

[section]

# Курс математической логики по Штукенбергу Д.Г.

Daniyar Huyaniyar Itegulov, Ignat Loskutov

23 января 2015 г.

## Содержание

<b>1</b>	<b>Базовые понятия</b>	<b>5</b>
1.1	Формальные системы и модели . . . . .	5
<b>2</b>	<b>Определения (нужно знать идеально)</b>	<b>7</b>
2.1	ИВ . . . . .	7
2.2	Общезначимость, доказуемость, выводимость . . . . .	7
2.3	Теорема о дедукции для ИВ . . . . .	7
2.4	Теорема о полноте исчисления высказываний . . . . .	8
2.5	ИИВ . . . . .	8
2.6	Теорема Гливенко . . . . .	8
2.7	Порядки . . . . .	8
2.8	Решетки (все свойства) . . . . .	9
2.9	Булевы/псевдобулевы алгебры . . . . .	9
2.10	Топологическая интерпретация ИИВ . . . . .	10
2.11	Модель Крипке . . . . .	10
2.12	Вложение Крипке в алгебры Гейтинга . . . . .	11
2.13	Полнота ИИВ в алгебрах Гейтинга и моделях Крипке . . . . .	11
2.14	Нетабличность ИИВ . . . . .	11
2.15	Предикаты . . . . .	11
2.16	Теорема о дедукции в предикатах . . . . .	11
2.17	Теорема о полноте исчисления предикатов . . . . .	12
2.18	Теории первого порядка, определение структуры и модели . . . . .	12
2.19	Аксиоматика Пеано . . . . .	12
2.20	Формальная арифметика – аксиомы . . . . .	12
2.20.1	Аксиомы . . . . .	13
2.21	Рекурсивные функции . . . . .	13
2.22	Функция Аккермана . . . . .	13
2.23	Существование рек.ф-й не явл. ф-ей Аккермана (определение конечной лем- мы) . . . . .	13
2.24	Представимость . . . . .	14
2.25	Выразимость . . . . .	14
2.26	Лемма о связи представимости и выразимости . . . . .	14
2.27	Бета-функция Гёделя, Г-последовательность . . . . .	14

2.28	Представимость рек.ф-й в ФА (знать формулы для самых простых) . . . . .	14
2.29	Гёделева нумерация (точно) . . . . .	15
2.30	Выводимость и рекурсивные функции (че там с Тьюрингом) . . . . .	15
2.31	Непротиворечивость . . . . .	15
2.32	$\omega$ -непротиворечивость . . . . .	15
2.33	Первая теорема Гёделя о неполноте . . . . .	15
2.34	Первая теорема Гёделя о неполноте в форме Россера . . . . .	16
2.35	Consis . . . . .	16
2.36	Условия Г-Б (наизусть) . . . . .	16
2.37	Лемма о самоприменении . . . . .	16
2.38	Вторая теорема Гёделя о неполноте ФА . . . . .	16
2.39	Теория множеств . . . . .	16
2.40	ZFC . . . . .	16
2.40.1	Аксиома равенства . . . . .	16
2.40.2	Аксиома пары . . . . .	17
2.40.3	Аксиома объединений . . . . .	17
2.40.4	Аксиома степени . . . . .	17
2.40.5	Схема аксиом выделения . . . . .	17
2.40.6	Аксиома выбора (не входит в ZF по дефолту) . . . . .	17
2.40.7	Аксиома бесконечности . . . . .	17
2.40.8	Аксиома фундирования . . . . .	17
2.40.9	Схема аксиом подстановки . . . . .	17
2.41	Ординальные числа, операции . . . . .	18
2.42	Кардинальные числа, операции . . . . .	18
2.43	Диагональный метод, теорема Лёвенгейма-Скулема . . . . .	19
2.44	Парадокс Скулема . . . . .	19
2.45	Теорема Генцена о непротиворечивости ФА . . . . .	19
<b>3</b>	<b>Ticket 1: ИВ</b>	<b>20</b>
3.1	Определения (исчисление, высказывание, оценка...) . . . . .	20
3.2	Общезначимость, доказуемость, выводимость . . . . .	20
3.3	Схемы аксиом и правило вывода . . . . .	20
3.4	Теорема о дедукции . . . . .	21
3.5	Корректность исчисления высказываний относительно алгебры Яськовского	21
<b>4</b>	<b>Ticket 2: полнота ИВ</b>	<b>22</b>
4.1	Полнота исчисления высказываний относительно алгебры Яськовского . . .	22
4.1.1	Контрапозиция . . . . .	22
4.1.2	Правило исключенного третьего . . . . .	22
4.1.3	Всякие очевидные вещи типа если выводится из А и из Б то из А и Б тоже . . . . .	22
4.1.4	Правило со звездочкой (14 доказательств) . . . . .	22
<b>5</b>	<b>Ticket 3: ИИВ</b>	<b>25</b>
5.1	ИИВ, структура, модель . . . . .	25
5.2	Опровергаемость исключенного третьего . . . . .	25
5.3	Решетки . . . . .	26

5.4	Алгебра Гейтинга, булева алгебра . . . . .	27
5.5	Алгебра Линденбаума-Тарского . . . . .	27
5.6	Теорема о полноте ИИВ относительно алгебры Гейтинга . . . . .	28
5.7	Дизъюнктивность ИИВ . . . . .	28
5.8	Теорема Гливенко . . . . .	29
5.9	Топологическая интерпретация . . . . .	30
<b>6</b>	<b>Ticket 4: ИИВ2</b>	<b>31</b>
6.1	Модели Крипке . . . . .	31
6.2	Корректность ИИВ относительно моделей Крипке . . . . .	31
6.3	Вложение Крипке в Гейтинга . . . . .	32
6.4	Полнота ИИВ в моделях Крипке . . . . .	32
6.5	Нетабличность интуиционистской логики . . . . .	32
<b>7</b>	<b>Ticket 5: Логика 2 порядка</b>	<b>34</b>
7.1	Основные определения . . . . .	34
7.2	Теорема о дедукции . . . . .	34
7.3	Корректность исчисления предикатов . . . . .	35
<b>8</b>	<b>Ticket 6: Полнота исчисления предикатов</b>	<b>36</b>
8.1	Свойства противоречивости . . . . .	36

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

# 1. Базовые понятия

## 1.1. 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 ( $\{\langle \rightarrow \rangle, \langle \cup \rangle, \langle \rangle\}$ )
- Misc – дополнительные элементы ( $\{\langle ( \rangle, \langle ) \rangle, \langle \rangle\}$ )
- arity:  $\text{Pr} \cup \text{F} \cup \text{C} \rightarrow \mathbb{N}$  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
- arity – функция, определяющая арность  $\text{Pr} \cup \text{F} \rightarrow \mathbb{N}$ .

2. Интерпретация – это приписывание символам значения и правил действия (отображения из  $\text{Pr} \cup \text{F} \cup \text{C}$  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.

## 2. Определения (нужно знать идеально)

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

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

### 2.2. 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.

### 2.3. Теорема о дедукции для ИВ

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

## 2.4. Теорема о полноте исчисления высказываний

**Теорема 2.1** (о полноте исчисления высказываний). Исчисление предикатов полно.

Общий ход д-ва: строим док-ва для конкретных наборов переменных,  $2^n$ , где  $n$  – количество возможных переменных. Потом их мерджим.

## 2.5. ИИВ

Берем ИВ, выкидываем 10 аксиому, добавляем  $\alpha \rightarrow \neg\alpha \rightarrow \beta$ .

Она доказывается и в ИВ:

**Лемма 2.2.**  $\alpha, \alpha \vee \neg\alpha, \neg\alpha \vdash \beta$

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

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

## 2.6. Теорема Гливенко

**Теорема 2.3.** Гливенко Если в ИВ доказуемо  $\alpha$ , то в ИИВ доказуемо  $\neg\neg\alpha$

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

## 2.7. 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.



## 2.8. Решетки (все свойства)

- Просто Решетка – это  $(L, +, *)$  в алгебраическом смысле и  $(L, \leq)$  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  $\inf$ :

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

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

- Дистрибутивная решетка – решетка, в которой работает дистрибутивность:  $a * (b + c) = (a * b) + (a * c)$
- Импликативная решетка – всегда существует псевдодополнение  $b$  ( $b \rightarrow a$ )  $a \rightarrow b = \max\{c \mid c * a \leq b\}$  Имеет свойства, что в ней всегда есть максимальный элемент  $a \rightarrow a$  и что она дистрибутивна.

## 2.9. Булевы/псевдобулевы алгебры

- Булева алгебра можно определить так:
  - $(L, +, *, -, 0, 1)$  с выполненными аксиомами – коммутативность, ассоциативность, поглощение, две дистрибутивности и  $a * -a = 0$ ,  $a + -a = 1$ .
  - Импликативная решетка над фундированным множеством. Тогда мы в ней определим 1 как  $a \rightarrow a$  (традиционно для импликативной), отрицание как  $-a = a \rightarrow 0$ , и тогда последняя аксиома из предыдущего определения будет свойством:

$$a * -a = a * (a \rightarrow 0) = a * (\max c : c * a \leq 0) = a * 0 = 0$$

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

$$a + -a = a + (a \rightarrow 0) = a + (\max c : c * a \leq 0) = a + 0 = a$$

// не 1

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

## 2.10. 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.  $a + b \Rightarrow a \cup b$
2.  $a * b \Rightarrow a \cap b$
3.  $a \rightarrow b \Rightarrow \text{Int}(a^c \cup b)$
4.  $\neg a \Rightarrow \text{Int}(a^c)$
5.  $0 \Rightarrow \emptyset$
6.  $1 \Rightarrow \mathbb{R}^n$

## 2.11. Модель Крипке

$\text{Var} = \{P, Q, \dots\}$  Модель Крипке – это  $\langle W, \leq, v \rangle$ , где

- $W$  – множество «миров»
- $\leq$  – частичный порядок на  $W$  (отношение достижимости)
- $v: W \times \text{Var} \rightarrow \{0, 1, \perp\}$  – оценка переменных на  $W$ , монотонна (если  $v(x, P) = 1$ ,  $x \leq y$ , то  $v(y, P) = 1$  – формулу нельзя ип'вынудить)

Правила:

- $W, x \models P \Leftrightarrow v(x, P) = 1$
- $W, x \models (A \& B) \Leftrightarrow W, x \models A \& W, x \models B$
- $W, x \models (A \vee B) \Leftrightarrow W, x \models A \vee W, x \models B$
- $W, x \models (A \rightarrow B) \Leftrightarrow \forall y \geq x (W, y \models A \Rightarrow W, y \models B)$
- $W, x \models \neg A \Leftrightarrow \forall y \in x (W, y \not\models A)$

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

## 2.12. 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.  $\leq$  – отношение «быть подмножеством». Определим 0 как  $\emptyset$  (пустое объединение поддеревьев); Определим операции:

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

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

## 2.13. 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.

## 2.14. 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.

## 2.15. Предикаты

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

Правила вывода:

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

$x$  не входит свободно в  $A$

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

$x$  не входит свободно в  $B$

## 2.16. 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  $\gamma$   $\Gamma, \gamma \vdash \alpha \Rightarrow \Gamma \vdash \gamma \rightarrow \alpha$

## 2.17. 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  $\models \alpha$ .

## 2.18. 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  $P = P_0, P_1 \dots$  – 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 индивидуальных переменных, и (естественным образом) вычислить результат.

Структура по-моему: Все то же самое определение из ИВ. Мы просто забиваем на предикаты в ИВ (не определяем 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).

## 2.19. Аксиоматика Пеано

Множество  $N$  удовлетворяет аксиоматике Пеано, если:

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

## 2.20. 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.  $P = \{\text{всякие штуки, которые мы можем получать из логических связок и } 0\}$  Определим оценки логических связок естественным

образом. Определим алгебраические связки так:  $+(a, 0) = a + (a, b') = (a + b)' * (a, 0) = 0$   
 $*(a, b') = a * b + a$

### 2.20.1. 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.  $\varphi[x := 0] \& \forall x. (\varphi \rightarrow \varphi[x := x']) \rightarrow \varphi$  //  $\varphi$  содержит св.п  $x$

### 2.21. Рекурсивные функции

$$Z(x) = 0$$

$$N(x) = x + 1$$

$$U_i^n(x_1, \dots, x_n) = x_i$$

$$S\langle f, g_1, \dots, g_n \rangle(x_1, \dots, x_m) = f(g_1(x_1 \dots x_m), \dots, g_n(x_1, \dots, x_m))$$

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

$$\mu\langle f \rangle(x_1, \dots, x_n) - \text{минимальное } k, \text{ такое что } f(x_1 \dots x_n, k) = 0$$

### 2.22. Функция Аккермана

$$A(0, n) = n + 1$$

$$A(m, 0) = A(m - 1, 1)$$

$$A(m, n) = A(m - 1, A(m, n - 1))$$

### 2.23. Существование рек.ф-й не явл. ф-ей Аккермана (определение конечной леммы)

Пусть  $f(n_1, \dots, n_k)$  – примитивная рекурсивная функция,  $k \geq 0$ .  $\exists J : f(n_1 \dots n_k) < A(J, \sum(n_1, \dots, n_k))$   
 Доказывается индукцией по рекурсивным функциям.

## 2.24. Представимость

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

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

## 2.25. Выразимость

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

1.  $n(x_1 \dots x_n) \Rightarrow \vdash N(x_1\sim, \dots x_n\sim)$
2.  $n(x_1 \dots x_n) \Rightarrow \vdash \neg N(x_1\sim, \dots x_n\sim)$

## 2.26. Лемма о связи представимости и выразимости

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

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

## 2.28. 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.  $u_i^n = (x_1 = x_1) \& \dots \& (x_n = x_n) \& (x_{n+1} = x_i)$
4.  $s(a_1 \dots a_m, b) = \exists b_1 \dots \exists b_n (G_1(a_1 \dots a_n, b_1) \& \dots \& G_n(a_1 \dots a_m, b_n))$
5.  $r(x_1, \dots, x_n, k, a) =$   
 $\exists b \exists c (\exists k (\beta(b, c, 0, k) \& \varphi(x_1, \dots, x_n, k)) \&$   
 $B(b, c, x_{n+1}, a) \&$   
 $\forall k (k < x_{n+1} \rightarrow \exists d \exists e (B(b, c, k, d) \& B(b, c, k', e) \& G(x_1 \dots x_n, k, d, e))))$
6.  $m\langle F \rangle(x_1, \dots, x_{n+1}) = F(x_1, \dots, x_n, x_{n+1}, 0) \& \forall y ((y < x_{n+1}) \rightarrow \neg F(x_1, \dots, x_n, y, 0))$

## 2.29. Гёделева нумерация (точно)

$a$	$\ulcorner a \urcorner$	описание
(	3	
)	5	
,	7	
$\neg$	9	
$\rightarrow$	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 ( $=$ )

## 2.30. Выводимость и рекурсивные функции (че там с Тьюрингом)

Основные тезисы по вопросу:

- $\text{Emulate}(\text{input}, \text{prog}) = \text{plog}(R < f, g > (< 'S, \text{input}, 0 >, , \text{pb}, \text{pc}, \text{tb}, \text{tc}, \text{steps}(-// -)), 1) == F$
- $\text{Proof}(\text{term}, \text{proof}) = \text{Emulate}(\text{proof}, \text{MY\_PROOFCHECKER}) \& \& (\text{plog}(\text{proof}, \text{len}(\text{proof})) = \text{term})$
- Любая представимая в ФА  $\phi$ -я является рекурсивной  $f(x_1 \dots x_n) = \text{plog}(\langle S \langle G_\phi, U_{n+1,1}, \dots, U_{n+1,n}, G_\phi \text{ тут принимает } n + 2 \text{ аргумента: } x_1 \dots x_n, p, b \text{ и возвращает } 0 \text{ если } p - \text{доказательство } \phi(x_1 \dots x, p), \text{ представляющего } f. \rangle \rangle$

## 2.31. Непротиворечивость

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

## 2.32. $\omega$ -непротиворечивость

Теория  $\omega$ -непротиворечива, если из  $\forall \phi(x) \vdash \phi(x \sim)$  следует  $\not\vdash \exists p \neg \phi(p)$ . Проще говоря, если мы взяли формулу, то невозможно вывести одновременно  $\exists x \neg A(x)$  и  $A(0), A(1), \dots$

## 2.33. Первая теорема Гёделя о неполноте

1. Если формальная арифметика непротиворечива, то недоказуемо  $\sigma(' \sigma )$
2. Если формальная арифметика  $\omega$ -непротиворечива, то недоказуемо  $\neg \sigma(' \sigma \sim )$

## 2.34. Первая теорема Гёделя о неполноте в форме Россера

Если формальная арифметика непротиворечива, то в ней найдется такая формула  $\varphi$ , что  $\not\vdash \varphi$  и  $\not\vdash \neg\varphi$

## 2.35. Consis

Consis – утверждение, формально доказывающее непротиворечивость ФА То есть  $\vdash \text{Consis} \Rightarrow$  непротиворечива

## 2.36. Условия Г-Б (наизусть)

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

1.  $\vdash a \Rightarrow \vdash ('a\sim)$
2.  $\vdash \pi('a\sim) \rightarrow \pi(\pi('a\sim)\sim)$
3.  $\vdash \pi('a\sim) \rightarrow \pi('a \rightarrow b)\sim \rightarrow \pi('b\sim)$

## 2.37. Лемма о самоприменении

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

1.  $\vdash a('b\sim) \rightarrow b$
2.  $\vdash \beta \rightarrow a('b\sim)$

## 2.38. Вторая теорема Гёделя о неполноте ФА

Если теория непротиворечива, в ней  $\not\vdash \text{Consis}$

## 2.39. 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  $\forall t(t \in z \leftrightarrow t \in x \vee t \in y)$   $D_j(x) \forall a \forall b (a \in x \& b \in x \& a \neq b \rightarrow a \cap b = \emptyset)$

## 2.40. ZFC

### 2.40.1. Аксиома равенства

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



### 2.40.2. Аксиома пары

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

### 2.40.3. Аксиома объединения

$\forall x (\exists y (y \in x) \rightarrow \exists p \forall y (y \in p \leftrightarrow \exists s (y \in s \& s \in x)))$  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  $s \in x$

### 2.40.4. Аксиома степени

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

### 2.40.5. 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.

### 2.40.6. Аксиома выбора (не входит в ZF по дефолту)

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

### 2.40.7. Аксиома бесконечности

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

### 2.40.8. Аксиома фундирования

$\forall x (x = \emptyset \vee \exists y (y \in x \& y \cap x = \emptyset)) \quad \forall x (x \neq \emptyset \rightarrow \exists y (y \in x \& y \cap x = \emptyset))$  равноценные формулы.

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

### 2.40.9. Схема аксиом подстановки

$\forall x \exists ! y. \varphi(x, y) \rightarrow \forall a \exists b \forall c (c \in b \leftrightarrow (\exists d. (d \in a \& \varphi(d, c))))$  Пусть формула  $\varphi$  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  $c$  отображением из его элементов в подмножество нашего по предикату.

## 2.41. Ординальные числа, операции

- Определение вполне упорядоченного множества (фундированное с линейным порядком).
- Определение транзитивного множества Множество  $X$  транзитивно, если  $\forall a \forall b ((a \in b \& b \in x) \rightarrow a \in x)$
- Ординал – транзитивное вполне упорядоченное отношением  $\in$  мн-во
- Верхняя грань множества ординалов  $S$   $C \{C = \min(X) \& C \in X \mid X = \{z \mid \forall (y \in S)(z \geq y)\}\}$   $C = \text{Upb}(S)$   $\text{Upb}(\{\emptyset\}) = \{\emptyset\}$
- Successor ordinal (сакцессорный ординал?) Это  $b = a' = a \cup \{a\}$
- Предельный ординал Ординал, не являющийся ни 0 ни successor'ом.
- Недостижимый ординал  $\varepsilon$  – такой ординал, что  $\varepsilon = w^\varepsilon$   $\varepsilon_0 = \text{Upb}(w, w^w, w^{w^w}, w^{w^{w^w}}, \dots)$  – минимальный из  $\varepsilon$
- Канторова форма – форма вида  $\sum(a * w^{b+c})$ , где  $b$  – ординал, последовательность строго убывает по  $b$ . Есть слабая канторова форма, где вместо  $a$  ( $a \in \mathbb{N}$ ) пишут  $a$  раз  $w^b$ . В канторовой форме приятно заниматься сложениями и прочим, потому что всякие  $\text{upb}$  – слишком ни о чем.

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

## 2.42. Кардинальные числа, операции

**Определение.** Будем называть множества равномоощными, если найдется биекция.

**Определение.** Будем называть  $A$  не превышающим по мощноти  $B$ , если найдется инъекция  $A \rightarrow B$  ( $|A| \leq |B|$ )

**Определение.** Будем называть меньше по мощноти, чем  $B$ , если  $|A| \leq |B| \& |A| \neq |B|$

**Определение.** Кардинальное число – число, оценивающее мощноть множества.

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

**Определение.** Кардинальное число  $\aleph$  – это ординальное число  $\alpha$ , такое что  $\aleph_i = P(\aleph_{i-1})$   
 $\aleph_0 = \aleph_0$   
 $+$  :  $|A| + |B| = \max(|A|, |B|)$  (если нет общих элементов)  $= |A \cup B|$

## 2.43. Диагональный метод, теорема Лёвенгейма-Скулема

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

## 2.44. 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.

## 2.45. 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  $S_\infty$  непротиворечива, то и  $S$  непротиворечива.

### 3. Ticket 1: ИВ

#### 3.1. 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.

#### 3.2. 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.

#### 3.3. Схемы аксиом и правило вывода

Аксиомы:

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

Правило вывода М.Р.:

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

### 3.4. Теорема о дедукции

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

1.  $A$   
 $A \rightarrow \alpha \rightarrow A$   
 $\alpha \rightarrow A$
2. (там где-то сзади уже было  $\alpha \rightarrow A$ ,  $\alpha \rightarrow A \rightarrow B$ )  
 $(\alpha \rightarrow A) \rightarrow (\alpha \rightarrow A \rightarrow B) \rightarrow (\alpha \rightarrow B)$   
 $(\alpha \rightarrow A \rightarrow B) \rightarrow (\alpha \rightarrow B)$   
 $\alpha \rightarrow B$
3.  $A \rightarrow A$  умеем доказывать

$\Leftarrow$  Если нужно переместить влево, то перемещаем, добавляем

$A \rightarrow B$  (последнее)

$A$  (перемещенное)

$B$

### 3.5. 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

## 4. Ticket 2: полнота ИВ

### 4.1. 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.

#### 4.1.1. Контрапозиция

**Лемма 4.1.**  $(\alpha \rightarrow \beta) \rightarrow (\neg\beta \rightarrow \neg\alpha)$

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

- |     |  |            |                                     |
|-----|--|------------|-------------------------------------|
| (1) | $\alpha \rightarrow \beta$   | Допущение  |                                     |
| (2) | $(\alpha \rightarrow \beta) \rightarrow (\alpha \rightarrow \neg\beta) \rightarrow \neg\alpha$ | Сх. акс. 9 |                                     |
| (3) | $(\alpha \rightarrow \neg\beta) \rightarrow \neg\alpha$  | М.Р. 1,2   |                                     |
| (4) | $\neg\beta \rightarrow \alpha \rightarrow \neg\beta$   | Сх. акс. 1 | После применения теоремы о дедукции |
| (5) | $\neg\beta$  | Допущение  |                                     |
| (6) | $\alpha \rightarrow \neg\beta$   | М.Р. 5,4   |                                     |
| (7) | $\neg\alpha$   | М.Р. 6,3   |                                     |

2 раза получим как раз то, что нужно

□

#### 4.1.2. Правило исключенного третьего

С помощью контрапозиции доказываем два утверждения:

$\neg(A|\neg A) \rightarrow \neg A$  (один раз контрапозицию от этого обратную, там  $A \rightarrow (A|\neg A)$  акс)

$\neg(A|\neg A) \rightarrow \neg\neg A$  Потом девятую аксиому и снимаем двойное отрицание

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

#### 4.1.4. Правило со звездочкой (14 доказательств)

1.  $\alpha, \beta \vdash \alpha \vee \beta$   
 $\alpha$   
 $\alpha \rightarrow \alpha \vee \beta$   
 $\alpha \vee \beta$
2.  $\alpha, \neg\beta \vdash \alpha \vee \beta$   
 $\alpha$   
 $\alpha \rightarrow \alpha \vee \beta$   
 $\alpha \vee \beta$
3.  $\neg\alpha, \beta \vdash \alpha \vee \beta$   
 $\beta$   
 $\beta \rightarrow \alpha \vee \beta$   
 $\alpha \vee \beta$

4.  $\neg\alpha, \neg\beta \vdash \neg(\alpha \vee \beta)$   
 $\neg\alpha$   
 $\neg\beta$   
 $(\alpha \vee \beta \rightarrow \alpha) \rightarrow (\alpha \vee \beta \rightarrow \neg\alpha) \rightarrow \neg(\alpha \vee \beta)$   
 $\neg\alpha \rightarrow \alpha \vee \beta \rightarrow \neg\alpha$   
 $\alpha \vee \beta \rightarrow \neg\alpha$   
 $\neg\alpha, \neg\beta, \alpha \vee \beta \vdash \alpha$   
 $\neg\alpha$   
 $\neg\beta$   
 $\alpha \vee \beta$   
 $\alpha \rightarrow \alpha$   
 $\dots // \Delta\text{-BO } \neg\beta, \neg\alpha \vdash \beta \rightarrow \alpha$   
 $\beta \rightarrow \alpha$   
 $(\alpha \rightarrow \alpha) \rightarrow ((\beta \rightarrow \alpha) \rightarrow (\alpha \vee \beta \rightarrow \alpha))$   
 $(\beta \rightarrow \alpha) \rightarrow (\alpha \vee \beta \rightarrow \alpha)$   
 $\alpha \vee \beta \rightarrow \alpha$   
 $\alpha$   
 $\alpha \vee \beta \rightarrow \alpha$   
 $(\alpha \vee \beta \rightarrow \neg\alpha) \rightarrow \neg(\alpha \vee \beta)$   
 $\neg(\alpha \vee \beta)$

5.  $\alpha, \beta \vdash \alpha \& \beta$   
 $\alpha$   
 $\beta$   
 $\alpha \rightarrow \beta \rightarrow \alpha \& \beta$   
 $\beta \rightarrow \alpha \& \beta$   
 $\alpha \& \beta$

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

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

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

9.  $\alpha, \beta \vdash \alpha \rightarrow \beta$   
 $\beta$   
 $\beta \rightarrow \alpha \rightarrow \beta$   
 $\alpha \rightarrow \beta$

10.  $\alpha, \neg\beta \vdash \neg(\alpha \rightarrow \beta)$

$\alpha$

$\neg\beta$

$\neg\beta \rightarrow ((\alpha \rightarrow \beta) \rightarrow \neg\beta)$

$(\alpha \rightarrow \beta) \rightarrow \neg\beta$

$\alpha, \neg\beta, \alpha \rightarrow \beta \vdash \beta$

$\alpha$

$\alpha \rightarrow \beta$

$\beta$

$(\alpha \rightarrow \beta) \rightarrow \beta$

$((\alpha \rightarrow \beta) \rightarrow \beta) \rightarrow ((\alpha \rightarrow \beta) \rightarrow \neg\beta) \rightarrow \neg(\alpha \rightarrow \beta)$

$((\alpha \rightarrow \beta) \rightarrow \neg\beta) \rightarrow \neg(\alpha \rightarrow \beta)$

$\neg\beta \rightarrow (\alpha \rightarrow \beta) \rightarrow \neg\beta$

$(\alpha \rightarrow \beta) \rightarrow \neg\beta$

$\neg(\alpha \rightarrow \beta)$

11.  $\neg\alpha, \beta \vdash \alpha \rightarrow \beta$

$\beta$

$\beta \rightarrow \alpha \rightarrow \beta$

$\alpha \rightarrow \beta$

12.  $\neg\alpha, \neg\beta \vdash \alpha \rightarrow \beta$

Ну тут типо очевидно (на самом деле тут боль и страдания)

13.  $\alpha \vdash \neg\neg\alpha$

Схема аксиом 9

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

$\neg\alpha$



## 5. Ticket 3: ИИВ

### 5.1. ИИВ, структура, модель

Сигнатура -  $(R, F, C, r)$ :  $R$  - множество символов для предикатов,  $F$  - функциональных символов,  $C$  - символов констант,  $r$  - функция, определяющая арифметичность  $x \in R \vee F$ . 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  $\alpha \rightarrow \neg\alpha \rightarrow \beta$ .

Она доказывается и в ИВ:

**Лемма 5.1.**  $\alpha, \alpha \vee \neg\alpha, \neg\alpha \vdash \beta$

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

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

**Лемма 5.2.**  $\alpha \rightarrow \alpha \vee \neg\alpha \rightarrow \neg\alpha \rightarrow \beta, \alpha \vee \neg\alpha \vdash \alpha \rightarrow \neg\alpha \rightarrow \beta$

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

### 5.2. Опровергаемость исключенного третьего

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

- конъюнкция: минимум из двух значений (например  $I \& H = H$ ).
- дизъюнкция: максимум из двух значений (например  $I \vee H = I$ ).
- импликация:  $I \rightarrow \alpha = \alpha, L \rightarrow \alpha = I, H \rightarrow L = L, H \rightarrow H = I, H \rightarrow I = I$ .

- отрицание:  $\neg H = L$ , а для остальных элементов все так же.

Назовем формулу *3-тавтологией*, если она принимает значение И при любых значениях переменных из множества  $\{И, Л Н\}$ . 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  $\alpha = Н$ . Следовательно она не 3-тавтология, а значит невыводима.

### 5.3. Решетки

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

- Аксиомы идемпотентности  
 $\alpha + \alpha = \alpha$   
 $\alpha * \alpha = \alpha$
- 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  $\inf$  ( $\sup(\varphi) = \min\{u | u \geq \forall x \in \varphi\}$ ,  $\inf(\varphi) = \max\{u | u \leq \forall x \in \varphi\}$ ).

$$\alpha + \beta = \sup(\{\alpha, \beta\})$$

$$\alpha * \beta = \inf(\{\alpha, \beta\})$$

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  $\alpha$  и  $\beta$  из множества существует псевдодополнение  $\alpha$  относительно  $\beta$  ( $\alpha \rightarrow \beta$ ), которое определяется так:

$$\alpha \rightarrow \beta = \max\{\gamma | \gamma * \alpha \leq \beta\}$$

Свойства импликативной решетки:

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

## 5.4. 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 дополненности
$$\alpha * \neg \alpha = 0$$
$$\alpha + \neg \alpha = 1$$

Также Булеву алгебру можно определить как импликативную решетку над фундированным множеством. Тогда 1 в ней будет  $\alpha \rightarrow \alpha$ ,  $\neg \alpha = \alpha \rightarrow 0$ . 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  $\neg \alpha = \alpha \rightarrow 0$

## 5.5. Алгебра Линденбаума-Тарского

Пусть  $V$  – множество формул ИИВ

Порядок для решетки:

$$\alpha \leq \beta \Leftrightarrow \alpha \vdash \beta$$

$$\alpha \sim \beta \Leftrightarrow \alpha \vdash \beta \& \beta \vdash \alpha$$

Определим операции и 0, 1:

$$0 = \alpha \& \neg \alpha = \perp$$

$$1 = \alpha \rightarrow \alpha = \top$$

$$\alpha \& \beta = \alpha * \beta$$

$$\alpha \vee \beta = \alpha + \beta$$

$$\neg \alpha = -\alpha$$

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

**Лемма 5.3.**  $\forall \beta \in V \perp \vdash \beta$  (Из лжи следует все)

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

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

□

## 5.6. Теорема о полноте ИИВ относительно алгебры Гейтинга

Возьмем в качестве алгебры Гейтинга алгебру Линденбаума-Тарского -  $\xi$ . Она очевидно является моделью.

**Теорема 5.4.**  $\models \alpha \Rightarrow \vdash \alpha$

*Доказательство.*  $\models \alpha \Rightarrow \llbracket \alpha \rrbracket^\xi = 1$

$\llbracket \alpha \rrbracket^\xi = 1 \Rightarrow 1 \leq \llbracket \alpha \rrbracket^\xi$  (По определению алгебры Л-Т)

$\beta \rightarrow \beta \vdash \alpha$  (По определению  $\leq$  в алгебре Л-Т)

Т.к.  $\beta \rightarrow \beta$  - тавтология, то и  $\alpha$  - тавтология

□

## 5.7. Дизъюнктивность ИИВ

Используем алгебру Гёделя  $\Gamma(A)$  ( $\gamma$  - 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  $\omega$  ( $\gamma(1) = \omega$ ). Таким образом  $\Gamma(A) = A \cup \{\omega\}$ . Порядок в  $\Gamma(A)$ :

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

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

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

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

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

**Лемма 5.5.** Гёделева алгебра является Гейтинговой

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

□

**Теорема 5.6.**  $\vdash \alpha \vee \beta \Rightarrow$  либо  $\vdash \alpha$ , либо  $\vdash \beta$

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

□

## 5.8. Теорема Гливенко

**Теорема 5.7.** Если в ИВ доказуемо  $\alpha$ , то в ИИВ доказуемо  $\neg\neg\alpha$ .

*Доказательство.* Разберем все встречающиеся в изначальном доказательстве формулы

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

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

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

Значит, если  $\alpha$  - аксиома с 1-ой по 9-ую, то  $\neg\neg\alpha$  так же может быть доказано

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

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

3. Приведем конструктивное доказательство:

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

Давайте для начала докажем, что  $\neg\neg\alpha, \neg\neg(\alpha \rightarrow \beta), \neg\beta, \alpha, \alpha \rightarrow \beta \vdash \beta$ .

(1)	$\alpha$	Допущение
(2)	$\alpha \rightarrow \beta$	Допущение
(3)	$\beta$	М.Р. 1,2

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

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

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

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

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

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

□

## 5.9. 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:

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

## 6. Ticket 4: ИИБ2

### 6.1. Модели Крипке

$W$  – множество миров

$V$  – множество вынужденных переменных

Введем отношение частичного порядка на  $W$  -  $\leq$  (отношение достижимости). И введем оценку переменной  $v : W \times V \rightarrow \{0, 1\}$ .  $v$  должна быть монотонна (Если  $v(x, P) = 1$  и  $x \leq y$ , то  $v(y, P) = 1$ ). Если переменная  $x$  истинна в мире  $w$ , то мы пишем  $w \models x$ .

Модель Крипке – это  $\langle W, \leq, v \rangle$ .

Теперь можно определить истинность любой формулы (в данном мире) индукцией по построению формулы. Правила:

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

### 6.2. Корректность ИИБ относительно моделей Крипке

**Теорема 6.1.** Если формула выводима в ИИБ, 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  $A$ ,  $A \rightarrow B$ , то истинно и  $B$
- Аксиомы:
  1.  $A \rightarrow (B \rightarrow A)$   
Пусть где-нибудь истинна  $A$ , в силу монотонности она истинна во всех б'ольших мирах, так что  $B \rightarrow A$  тоже будет истинно.
  2.  $(A \rightarrow B) \rightarrow ((A \rightarrow (B \rightarrow C)) \rightarrow (A \rightarrow C))$   
Пусть где-нибудь истинно  $A \rightarrow B$ , тогда необходимо доказать, что истинно и  $((A \rightarrow (B \rightarrow C)) \rightarrow (A \rightarrow C))$ .
    - Пусть истинны  $A, B$ . Тогда если истинно  $A \rightarrow (B \rightarrow C)$ , то истинно и  $C$  по монотонности  $A$  и  $B$ .  $A, B, C$  истинны, значит  $A \rightarrow C$  истинно.
    - Пусть не истинны ни  $A$ , ни  $B$ . Тогда  $A \rightarrow (B \rightarrow C)$  не истинно и  $C$  не истинно. Значит  $A \rightarrow C$  не может быть истинно, т.к. ни  $A$ , ни  $B$ , ни  $C$  не истинны.
  3. Подобным образом доказываем все аксиомы

□

### 6.3. Вложение Крипке в Гейтинга

Не нужно

### 6.4. Полнота ИИВ в моделях Крипке

**Теорема 6.2.** 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  $b \in M$ . Докажем, что если  $M \vdash a$ , то  $a \in M$ :  
Пусть это не так. Рассмотрим  $a \rightarrow a \vee \neg a$ . 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:
  - (a)  $W, x \Vdash P \Leftrightarrow v(x, P) = 1$  если  $P \in V$  ( $V$  - множество вынужденных переменных).  
Монотонность выполняется по определению дерева
  - (b)  $W, x \Vdash (A \& B) \Leftrightarrow W, x \Vdash A$  и  $W, x \Vdash B$   
С помощью аксиомы  $A \& B \rightarrow A$  доказываем  $W \vdash A$ , значит  $A \in W$ . Аналогично с  $B$
  - (c)  $W, x \Vdash (A \vee B) \Leftrightarrow W, x \Vdash A$  или  $W, x \Vdash B$   
Очевидно по определению дизъюнктивности
  - (d)  $W, x \Vdash (A \rightarrow B) \Leftrightarrow \forall y \geq x (W, y \Vdash A \Rightarrow W, y \Vdash B)$   
Мы знаем, что  $W \vdash A \rightarrow B$ . Пусть в  $W$  есть  $A$ , тогда по М.Р. докажем, что  $B$ . Пусть в  $W$  есть  $B$ , тогда мы уже получили  $B$ .
  - (e)  $W, x \Vdash \neg A \Leftrightarrow \forall y \geq x (W, y \not\Vdash A)$   
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  $W_0 = \{\text{все тавтологии ИИВ}\}$ .  $W_0 \Vdash A$ , т.е.  $\vdash A$ .

□

### 6.5. Нетабличность интуиционистской логики

**Теорема 6.3.** 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 Яськовского  $V = \{0, 1\}$ ,  $0 \leq 1$ . Пусть имеется  $V = \{\dots\}$ ,  $|V| = n$  - множество истинностных значений. Пусть его размер больше 2. Тогда построим формулу  $\bigvee_{(1 \leq j < i \leq n+1)} (p_i \rightarrow p_j)$  - такая большая дизъюнкция из импликаций



1. Она общезначима, т.к. всего таких импликаций у нас будет  $C_n^2 \geq n$  (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  $\{0, w_1, w_2, \dots, 1\}$ . 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  $j < i$  if  $(a_i \rightarrow a_j) = f(a_i) \rightarrow f(a_j) = f(a_j)$ . Последнее выражение не может являться 1, так что формула недоказуема. (ИИВ полно относительно алгебры Гейтинга)

□

## 7. Ticket 5: Логика 2 порядка

### 7.1. Основные определения

Смотрим коснпект  $\mathcal{D}\Gamma$

### 7.2. Теорема о дедукции

**Теорема 7.1.** Если  $\Gamma, \alpha \vdash \beta$ , и в доказательстве отсутствуют применения правил для кванторов, использующих свободные переменные из формулы  $\alpha$ , то  $\Gamma \vdash \alpha \rightarrow \beta$

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

1.  $\delta_i$  - старая аксиома, совпадает с  $\alpha$  или выводится по правилу М.Р.  
Тогда мы знаем, что делать из Теоремы о дедукции для ИВ
2.  $\delta_i$  - новая аксиома  
Тогда все то же самое, что и в старой аксиоме, но нужно так же проверить условие.
3.  $\exists x(\psi) \rightarrow \varphi$  - новое правило вывода
  - Докажем вспомогательную лемму:

**Лемма 7.2.**  $(\alpha \rightarrow (\beta \rightarrow \gamma)) \rightarrow (\beta \rightarrow (\alpha \rightarrow \gamma))$

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

- |     |   |           |
|-----|---|-----------|
| (1) | $\alpha \rightarrow \beta \rightarrow \gamma$ | Допущение |
| (2) | $\alpha$                                      | Допущение |
| (3) | $\beta \rightarrow \gamma$                    | М.Р. 2,1  |
| (4) | $\beta$                                       | Допущение |
| (5) | $\gamma$                                      | М.Р. 4,3  |

□

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

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

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

- Докажем вспомогательную лемму 1

**Лемма 7.3.**  $(\alpha \& \beta \rightarrow \gamma) \rightarrow (\alpha \rightarrow \beta \rightarrow \gamma)$

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

- |     |  |            |
|-----|--|------------|
| (1) | $\alpha$   | Допущение  |
| (2) | $\beta$  | Допущение  |
| (3) | $\alpha \rightarrow \beta \rightarrow \alpha \& \beta$ | Сх. акс. 1 |
| (4) | $\beta \rightarrow \alpha \& \beta$                    | М.Р. 1,3   |
| (5) | $\alpha \& \beta$                                      | М.Р. 2,4   |
| (6) | $\alpha \& \beta \rightarrow \gamma$                   | Допущение  |
| (7) | $\gamma$   | М.Р. 5,6   |

□

- Докажем вспомогательную лемму 2

**Лемма 7.4.**  $(\alpha \rightarrow \beta \rightarrow \gamma) \rightarrow (\alpha \& \beta \rightarrow \gamma)$

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

- |     |   |            |
|-----|---|------------|
| (1) | $\alpha \& \beta \rightarrow \alpha$          | Сх. акс. 4 |
| (2) | $\alpha \& \beta$                             | Допущение  |
| (3) | $\alpha$                                      | М.Р. 2,1   |
| (4) | $\alpha \& \beta \rightarrow \beta$           | Сх. акс. 5 |
| (5) | $\beta$                                       | М.Р. 2,4   |
| (6) | $\alpha \rightarrow \beta \rightarrow \gamma$ | Допущение  |
| (7) | $\beta \rightarrow \gamma$                    | М.Р. 3,6   |
| (8) | $\gamma$                                      | М.Р. 5,7   |

□

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

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

□

### 7.3. Корректность исчисления предикатов

Смотрим конспект ДГ

## 8. Ticket 6: Полнота исчисления предикатов

Тут можно почитать конспект Д.Г.

### 8.1. Свойства противоречивости

Противоречивая теория – теория, в которой можно вывести  $p, \neg p$ .

**Лемма 8.1.** 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) | $\alpha$   | Допущение   |
| (3) | $\alpha \rightarrow \neg \alpha \rightarrow (\alpha \& \neg \alpha)$ | Сх. акс. 10 |
| (4) | $\neg \alpha \rightarrow (\alpha \& \neg \alpha)$                    | 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).