Курс математической логики по Штукенбергу Д.Г.

Daniyar Lolka Itegulov, Ignat Loskutov

23 января 2015 г.

Содержание

1 Базовые понятия **2**
1.1 Формальные системы и модели 2

2 Определения (нужно знать идеально) **4**
2.1 ИВ 4
2.2 Общезначимость, доказуемость, выводимость 4
2.3 Теорема о дедукции для ИВ 5
2.4 Теорема о полноте исчисления высказываний 5
2.5 ИИВ 5
2.6 Теорема Гливенко 5
2.7 Порядки 5
2.8 Решетки (все свойства) 6
2.9 Булевы/псевдобулевы алгебры 6
2.10 Топологическая интерпретация ИИВ 7
2.11 Модель Крипке 7
2.12 Вложение Крипке в алгебры Гейтинга 7
2.13 Полнота ИИВ в алгебрах Гейтинга и моделях Крипке 8
2.14 Нетабличность ИИВ 8
2.15 Предикаты 8
2.16 Теорема о дедукции в предикатах 8
2.17 Теорема о полноте исчисления предикатов 8
2.18 Теории первого порядка, определение структуры и модели 8
2.19 Аксиоматика Пеано 9
2.20 Формальная арифметика - аксиомы 9
2.20.1 Аксиомы 9
2.21 Рекурсивные функции 10
2.22 Функция Аккермана 10
2.23 Существование рек.ф-й не явл. ф-ей Аккермана (определение конечной леммы) 10
2.24 Представимость 10
2.25 Выразимость 11
2.26 Лемма о связи представимости и выразимости 11
2.27 Бета-функция Гёделя, Г-последовательность 11

2.28 Представимость рек.ф-й в ФА (знать формулы для самых простых) 11
2.29 Гёделева нумерация (точно) 12
2.30 Выводимость и рекурсивные функции (че там с Тьюрингом) 12
2.31 Непротиворечивость 12
2.32 w-непротиворечивость 12
2.33 Первая теорема Гёделя о неполноте 12
2.34 Первая теорема Гёделя о неполноте в форме Россера 13
2.35 Consis 13
2.36 Условия Г-Б (наизусть) 13
2.37 Лемма о самоприменении 13
2.38 Вторая теорема Гёделя о неполноте ФА 13
2.39 Теория множеств 13
2.40 ZFC 13
2.40.1 Аксиома равенства 13
2.40.2 Аксиома пары 14
2.40.3 Аксиома объединений 14
2.40.4 Аксиома степени 14
2.40.5 Схема аксиом выделения 14
2.40.6 Аксиома выбора (не входит в ZF по дефолту) 14
2.40.7 Аксиома бесконечности 14
2.40.8 Аксиома фундирования 14
2.40.9 Схема аксиом подстановки 14
2.41 Ординальные числа, операции 15
2.42 Кардинальные числа, операции 15
2.43 Диагональный метод, теорема Лёвенгейма-Скулема 16
2.44 Парадокс Скулема 16
2.45 Теорема Генцена о непротиворечивости ФА 16

3 Ticket 1: ИВ **17**
3.1 Определения (исчисление, высказывание, оценка...) 17
3.2 Общезначимость, доказуемость, выводимость 17
3.3 Схемы аксиом и правило вывода 17
3.4 Теорема о дедукции 18
3.5 Корректность исчисления высказываний относительно алгебры Яськовского 18

4 Ticket 2: полнота ИВ **19**
4.1 Полнота исчисления высказываний относительно алгебры Яськовского . . . 19
4.1.1 Контрапозиция 19
4.1.2 Правило исключененного третьего 19
4.1.3 Всякие очевидные вещи типа если выводится из А и из Б то из А и Б тоже 19
4.1.4 Правило со звездочкой (14 доказательств) 19

5 Ticket 3: ИИВ **22**
5.1 ИИВ, структура, модель 22
5.2 Опровергаемость исключенного третьего 22
5.3 Решетки 23

5.4 Алгебра Гейтинга, булева алгебра 24
5.5 Алгебра Линденбаума-Тарского 24
5.6 Теорема о полноте ИИВ относительно алгебры Гейтинга 25
5.7 Дизъюнктивность ИИВ 25
5.8 Теорема Гливенко 26
5.9 Топологическая интерпретация 27

6 Ticket 4: ИИВ2 **28**
6.1 Модели Крипке 28
6.2 Корректность ИИВ относительно моделей Крипке 28
6.3 Вложение Крипке в Гейтинга 29
6.4 Полнота ИИВ в моделях Крипке 29
6.5 Нетабличность интуиционистской логики 29

7 Ticket 5: Логика 2 порядка **31**
7.1 Основные определения 31
7.2 Теорема о дедукции 31
7.3 Корректность исчисления предикатов 32

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 ({" $\to$ "," $\cup$ ",""})
   - Misc - дополнительные элементы ({"(", ")", " "})
   - arity: $\mathsf{Foo} \cup \mathsf{Pr} \cup \mathsf{C} \to \mathsf{N}$ 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 $\mathsf{Pr} \cup \mathsf{F} \to \mathsf{N}$.
2. Интерпретация - это приписывание символам значения и правил действия (отображения из Pr $\cup$ F $\cup$ 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 остановится, 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 $\in V$ - 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.

s

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. $\alpha \to \beta \to \alpha$
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. $\neg\neg\alpha \to \alpha$

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_∞)
- 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 $\Gamma \vdash \alpha \to \beta$ и наоборот.
Доказывается вправо поформульным преобразованием, влево добавлением 1 формулы.
Работает в ИВ, ИИВ, предикатах.

2.4. Теорема 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.

2.5. ИИВ

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

Лемма 2.1. $\alpha, \alpha \vee \neg\alpha, \neg\alpha \vdash \beta$

(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

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

2.6. Теорема 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.

2.7. Порядки

Частичный порядок – рефлексивное, антисимметричное, транзитивное отношение.
Частично упор. мн-во - множество с частичным порядком на элементах.
Линейно упорядоч. мн-во - множество с частичным порядком, в котором два любых элемента сравнимы.
Фундированное мн-во - частично упорядоч. множество, в котором каждое непустое подмножество имеет минимальный элемент.
Вполне упорядоченное множество - фундированное множество с линейным порядком.

2.8. Решетки (все свойства)

- Просто 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:

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

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

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

- Импликативная решетка – всегда существует псевдодополнение b $(b \to a)$ $a \to b = \max\{c|c \times a \leqslant b\}$ Имеет свойства, что в ней всегда есть максимальный элемент $a \to a$ и что она дистрибутивна.

2.9. Булевы/псевдобулевы алгебры

- Булева алгебра 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.

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

     // не 1

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

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. $a + b => a \cup b$
2. $a * b => a \cap b$
3. $a \to b => Int(a^c \cup b)$
4. $-a => \mathrm{Int}(a^c)$
5. $0 =>$ ◎
6. $1 =>$ ◎$\{-L\}$

2.11. Модель Крипке

$Var = \{P, Q, \dots\}$ Модель Крипке – это $< W, \leq, \nu >$, где

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

Правила:

- $W, x \models P$◎◎$\nu(x, P) = 1 P \in Var$
- $W, x \models (A \& B)$◎◎$W, x \models A \& W, x \models B$
- $W, x \models (A \vee B)$◎◎$W, x \models A \vee W, x \models B$
- $W, x \models (A \to B)$◎◎◎$y \geq x(W, y \models A$◎$W, y \models B)$
- $W, x \models \neg A$◎◎◎$y \in x(W, x \neg \models A)$

В мире разрешается быть не вынужденной переменной и ее отрицанию одновремеменно. 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:

- = ∪, * = ∩,

$a \to b = \cup\{z \in H | z \leq x^c \cup y\}$ Так созданное множество с операциями является импликативной решеткой, в которой мы определим $-a = a \to 0$, 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, привев 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 $\circledcirc x.A \rightarrow A[x := \eta]$, где η 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 сводобно 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 γ $\Gamma, \gamma \vdash \alpha => \Gamma \vdash \gamma \rightarrow \alpha$

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 $< D, F, P >$, 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 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).

2.19. 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. $P(0) \& \forall n.(P(n) \to P(succ(n))) \to \forall n.P(n)$

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 = {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. $a = b \to a' = b'$
2. $a = b \to a = c \to b = c$
3. $a' = b' \to a = b$
4. $\neg(a' = 0)$

5. $a + b' = (a + b)'$

6. $a + 0 = a$

7. $a * 0 = 0$

8. $a * b' = a * b + a$

9. $\varphi[x := 0] \& \forall x.(\varphi \to \varphi[x := x']) \to \varphi$ // φ содержит св.п x

2.21. Рекурсивные функции

$Z(x) = 0$
$N(x) = x + 1$
$U_i^n(x_1, \dots, x_n) = x_i$
$S\langle f, g_1, \dots, g_n\rangle(x_1, \dots, x_m) = f(g_1(x_1 \dots x_m), \dots g_n(x_1, \dots, x_m))$
$R\langle f, g\rangle(x_1 \dots x_n, n) = \begin{cases} f(x_1 \dots x_n) & n = 0 \\ g(x_1 \dots x_n, n, R\langle f, g\rangle(x_1 \dots x_n, n-1)) & n > 0 \end{cases}$
$\mu\langle f\rangle(x_1, \dots, x_n)$ - минимальное k, такое что $f(x_1 \dots x_n, k) = 0$

2.22. Функция Аккермана

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

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

Пусть $f(n_1 \dots n)$ - примитивная рекурсинвная 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 $f : N^n \to N$ называется представимой в формальной арифметике, если существует отношение $a(x_1 \dots x_{n+1})$, ее представляющее, причем выполнено следующее:

1. $f(a, b, \dots) = x <=> \vdash a(a\sim, b\sim, \dots x\sim)$

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 !n

2.27. Бета-функция Гёделя, Г-последовательность

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

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:

- $Emulate(input, prog) = plog(R < f, g > (< `S, input, 0 >, , pb, pc, tb, tc, steps(-//-)), 1) == F$
- $Proof(term, proof) = Emulate(proof, MY_PROOFCHECKER)\&\&(plog(proof, len(proof)) = term)$
- Любая представимая в ФА ф-я является рекурсивной $f(x_1 \dots x_n) = plog(\langle S\langle G_\varphi, U_{n+1,1}, \dots, U_{n+1,n},$ 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.

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. w-непротиворечивость

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

2.33. Первая теорема Гёделя о неполноте

1. Если формальная арифметика непротиворечива, то недоказуемо σ(‘σ~)
2. Если формальная арифметика w-непротиворечива, то недоказуемо ¬(‘~)

2.34. Первая теорема Гёделя о неполноте в форме Россера

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

2.35. Consis

Consis - утверждение, формально доказывающее непротиворечивость ФА То есть $\vdash Consis =>$ непротиворечива

2.36. Условия Г-Б (наизусть)

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

1. $\vdash a =>\vdash (`a\sim)$
2. $\vdash (`a\sim) \to (`(`a\sim)\sim)$
3. $\vdash (`a\sim) \to (`(a \to b)\sim) \to (`b\sim)$

2.37. Лемма о самоприменении

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

1. $\vdash a(`b\sim) \to b$
2. $\vdash \beta \to a(`b\sim)$

2.38. Вторая теорема Гёделя о неполноте ФА

Если теория непротиворечива, в ней $\nvdash Consis$

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 $\circledcirc t(t \in z \leftrightarrow t \in x \& t \in y)$ $x \cup y = z$, тогда $\circledcirc t(t \in z \leftrightarrow t \in x \vee t \in y)$ $D_j(x) \forall a \forall b(a \in x \& b \in x \& a \neq b \to a \cap b = \emptyset)$

2.40. ZFC

2.40.1. 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

2.40.2. 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. $\{x, y\}$

2.40.3. 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

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 $2^{@}$ - 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 $a \neq 0$, то $x \in a \neq 0$

2.40.7. Аксиома бесконечности

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

2.40.8. 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"

2.40.9. 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.

2.41. Ординальные числа, операции

- Определение вполне упорядоченного множества (фундированное с линейныи 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 $C|\{C = min(X) \& C \in X | X = \{z|\circledcirc(y \in S)(z \geq y)\}\}$ $C = Upb(S)$ $Upb(\{\emptyset\}) = \{\emptyset\}$
- Successor ordinal (сакцессорный ординал?) Это b = a' = a ∪ {a}
- Предельны ординал Ординал, не являющийся ни 0 ни successor'ом.
- Недостижимый ординал ε - такой ординал, что $\varepsilon = w^{\varepsilon}$ $\varepsilon_0 = \mathrm{Upb}(w, w^w, w^{w^w}, w^{w^{w^w}}, \dots)$ - 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.

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

2.42. Кардинальные числа, операции

Будем называть множества равномощными, если найдется биекция. Будем называть A не превышающим по мощности B, если найдется инъекция $A \to B(|A| \leq |B|)$ Будем называть A меньше по мощности, чем B, если $|A| \leq |B| \& |A| \neq |B|$ Кардинальное число - число, оценивающее мощность множества. Кардинальное число $\circledcirc$ - это ординальное число a, такое что $\forall x \leq a |x| \leq |a|$ $\aleph_0 = w$ по определению; $\aleph_1 =$ минимальный кардинал, следующий за $\aleph_0$ Кардинальное число $\circledcirc$ - это ординальное число a, такое что $= P(_{i-1})\ _0 = \aleph_0$ +: |A| + |B| = max(|A|, |B|) (если нет общих элементов) = |A ∪ 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_∞ 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. $\alpha \to \beta \to \alpha$
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.:

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

3.4. Теорема о дедукции

$\Rightarrow$ Если нужно переместить последнее предположение вправо, то рассматриваем случаи – аксиома или предположение, MP, 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. $A \to A$ умеем доказывать

$\Leftarrow$ Если нужно переместить влево, то перемещаем, добавляем
$A \to B$ (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. $(\alpha \to \beta) \to (\neg\beta \to \neg\alpha)$

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)	$(\alpha \to \neg\beta) \to \neg\alpha$	M.P. 1,2	
(4)	$\neg\beta \to \alpha \to \neg\beta$	Сх. акс. 1	После применения теоремы о дедукции
(5)	$\neg\beta$	Допущение	
(6)	$\alpha \to \neg\beta$	M.P. 5,4	
(7)	$\neg\alpha$	M.P. 6,3	

2 раза получим как раз то, что нужно □

4.1.2. 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

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

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 арность $x \in R \vee F$. Интерпретация - это приписывание символам значения и правил действия Структура - это носитель M (множство 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 5.1. $\alpha, \alpha \vee \neg\alpha, \neg\alpha \vdash \beta$

(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 5.2. $\alpha \to \alpha \vee \neg\alpha \to \neg\alpha \to \beta, \alpha \vee \neg\alpha \vdash \alpha \to \neg\alpha \to \beta$

(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

5.2. Опровергаемость исключенного третьего

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

- конъюнкция: минимум из двух значений (например И&Н $=$ Н).
- дизъюнкция: максимум из двух значений (например И $\vee$ Н $=$ И).
- импликация: И $\to \alpha = \alpha$, Л $\to \alpha =$ И, Н $\to$ Л $=$ Л, Н $\to$ Н $=$ И, Н $\to$ Н $=$ И.

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

Назовем формулу *3-тавтологией*, если она принимает значение $\mathsf{И}$ при любых значениях переменных из множества $\{\mathsf{И}, \mathsf{Л}\, \mathsf{H}\}$. 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 H при $\alpha = \mathsf{H}$. 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 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 ($sup(\varphi) = min\{u|u \geq \forall x \in \varphi\}$, $inf(\varphi) = max\{u|u \leq \forall x \in \varphi\}$).
$\alpha + \beta = sup(\{\alpha, \beta\})$
$\alpha * \beta = inf(\{\alpha, \beta\})$
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 α и β из множества существует псевдодополнение α относительно β ($\alpha \to \beta$), которое определяется так:
$\alpha \to \beta = max\{\gamma|\gamma * \alpha \leq \beta\}$
Свойства *импликативной решетки*:

- Существует максимальный элемент $\alpha \to \alpha$, 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 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 $\neg\alpha = \alpha \to 0$

5.5. Алгебра Линденбаума-Тарского

Пусть V – множество формул ИИВ
Порядок для решетки:
$\alpha \le \beta \Leftrightarrow \alpha \vdash \beta$
$\alpha \sim \beta \Leftrightarrow \alpha \vdash \beta \& \beta \vdash \alpha$
Определим операции и 0, 1:
$0 - \alpha \& \neg\alpha = \perp$
$1 - \alpha \to \alpha = \top$
$\alpha \& \beta = \alpha * \beta$
$\alpha \vee \beta = \alpha + \beta$
$\neg\alpha = -\alpha$
Получившаяся алгебра называется *алгеброй Линденбаума-Тарского* и является алгеброй Гейтинга, т.к. для нее выполняется аксиома $\alpha * \neg\alpha = 0$ (по определению).

Лемма 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)	$\alpha\&\neg\alpha \to \alpha$	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

□

5.6. Теорема о полноте ИИВ относительно алгебры Гейтинга

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

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

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

5.7. 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 $\Gamma(A)$:

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

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

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

$a \to b$	$b=1$	$b=\gamma(v)$
$a=1$	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 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 $[\![\alpha \vee \beta]\!]^{A} = 1$ 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. □

5.8. Теорема Гливенко

Теорема 5.7. 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 $\neg\neg\alpha$ так же 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 доказтельстве 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)	$\alpha \to \neg\neg(\alpha \to \beta)$	M.P. 4,3
(6)	$(\alpha \to \neg\neg(\alpha \to \beta)) \to \neg\alpha$	M.P. 2,1
(7)	$\neg\alpha$	M.P.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)	$\neg\beta \to \neg\neg\alpha$	M.P. 4,3
(6)	$(\neg\beta \to \neg\neg\alpha) \to \neg\neg\beta$	M.P. 2,1
(7)	$\neg\neg\beta$	M.P. 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:

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

6. Ticket 4: ИИВ2

6.1. Модели Крипке

W – множество миров
V – множество вынужденных переменных
Введем отношение частичного порядка на W - $\leq$ (отношение достижимости). И введем оценку переменной $\nu : W \times V \to \{0, 1\}$. ν должна быть монотонна (Если $\nu(x, P) = 1$ и $x \leq y$, то $\nu(y, P) = 1$). Если пременная x истинна в мире w, то мы пишем $w \Vdash x$.
Модель Крипке – это $< W, \leq, \nu >$.
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 $u \geq w$, в котором истинна A, истинна так же истинна и B;
- $w \Vdash \neg A \Leftrightarrow$ ни в каком мире $u \geq w$ формула A не является истинной;

6.2. Корректность ИИВ относительно моделей Крипке

Теорема 6.1. 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 б‘ольших 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.
  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 $a \to a \vee \neg a$. 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:

   (a) $W, x \Vdash P \Leftrightarrow \nu(x, P) = 1$ 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 $A \& B \to A$ 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) $W, x \Vdash (A \to B) \Leftrightarrow \forall y \geq x (W, y \Vdash A \Rightarrow W, y \Vdash B)$
   Мы знаем, что $W \vdash A \to B$. Пусть в W есть A, тогда по М.Р. докажем, что B. Пусть в W есть B, тогда мы уже получили B.

   (e) $W, x \Vdash \neg A \Leftrightarrow \forall y \geq x (W, x \nVdash A)$
   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. $\vdash A$.

□

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 J_0 Яськовского $V = \{0, 1\}, 0 \leq 1$.
Пусть имеется $V = \{...\}$, $|V| = n$ - множество истиностных значений. Пусть его размер больше 2. Тогда построим формулу $\vee_{(1 \leq j < i \leq n+1)}(p_i \to p_j)$ - 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)

$\square$

7. Ticket 5: *Логика 2 порядка*

7.1. Основные определения

Смотрим косплект ДГ

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 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 7.2. $(\alpha \to (\beta \to \gamma)) \to (\beta \to (\alpha \to \gamma))$

     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 7.3. $(\alpha \& \beta \to \gamma) \to (\alpha \to \beta \to \gamma)$

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

□

- Докажем вспомогателньую лемму 2

Лемма 7.4. $(\alpha \to \beta \to \gamma) \to (\alpha\&\beta \to \gamma)$

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

□

- 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

□

7.3. Корректность исчисления предикатов

Смотрим конспект ДГ