в которой для любых двух элементов α и β из множества существует псевдодополнение α относительно β ($\alpha \to \beta$), которое определяется так:

$$\alpha \to \beta = max\{\gamma | \gamma * \alpha \leqslant \beta\}$$

Свойства *импликативной решетки*:

- Существует максимальный элемент $\alpha \to \alpha$, обычно обозначаемый как 1
- Всякая *импликативная решетка* дистрибутивна

3.4. Алгебра Гейтинга, булева алгебра

Булева алгебра – $(L, +, *, -, 0, 1)$, с аксиомами:

- Аксиомы коммутативности
  $\alpha + \beta = \beta + \alpha$
  $\alpha * \beta = \beta * \alpha$
- Аксиомы ассоциативности
  $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$
  $(\alpha * \beta) * \gamma = \alpha * (\beta * \gamma)$
- Аксиомы поглощения
  $\alpha + (\alpha * \beta) = \alpha$
  $\alpha * (\alpha + \beta) = \alpha$
- Аксиомы дистрибутивности
  $\alpha + (\beta * \gamma) = (\alpha + \beta) * (\alpha + \gamma)$
  $\alpha * (\beta + \gamma) = (\alpha * \beta) + (\alpha * \gamma)$
- Аксиомы дополнительности
  $\alpha * \neg\alpha = 0$
  $\alpha + \neg\alpha = 1$

Также *булеву алгебру* можно определить как импликативную решетку над фундированным множеством. Тогда 1 в ней будет $\alpha \to \alpha$, $\neg\alpha = \alpha \to 0$. Тогда $\alpha * \neg\alpha = 0$ будет уже свойством, а $\alpha + \neg\alpha = 1$ все еще аксиомой.

Псевдобулева алгебра (алгебра Гейтинга) – это импликативная решетка над фундированным множеством с $\neg\alpha = \alpha \to 0$ (нет аксиомы $\alpha + \neg\alpha = 1$)

3.5. Алгебра Линденбаума-Тарского

Пусть V – множество формул ИИВ
Порядок для решетки:
$\alpha \leqslant \beta \Leftrightarrow \alpha \vdash \beta$
$\alpha \sim \beta \Leftrightarrow \alpha \vdash \beta$ и $\beta \vdash \alpha$
Определим операции и 0, 1:
0 – $\alpha \& \neg\alpha = \perp$

$1 - \alpha \to \alpha = \top$
$\alpha \& \beta = \alpha * \beta$
$\alpha \vee \beta = \alpha + \beta$
$\neg \alpha = -\alpha$
Получившаяся алгебра называется *алгеброй Линденбаума-Тарского* и является алгеброй Гейтинга, т.к. для нее выполняется аксиома $\alpha * \neg \alpha = 0$ (по определению).

Лемма 3.3. $\forall \beta \in V \perp \vdash \beta$ (Из лжи следует все)

Доказательство. $\alpha \& \neg \alpha \vdash \beta$

(1)	$\alpha \& \neg \alpha$	Допущение
(2)	$\alpha \& \neg \alpha \to \alpha$	Сх. акс. 4
(3)	$\alpha \& \neg \alpha \to \neg \alpha$	Сх. акс. 5
(4)	α	М.Р. 1,2
(5)	$\neg \alpha$	М.Р. 1,3
(6)	$\alpha \to \neg \alpha \to \beta$	Сх. акс. 10
(7)	$\neg \alpha \to \beta$	М.Р. 4,6
(8)	β	М.Р. 5,7

□

3.6. Теорема о полноте ИИВ относительно алгебры Гейтинга

Возьмем в качестве алгебры Гейтинга алгебру Линденбаума-Тарского - ξ. Она очевидно является моделью.

Теорема 3.4. $\models \alpha \Rightarrow \vdash \alpha$

Доказательство. $\models \alpha \Rightarrow [\![\alpha]\!]^{\xi} = 1$
$[\![\alpha]\!]^{\xi} = 1 \Rightarrow 1 \leqslant [\![\alpha]\!]^{\xi}$ (По определению алгебры Л-Т)
$\beta \to \beta \vdash \alpha$ (По определению $\leqslant$ в алгебре Л-Т)
Т.к. $\beta \to \beta$ - тавтология, то и α - тавтология □

3.7. Дизъюнктивность ИИВ

Используем алгебру Гёделя $\Gamma(A)$ (γ - функция преобразования). Можно преобразовать любую алгебру Гейтинга, возьмем алгебру Л-Т. Алгебра Гёделя использует функцию преобразования: $\gamma(a) = b$ значит, что в алгебре A элементу a соответствует элемент b из алгебры Гёделя. Порядок сохраняется естественным образом. Также добавим еще один элемент ω ($\gamma(1) = \omega$). Таким образом $\Gamma(A) = A \cup \{\omega\}$. Порядок в $\Gamma(A)$:

- $\forall a \in \Gamma(A) \setminus \{1\}\ a \leqslant \omega$
- $\omega \leqslant 1$

$a + b$	$b = 1$	$b = \gamma(v)$
$a = 1$	1	1
$a = \gamma(u)$	1	$\gamma(u + v)$

$a * b$	$b = 1$	$b = \gamma(v)$
$a = 1$	1	$\gamma(a * v)$
$a = \gamma(u)$	$\gamma(u * b)$	$\gamma(u * v)$

$a \to b$	$b = 1$	$b = \gamma(v)$
$a = 1$	1	$\gamma(a \to v)$
$a = \gamma(u)$	1	$u \to v$

a	$\neg a$
$a = 1$	$\gamma(\neg a)$
$a = \gamma(u)$	$\neg u$

Лемма 3.5. Гёделева алгебра является Гейтинговой

Доказательство. Необходимо просто доказать аксиомы коммутативности, ассоциативности и поглощения. □

Теорема 3.6. $\vdash \alpha \vee \beta \Rightarrow$ *либо* $\vdash \alpha$, *либо* $\vdash \beta$

Доказательство. Возьмем A, построим $\Gamma(A)$. Если $\vdash \alpha \vee \beta$, то $[\![\alpha \vee \beta]\!]^{A} = 1$ и $[\![\alpha \vee \beta]\!]^{\Gamma(A)} = 1$. Тогда по определению $+$ в алгебре Гёделя, $[\![\alpha]\!]^{\Gamma(A)} = 1$, либо $[\![\beta]\!]^{\Gamma(A)} = 1$. Тогда оно такое же и в алгебре Л-Т, а алгебра Л-Т полна. □

3.8. Теорема Гливенко

Теорема 3.7. Если в ИВ доказуемо α, то в ИИВ доказуемо $\neg\neg\alpha$.

Доказательство. Разберем все втречающиеся в изначальном доказательстве формулы

1. Заметим, что если в ИИВ доказуемо α, то $\neg\neg\alpha$ так же доказуемо.

   Докажем, что $\alpha \vdash \neg\neg\alpha$

(1)	α	Допущение
(2)	$\alpha \to \neg\alpha \to \alpha$	Сх. акс. 1
(3)	$\neg\alpha \to \alpha$	М.Р. 1,2
(4)	$\neg\alpha \to (\neg\alpha \to \neg\alpha)$	Сх. акс. 1
(5)	$(\neg\alpha \to (\neg\alpha \to \neg\alpha)) \to (\neg\alpha \to ((\neg\alpha \to \neg\alpha) \to \neg\alpha)) \to (\neg\alpha \to \neg\alpha)$	Сх. акс. 2
(6)	$(\neg\alpha \to ((\neg\alpha \to \neg\alpha) \to \neg\alpha)) \to (\neg\alpha \to \neg\alpha)$	М.Р. 4,5
(7)	$(\neg\alpha \to ((\neg\alpha \to \neg\alpha) \to \neg\alpha))$	Сх. акс. 1
(8)	$\neg\alpha \to \neg\alpha$	М.Р. 7,6
(9)	$(\neg\alpha \to \alpha) \to (\neg\alpha \to \neg\alpha) \to \neg\neg\alpha$	Сх. акс. 9
(10)	$(\neg\alpha \to \neg\alpha) \to \neg\neg\alpha$	М.Р. 3,9
(11)	$\neg\neg\alpha$	М.Р. 8,10

   Значит, если α – аксиома с 1-ой по 9-ую, то $\neg\neg\alpha$ также может быть доказано

2. Пусть α получилось по 10-ой аксиоме $\neg\neg\alpha \to \alpha$. Докажем, что $\vdash \neg\neg(\neg\neg\alpha \to \alpha)$

(1)	$\alpha \to \neg\neg\alpha \to \alpha$	Сх. акс. 1
(2)	$\neg(\neg\neg\alpha \to \alpha) \to \neg\alpha$	Контрпозиция
(3)	$\neg\alpha \to \neg\neg\alpha \to \alpha$	Сх. акс. 10
(4)	$\neg(\neg\neg\alpha \to \alpha) \to \neg\neg\alpha$	Контрпозиция
(5)	$(\neg(\neg\neg\alpha \to \alpha) \to \neg\alpha) \to (\neg(\neg\neg\alpha \to \alpha) \to \neg\neg\alpha) \to \neg\neg(\neg\neg\alpha \to \alpha)$	Сх. акс. 9
(6)	$(\neg(\neg\neg\alpha \to \alpha) \to \neg\neg\alpha) \to \neg\neg(\neg\neg\alpha \to \alpha)$	М.Р. 2,5
(7)	$\neg\neg(\neg\neg\alpha \to \alpha)$	М.Р. 4,6

3. Приведем конструктивное доказательство:

   - Если α - аксиома, то $\neg\neg\alpha$ доказывается с помощью 1-го и 2-го пунктов
   - Если был применен М.Р., то в изначальном доказательстве были α, $\alpha \to \beta$, β. По индукционному предположению мы знаем, что $\neg\neg\alpha$, $\neg\neg(\alpha \to \beta)$. Нужно доказать

$\neg\neg\beta$.
Давайте для начала докажем, что

$$\neg\neg\alpha, \neg\neg(\alpha \to \beta), \neg\beta, \alpha, \alpha \to \beta \vdash \beta$$

.

(1)	α	Допущение
(2)	$\alpha \to \beta$	Допущение
(3)	β	М.Р. 1,2

Значит мы знаем, что $\neg\neg\alpha, \neg\neg(\alpha \to \beta), \neg\beta, \alpha \vdash (\alpha \to \beta) \to \beta$. Теперь докажем, что

$$\neg\neg\alpha, \neg\neg(\alpha \to \beta), \neg\beta, \alpha, (\alpha \to \beta) \to \beta \vdash \neg(\alpha \to \beta.)$$

(1)	$((\alpha \to \beta) \to \beta) \to ((\alpha \to \beta) \to \neg\beta) \to \neg(\alpha \to \beta)$	Сх. акс. 9
(2)	$((\alpha \to \beta) \to \beta)$	Допущение
(3)	$\neg\beta \to (\alpha \to \beta) \to \neg\beta$	Сх. акс. 1
(4)	$\neg\beta$	Допущение
(5)	$(\alpha \to \beta) \to \neg\beta$	М.Р. 4,3
(6)	$((\alpha \to \beta) \to \neg\beta) \to \neg(\alpha \to \beta)$ М.Р. 2,1	
(7)	$\neg(\alpha \to \beta)$ М.Р. 5,6	

Теперь мы знаем, что $\neg\neg\alpha, \neg\neg(\alpha \to \beta), \neg\beta \vdash \alpha \to \neg(\alpha \to \beta)$. Докажем, что

$$\neg\neg\alpha, \neg\neg(\alpha \to \beta), \neg\beta, \alpha \to \neg(\alpha \to \beta) \vdash \neg\alpha.$$

(1)	$(\alpha \to \neg(\alpha \to \beta)) \to (\alpha \to \neg\neg(\alpha \to \beta)) \to \neg\alpha$	Сх. акс. 9
(2)	$\alpha \to \neg(\alpha \to \beta)$	Допущение
(3)	$\neg\neg(\alpha \to \beta) \to \alpha \to \neg\neg(\alpha \to \beta)$	Сх. акс. 1
(4)	$\neg\neg(\alpha \to \beta)$	Допущение
(5)	$\alpha \to \neg\neg(\alpha \to \beta)$	М.Р. 4,3
(6)	$(\alpha \to \neg\neg(\alpha \to \beta)) \to \neg\alpha$	М.Р. 2,1
(7)	$\neg\alpha$	М.Р.5,6

Теперь мы знаем, что $\neg\neg\alpha, \neg\neg(\alpha \to \beta) \vdash \neg\beta \to \neg\alpha$. Наконец докажем, что

$$\neg\neg\alpha, \neg\neg(\alpha \to \beta), \neg\beta \to \neg\alpha \vdash \neg\neg\beta$$

(1)	$(\neg\beta \to \neg\alpha) \to (\neg\beta \to \neg\neg\alpha) \to \neg\neg\beta$	Сх. акс. 9
(2)	$\neg\beta \to \neg\alpha$	Допущение
(3)	$\neg\neg\alpha \to \neg\beta \to \neg\neg\alpha$	Сх. акс. 1
(4)	$\neg\neg\alpha$	Допущение
(5)	$\neg\beta \to \neg\neg\alpha$	М.Р. 4,3
(6)	$(\neg\beta \to \neg\neg\alpha) \to \neg\neg\beta$	М.Р. 2,1
(7)	$\neg\neg\beta$	М.Р. 5,6

□

3.9. Топологическая интерпретация

Булеву алгебру и алгебру Гейтинга можно интерпретировать на множестве $\mathbb{R}^n$. Тогда заключения о общезначимости формулы можно делать более наглядно. Давайте возьмем в качестве множества алгебры все открытые подмножества $\mathbb{R}^n$. Определим операции следующим образом:

- $\alpha + \beta = \alpha \cup \beta$
- $\alpha * \beta = \alpha \cap \beta$
- $\alpha \to \beta = \mathtt{Int}(\alpha^c \cup \beta)$
- $-\alpha = \mathtt{Int}(\alpha^c)$
- $0 = \emptyset$
- $1 = \cup\{V \subset L\}$

4. Ticket 4: ИИВ2

4.1. Модели Крипке

W – множество миров
V – множество вынужденных переменных
Введем отношение частичного порядка на W - $\leqslant$ (отношение достижимости). И введем оценку переменной $\nu : W \times V \to \{0, 1\}$. ν должна быть монотонна (Если $\nu(x, P) = 1$ и $x \leqslant y$, то $\nu(y, P) = 1$). Если преременная x истинна в мире w, то мы пишем $w \Vdash x$.
Модель Крипке – это $\langle W, \leqslant, \nu \rangle$.
Теперь можно определить истинность любой формулы (в данном мире) индукцией по построению формулы. Правила:

- $w \Vdash A \& B \Leftrightarrow w \Vdash A$ и $w \Vdash B$;
- $w \Vdash A \vee B \Leftrightarrow w \Vdash A$ *или* $w \Vdash B$;
- $w \Vdash A \to B \Leftrightarrow$ в любом мире $u \geqslant w$, в котором истинна A, так же истинна и B;
- $w \Vdash \neg A \Leftrightarrow$ ни в каком мире $u \geqslant w$ формула A не является истинной;

4.2. Корректность ИИВ относительно моделей Крипке

Теорема 4.1. Если формула выводима в ИИВ, то она истинна в моделях Крипке.

Доказательство. Проверим М.Р. и аксиомы (что они истинны во всех мирах):

- М.Р.: по определению импликации в моделях Крипке, если в мире истинно A, $A \to B$, то истинно и B
- Аксиомы:
  1. $A \to (B \to A)$
     Пусть где-нибудь истинна A, в силу монотонности она истинна во всех бо́льших мирах, так что $B \to A$ тоже будет истинно.
  2. $(A \to B) \to ((A \to (B \to C)) \to (A \to C))$
     Пусть где-нибудь истинно $A \to B$, тогда необходимо доказать, что истинно и $((A \to (B \to C)) \to (A \to C))$.
     – Пусть истинны A, B. Тогда если истинно $A \to (B \to C)$, то истинно и C по монотонности A и B. A, B, C истинны, значит $A \to C$ истинно.
     – Пусть не истинны ни A, ни B. Тогда $A \to (B \to C)$ не истинно и C не истинно. Значит $A \to C$ не может быть истинно, т.к. ни A, ни B, ни C не истинны. Сомнение насчет этого места
  3. Подобным образом доказываем все аксиомы

□

4.3. Вложение Крипке в Гейтинга

Не нужно (Д.Г. обещал не спрашивать это)

4.4. Полнота ИИВ в моделях Крипке

Теорема 4.2. ИИВ полно относительно моделей Крипке

Доказательство. Докажем в несколько шагов

1. *Дизъюнктивное множество* M – такое множество, что если в $M \vdash a \vee b$, то $a \in M$ или $b \in M$.

   Лемма 4.3. $M \vdash a \Rightarrow a \in M$

   Доказательство. Пусть это не так. Рассмотрим $a \to a \vee \neg a$. Раз $M \vdash a$, то $M \vdash a \vee \neg a$. Т.к. $a \notin M$, то $\neg a \in M$ по определению дизъюнктивности M. Но тогда из $M \vdash a$ и $M \vdash \neg a$ мы можем доказать, что $M \vdash a \& \neg a$. □

2. Возьмем множество всех дизъюнктивных множеств с формулами из ИИВ. Мы можем это сделать, т.к. ИИВ дизъюнктивно. Для любого элемента $W_i \vdash a, a \in W_i$, значит в этом мире a вынуждено. Построим дерево с порядком «быть подмножеством». Докажем, что это множество - модель Крипке. Проверим 5 свойств:

   (а) $W, x \Vdash P \Leftrightarrow \nu(x, P) = 1$ если $P \in V$ (V - множество вынужденных переменных). Монотонность выполняется по определению дерева

   (б) $W, x \Vdash (A \& B) \Leftrightarrow W, x \Vdash A$ и $W, x \Vdash B$
   С помощью аксиомы $A \& B \to A$ доказываем $W \vdash A$, значит $A \in W$. Аналогично с B

   (в) $W, x \Vdash (A \vee B) \Leftrightarrow W, x \Vdash A$ или $W, x \Vdash B$
   Очевидно по определению дизъюнктивности

   (г) $W, x \Vdash (A \to B) \Leftrightarrow \forall y \geqslant x (W, y \Vdash A \Rightarrow W, y \Vdash B)$
   Мы знаем, что $W \vdash A \to B$. Пусть в W есть A, тогда по M.P. докажем, что B. Пусть в W есть B, тогда мы уже получили B.

   (д) $W, x \Vdash \neg A \Leftrightarrow \forall y \geqslant x (W, x \nVdash A)$
   Если где-то оказалось A, то оно доказуемо, а значит мы сможем доказать и $A \& \neg A$

3. $\Vdash A$, тогда $W_i \Vdash A$. Рассмотрим $W_0 = \{$все тавтологии ИИВ$\}$. $W_0 \Vdash A$, т.е. $\vdash A$.

□

4.5. Нетабличность интуиционистской логики

Теорема 4.4. Не существует полной модели, которая может быть выражена таблицей

Доказательство. Докажем от противного. Построим табличную модель и докажем, что она не полна. В ИВ мы обычно пользуемся алгеброй J_0 Яськовского $V = \{0, 1\}$, $0 \leqslant 1$.
Пусть имеется $V = \{...\}$, $|V| = n$ - множество истиностных значений. Пусть его размер больше 2. Тогда построим формулу $\bigvee_{(1 \leqslant j < i \leqslant n+1)}(p_i \to p_j)$ - такая большая дизъюнкция из импликаций

1. Она общезначима, т.к. всего таких импликаций у нас будет $C_n^2 >= n$ (по принципу Дирихле встретятся два одинаковых значения и она будет верна, тогда все выражение будет верно)

2. Недоказуемость. Построим такую модель Крипке, в которой она будет не общезначима.
   J_0 - алгебра Яськовского. Определим последовательность алгебр L_n по следующим правилам: $L_0 = J_0$, $L_n = \Gamma(L_{n-1})$. Таким образом L_n - упорядоченное множество $\{0, w_1, w_2, ..., 1\}$. Пусть f - оценка в L_n, действующая по следующим правилам на нашу формулу: $f(a_1) = 0$, $f(a_{n+1}) = 1$, $f(a_i) = w_i$ при $j < i : f(a_i \to a_j) = f(a_i) \to f(a_j) = f(a_j)$. Последнее выражение не может являться 1, так что формула недоказуема. (ИИВ полно относительно алгебры Гейтинга)

$\square$

5. Ticket 5: *Логика 2 порядка*

5.1. Основные определения

Смотрим коснпект ДГ

5.2. Теорема о дедукции

Теорема 5.1. Если $\Gamma, \alpha \vdash \beta$, и в доказательстве отсутствуют применения правил для кванторов, использующих свободные переменные из формулы α, то $\Gamma \vdash \alpha \to \beta$

Доказательство. Будем рассматривать формулы в порядке сверху вниз. На i-ой строке встретили формулу δ_i. Тогда докажем, что $\alpha \to \delta_i$. Разберем случаи:

1. δ_i - старая аксиома, совпадает с α или выводится по правилу М.Р.
   Тогда мы знаем, что делать из Теоремы о дедукции для ИВ

2. δ_i - новая аксиома
   Тогда все то же самое, что и в старой аксиоме, но нужно так же проверить условие.

3. $\exists x(\psi) \to \varphi$ - новое правило вывода

   - Докажем вспомогательную лемму:

     Лемма 5.2. $(\alpha \to (\beta \to \gamma)) \to (\beta \to (\alpha \to \gamma))$

     Доказательство. Докажем, что $\alpha \to (\beta \to \gamma), \beta, \alpha \vdash \gamma$:

(1)	$\alpha \to \beta \to \gamma$	Допущение
(2)	α	Допущение
(3)	$\beta \to \gamma$	М.Р. 2,1
(4)	β	Допущение
(5)	γ	М.Р. 4,3

     □

   - По индукционному преположению мы знаем, что $\alpha \to \psi \to \varphi$. Тогда докажем, что $\alpha \to \psi \to \varphi, (\alpha \to \psi \to \varphi) \to (\psi \to \alpha \to \varphi) \vdash \alpha \to \exists x(\psi) \to \varphi$:

(1)	$(\alpha \to \psi \to \varphi) \to (\psi \to \alpha \to \varphi)$	Допущение
(2)	$\alpha \to \psi \to \varphi$	Допущение
(3)	$\psi \to \alpha \to \varphi$	М.Р. 2,1
(4)	$\exists x(\psi) \to \alpha \to \varphi$	Правило вывода 1
(5)	$(\exists x(\psi) \to \alpha \to \varphi) \to (\alpha \to \exists x(\psi) \to \varphi)$	Допущение
(6)	$\alpha \to \exists x(\psi) \to \varphi$	М.Р. 4,5

4. $\varphi \to \forall x(\psi)$ - новое правило вывода

   - Докажем вспомогательную лемму 1

     Лемма 5.3. $(\alpha \& \beta \to \gamma) \to (\alpha \to \beta \to \gamma)$

Доказательство. Докажем, что $(\alpha\&\beta \to \gamma), \alpha, \beta \vdash \gamma$:

(1)	α	Допущение
(2)	β	Допущение
(3)	$\alpha \to \beta \to \alpha\&\beta$	Сх. акс. 1
(4)	$\beta \to \alpha\&\beta$ М.Р. 1,3	
(5)	$\alpha\&\beta$	М.Р. 2,4
(6)	$\alpha\&\beta \to \gamma$	Допущение
(7)	γ	М.Р. 5,6

$\square$

- Докажем вспомогателньую лемму 2

  Лемма 5.4. $(\alpha \to \beta \to \gamma) \to (\alpha\&\beta \to \gamma)$

  Доказательство. Докажем, что $\alpha \to \beta \to \gamma, \alpha\&\beta \vdash \gamma$:

(1)	$\alpha\&\beta \to \alpha$	Сх. акс. 4
(2)	$\alpha\&\beta$	Допущение
(3)	α	М.Р. 2,1
(4)	$\alpha\&\beta \to \beta$	Сх. акс. 5
(5)	β	М.Р. 2,4
(6)	$\alpha \to \beta \to \gamma$	Допущение
(7)	$\beta \to \gamma$	М.Р. 3,6
(8)	γ	М.Р. 5,7

$\square$

- По индукционному предположению мы знаем, что $\alpha \to \psi \to \varphi$. Тогда докажем, что $\alpha \to \psi \to \varphi \vdash \alpha \to \psi \to \forall(\varphi)$.

(1)	$(\alpha \to \psi \to \varphi) \to (\alpha\&\psi \to \varphi)$	Вспомогательная лемма 1
(2)	$\alpha \to \psi \to \varphi$	Допущение
(3)	$\alpha\&\psi \to \varphi$	М.Р. 2,1
(4)	$\alpha\&\psi \to \forall(\varphi)$	Правило вывода 2
(5)	$(\alpha\&\psi \to \forall(\varphi)) \to (\alpha \to \psi \to \forall(\varphi))$	Вспомогательная лемма 2
(6)	$\alpha \to \psi \to \forall(\varphi)$	М.Р. 4,5

$\square$

5.3. Корректность исчисления предикатов

Смотрим конспект ДГ

6. Ticket 6: Полнота исчисления предикатов

Тут можно почитать конспект Д.Г.

6.1. Свойства противоречивости

Противоречивая теория – теория, в которой можно вывести p, ¬p.

Лемма 6.1. Теория противоречива $\Leftrightarrow$ в ней выводится $a\&\neg a$

Доказательство. $\Leftarrow$ Если выводится $a\&\neg a$, то противоречива – очевидно через аксиомы
$\Rightarrow$ Если противоречива, то выводится $a\&\neg a$

(1)	$\neg\alpha$	Допущение
(2)	α	Допущение
(3)	$\alpha \to \neg\alpha \to (\alpha\&\neg\alpha)$	Сх. акс. 10
(4)	$\neg\alpha \to (\alpha\&\neg\alpha)$	М.Р. 1,3
(5)	$\alpha\&\neg\alpha$	М.Р. 2,4

□

Заметим, что всякое подмножество непротиворечивого множества непротиворечиво.
Заметим, что всякое бесконечное прот. множество содержит конечное противоречивое подмножество ввиду конечности вывода.
Совместное множество – множество с моделью (все формулы множества верны в какой-либо интерпретации).

6.2. Лемма о дополнении непротиворечивого множества

Лемма 6.2. Для всякого непротиворечивого множества Γ замкнутых формул сигнатуры σ существует множество Γ', являющееся к тому же полным, имеющее ту же сигнатуру и содержащее Γ.

Доказательство. Для не более чем счетных сигнатур:
Давайте добавлять недостающие формулы в Γ – если есть формула α, добавим α или $\neg\alpha$ в зависимости от того, является ли $\Gamma \cup \alpha$ или $\Gamma \cup \neg\alpha$ противоречивым или нет (выберем непротиворечивый вариант). Одно всегда верно, потому что:

1. $\Gamma \cup \alpha$, $\Gamma \cup \neg\alpha$ противоречивы обе $\Rightarrow$ Мы можем доказать, что Γ изначально было противоречиво

2. $\Gamma \cup \alpha$, $\Gamma \cup \neg\alpha$ не противоречивы обе $\Rightarrow$ Тогда можно сказать, что $\alpha \to \neg\alpha \to \alpha\&\neg\alpha$.

□

6.3. Условие о интерпретации непротиворечивого мн-ва

Будем называть интерпретацией непротиворечивого множества формул функцию оценки, тождественно равную 1 на элементах из этого множества. Будем говорить, что $\Gamma \models \alpha$, если она тождественна в любой модели Γ.

6.4. Несколько лемм

Лемма 6.3. $\Gamma \vdash \alpha \Rightarrow \Gamma \vDash \alpha$

Доказательство. Механическая проверка аксиом □

Лемма 6.4. Если у Γ есть модель, то Γ непротиворечиво

Доказательство. Пусть Γ имеет модель, но противоречиво, тогда из Γ выводится $\alpha, \neg\alpha$, по корректности $\Gamma \vDash \alpha, \neg\alpha$, но формула и ее отрицание не могут быть общезначимыми одновременно. □

Лемма 6.5. Пусть Γ – полное непротиворечивое множество бескванторных формул. Тогда существует модель для Γ.

Доказательство. Построим модель структурной индукцией по формулам.
Предметное множество – строки, содержащие выражения.
Например $[\![c_1]\!] =$ «c_1», $[\![f_1(c_1, f_2(c_2))]\!] =$ «$f_1(c_1, f_2(c_2))$»

Мы не хотим заниматься подсчетом, а предпочитаем оставлять то, что нужно вычислить как отдельную функцию. Рассмотрим формулу – предикат. Его оценка истина, если он принадлежит носителю, ложна если его отрицание в носителе (в предметном множестве). Элементы всегда входят противоречиво (элемент не вдохит со своим отрицанием. Связки определим естественным образом. Докажем, что $\gamma \in \Gamma \Leftrightarrow \gamma$ истинна (Γ – предметное множество)

- База:
  Если атомарная формула лежит в Γ, то она истинна по определению.
  Если атомарная формула истинна, то лежит в Γ

- Переход:

  1. $\alpha\&\beta$

     Если $\alpha\&\beta$ лежит в Γ, то оно истинно по определению

     – Пусть $[\![\alpha\&\beta]\!] = \text{И}$, тогда покажем, что $\alpha\&\beta \in \Gamma$.
       По таблице истинности & ясно, что $[\![\alpha]\!] = \text{И}$ и $[\![\beta]\!] = \text{И}$. Тогда α и β лежат в Γ по индукционному предположению. Тогда с помощью $\alpha \to \beta \to \alpha\&\beta$ можно показать, что и $\alpha\&\beta \in \Gamma$.

     – Пусть $[\![\alpha\&\beta]\!] = \text{Л}$, тогда покажем, что $\neg(\alpha\&\beta) \in \Gamma$.
       По таблице истинности & ясно, что $[\![\alpha]\!] = \text{Л}$ или $[\![\beta]\!] = \text{Л}$. Для определенности возьмем, что α – ложь. Тогда $\neg\alpha$ лежат в Γ по индукционному предположению.
       Докажем, что $\neg\alpha \vdash \neg(\alpha\&\beta)$:

(1)	$\neg\alpha$	Предположение
(2)	$\neg\alpha \to \alpha\&\beta \to \neg\alpha$	Сх. акс. 1
(3)	$\alpha\&\beta \to \neg\alpha$	М.Р. 1,2
(4)	$\alpha\&\beta \to \alpha$	Сх. акс. 4
(5)	$(\alpha\&\beta \to \alpha) \to (\alpha\&\beta \to \neg\alpha) \to \neg(\alpha\&\beta)$	Сх. акс. 9
(6)	$(\alpha\&\beta \to \neg\alpha) \to \neg(\alpha\&\beta)$	М.Р. 5,4
(7)	$\neg(\alpha\&\beta)$	М.Р. 6,3

  2. $\alpha \vee \beta$

- $[\![\alpha \vee \beta]\!] =$ И. Тогда по таблице истинности $\vee$ либо $[\![\alpha]\!] =$ И, либо $[\![\beta]\!] =$ И. Не умаляя общности скажем, что $[\![\alpha]\!] =$ И. Тогда $\alpha \in \Gamma$ по предположению индукции. Легко можно доказать, что и $\alpha \vee \beta \in \Gamma$ с помощью $\alpha \to \alpha \vee \beta$.
- $[\![\alpha \vee \beta]\!] =$ Л. Тогда по таблице истинности $\vee$ и $[\![\alpha]\!] =$ Л, и $[\![\beta]\!] =$ Л. Тогда $\neg\alpha \in \Gamma$ и $\neg\beta \in \Gamma$ по предположению индукции. С помощью 9-ой схемы аксиом мы можем доказать, что и $\neg(\alpha \vee \beta) \in \Gamma$.

3. Аналогично нужно доказать все связки

□

6.5. Построение Γ^*

Теорема 6.6. Можно построить из нашего множества формул множество бескванторных формул

Доказательство. Для этого определим такую операцию избавления от 1 квантора: Построим новый язык, отличающийся от нашего контантами, там будут d_i^j, где нижний индекс – это поколение, верхний – нумерационный. Возьмем непротиворечивое множество формул Γ_i и пополним его, получив непротиворечивое множество формул Γ_{i+1}, такое что $\Gamma_i \subset \Gamma_{i+1}$. Возьмем формулу $\gamma \in \Gamma_i$. Рассмотрим случаи:

1. Не содержит кванторов
   Тогда делать ничего не нужно

2. $\gamma = \forall x(a)$
   Тогда возьмем все константы, использующиеся в Γ_i – это будут c_i, d_a^j, где $a \leqslant i$. Занумеруем их $\theta_1, \theta_2, \ldots$. И добавим формулы $a_1 = a[x := \theta_1], \ldots$ к Γ_{i+1}.

3. $\gamma = \exists x(a)$
   Тогда возьмем новую константу d_{i+1}^j и добавим $a[x := d_{i+1}^j]$ к Γ_{i+1}.

Заметим, что сами формулы с кванторами мы не выкидываем – ведь в будущем появятся новые формулы, и процесс для уже использованных кванторных формул нужно будет повторить. Покажем, что полученные множества остаются непротиворечивыми. Γ_i непротиворечиво, а Γ_{i+1} противоречиво, тогда $\Gamma_{i+1} \vdash \alpha\&\neg\alpha$, тогда выпишем конечное доказательство, найдем посылки, новые в Γ_{i+1}, которых нету в Γ_i, выпишем их и впихнем направо по теореме о дедукции: $\Gamma_i \vdash \gamma_1 \to \gamma_2 \to \gamma_3 \to \cdots \to \gamma_n \to \beta\&\neg\beta$ Новые посылки у нас получаются только из пунктов 2 и 3.

1. $\gamma_1 = a[x := \theta_1]$ из $\forall x(a)$. Тогда рассмотрим доказательство:

(1)	$\forall x\alpha \to \alpha[x := \theta]$	Сх. акс. $\forall$
(2)	$\forall x\alpha$	$\forall x\alpha$ из Γ_g
(3)	$\alpha[x := \theta]$	М.Р. 2, 1
$(4 \ldots k)$	$\alpha[x := \theta] \to (\gamma_2 \to \ldots \gamma_n \to \beta\&\neg\beta)$	Исх. формула
$(k+1)$	$\gamma_2 \to \ldots \gamma_n \to \beta\&\neg\beta$	М.Р. 3, k

2. $\gamma_1 = a[x := d_{i+1}^k]$ из $\exists x(a)$ выберем переменную, не участвующую в выводе противоречия – z. Заменим все вхождения d^k в д-ве на z. Поскольку d_{i+1}^k – константа, мы можем

делать такие замены. Поскольку z – константа, специально введенная для замены и раньше не встречавшаяся, то она отсутствует в $\gamma_2, \dots$ + мы можем правильно выбрать b, чтобы и в нем отсутствовала d_{i+1}^k. Значит мы можем применить правило для выведения $\exists$:

$(1 \dots k)$	$\alpha[x := y] \to (\gamma_2 \to \dots \gamma_n \to \beta \& \neg\beta)$	Исх. формула
$(k+1)$	$\exists y \alpha[x := y] \to (\gamma_2 \to \dots \gamma_n \to \beta \& \neg\beta)$	Правило для $\exists$
$(k+2)$	$\exists x \alpha$	Т.к. $\exists x \alpha$ из Γ_g
$(k+3 \dots l)$	$\exists y \alpha[x := y]$	Доказуемо
$(l+1)$	$\gamma_2 \to \dots \gamma_n \to \beta \& \neg\beta$	М.Р. $l, k+1$

Возьмем $\Gamma_0 = \Gamma$. $\Gamma^* = \cup \Gamma_i$. Γ^* также не противоречиво, потому что д-во использует конечное количество предположений, добавленных на каком-то шаге j максимум, значит множество $_j$ тоже противоречиво, что невозможно по условию. □

6.6. Доказательство того, что дополненное бескванторное подмножество Γ^* – модель для Γ

Теорема 6.7. Дополненное бескванторное подмножество Γ^* – модель для Γ

Доказательство. Выделим в Γ^* бескванторное подмножество G. Пополним его по лемме 2 (лемма о дополнении непротиворечевиого множества) модель сделаем из него по лемме о бескванторной модели. Покажем, что это модель для всего Γ^*, а значит и для Γ. Рассмотрим $\gamma \in \Gamma^*$, покажем, что $[\gamma] = \text{И}$.

- База
  Формула не содержит кванторов. Истинность гарантируется леммой о бескванторном множестве.

- Переход
  Пусть G это модель для любой формулы из Γ^* с r кванторами, покажем что она остается моделью для $r+1$ квантора.

  1. $\gamma = \forall x(a)$
     Покажем, что формула истинна для любого $t \in D$. По построению подели есть такое θ, что $t =$ "θ (string). По построению Γ^* начиная с шага $p+1$ мы добавляем формулы вида $a[x := k]$, где k – конструкция из констант и ф.симв. Также каждая константа (c_i или d_i^j) из θ добавлена на некотором шаге s_k. То есть будет шаг $l = max(max(s_k), p)$, на котором θ обретет смысл и в Γ_{l+1} будет присутствовать $a[x := \theta]$. В формуле a на один квантор меньше, значит она истинна по предположению индукции.

  2. $\gamma = \exists x(a)$
     По построению Γ^* как только добавили a к Γ_i, так сразу в следующем мире Γ_{i+1} появляется $a[x := d_{i+1}^k]$. Значит формула истинна на значении "d_{i+1}^k", то есть истинна.

□

6.7. Следствие – если $\vDash \alpha$, то $\vdash \alpha$

Теорема 6.8. $\vDash \alpha \Rightarrow \vdash \alpha$

Доказательство.

- Пусть $\Gamma \nvdash a$, тогда по полноте множества Γ, $\Gamma \vdash \neg a$, но у Γ есть модель, в которой $\Gamma \vDash \neg a$. То есть $\Gamma \nvDash a$. Но Γ по построению то же, что и модель теории, то есть все рассуждения $\Gamma \vdash a$ равноценны в предикатах $\vdash a$.

- Пусть $\nvdash a$, тогда пусть $\Gamma = \{\neg a\}$

  1. Γ непротиворечиво
     Пусть Γ противоречиво, значит $\forall b \Gamma \vdash b, \Gamma \vdash \neg b$;
     (a) $\neg a \vdash b, \neg a \vdash b$;
     (b) $\neg a \vdash a, \neg a \vdash \neg a$;
     (c) $\vdash \neg a \to a, \neg a \to \neg a$;
     (d) $\vdash (\neg a \to a) \to (\neg a \to \neg a) \to \neg\neg a$;
     (e) $\vdash \neg\neg a \to a$;
     (f) $\vdash a \to\leftarrow$ недоказуемо по условию.;
  2. Γ подходит под условие теоремы Гёделя о полноти исчисления предикатов, то есть у Γ есть модель. Тогда в ней оценка $[\neg a] = 1$, значит оценка $[a] = 0$, то есть $\nvDash a$. Мы доказали мета-контрпозицию $\nvdash a \Rightarrow \nvDash a$.

□

7. Ticket 7: ФА

7.1. Структуры и модели, теория первого порядка

Теория первого порядка - это формальная система с кванторами по функциональным символам, но не по предикатам. Рукомахательное определение – это фс с логикой первого порядка в основе, в которой абстрактные предикаты и функциональные символы определяются точно (а может такое определение даже лучше).

Структура по ДГ:

Структурой теории первого порядка мы назовем упорядоченную тройку $\langle D, F, P \rangle$, где F – списки оценок для 0-местных, 1-местных и т.д. функций, и $P = P_0, P_1, \ldots$ – списки оценок для 0-местных, 1-местных и т.д. предикатов, D — предметное множество.

Понятие структуры — развитие понятия оценки из исчисления предикатов. Но оно касается только нелогических составляющих теории; истинностные значения и оценки для связок по-прежнему определяются исчислением предикатов, лежащим в основе теории. Для получения оценки формулы нам нужно задать структуру, значения всех свободных индивидных переменных, и (естественным образом) вычислить результат.

Структура по-моему:

Все то же самое определение из ИВ. Мы просто забиваем на предикаты в ИВ (не определяям их), расширяем нашу сигнатуру (добавляя конкретные предикаты и функциональные символы), определяем для нее интерпретацию.

Модель – это корректная структура (любое доказуемое утверждение должно быть в ней общезначимо).

7.2. Аксиомы Пеано

Множество N удовлетворяет аксиоматике Пеано, если:

1. $0 \in N$
2. $x \in N, succ(x) \in N$
3. $\nexists x \in N : (S(x) = 0)$
4. $(succ(a) = c \& succ(b) = c) \to a = b$
5. $P(0) \& \forall n.(P(n) \to P(succ(n))) \to \forall n.P(n)$

7.3. Формальная арифметика – аксиомы, схемы, правила вывода

Формальная арифметика – это теория первого порядка, у которой сигнатура определена как: (циферки, логические связки, алгебр. связки, ′), а интерпретацию сейчас будем определять. Интерпретация определяет два множества – V, P – истинностные и предметные значения. На самом деле нет никакого множества P, мы определяем только V, потому что оно нужно для оценок. Все элементы, которые мы хотели бы видеть, выражаются в сигнатуре.

Пусть множество $V = \{0, 1\}$ по-прежнему. Определим оценки логических связок естественным образом. Определим алгебраические связки так:

$$
\begin{aligned}
+(a, 0) &= a \\
+(a, b') &= (a + b)' \\
*(a, 0) &= 0 \\
*(a, b') &= a * b + a
\end{aligned}
$$

Тут должно быть что-то на уровне док-ва $2 + 2 = 4$

7.3.1. Аксиомы

1. $a = b \rightarrow a' = b'$
2. $a = b \rightarrow a = c \rightarrow b = c$
3. $a' = b' \rightarrow a = b$
4. $\neg(a' = 0)$
5. $a + b' = (a + b)'$
6. $a + 0 = a$
7. $a * 0 = 0$
8. $a * b' = a * b + a$
9. $\varphi[x := 0] \& \forall x.(\varphi \rightarrow \varphi[x := x']) \rightarrow \varphi$

7.3.2. a = a

Лемма 7.1. $\vdash a = a$

Доказательство. $\vdash a = a$

$$
\begin{array}{lll}
(1) & a = b \to a = c \to b = c & \text{Сх. акс. ФА 2} \\
(2) & T & \text{Сх. акс.} \\
(3) & (a = b \to a = c \to b = c) \to T \to (a = b \to a = c \to b = c) & \text{Сх. акс. 1} \\
(4) & T \to (a = b \to a = c \to b = c) & \text{М.Р. 1,3} \\
(5) & T \to \forall a(a = b \to a = c \to b = c) & \text{ПВ } \forall \\
(6) & T \to \forall a \forall b(a = b \to a = c \to b = c) & \text{ПВ } \forall \\
(7) & T \to \forall a \forall b \forall c(a = b \to a = c \to b = c) & \text{ПВ } \forall \\
(8) & \forall a \forall b \forall c(a = b \to a = c \to b = c) & \text{М.Р. 2,7} \\
(9) & \forall a \forall b \forall c(a = b \to a = c \to b = c) \to & \\
 & \qquad \forall b \forall c(a + 0 = b \to a + 0 = c \to b = c) & \text{Сх. акс. ИП 1} \\
(10) & \forall b \forall c(a + 0 = b \to a + 0 = c \to b = c) & \text{М.Р. 8,9} \\
(11) & \forall b \forall c(a + 0 = b \to a + 0 = c \to b = c) \to & \\
 & \qquad (\forall c(a + 0 = a \to a + 0 = c \to a = c)) & \text{Сх. акс. ИП 1} \\
(12) & \forall c(a + 0 = a \to a + 0 = c \to a = c) & \text{М.Р. 10,11} \\
(13) & (\forall c(a + 0 = a \to a + 0 = c \to a = c)) \to & \\
 & \qquad (a + 0 = a \to a + 0 = a \to a = a) & \text{Сх. акс. ИП 1} \\
(14) & a + 0 = a \to a + 0 = a \to a = a & \text{М.Р. 12,13} \\
(15) & a + 0 = a & \text{Сх. акс. ФА 6} \\
(16) & a + 0 = a \to a = a & \text{М.Р. 15,14} \\
(17) & a = a & \text{М.Р. 15,16}
\end{array}
$$

□

8. Ticket 8: рекурс, Аккерман

8.1. Рекурсивные функции

Рассмотрим примитивы, из которых будем собирать выражения:

1. $Z: \mathbb{N} \to \mathbb{N}$, $Z(x) = 0$
2. $N: \mathbb{N} \to \mathbb{N}$, $N(x) = x'$
3. Проекция. $U_i^n: \mathbb{N}^n \to \mathbb{N}$, $U_i^n(x_1, \dots, x_n) = x_i$
4. Подстановка. Если $f: \mathbb{N}^n \to \mathbb{N}$ и $g_1, \dots, g_n: \mathbb{N}^m \to \mathbb{N}$, то $S\langle f, g_1, \dots, g_n\rangle: \mathbb{N}^m \to \mathbb{N}$.
   При этом $S\langle f, g_1, \dots, g_n\rangle(x_1, \dots, x_m) = f(g_1(x_1, \dots, x_m), \dots, g_n(x_1, \dots, x_m))$
5. Примитивная рекурсия. Если $f: \mathbb{N}^n \to \mathbb{N}$ и $g: \mathbb{N}^{n+2} \to \mathbb{N}$, то

$$R\langle f, g\rangle(x_1 \dots x_n, n) = \begin{cases} f(x_1, \dots, x_n) & n = 0 \\ g(x_1, \dots, x_n, n, R\langle f, g\rangle(x_1, \dots, x_n, n-1)) & n > 0 \end{cases}$$

6. Минимизация. Если $f: \mathbb{N}^{n+1} \to \mathbb{N}$, то $\mu\langle f\rangle: \mathbb{N}^n \to \mathbb{N}$, при этом $\mu\langle f\rangle(x_1, \dots, x_n)$ — такое минимальное число y, что $f(x_1, \dots, x_n, y) = 0$. Если такого y нет, результат данного примитива неопределен.

Пример:

$a + b = R\langle U_1^2, S\langle N, U_3^3\rangle\rangle(a, b)$

8.2. Характеристическая функция и рекурсивное отношение

- *Характеристическая фукнция* – функция от выражения, которая возвращает 1 если выражение истинно, 0 иначе.
- *Рекурсивное отношение* – отношение, характеристическая функция которого рекурсивна.

8.3. Аккерман не примитивно-рекурсивен, но рекурсивен (второе)

Функция Аккермана – это функция, удовлетворяющая следующим правилам:

$$A(m, n) = \begin{cases} n + 1 & m = 0 \\ A(m-1, n) & m > 0, n = 0 \\ A(m-1, A(m, n-1)) & m > 0, n > 0 \end{cases}$$

Например:

$A(2, 0) = A(1, 1) = A(0, A(1, 0)) = A(0, 2) = 3$

Лемма 8.1. $A(m, n) \geqslant 1$

Доказательство. $A(m, n)$ определена только на натуральных числах
$A(0, 0) = 1, A(1, 0) = A(0, 1) = 2, A(0, 1) = 2$, а все остальное ещё больше □

Лемма 8.2. $A(1, n) = n + 2$

Доказательство.

$$\begin{aligned} A(1, n) &= A(0, A(1, n-1)) \\ &= A(0, A(0, A(1, n-2))) \\ &= A(0, A(0, A(0, \dots A(1, 0)))) \\ &= A(0, A(0, A(0, \dots 2))) \\ &= n + 2 && \text{(n раз инкрементируем двойку)} \end{aligned}$$

□

Лемма 8.3. $A(2, n) = 2n + 3$

Доказательство. $A(2, n) = A(1, A(1, \dots A(2, 0))) = A(1, A(1, \dots 3)) = 2n + 3$ (n раз к тройке прибавляем $A(0, 1) = 2$) □

Лемма 8.4. $A(m, n) \geqslant n + 1$

Доказательство. В первом случае $A \geqslant n + 1 = n + 1$
Во втором A может перейти в первый случай, который работает хорошо, или в третий.
В третьем случае мы можем получить $A(0, n)$ если первый аргумент был нулем, тогда все ок, можем получить $A(1, 0)$, тогда это второй случай, для него условие выполнено.
Третий ссылается на второй, а второй на третий, но тут нет противоречия, потому что мы знаем, что функция Аккермана завершается. □

Лемма 8.5. $A(m, n) < A(m, n + 1)$

Доказательство. Проведем индукцию по m:

- База:
  $A(0, n) = n + 1 < n + 2 = A(0, n + 1)$
- Переход:
  $A(k + 1, m) < A(k + 1, m) + 1$
  $\leqslant A(k, A(k + 1, m))$ (По 8.4)
  $\leqslant A(k + 1, m + 1)$ (3-е свойства ф-ии Аккермана)

□

Лемма 8.6. $A(m, n + 1) \leqslant A(m + 1, n)$

Доказательство. Проведем индукцию по n:

- База:
  $A(m, 0 + 1) = A(m, 1) = A(m + 1, 0)$ (ii)

- Переход, предположение:

$$
\begin{aligned}
A(m, j+1) &\leqslant A(m+1, j) && \text{По 8.4} \\
(j+1)+1 &\leqslant A(m, j+1) && \\
A(m, (j+1)+1) &\leqslant A(m, A(m, j+1)) && \text{По монотонности} \\
A(m, A(m, j+1)) &\leqslant A(m, A(m+1, j)) && \text{По монотонности + предположение} \\
A(m, (j+1)+1) &\leqslant A(m, A(m+1, j)) = A(m+1, j+1) && \\
& && \text{По 3-му свойству ф-ии Аккермана}
\end{aligned}
$$

□

Лемма 8.7. $A(m, n) < A(m+1, n)$

Доказательство. $A(m, n) < A(m, n+1) \leqslant A(m+1, n)$ (По 8.5, 8.6) □

Лемма 8.8. $A(m_1, n) + A(m_2, n) < A(\max(m_1, m_2) + 4, n)$

Доказательство.

$$
\begin{aligned}
& A(m_1, n) + A(m_2, n) && \\
\leqslant\ & A(\max(m_1, m_2), n) + A(\max(m_1, m_2), n) && \\
=\ & 2 \cdot A(\max(m_1, m_2), n) && \\
<\ & 2 \cdot A(\max(m_1, m_2), n) + 3 && \\
=\ & A(2, A(\max(m_1, m_2), n)) && \text{По 8.2} \\
<\ & A(2, A(\max(m_1, m_2) + 3, n)) && \text{Строгая монотонность по обоим арг.} \\
<\ & A(\max(m_1, m_2) + 2, A(\max(m_1, m_2) + 3, n)) && \text{По 8.7} \\
=\ & A(\max(m_1, m_2) + 3, n+1) && \text{3-е свойство ф-ии Аккермана} \\
\leqslant\ & A(\max(m_1, m_2) + 4, n) && \text{По 8.6}
\end{aligned}
$$

□

Лемма 8.9. $A(m, n) + n < A(m+4, n)$

Доказательство.

$$
\begin{aligned}
& A(m, n) + n \\
<\ & A(m, n) + n + 1 \\
=\ & A(n, m) + A(0, n) \\
<\ & A(m+4, n)
\end{aligned}
$$

□

Теорема 8.10. Функция аккерманна не притивно-рекурсивна

Доказательство. Пусть $f(n_1 \dots n_k)$ - примитивная рекурсивная функция, $k \geqslant 0$.
$\exists J : f(n_1 \dots n_k) < A(J, \sum(n_1 \dots n_k))$

Пусть $\overline{n} = (n_1, \dots, n_k)$

Индукция по рекурсивным функциям

- База:
  $f(\overline{n})$ - N или Z или U_j^k

  1. $f(\overline{n}) = N, k = 1$; Пусть $J = 1$, по (i) и лемме 3c
     $f(n) = N(n) = n + 1 = A(0, n) < A(1, n) = A(J, n) = A(J, \sum(\overline{n}))$
  2. $f(\overline{n}) = Z, k = 1$;
     $f(n) = 0 < A(J, n)$ (потому что $A \geqslant 1) = A(J, \sum(\overline{n}))$
  3. $f(\overline{n}) = U_j^k; k = k$;
     Пусть $J = 1$
     $f(n_1 \ldots, n_k) = U_{kj}(n_1 \ldots, n_k) = n_j$
     Пусть $n_j = 0$, тогда $f(n) = 0 < A(J, \sum(\overline{n}))$ для любого нормального J Пусть $n_j > 0$, тогда $f(n) = (n_j - 1) + 1 = A(0, n_j - 1) < A(1, n) = A(J, \sum(\overline{n}))$

- Переход

  1. Предположим, что $f(\overline{n}) = S\langle h, g_1 \ldots g_m\rangle(\overline{n}) = h(g_1(\overline{n}) \ldots g_m(\overline{n}))$
     По предположению индукции существует J_0 для h, $J_1, \ldots, J_m$ для $g_1 \ldots g_m$.

$$
\begin{aligned}
& f(\overline{n}) = h(g_1(\overline{n}), ..) \\
\leqslant\ & A(J_0, \sum\{i = 1..m\}(\overline{n})) && \text{По выбору } J_0 \\
<\ & (J_0, \sum(A(J_i, \sum(\overline{n})))) && \text{По выбору } J_i \text{ и строгой монотонности} \\
& //J* = \max(J_1..J_m) + 4(m-1) \\
<\ & A(J_i, A(J*, \sum(\overline{n}))) && \text{По 8.8 примененной } m-1 \text{ раз} \\
<\ & A(J_i, A(J*+1, \sum(\overline{n}))) && \text{По монотонности} \\
\leqslant\ & A(J_0, A(\max(J_0, J*) + 1, \sum(\overline{n}))) && \text{По монотонности} \\
\leqslant\ & A(\max(J_0, J*) + 1, \sum(\overline{n}) + 1) && \text{3-е свойство ф-ии Аккермана} \\
=\ & A(\max(J_0, J*) + 2, \sum(\overline{n})) && \text{По 8.6}
\end{aligned}
$$

     Тогда пусть $j = \max(J_0, J*) + 2$
  2. Пусть $f(\overline{n}) = R\langle h, g\rangle(\overline{n})$
     $f(n_1, \ldots, n_k, 0) = h(n_1, \ldots, n_k)$
     $f(n_1, \ldots, n_k, m + 1) = g(n_1, \ldots, n_k, m, f(n_1, \ldots, n_k, m))$
     По предположению имеем $J_0(h), J_1(g)$.
     Пусть $J = \max(J_0, J_1) + 4$

(а)

$$
\begin{aligned}
& f(\overline{n}, 0) \\
\leqslant\ & f(\overline{n}, 0) + \sum(\overline{n}) \\
=\ & h(\overline{n}) + \sum(\overline{n}) \\
<\ & A(J_0, \sum(\overline{n})) + \sum(\overline{n}) \\
<\ & A(J_0 + 4, \sum(\overline{n})) && \text{По 8.9} \\
<\ & A(J, \sum(\overline{n})) && \text{По монотонности} \\
=\ & A(J, \sum(\overline{n}) + 0)
\end{aligned}
$$

(б)

$$
\begin{aligned}
& f(\overline{n}, k+1) \\
=\ & g(\overline{n}, k, f(\overline{n}, k)) \\
<\ & A(J_1, \sum(\overline{n}) + k + f(\overline{n}, k)) && \text{По выбору } J_1 \\
<\ & A(J_1, \sum(\overline{n}) + k + 1 + f(\overline{n}, k)) && \text{По монотонности} \\
=\ & A(J_1, A(0, \sum(\overline{n}) + k) + f(\overline{n}, k)) && \text{По 1-му свойству ф-ии Аккермана} \\
<\ & A(J_1, A(0, \sum(\overline{n}) + k) + H(J, \sum(\overline{n}) + k)) && \text{По предположению} \\
<\ & A(J_1, A(J, \sum(\overline{n}) + k) + A(J, \sum(\overline{n}) + k)) && \text{По монотонности } (J > 0) \\
=\ & A(J_1, 2 * [A(J, \sum(\overline{n}) + k)]) \\
<\ & A(J_1, 2 * [A(J, \sum(\overline{n}) + k)] + 3) \\
=\ & A(J_1, A(2, A(J, \sum(\overline{n}) + k))) && \text{По 8.2} \\
<\ & A(J_1, A(J_1 + 1, A(J, \sum(\overline{n}) + k))) && \text{По строгой монотонности } (J_1 > 2) \\
=\ & A(J_1 + 1, A(J, \sum(\overline{n}) + k) + 1) && \text{По 3-му свойству ф-ии Аккермана} \\
\leqslant\ & A(J_1 + 2, A(J, \sum(\overline{n}) + k)) \\
<\ & A(J - 1, A(J, \sum(\overline{n}) + k)) && \text{По монот. } J > \max(..) + 4 \\
=\ & A(J, \sum(\overline{n}) + (k+1)) && \text{По 3-му свойству ф-ии Аккермана, } J \neq 0
\end{aligned}
$$

□

Теорема 8.11. Функция Аккермана рекурсивна

Доказательство. Можем сказать, что он рекурсивный, потому что мы можем его написать на компьютере, а тьюринг выражается в рекурсивных функциях. □

9. Ticket 9: представимость

9.1. Функции, их представимость

Арифметическая функция – это отображение $f : N_0^n \to N_0$
Арифметическое отношение – это $P \in N_0^n$
Если $k \in N_0$, то $\overline{k} = 0''''^{\cdots}$, где количество штрихов есть k.

- Арифметическое отношение $R \in N_0^n$ выразимо в ФА, если $\exists a$ с n свободными переменными: $a(x_1, \dots, x_n)$, такая что

  1. Если $R(k_1, \dots, k_n)$, то $\vdash a(\overline{k_1}, \dots, \overline{k_n})$
  2. Если $\neg R(k_1, \dots, k_n)$, то $\vdash \neg a(\overline{k_1}, \dots, \overline{k_n})$

- C_R - функция, равная 1, если R, и равная 0, если $\neg R$

- $\exists! y.\varphi(y) = \exists y.\varphi(y) \& \forall a \forall b(\varphi(a) \& \varphi(b) \to a = b)$

- $f : N_0^n \to N_0$ представима в ФА, если $\exists a(x_1 \dots x_{n+1})$, что $\forall x_1 \dots x_{n+1}$:

  1. $f(x_1, \dots, x_n) = x_{n+1} \Leftrightarrow \vdash a(\overline{x_1}, \dots, \overline{x_{n+1}})$
  2. $\exists! b(a(\overline{x_1}, \dots, \overline{x_n}, b))$

9.2. Теорема о связи представимости и выразимости

Теорема 9.1. R выразимо $\Leftrightarrow C_r$ представимо

Доказательство. $\Rightarrow$ a выражает R
$(a \to (x_{n+1} = 0')) \& (\neg a \to (x_{n+1} = 0))$ представляет C_r
По выразимости $R \vdash a$; тогда $\top \to a \to \top => a \to \top$
По 10i, перенесенной к нам $a \to (\neg a \to \bot)$
правило с единственностью вроде понятно (хотя руками помахал, да)

$\Leftarrow$ C_r представимо $\to$ R выразимо Пусть представлять C_r будет $a(x_1, \dots, x_n, x_{n+1})$ Тогда определим, какая формула выражает R: $a(\dots, 1)$ Из представимости:

- $\exists b.a(x_1 \dots x_{n+1})$

- $\forall x \forall y(a(\dots x) \& a(\dots y) \to x = y)$

- если $C_r(x_1 \dots x_n) = 1$, то $\vdash a(x_1 \dots x_n, 1)$

- если $C_r(\dots) = 0$, то $\vdash a(\dots, 0)$

Докажем выводимость

1. Покажем, что если $R(x_1 \dots x_n)$, то $\vdash a(x_1 \dots x_n, 1)$ Из представимости прямо ровно.

2. Покажем, что если $\neg R(x_1 \ldots . x_n)$, $\vdash \neg a(x_1 \ldots x_n, 1)$
   По единственности

   $\forall x \forall y (a(x_1 \ldots x_n, x) \& a(x_1 \ldots x_n, y) \to x = y)$
   $a(x_1 \ldots x_n, 0) \& a(x_1 \ldots x_n, 1) \to (0 = 1)$ (спустя две акс. и 2 MP)
   Делаем дедукцию
   $a(x_1 \ldots x_n, 0) \& a(x_1 \ldots x_n, 1) \vdash \perp$
   $a(x_1 \ldots x_n, 0) \& a(x_1 \ldots x_n, 1) \to a(x_1 \ldots x_n, 0)$
   $a(x_1 \ldots x_n, 0)$
   $\neg a(x_1 \ldots x_n, 0)$ по представимости $a(x_1 \ldots x_n, 0) \to (\neg a(x_1 \ldots x_n, 0) \to \neg a(x_1 \ldots x_n, 1))$ (10i в ИИВ, доказуема в предикатах)
   $\neg a(x_1 \ldots x_n, 1)$
   Хотим $\neg a(x_1 \ldots x_n, 1)$

□

9.3. β-функция Гёделя, китайская теорема об остатках

$\beta(b, c, i) = b\%(1 + c * (1 + i))$
Где $\%(a, b) = d$, что $\forall m.(d + m * b = a), m \geqslant 0, 0 \leqslant d \leqslant b$

9.3.1. Китайская теорема об остатках

Теорема 9.2. $n_1 \ldots n_k$ - попарно взаимно простые целый числа
$r_1 \ldots r_k$ - любые целые числа, что $0 \leqslant r_1 < n_1$
Тогда: $\exists b \forall i r_1 = b\% n_k$

Доказательство. Без доказательства □

9.3.2. Гёделева Γ-последовательность

$\Gamma_1 = (i + 1) * c + 1$
$\Gamma(c) = 1 * c + 1, 2 * c + 1, 3 * c + 1, \ldots (n + 1) * c + 1$

Теорема 9.3. $\Gamma(c)$ подходит на роль $n_1 \ldots n_k$ в китайской теореме об остатках

Доказательство. Выделим последовательность размера n: $k_1 \ldots k_n$.
Чтобы это выполнялось возьмем $c = (max(k_1 \ldots k_n))!$

1. В Γ любые два элемента попарно взаимно простые Пусть $\Gamma_1 \vdots \Gamma_j$ имеют общий делитель $p > 1$. Мы можем его разложить на простые множители и взять какой-нибудь простой (любое число раскладывается на простые множители).
   Тогда $(\Gamma_1 - \Gamma_j) \vdots p$, $(c*(i-j)) \vdots p$. Заметим, что $\neg(c \vdots p)$, потому что иначе $\Gamma_1 = 1 + c*(i+1) \vdots p$ и $c*(i+1) \vdots p$, а они отличаются на единицу. Тогда $(i-j) \vdots p$, но $c = m!$, $m > n$, а $i - j < n$, значит $c \vdots p$.

2. Каждое $k_1 <_1 k_1 \leqslant c < 1 + c * (i + 1) = \Gamma_1$

□

9.3.3. Лемма о β-функции

Лемма 9.4. Увидим, что $\beta(b, c, i)$ считает остаток от деления b на $(i+1) * c + 1$ - элемент Геделевой последовательности.

Доказательство. $< a_0 \dots a_n > \in N \to \exists b \exists c (a_k = \beta(b, c, i))$ - β-функция кодирует последовательность натуральных чисел и может доставать по индексу i

$a_0 \dots a_n$ - последовательность натуральных чисел тогда существует такое c, что $\Gamma = 1 * c + 1, 2 * c + 1, \dots$ если $c \geqslant max(a_0 \dots a_n)$, то $a_k < (i+1) * c + 1$
Но по свойству Γ элементы попарно взаимно просты тогда сравнения:
$a_0 \% (0+1) * c + 1$
$a_1 \% (1+1) * c + 1$
$\dots$
$a_n \% (n+1) * c + 1$
Имеют общее решение b по китайской теореме об остатках, тогда $a_1 = b \% (i+1) * c + 1$
Но это и есть β-функция:
$a_i = \beta(b, c, i)$ □

9.3.4. Представимость β-функции Гёделя в ФА

Лемма 9.5. β-функция представима в ФА отношением
$B(b, c, i, d) = \exists q((b = q * (1 + c * (i+1)) + d) \& (d < 1 + c * (i+1)))$

Доказательство. Пусть $1 + c * (i+1) = z$
Докажем условия представимости:

1. Эквивалентность
   (а) $\beta(b, c, i) = d$, тогда $\vdash B(b, c, i, d)$
   $b = z * (1 + c * (i+1))$ (это и следующее - из леммы о β)
   $d < 1 + c * (i+1)$
   $P \to Q \to P \& Q$
   $P \& Q$
   $P \& Q \to \exists q.(P \& Q)[z := q]$
   $\exists q.(P \& Q)$
   (б) Пусть $\vdash B(b, c, i, d)$, тогда
   $\exists q.(P \& Q)$
   Подберем такое q (по лемме)
   $P \& Q \to P$
   $P \& Q \to Q$
   P
   Q
   значит $\beta(b, c, i) = d$
2. Единственность Следует из леммы.

□

9.4. Теорема о представимости рекурсивных функций Z, N, U

1. Z $Z(a, b) = (b = 0)$

   - $Z(a) = b$ верно, тогда $b = 0$
     $b = 0$
   - $(b = 0)$
     $b = 0$
     Тогда $Z(0) = 0$, все ок
   - $\exists y.\varphi(y)\&\forall a \forall b(\varphi(a)\&\varphi(b) \rightarrow a = b)$
     Тоже как-то не сложно

2. N
   $N(a, b) = (a = b')$

   - $N(a) = b$, тогда $a = b'$
     $a = b'$
   - $a = b'$, тогда
     $N(a) = b$
   - Третье не хочу

3. U_n^i
   $U_n^i(x_1 \dots x_n) = (x_1 = x_1)\&(x_2 = x_2)\&\dots\&(x_{n+1} = x_i)$

   - $U_n^i(..) = x_i$, тогда $x_{n+1} = x_i$
     $x_1 = x_1$ доказывается
     $\dots$
     $x_n = x_n$ доказывается
     $x_{n+1} = x_i$ по условию
     объединяем все с помощью &
   - $(x_1 = x_1)\&\dots$
     Вытаскиваем каждый элемент и тогда видим, что проекция делает ровно то, что должна.
   - $\exists q.(x_{n+1} = q)$
     ХЗ
   - $\forall a \forall b(x(\dots a)\&x(\dots .b) \rightarrow a = b)$
     Для конкретных a, b обявляем $a = b - \top$, тогда выводим из него конъюнкцию и навешиваем два квантора

9.5. Теорема о представимости S

Лемма 9.6. Если f и $g_1 \dots g_n$ представимы, то $S\langle f, g_1 \dots g_n \rangle$ представима

Доказательство. Пусть F, $G_1 \dots G_n$ представляют их.
$S(a_1 \dots a_m, b) = \exists b_1 \dots \exists b_n(G_1(a_1 \dots a_n, b_1)\&\dots\&Gn(a_1 \dots a_m, b_n)\&F(b_1 \dots b_n, b))$

- Пусть $S(a_1 \dots a_n) = b$, тогда существуют такие $b_1 \dots b_n$, что *каждый аргумент*
  Поскольку $f, g_1 \dots g_n$ представимы, то доказуемы по представимости
  $f(b_1 \dots b_n, b)$
  $g_1(a_1 \dots a_n, b_1)$
  $\dots$
  $g_n(a_1 \dots a_n, b_n)$
  $g_1 \& g_2 \& \dots \& g_n \& f$ объединили & – $''P''$
  $''P'' \rightarrow \exists b_1.$"$P[b_1 := b_1]$" + M.P.
  $\dots$
  Ну и навесили кванторы, да.

- Пусть верна формула с кванторами. Тогда она и есть уже то, что надо

- не могу, да и вообще нигде это свойство не доказывается

$\square$