Курс математической логики по Штукенбергу Д.Г.

January 22, 2015

Contents

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 (Num + BigLatinChar)
   - F - множество функций (большие заглавные латинские чары)
   - C - описывает константы
   - Links - множество связок ({"->", "∪", " "})
   - Misc - дополнительные элементы ({"(", ")", " "})

- arity: $Foo \cup Pr \cup C \to N$ 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 $Pr \cup F \to N$.

2. Интерпретация - это приписывание символам значения и правил действия (отображения из Pr ∪ F ∪ 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.

2 Определения (нужно знать идеально)

Определения тут зачастую дублицируют 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. $a \to b \to a$
2. $(a \to b) \to (a \to b \to c) \to (a \to c)$
3. $a \to b \to a \& b$
4. $a \& b \to a$
5. $a \& b \to b$
6. $a \to a \vee b$
7. $b \to a \vee b$
8. $(a \to b) \to (c \to b) \to (a \vee c \to b)$
9. $(a \to b) \to (a \to \neg b) \to \neg a$
10. $\neg\neg a \to a$

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 $, a \vdash b$ следует $\vdash a \to b$ и наоборот. Доказывается вправо поформульным преобразованием, влево добавлением 1 формулы. Работает в ИВ, ИИВ, предикатах.

2.4 Теорема о полноте исчисления высказываний

Типа исчисление предикатов полно относительно вот той булевой алгебры. Общий ход д-ва: строим док-ва для конкретных наборов перменных, 2^n, где n - количество возможных переменных. Потом их мерджим.

2.5 ИИВ

Это такое ИВ, в котором убрали десятую аксиому, а вместо нее добавили 10i. 10i: $a \to \neg a \to b$ Кстати она доказывается и в ИВ

1. $(a \to a \vee \neg a) \to (a \to a \vee \neg a \to (\neg a \to b)) \to a \to (\neg a \to b)$

2. $a, a \vee \neg a, \neg a \vdash b$
   a
   $\neg a$

$b \to a$
$b \to \neg a$
$(b \to a) \to (b \to \neg a) \to \neg b$
$\neg b \to a$
$\neg b \to \neg a$
$(\neg b \to a) \to (\neg b \to \neg a) \to \neg\neg b$
$\neg\neg b \to b$
b

3. $a \to (\neg a \to b)$

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

2.6 Теорема Гливенко

Если в ИВ доказуемо a, то в ИИВ доказуемо $\neg\neg a$ Общий ход д-ва: говорим, что если в ИИВ доказуема F, то в ней же доказуема $\neg\neg F$. 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)

- Решетка 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:

$$\sup p = \text{min}\{u|u \geq alls \in p\}$$
$$\inf p = \text{max}\{u|u \leq alls \in p\}$$
$$a + b = \text{sup}\{a, b\}$$
$$a * b = \text{inf}\{a, b\}$$

Если для двух элементов всегда можно определить a + b и a * b, то такое множество назывется 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 R^n. Тогда заключения о общезначимости формулы можно делать более наглядно. Давайте возьмем в качестве множества алгебры все открытые подмножества 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. $-a =>$ Int(a^c)
5. $0 => \circledcirc$
6. $1 => \circledcirc\{-L\}$

2.11 Модель Крипке

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

- W - множество ”миров”
- ≤ - частичный порядок на W (отношение достижимости)
- v: $W \times Var \to \{0, 1, \_\}$ - оценка перменных на W, монотонна (если v(x, P) = 1, x ≤ y, то v(y, P) = 1 – формулу нельзя un’вынудить)

Правила:

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

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. ≤ - отношение "быть подмножеством". Определим 0 как ⊚ (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 ⊚$x.A \to A[x := \,]$, где θ свободна для подстановки в A $A[x := \,] \to \exists x.A, -//-$

Правила вывода:

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

x не входит сводобно в A

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

x не входит свободно в B

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 , $\vdash a$ => $\vdash \ \to a$

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 $\models a$.

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 = hP 0 , P 1 , ...i — 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. $\circledcirc x \in N : (succ(x) = 0)$
4. $(succ(a) = c \& succ(b) = c) \to a = b$
5. $P(0) \& \circledcirc n.(P(n) \to P(succ(n))) \to \circledcirc n.P(n)$

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

2.21 Рекурсивные функции

$Z(x) = 0$
$N(x) = x + 1$
$U(x_1, \dots, x_n) = x$
$S\langle f, g_1, \dots, g\rangle(x_1, \dots, x) = f(g_1(x_1 \dots x), \dots g(x_1, \dots, x))$
$R\langle f, g\rangle(x_1 \dots x, n) = \begin{cases} f(x_1 \dots x) & n = 0 \\ g(x_1 \dots x, n, R\langle f, g\rangle(x_1 \dots x, n-1)) & n > 0 \end{cases}$
$\mu\langle f\rangle(x_1, \dots, x_n)$ - 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 ≥ 0. $\exists J$: $f(n_1 \dots n) < A(J, \sum(n_1, \dots n))$ Доказывается индукцией по рекурсивным функциям.

2.24 Представимость

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

1. $f(a, b, \dots) = x <=>\vdash a(a$~$, b$~$, \dots x$~$)$
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. $n(x_1 \dots x_n) =>\vdash N(x_1$~$, \dots x$~$)$
2. $n(x_1 \dots x) =>\vdash \neg N(x_1$~$, \dots x$~$)$

2.26 Лемма о связи представимости и выразимости

Если n выразимо, то C◎ представимо. C◎ = 1 если n, и нулю если !n

2.27 Бета-функция Гёделя, Г-последовательность

β(b, c, i) = k◎ Функция, отображающая конечную последовательность из N (a◎) в k◎. 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. $u = (x_1 = x_1)\& \ldots \&(x = x)\&(x_{+1} = x)$

4. $s(a_1 \ldots a, b) = \exists b_1 \ldots \exists b(G_1(a_1 \ldots a, b_1)\& \ldots \&Gn(a_1 \ldots a, b)$

5. $r(x_1, \ldots, x_n, k, a) =$

$$\begin{aligned} &\exists b \exists c(\exists k(\beta(b, c, 0, k)\&\varphi(x_1, \ldots, x_n, k))\& \\ &\quad B(b, c, x_{n+1}, a)\& \\ &\quad \forall k(k < x_{n+1} \to \exists d \exists e(B(b, c, k, d)\&B(b, c, k', e)\&G(x_1 \ldots x, k, d, e)))) \end{aligned}$$

6. $m\langle F\rangle(x_1, \ldots, x_{n+1}) = F(x_1, \ldots, x_n, x_{n+1}, 0)\&\forall y((y < x_{n+1}) \to \neg F(x_1, \ldots, x_n, y, 0))$

2.29 Гёделева нумерация (точно)

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

2.30 Выводимость и рекурсивные функции (че там с Тьюрингом)

Основные тезисы по вопросу:

- $Emulate(input, prog) = \text{plog}(R < f, g > (< `S, input, 0 >, \ , pb, pc, tb, tc, steps(-//-)), 1) =$ F

- $Proof(term, proof) = Emulate(proof, MY_PROOFCHECKER)\&\&(\text{plog}(proof, len(proo$ $term)$

- Любая представимая в ФА ф-я является рекурсивной $f(x_1 \dots x) =$ plog$(\langle S \langle G_\varphi, U_{n+1,1}, \dots, U_{n+1,n},$ plog$(U_{n+1,n+1}, 1),$ plog$(U_{n+1,n+1}, 2) \rangle \rangle (x_1, \dots, x_n), 1)$. G_φ тут принимает $n + 2$ аргумента: $x_1 \dots x_n, p, b$ и возвращает 0 если p - доказательство $\varphi(x_1 \dots x, p)$, представляющего f.

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 $\circledcirc\varphi(x) \vdash \varphi(x\text{~})$ следует $\circledcirc\exists p \neg\varphi(p)$. 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 $\neg$(‘~)

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. $\vdash a => \vdash (`a\text{~})$
2. $\vdash (`a\text{~}) \to (`(`a\text{~})\text{~})$
3. $\vdash (`a\text{~}) \to (`(a \to b)\text{~}) \to (`b\text{~})$

2.37 Лемма о самоприменении

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

1. $\vdash a(`b\text{~}) \to b$
2. $\vdash \ \to a(`b\text{~})$

2.38 Вторая теорема Гёделя о неполноте ФА

Если теория непротиворечива, в ней ◎$Consis$

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 ◎$t(t \in z \leftrightarrow t \in x \& t \in y)$ $x \cup y = z$, тогда ◎$t(t \in z \leftrightarrow t \in x \vee t \in y)$ $Dj(x)$◎a◎$b(a \in x \& b \in x \& a \neq b \to a \cap b =$ ◎$)$

2.40 ZFC

2.40.1 Аксиома равенства

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

2.40.2 Аксиома пары

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

2.40.3 Аксиома объединений

$\circledcirc x(\exists y(y \in x) \to \exists p \circledcirc y(y \in p \leftrightarrow \exists s(y \in s \& s \in x)))$ 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

$\circledcirc x \exists p \circledcirc y(y \in p \leftrightarrow y \in x)$ 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

$\circledcirc x \exists b \circledcirc y(y \in b \leftrightarrow (y \in x \& \varphi(y)))$ 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

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

2.40.8 Аксиома фундирования

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

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

2.40.9 Схема аксиом подстановки

$\circledcirc x\exists!y.\varphi(x,y) \to \circledcirc a\exists b\circledcirc c(c \in b \leftrightarrow (\exists d.(d \in a\&\varphi(d,c))))$ 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 $\circledcirc a\circledcirc b((a \in b\&b \in x) \to a \in x)$
- Ординал - транзитивное вполне упорядоченное отношением $\in$ мн-во
- Верхняя грань множества ординалов S $C|\{C = min(X)\&C \in X|X = \{z|\circledcirc(y \in S)(z{\geq}y)\}\}$ $C = Upb(S)$ $Upb(\{\circledcirc\}) = \{\circledcirc\}$
- 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 $\varepsilon = w^{\varepsilon}$ ε_0 = Upb$(w, w^w, w^{w^w}, w^{w^{w^w}}, \dots)$ - минимальный из ε
- Канторова форма - форма вида ∑(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.

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

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 ◎ - это ординальное число a, такое что ◎ x ≤ a |x| ≤ |a| $\aleph_0 = w$ по определению; $\aleph_1 =$ минимальный кардинал, следующий за $\aleph_0$ Кардинальное число ◎ - это ординальное число a, такое что $= P(_{i-1})\ _0 = {}_0$ +: |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_∞)
- 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. $a \to b \to a$
2. $(a \to b) \to (a \to b \to c) \to (a \to c)$

3. $a \to b \to a\&b$

4. $a\&b \to a$

5. $a\&b \to b$

6. $a \to a \vee b$

7. $b \to a \vee b$

8. $(a \to b) \to (c \to b) \to (a \vee c \to b)$

9. $(a \to b) \to (a \to \neg b) \to \neg a$

10. $\neg\neg a \to a$

Правило вывода: MP:

$$\frac{A \quad (A \to B)}{B}$$

3.4 Теорема о дедукции

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

1. A
   $A \to a \to A$
   $a \to A$

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

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

Хотим: $(a \to b) \to (\neg b \to \neg a)$
$(a \to b), \neg b \vdash \neg a$
$a \to b$
$(a \to b) \to (a \to \neg b) \to \neg a$
$(a \to \neg b) \to \neg a$
$\neg b \to a \to \neg b$
$\neg b$
$a \to \neg b$
$\neg a$
+2 раза дедукцию применить

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. $a, b \vdash a \vee b$
   a
   $a \to a \vee b$
   $a \vee b$

2. $a, \neg b \vdash a \vee b$
   a
   $a \to a \vee b$
   $a \vee b$

3. $\neg a, b \vdash a \vee b$
   b
   $b \to a \vee b$
   $a \vee b$

4. $\neg a, \neg b \vdash \neg(a \vee b)$
   $\neg a$
   $\neg b$
   $(a \vee b \to a) \to (a \vee b \to \neg a) \to \neg(a \vee b)$
   $\neg a \to a \vee b \to \neg a$
   $a \vee b \to \neg a$
   $\neg a, \neg b, a \vee b \vdash a$
   $\neg a$
   $\neg b$
   $a \vee b$
   $a \to a$
   … //д-во $\neg b, \neg a \vdash b \to a$
   $b \to a$
   $(a \to a) \to ((b \to a) \to (a \vee b \to a))$
   $(b \to a) \to (a \vee b \to a)$
   $a \vee b \to a$
   a
   $a \vee b \to a$
   $(a \vee b \to \neg a) \to \neg(a \vee b)$
   $\neg(a \vee b)$

5. $a, b \vdash a\&b$
   a
   b
   $a \to b \to a\&b$
   $b \to a\&b$
   $a\&b$

6. $a, \neg b \vdash \neg(a\&b)$
   $\neg b$
   $((a\&b) \to b) \to ((a\&b) \to \neg b) \to \neg(a\&b)$
   $a\&b \to b$
   $(a\&b \to \neg b) \to \neg(a\&b)$
   $\neg b \to a\&b \to \neg b$
   $a\&b \to \neg b$
   $\neg(a\&b)$

7. $\neg a, b \vdash \neg(a\&b)$
   аналогично

8. $\neg a, \neg b \vdash \neg(a\&b)$
   аналогично

9. $a, b \vdash a \to b$
   b
   $b \to a \to b$
   $a \to b$

10. $a, \neg b \vdash \neg(a \to b)$
    a
    $\neg b$
    $\neg b \to ((a \to b) \to \neg b)$
    $(a \to b) \to \neg b$
    $a, \neg b, a \to b \vdash b$
    a
    $a \to b$
    b
    $(a \to b) \to b$
    $((a \to b) \to b) \to ((a \to b) \to \neg b) \to \neg(a \to b)$
    $((a \to b) \to \neg b) \to \neg(a \to b)$

$\neg b \to (a \to b) \to \neg b$
$(a \to b) \to \neg b$
$\neg(a \to b)$

11. $\neg a, b \vdash a \to b$
b
$b \to a \to b$
$a \to b$