Курс математической логики по Штукенбергу Д.Г.

January 21, 2015

Contents

Должно отображаться корректно: x_1,x_2x_3x◎, θ, ◎, ∑, ◎

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 ∪ Pr ∪ C ◎ 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 $Pr \cup F \circledcirc N$.

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 $\sigma \circledcirc V$ - 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 ⊚ b ⊚ a
2. (a ⊚ b) ⊚ (a ⊚ b ⊚ c) ⊚ (a ⊚ c)
3. a ⊚ b ⊚ a & b
4. a & b ⊚ a
5. a & b ⊚ b
6. a ⊚ a V b
7. b ⊚ a V b
8. (a ⊚ b) ⊚ (c ⊚ b) ⊚ (a V c ⊚ b)
9. (a ⊚ b) ⊚ (a ⊚ ¬b) ⊚ ¬a
10. ¬¬a ⊚ 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 Γ, a ⊚ b следует Γ ⊚ a ⊚ 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 ⊚ ¬a ⊚ b Кстати она доказывается и в ИВ

1. (a ⊚ aV¬a) ⊚ (a ⊚ aV¬a ⊚ (¬a ⊚ b)) ⊚ a ⊚ (¬a ⊚ b)
2. a, aV¬a, ¬a ⊚ b a ¬a b ⊚ a b ⊚ ¬a (b ⊚ a) ⊚ (b ⊚ ¬a) ⊚ ¬b ¬b ⊚ a ¬b ⊚ ¬a (¬b ⊚ a) ⊚ (¬b ⊚ ¬a) ⊚ ¬¬b ¬¬b ⊚ b b
3. a ⊚ (¬a ⊚ b)

А еще в ИИВ главная фишка - недоказуемо A V ¬A (можно подобрать модель).

2.6 Теорема Гливенко

Если в ИВ доказуемо a, то в ИИВ доказуемо ¬¬a Общий ход д-ва: говорим, что если в ИИВ доказуема F, то в ней же доказуема ¬¬F. Доказываем руками двойное отрицание 10 аксиомы и то же самое для MP.

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, ≤) 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 = min {u | u ≥ all s ⊚ p} inf p = max {u | u ≤ all s ⊚ p} a + b = sup {a, b} a * b = 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 ⊚ a) a ⊚ b = max c | c * a ≤ b Имеет свойства, что в ней всегда есть максимальный элемент a ⊚ 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 ⊚ a (традиционно для импликативной), отрицание как -a = a ⊚ 0, и тогда последняя аксиома из предыдущего определения будет свойством: a * -a = a * (a ⊚ 0) = a * (max c: c * a ≤ 0) = a * 0 = 0 Насчет второй аксиомы - должно быть 1. То есть лучше как-то через аксиомы определять, видимо. a + -a = a + (a ⊚ 0) = a + (max c: c * a ≤ 0) = a + 0 = a // не 1

- Псевдобулева алгебра - это импликативная решетка над фундированным множеством с ¬a = (a ⊚ 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 ∪ b
2. a * b => a ∩ b
3. a ◎ b => Int(a◎ ∪ b)
4. -a => Int(a◎)
5. 0 => ◎
6. 1 => ◎{всех мн-в в L}

2.11 Модель Крипке

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

- W - множество ”миров”
- ≤ - частичный порядок на W (отношение достижимости)
- v: W × Var ◎ {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 ◎ P ◎◎ v(x, P) = 1 если P ◎ Var
- W, x ◎ (A & B) ◎◎ W, x ◎ A & W, x ◎ B
- W, x ◎ (A V B) ◎◎ W, x ◎ A V W, x ◎ B
- W, x ◎ (A ◎ B) ◎◎ ◎ y ≥ x (W, y ◎ A ◎ W, y ◎ B)
- W, x ◎ ¬A ◎◎ ◎ y ◎ x (W, x ¬◎ A)

В мире разрешается быть не вынужденной переменной и ее отрицанию одноврememенно. 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 ◎ b = ∪{z ◎ H | z ≤ x◎ ∪ y} Так созданное множество с операциями является импликативной решеткой, в которой мы определим -a = a ◎ 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 ◎ A[x:=θ], где θ свободна для подстановки в A A[x:=θ] ◎ ◎x.A, -//-

Правила вывода: $\underline{A_{◎B}}$ A ◎ ◎x.B x не входит сводобно в A

$\underline{A_{◎B}}$ ◎x.A ◎ 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 Γ, γ ◎ a => Γ ◎ γ ◎ 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 ◎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 ◎ N
2. x ◎ N, succ(x) ◎ N
3. ◎ x ◎ N : (succ(x) = 0)

4. (succ(a) = c & succ(b) = c) ◎ a = b
5. P(0) & ◎n.(P(n) ◎ P(succ(n))) ◎ ◎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 ◎ a′ = b′
2. a = b ◎ a = c ◎ b = c
3. a′ = b′ ◎ a = b
4. ¬(a′ = 0)
5. a + b′ = (a + b)′
6. a + 0 = a
7. a * 0 = 0
8. a * b′ = a * b + a
9. φ[x:=0] & ◎x.(φ ◎ φ[x:=x′]) ◎ φ // φ содержит св.п x

2.21 Рекурсивные функции

Z(x) = 0 N(x) = x + 1 $U_{◎◎}(x_1 \ldots x_{◎}) = x_{◎}$ S<f, $g_1 \ldots g_{◎}$>($x_1 \ldots x_{◎}$) = f($g_1(x_1 \ldots x_{◎}), \ldots g_{◎}(x_1 \ldots x_{◎})$)
R<f, g>($x_1 \ldots x_{◎}$, n) = if n = 0 f($x_1 \ldots x_{◎}$) else g($x_1 \ldots x_{◎}$, n, R<f, g>($x_1 \ldots x_{◎}$, n - 1))
μ<f>($x_1 \ldots x_{◎}$) - минимальное k, такое что f($x_1 \ldots x_{◎}$, 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…n◎) - примитивная рекурсинвная функция, $k \geq 0$. ◎J:f(n_1…n◎)<A(J, ∑(n_1,…n◎)) Доказывается индукцией по рекурсивным функциям.

2.24 Представимость

Функция f:N^n◎N называется представимой в формальной арифметике, если существует отношение a(x_1…x◎+1), ее представляющее, причем выполнено следующее:

1. f(a,b,…) = x <=> ◎ a(a~,b~,…x~)
2. ◎!x.f(a,b,…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…x◎) истинно => ◎ N(x_1~, …x◎~)
2. n(x_1…x◎) ложно => ◎ ¬N(x_1~, …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. $u◎◎ = (x_1 = x_1)$ & … & $(x◎ = x◎)$ & $(x_{◎+1} = x◎)$
4. $s(a_1 \ldots a◎, b) = ◎b_1 \ldots ◎b◎(G_1(a_1 \ldots a◎, b_1)$ & … & $Gn(a_1 \ldots a◎, b◎)$
5. $r(x_1 \ldots x◎, k, a) = ◎b◎c(\ ◎k(\beta(b, c, 0, k)$ & $\varphi(x_1 \ldots x◎, k))$ & $B(b, c, x_{◎+1}, a)$ & $◎k(k<x_{◎+1}$ ◎ $◎d◎e(B(b,c,k,d)$&$B(b,c,k',e)$&$G(x_1 \ldots x◎,k,d,e))))$
6. $m<F>(x_1 \ldots x_{◎+1}) = F(x_1 \ldots x◎, x_{◎+1}, 0)$ & $◎y((y < x_{◎+1})$ ◎ $\neg F(x_1 \ldots x◎, y, 0))$

2.29 Гёделева нумерация (точно)

a	‘a	описание
(	3	
)	5	
,	7	
¬	9	
◎	11	
V	13	
&	15	
◎	17	
◎	19	
x◎	21 + 6 * k	переменные
f^n◎	$23 + 6 ^{*k} * 3^n$	n-местные функцион. символы (’, +, *)
P^n◎	$25 + 6 ^{*k} * 3^n$	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 $f(x_1 \ldots x◎)$ = plog(μ<S<G_φ, $U_{◎+1,1}, \ldots U_{◎+1,◎}$, plog($U_{◎+1,◎+1}$, 1), plog($U_{◎+1,◎+1}$, 2)»($x_1 \ldots x◎$), 1). G_φ тут принимает n + 2 аргумента: $x_1 \ldots x◎$, p, b и возвращает 0 если p - доказательство $\varphi(x_1 \ldots x◎, p)$, представляющего f.

2.31 Непротиворечивость

Теория непротиворечива, если в ней нельзя одновременно вывести a и ¬a. Одновременная выводимоbm ¬a и a эквивалента выводимости a & ¬a

2.32 w-непротиворечивость

Теория ω-непротиворечива, если из ◎φ(x) ◎φ(x~) следует ◎ ◎p¬φ(p). Проще говоря, если мы взяли формулу, то невозможно вывести одновременно ◎x¬A(x) и A(0), A(1), …

2.33 Первая теорема Гёделя о неполноте

1. Если формальная арифметика непротиворечива, то недоказуемо σ(‘σ~)

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

2.34 Первая теорема Гёделя о неполноте в форме Россера

Если формальная арифметика непротиворечива, то в ней найдется такая формула φ, что ◎φ и ◎¬φ

2.35 Consis

Consis - утверждение, формально доказывающее непротиворечивость ФА То есть ◎ Consis => ФА непротиворечива

2.36 Условия Г-Б (наизусть)

Пусть πg(x, p) выражает Proof(x, p). π(x) = ◎t.πg(x, t) действительно показывает, что выражение доказуемо, если

1. ◎ a => ◎ π(‘a~)

2. ◎ π(‘a~) ◎ π(‘π(‘a~)~)

3. ◎ π(‘a~) ◎ π(‘(a ◎ b)~) ◎ π(‘b~)

2.37 Лемма о самоприменении

a(x) - формула, тогда ◎b такой что

1. ◎ a(‘b~) ◎ b
2. ◎ β ◎ a(‘b~)

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 ◎ (в ФА был =), есть связка ◎◎, есть пустое множество, операции пересечения и объединения. x ∩ y = z, тогда ◎t(t ◎ z ◎◎ t ◎ x & t ◎ y) x ∪ y = z, тогда ◎t(t ◎ z ◎◎ t ◎ x V t ◎ y) Dj(x) ◎a◎b(a ◎ x & b ◎ x & a ≠ b ◎ a ∩ b = ◎)

2.40 ZFC

2.40.1 Аксиома равенства

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

2.40.2 Аксиома пары

◎x◎y(¬(x=y) ◎ ◎p(x ◎ p & y ◎ p & ◎z(z ◎ p ◎ (x = z V y = z)))) x ≠ y, тогда сущ. {x, y}

2.40.3 Аксиома объединений

◎x(◎y(y◎x) ◎ ◎p◎y(y ◎ p ◎◎ ◎s(y ◎ s & s ◎ 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

◎x◎p◎y(y ◎ p ◎◎ y ◎ 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

◎x◎b◎y(y ◎ b ◎◎ (y ◎ x & φ(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 ≠ 0, то x ◎ a ≠ 0

2.40.7 Аксиома бесконечности

◎N(◎ ◎ N & ◎x(x ◎ N ◎ x ∪ {x} ◎ N))

2.40.8 Аксиома фундирования

◎x(x = ◎ V ◎y(y ◎ x & y ∩ x = ◎)) ◎x(x ≠ ◎ ◎ ◎y(y ◎ x & y ∩ x = ◎)) Равноценные формулы.

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

2.40.9 Схема аксиом подстановки

◎x◎!y.φ(x,y) ◎ ◎a◎b◎c(c ◎ b ◎◎ (◎d.(d ◎ a & φ(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 ◎a◎b((a ◎ b & b ◎ x) ◎ a ◎ x)
- Ординал - транзитивное вполне упорядоченное отношением ◎ мн-во
- Верхняя грань множества ординалов S C | {C = min(X) & C ◎ X | X = {z | ◎(y◎S)(z ≥ y)}} C = Upb(S) Upb({◎}) = {◎}
- 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^{ww}, w^{www}, ...) - 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 ◎ N) пишут a раз w^b. В канторовой форме приятно заниматься сложениями и прочим, потому что всякие upb - слишком ниочем.

  x + 0 = x x + c′ = (x + c)′ x + lim(a) = Upb{x + c | c < a}

  x * 0 = 0 x * c′ = x * c + x x * lim(a) = Upb{x * c | c < a}

  x ^ 0 = 1 x ^ c′ = (x ^ c) * x x ^ lim(a) = Upb{x ^ c | c < a}

2.42 Кардинальные числа, операции

Будем называть множества равномощными, если найдется биекция. Будем называть A не превышающим по мощности B, если найдется инъекция A ◎ B (|A| ≤ |B|) Будем называть A меньше по мощности, чем B, если |A| ≤ |B| & |A| ≠ |B| Кардинальное число - число, оценивающее мощность множества. Кардинальное число ◎ - это ординальное число a, такое что ◎ x ≤ a |x| ≤ |a| $◎_0$ = w по определению; $◎_1$ = минимальный кардинал, следующий за $◎_0$ Кардинальное число ◎ - это ординальное число a, такое что ◎◎ = P(◎$◎_{-1}$) $◎_0$ = $◎_0$ +: |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 ◎ b ◎ a
2. (a ◎ b) ◎ (a ◎ b ◎ c) ◎ (a ◎ c)
3. a ◎ b ◎ a & b
4. a & b ◎ a
5. a & b ◎ b
6. a ◎ a V b
7. b ◎ a V b
8. (a ◎ b) ◎ (c ◎ b) ◎ (a V c ◎ b)
9. (a ◎ b) ◎ (a ◎ ¬b) ◎ ¬a
10. ¬¬a ◎ a

Правило вывода: MP: ◎ A and ◎ A ◎ B => ◎ B

3.4 Теорема о дедукции

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

1. A A◎a◎A a◎A
2. (там где-то сзади уже было a◎A, a◎A◎B) (a◎A)◎(a◎A◎B)◎(a◎B) (a◎A◎B)◎(a◎B) a◎B
3. A◎A умеем доказывать

◎ Если нужно переместить влево, то перемещаем, добавляем A◎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 ⊚ b) ⊚ (¬b ⊚ ¬a) (a ⊚ b), ¬b ⊚ ¬a a ⊚ b (a ⊚ b) ⊚ (a ⊚ ¬b) ⊚ ¬a (a ⊚ ¬b) ⊚ ¬a ¬b ⊚ a ⊚ ¬b ¬b a ⊚ ¬b ¬a +2 раза дедукцию применить

4.1.2 Правило исключененного третьего

С помощью контрапозиции доказываем два утверждения: ¬(A|¬A)⊚¬A (один раз контрапозицию от этого обратную, там A⊚(A|¬A) акс) ¬(A|¬A)⊚¬¬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 ⊚ a V b a a ⊚ a V b a V b

2. a, ¬b ⊚ a V b a a ⊚ a V b a V b

3. ¬a, b ⊚ a V b b b ⊚ a V b a V b

4. ¬a, ¬b ⊚ ¬(a V b) ¬a ¬b (a V b ⊚ a) ⊚ (a V b ⊚ ¬a) ⊚ ¬(a V b) ¬a ⊚ a V b ⊚ ¬a a V b ⊚ ¬a ¬a, ¬b, a V b ⊚ a ¬a ¬b a V b a ⊚ a … //д-во ¬b, ¬a ⊚ b ⊚ a

b ⊚ a (a ⊚ a) ⊚ ((b ⊚ a) ⊚ (a V b ⊚ a)) (b ⊚ a) ⊚ (a V b ⊚ a) a V b ⊚ a a a V b ⊚ a (a V b ⊚ ¬a) ⊚ ¬(a V b) ¬(a V b)

5. a, b ⊚ a & b a b a ⊚ b ⊚ a & b b ⊚ a & b a & b

6. a, ¬b ⊚ ¬(a & b) ¬b ((a & b) ⊚ b) ⊚ ((a & b) ⊚ ¬b) ⊚ ¬(a & b) a & b ⊚ b (a & b ⊚ ¬b) ⊚ ¬(a & b) ¬b ⊚ a & b ⊚ ¬b a & b ⊚ ¬b ¬(a & b)

7. ¬a, b ⊚ ¬(a & b) аналогично

8. ¬a, ¬b ⊚ ¬(a & b) аналогично

9. a, b ⊚ a ⊚ b b b ⊚ a ⊚ b a ⊚ b

10. a, ¬b ⊚ ¬(a ⊚ b) a ¬b ¬b ⊚ ((a ⊚ b) ⊚ ¬b) (a ⊚ b) ⊚ ¬b a, ¬b, a ⊚ b ⊚ b a a ⊚ b b (a ⊚ b) ⊚ b ((a ⊚ b) ⊚ b) ⊚ ((a ⊚ b) ⊚ ¬b) ⊚ ¬(a ⊚ b) ((a ⊚ b) ⊚ ¬b) ⊚ ¬(a ⊚ b) ¬ b ⊚ (a ⊚ b) ⊚ ¬b (a ⊚ b) ⊚ ¬b ¬(a ⊚ b)

11. ¬a, b ⊚ a ⊚ b b b ⊚ a ⊚ b a ⊚ b

12. ¬a, ¬b ⊚ a ⊚ b def implicationFF(a: Expr, b: Expr): Derivation = mkD(List(¬¬(a), ¬¬(b)), simpleDeductionApply(mkD(List(¬¬(a), ¬¬(b), a), List(¬¬(a), ¬¬(b), a, (¬¬(b) ⊚ a) ⊚ ((¬¬(b) ⊚ ¬¬(a)) ⊚ ¬¬(¬¬(b))), a ⊚ (¬¬(b) ⊚ a), ¬¬(b) ⊚ a, ¬¬(a) ⊚ (¬¬(b) ⊚ ¬¬(a)), ¬¬(b) ⊚ ¬¬(a), (¬¬(b) ⊚ ¬¬(a)) ⊚ ¬¬(¬¬(b)), ¬¬(¬¬(b)), ¬¬(¬¬(b)) ⊚ b, b))).$_2$)

13. a ⊚ ¬¬a 9 акс

14. ¬a ⊚ ¬a ¬a

4.1.5 Лемма об исключении последнего в предположениях

Г, P ⊚ a, Г, ¬P ⊚ a => Г ⊚ a Докажем, что если Г |- P⊚A, Г |- ¬P⊚A, то A P⊚A ¬P⊚A PV¬P (P⊚A)⊚(¬P⊚A)⊚(PV¬P⊚A) три раза MP

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 ⊚ R V 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 A⊚(¬A⊚B) 10i: a ⊚ ¬a ⊚ b Кстати она доказывается и в ИВ

1. (a ⊚ aV¬a) ⊚ (a ⊚ aV¬a ⊚ (¬a ⊚ b)) ⊚ a ⊚ (¬a ⊚ b)
2. a, aV¬a, ¬a ⊚ b a ¬a b ⊚ a b ⊚ ¬a (b ⊚ a) ⊚ (b ⊚ ¬a) ⊚ ¬b ¬b ⊚ a ¬b ⊚ ¬a (¬b ⊚ a) ⊚ (¬b ⊚ ¬a) ⊚ ¬¬b ¬¬b ⊚ b b
3. a ⊚ (¬a ⊚ b)

5.2 Опровергаемость исключенного третьего

Вводим в наше множество истинностных значений Н Л < Н < И & - max V - min ¬И=Л, ¬Л=И, ¬Н=Л И⊚x=x, Л⊚x=И, Н⊚Л=Л, Н⊚Н=И, Н⊚И=И

1. Все аксиомы ИИВ являются 3-тавтологиями (ручная проверка) Значит любая интуиционистски выводимая формула 3-тавтология
2. q V ¬q = Н, значит она невыводима (контрпозиция пред. утв)

5.3 Решетки

- Решетка Решетка - это (L, +, *) в алгебраическом смысле и (L, ≤) 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 = min {u | u ≥ all s ⊚ p} inf p = max {u | u ≤ all s ⊚ p} a + b = sup {a, b} a * b = 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 ⊚ a) a ⊚ b = max c | c * a ≤ b Имеет свойства, что в ней всегда есть максимальный элемент a ⊚ a и что она дистрибутивна.

5.4 Лемма о дистрибутивности импликативной решетки

1. Полезные леммы

   (a) Лемма о домножении слева $b \le c \le a * c$, тогда $a * b \le a * c$ $a * b \le b \le c \le a * c$

   (b) Лемма о перенесении импликации $a * b \le c \Rightarrow a$

2. $a * (b + c) \ge a * b + a * c$

   (a) $a * (b + c) \ge a * b$ $a * b \le a$ $a * b \le b \le b + c$ $a * b \le a * (b + c)$ (из двух предыдущих)

   (b) $a * (b + c) \ge a * c$ $a * c \le a$ $a * c \le c \le b + c$ $a * c \le a * (b + c)$

   (c) $a * (b + c) \ge a * b + a * c$ (поскольку оно больше и того и другого)

3. $a * (b + c) \le a * b + a * c$ (пусть правая часть - q)

   (a) $b * a \le q$ (по определению *) $b \le a \circledcirc q$ (то самое место где мы пользуемся импликативностью)

   (b) $c * a \le q$ $c \le a \circledcirc q$

   (c) $b + c \le a \circledcirc q$ $(b + c) * a \le q$ $a * (b + c) \le q = a * b + a * c$

4. $a * (b + c) = a * b + a * c$

5.5 Алгебра Гейтинга, булева алгебра

- 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 $a \circledcirc a$ (традиционно для импликативной), отрицание как $-a = a \circledcirc 0$, и тогда последняя аксиома из предыдущего определения будет свойством: $a * -a = a * (a \circledcirc 0) = a * (\max c\colon c * a \le 0) = a * 0 = 0$ Насчет второй аксиомы - должно быть 1. То есть лучше как-то через аксиомы определять, видимо. $a + -a = a + (a \circledcirc 0) = a + (\max c\colon c * a \le 0) = a + 0 = a$ // не 1

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

5.6 Алгебра Линденбаума-Тарского

V - множество формул ИИВ

- Порядок для решетки: a ≤ b ⊚ a |- b a ~ b ⊚ a |- b & b |- a
- Дополняяем множество V: 0: a & ¬a = ⊚ 1: a ⊚ a = T
- Операции в алгебра: *: a & b +: a V b ⊚: a ⊚ b -: ¬a
- Эта алгебра является алгеброй Гейтинга, поскольку для нее выполняются -a * a = 0 (по определению), a 0: ⊚ x : x ≤ 0 в ней это ⊚ x (x – формула ИИВ) : ⊚ ⊚ x (из лжи следует все что угодно): a & ¬a a & ¬a ⊚ a a & ¬a ⊚ ¬a (b ⊚ a) ⊚ (b ⊚ ¬a) ⊚ ¬b (ну или 10i в ИИВ)

5.7 Теорема о полноте ИИВ относительно алгебры Гейтинга

Давайте возьмем в качестве Гейтинга алгебру Л-Т. Она нормальная себе такая структура (модель, наверное, несложно проверить): Пользуемся стандартной топологической интерпретацией (& = *, V = +, ⊚ = ⊚, ¬ = -) Алгебра

- Доказательство полноты a - обшезначимо [a] = 1 1 ≤ [a] x ⊚ x ⊚ a (по определению алгебры Л-Т) x ⊚ x доказума и так, значит ⊚ a
- Дойдем до 1 ≤ [a], значит A ⊚ A ⊚ a

5.8 Дизъюнктивность ИИВ

Мы доказываем, что если ⊚ aVb, то ⊚a или ⊚b

- Юзанем алгебру Гёделя Γ(A) (γ – функция преобразования a ⊚ a_{godel}): Мы можем ее обернуть над любой Гейтинговой алгеброй, возьмем Л-Т. Алгебра Гёделя строится с помощью γ. γ(a) = b значит, что в алгебре A элементу a соответствует элемент b из алгебры Гёделя. Порядок сохраняется естественным образом (я не очень точно знаю как, но предполагается, что a ≤ b, a и b сравнимы - γ(a) ≤ γ(b), они сравнимы. Ну и такое). Гёделева алгебра добавляет один элемент w. γ(1) = w γ(x) = x Таким образом Γ(A) = A∪{w}, порядок в Γ(A):
  - a≤w если a!=1
  - a≤b ⊚⊚ a≤⊚a (сравнение обычных элементов как и раньше)

– $w \le 1$

Связки определяем через таблицы:

$x + y$	$y=1$	$y=\gamma(v)$
$x=1$	1	1
$x=\gamma(u)$	1	$\gamma(u+v)$

$x * y$	$y=1$	$y=\gamma(v)$
$x=1$	1	$\gamma(x*\circledcirc v)$
$x=\gamma(u)$	$\gamma(u*\circledcirc y)$	$\gamma(u*\circledcirc v)$

$x \circledcirc y$	$y=1$	$y=\gamma(v)$
$x=1$	1	$\gamma(x\circledcirc\circledcirc v)$
$x=\gamma(u)$	1	$u\circledcirc\circledcirc v$

x	$\neg x$
$x=1$	$\gamma(\neg\circledcirc x)$
$x=\gamma(u)$	$\neg\circledcirc u$

- Докажем, что Гёделева алгебра является Гейтинговой. Для этого нужно доказать, что в ней выполняется коммутативность, ассоциативность и законы поглощения (это альтернативное определение эквивалентно заданию множества с фундированным порядком).

  1. Коммутативность
     (a) $A * B = B * A$
     (b) $A + B = B + A$
  2. Ассоциативность
     (a) $A * (B * C) = (A * B) * C$
     (b) $A + (B + C) = (A + B) + C$
  3. Поглощение
     (a) $A * (A + B) = A$
     (b) $A + (A * B) = A$

  Внимательное прослеживание свойств связок подтверждает тот факт, что Гёделева алгебра есть алгебра Гейтинга. Нужно также учитывать тот факт, что внутренняя алгебра тоже Гейтингова.

- Если ◎ a V b, то [a V b]◎ = 1, $[a \vee b]_{\Gamma} = 1$, тогда по определению связки + в Гёделевской $[a]_{\Gamma} = 1$ или $[b]_{\Gamma} = 1$, тогда оно такое же и в Линденбауме-Тарском, а Л-Т полно, то есть ◎a или ◎b.

5.9 Теорема Гливенко

1. Заметим, что если A доказуемо в ИИВ, то ¬¬A тоже доказуемо. A A ◎ ¬A ◎ A ¬A ◎ A ¬A ◎ ¬A (как обычно) (¬A ◎ A) ◎ (¬A ◎ ¬A) ◎ ¬¬A Значит если A - аксиома по схеме 1-9, то ¬¬A доказуемо в ИИВ

2. Пусть выражение A получилось по 10 схеме классического ИВ F = ¬¬A ◎ A Докажем: A ◎ ¬¬A ◎ A (акс. 1) ¬(¬¬A ◎ A) ◎ ¬A (к/поз) ¬A ◎ ¬¬A ◎ A (акс. 10и) ¬(¬¬A ◎ A) ◎ ¬¬A (к/поз) (¬(¬¬A ◎ A) ◎ ¬A) ◎ (¬(¬¬A ◎ A) ◎ ¬¬A) ◎ ¬¬(¬¬A ◎ A) (акс. 9) ¬¬(¬¬A ◎ A) (2x m.p.)

3. Делаем индукцию по длине доказательства в ИВ:

   (a) A - аксиома, !!(A) доказывается по пункту 1-2

   (b) MP A A ◎ B B
   В ИИВ имеем ¬¬(A) ¬¬(A ◎ B) (¬B ◎ ¬A) ◎ (¬B ◎ ¬¬A) ◎ ¬¬B
   ¬¬A, ¬¬(A ◎ B), ¬B ◎ ¬A (A ◎ ¬(A ◎ B)) ◎ (A ◎ ¬¬(A ◎ B)) ◎ ¬A
   ¬¬A, ¬¬(A ◎ B), ¬B, A ◎ ¬(A ◎ B) ((A ◎ B) ◎ B) ◎ ((A ◎ B) ◎ ¬B) ◎ ¬(A ◎ B)
   ¬¬A, ¬¬(A ◎ B), ¬B, A, A ◎ B ◎ B A A ◎ B B

5.10 Топологическая интерпретация

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 ∪ b

2. a * b => a ∩ b

3. a ◎ b => Int(a◎ ∪ b)

4. -a => Int(a◎)

5. 0 => ◎

6. 1 => ◎{всех мн-в в L}

6 Ticket 4: ИИВ2

6.1 Модели Крипке

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

- W - множество ”миров”
- ≤ - частичный порядок на W (отношение достижимости)
- v: W × Var ◎ {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 ◎ P ◎◎ v(x, P) = 1 если P ◎ Var
- W, x ◎ (A & B) ◎◎ W, x ◎ A & W, x ◎ B
- W, x ◎ (A V B) ◎◎ W, x ◎ A V W, x ◎ B
- W, x ◎ (A ◎ B) ◎◎ ◎ y ≥ x (W, y ◎ A ◎ W, y ◎ B)
- W, x ◎ ¬A ◎◎ ◎ y ◎ x (W, x ¬◎ 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.

6.2 Корректность ИИВ относительно моделей Крипке

Если формула выводима в ИИВ, то она истинна по шкале Крипке Проверим MP и аксиомы (что они истинны во всех мирах)

1. MP По определению импликации в моделях Крипке, если в мире вынуждено A, A◎B, то вынуждено и B.
2. Аксиомы
   (a) A ◎ (B ◎ A) Пусть где-нибудь вынуждена A, в силу монотонности она вынуждена везде правее, тогда если там где-то будет B, то B ◎ A тоже будет вынуждено

(b) (A ⊚ B) ⊚ ((A ⊚ (B ⊚ C)) ⊚ (A ⊚ C)) Пусть где-нибудь вынуждено A ⊚ B, докажем, что если где-то есть A ⊚ B, то там есть и ((A ⊚ (B ⊚ C)) ⊚ (A ⊚ C)).

   i. В мире вынуждено A, B; тогда если правее вынуждено A ⊚ (B ⊚ C), то вынуждено C по монотонности A, B; значит Везде правее A ⊚ (B ⊚ C) есть A, B, C, значит вынуждено A ⊚ C;

   ii. В мире не вынуждено ни A, ни B, тогда если не вынуждено A ⊚ (B ⊚ C), то A ⊚ C тоже не может быть вынуждено, потому что ни A, ни B, ни C там нет.

(c) A ⊚ (¬A ⊚ B)

   i. Если вынуждена A, то вынуждена ¬A ⊚ B Если вынуждена A, то не вынуждена ¬A, тогда ¬A ⊚ B можно вынудить вне зависимости от вынужденности B.

   ii. Если не вынуждена A, то что угодно нас устроит.

(d) etc (как-то легко на уровне)

6.3 X Вложение Крипке в Гейтинга (Д-во псевдодоп-я)

Нарисуем модель Крипке, возьмем какое-то объединение поддеревьев со всеми потомками, каждое такое объединение пусть будет входить в алгебру Гейтинга. ≤ - отношение "быть подмножеством". Определим операции:

- = ∪, * = ∩,

Докажем, что с ними все ок: ≤ - частичный порядок.

1. Антисимметричность - a ⊚ b & b ⊚ a => a = b

2. Транзитивность - a ⊚ b, b ⊚ c => a ⊚ c

3. Рефлексивность - ⊚ a (a ⊚ a)

+, * замкнуты. Объединение сохраняет свойства поддеревьев, а пересечение может быть либо пустым, либо поддеревом одного из аргументов, в любом случае все ок. Можно пользоваться строгим условием монотонности миров.

Докажем, что + - это sup, * - inf.

1. sup a + b ≤ x <=> a ≤ x & b ≤ x - верхняя граница a ∪ b ⊚ x <=> a ⊚ x & b ⊚ x - выполняется

2. inf $x \leq a * b \iff x \leq a \& x \leq b$ - нижняя граница x ◎ a ∩ b <=> x ◎ a & x ◎ b - выполняется

Определим 0 как ◎; a ◎ b = ∪T(x, y), где T(x, y) = {z ◎ H | z ≤ x◎ ∪ y} Доказать, что a ◎ b - псевдодополнение, a ≤ b ◎ c ~ a * b ≤ c –> TODO

Докажем, что если в Крипке что-то общезначимо, то оно общезначимо и в созданной алгебре Гейтинга. Делается индукцией по структуре. A - булева алгебра, M - модель крипке ◎◎ a <=> ◎◎ a Пусть оценка a в нашей алгебре Гейтинга - это множество, являющееся объединением всех поддеревьев миров, в которых вынуждено a. Общезначимо значит равно объединению всех множеств V в нашей алгебре. Если переменная в Крипке тавтология, то она вынуждена во всех мирах, значит ее оценка в Гейтинге = 1 Нужно еще проверить все связки.

6.4 Полнота ИИВ в моделях Крипке

1. Докажем для дизъюнктивных множество такое: Пусть дизъюнктивная множество M – это такое, что если в формальной системе M◎aVb, то a ◎ M или b ◎ M. (inb4: носитель модели крипке является дизъюнктивным мн-м, поскольку если в ИИВ доказано aVb, то оно по корректности вынуждено во всех мирах, а значит вынуждено одно из двух, а значит принадлежит множеству вынужденных формул шкал Крипке)

   - В дизъюнктивном множестве, если G ◎ a, то a ◎ G. Пусть это не так. В нашем множестве мы можем иметь что угодно. a ◎ a V ¬a, тогда G ◎ a V ¬a. Пусть a ¬◎ G, тогда по дизъюнктивности M ¬a ◎ G. Но тогда мы можем доказать a&¬a.

2. Возьмем множество всех дизъюнктивных множеств с формулами из ИИВ. Мы можем это сделать, потому что ИИВ дизъюнктивно. Для любого элемента W◎ a, a ◎ W◎ значит что в этом мире a вынуждено. Построим дерево с порядком "быть подмножеством". Докажем, что это множество – модель крипке. Проверим 5 свойств (про монотонности всякие и вынужденности)

   (a) W, x ◎ P ◎◎ v(x, P) = 1 если P ◎ Var Монотонности выполняются по построению дерева

   (b) W, x ◎ (A & B) ◎◎ W, x ◎ A & W, x ◎ B W ◎ A (через A & B ◎ A), значит A ◎ W, B аналогично

(c) W, x ◎ (A V B) ◎◎ W, x ◎ A V W, x ◎ B По дизъюнктивности (если лежит в W, значит из него доказуемо)

(d) W, x ◎ (A ◎ B) ◎◎ ◎ y ≥ x (W, y ◎ A ◎ W, y ◎ B) W ◎ A ◎ B. Пусть в W есть A, тогда докажем B (MP) и оно тоже в нем Пусть есть B, тогда все уже хорошо

(e) W, x ◎ ¬A ◎◎ ◎ y ◎ x (W, x ¬◎ A) Если вдруг где-то нашлось A, то оно доказуемо, значит мы сможем доказать A & ¬A

3. ◎a, тогда W◎◎a, но для W_0 - дизъюнктивного множества всех доказуемых формул W, W_0◎a. W_0 такое, что что бы не было доказуемо из W_0, оно тоже лежит в нем. Поскольку a тавтология, то a была доказана и попала в W_0 не случайно.

6.5 ИИВ не таблично

Под этим мы подразумеваем, что 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. В ИВ мы обычно пользуемся алгеброй J_0 Яськовского (хз почему так названа)

- это V={0, 1}, 0 ≤ 1

Пусть имеется V = {…}, |V| = n - множество истинностных значений. Пусть размер больше 2. Тогда построим формулу: ◎$_{(1≤j<i≤n+1)}$(a◎◎a◎);

1. Общезначимость. По принципу Дирихле (количество таких формул - c(n, 2) ≥ n) В какой-то формуле встретятся два одинаковых значения и она будет верна, тогда все выражение будет истинно.

2. Недоказуемость

   (a) J_0 - алгебра Яськовского Определим последовательность алгебр L◎, L_0 = J_0, L◎=Γ(L◎$_{-1}$) - Гёделева алгебра Таким образом L◎ - упорядоченное множество {0, ω_1, ω_2,…1} Пусть f - оценка в L◎, действующая по таким правилам на нашу формулу: f(a_1) = 0, f(a◎$_{+1}$) = 1, f(a◎) = w◎ при j<i f(a◎ ◎ a◎) = f(a◎) ◎ f(a◎) = f(a◎) ≠ 1 Поскольку ИИВ полно относительно алгебры Гейтинга (L◎ псевдобулева), то формула недоказуема

(b) Строим модель Крипке как вершину с n+1 сыновьями, в которых вынуждено по одной переменной. Тогда если в вершине вынуждена формула, то хотя бы один элемент связки должен быть вынужден, но там везде по одной переменной и импликация не работает.

7 Ticket 5: логика 2 порядка

Как разрешается конфликт с другим правилом вывода?

7.1 Определения исчисления предикатов, грамматика (Gen ⚜⚜ 1,2 ПВ)

Описываем грамматику (goto конспект ДГ) Описываем модель – предметное множество, формулы для функциональных символов и предикатов, задать свободные переменные. f: $[f]:D^n$◎D P: $[P]:D^m$◎V x: [x]:D (+ немного очевидные формальные правила как делать оценку - если ◎xP, то […] = 1, если для любого x P == 1 и так далее)

Добавляются две новые аксиомы ◎x.A ◎ A[x:=θ], где θ свободна для подстановки в A A[x:=θ] ◎ ◎x.A, -//-

Новое правило вывода: A ◎ ◎x.A GEN

Мы это правило представляем в виде двух утверждений (второй неочевидно откуда) $\underline{A_{◎B}}$ A ◎ ◎x.B

$\underline{A_{◎B}}$ ◎x.A ◎ B

переход от 1 к Gen легко доказать A A ◎ ◎ ◎ A ◎ ◎ A ◎ ◎ ◎x.A ◎x.A

Переход от Gen к 1 A ◎ B ◎ A ◎ ◎x.B ???

В общем-то нам нет необходимости думать о том, как делать переход, но вопрос интересный (теорему Генцена о непротиворечивости ФА можно видоизменить с GEN на наши два правила)

7.2 Теорема о дедукции

◎ Если нужно переместить последнее предположение вправо, то рассматриваем случаи – старая аксиома или предположение, MP, это самое выражение, две новых аксиомы с условиями выполнимости, два новых правила с условиями выполнимости.

1. Старая аксиома или предположение A A ◎ a ◎ A a ◎ A

2. MP a ◎ A (по индукции) … a ◎ A ◎ B (по индукции) … (a ◎ A) ◎ (a ◎ A ◎ B) ◎ (a ◎ B) (a ◎ A ◎ B) ◎ (a ◎ B) a ◎ B
3. A ◎ A умеем доказывать
4. Новые аксиомы как старые, только проверяем условие
5. ◎x.A ◎ B - первое новое правило вывода, проверяем условие
   (a) Вспомогательная лемма: (a ◎ (b ◎ c)) ◎ (b ◎ (a ◎ c)) a ◎ (b ◎ c), b, a ◎ c a ◎ b ◎ c b ◎ c c
   (b) a ◎ A ◎ B (в первоначальном доказательстве было A ◎ B) … (a ◎ A ◎ B) ◎ (A ◎ a ◎ B) A ◎ a ◎ B ◎x.A ◎ a ◎ B (это же правило вывода) (◎x.A ◎ a ◎ B) ◎ (a ◎ ◎x.A ◎ B) a ◎ ◎x.A ◎ B
6. A ◎ ◎x.B - второе новое правило вывода, проверяем условие
   (a) Вспомагательная лемма 1: (a & b ◎ c) ◎ (a ◎ b ◎ c) a & b ◎ c, a, b ◎ c a b a ◎ b ◎ a & b b ◎ a & b a & b a & b ◎ c c
   (b) Вспомагательная лемма 2: (a ◎ b ◎ c) ◎ (a & b ◎ c) a ◎ b ◎ c, a & b ◎ c a & b ◎ a a a & b ◎ b b b ◎ c c
   (c) a ◎ A ◎ B … (a ◎ A ◎ B) ◎ (a & A ◎ B) a & A ◎ B a & A ◎ ◎x.B (a & A ◎ ◎x.B) ◎ (a ◎ A ◎ ◎x.B) a ◎ A ◎ ◎x.B

◎ Если нужно переместить влево, то перемещаем, добавляем A◎B (последнее) A (перемещенное) B (тут все как в ИВ)

7.3 Корректность исчисления предикатов

- *Лемма о корректности подстановки* $[a]^{(x:=[\theta])} = [a(x:=[\theta])]$

  Структурная индукция по a: База: Пусть a - это предикат, тогда из способа оценки предиката понятно, что $[P(\theta,..)]=[P(x,\ldots)]^{(x:=[\theta])}$ Индукционный переход:

  1. a ◎ b, a & b, a V b, ¬a
     (a) a & b: $[a \& b]^{(x:=[\theta])} = [a[x:=\theta]] \& [b[x:=\theta]] = [a[x:=\theta] \& b[x:=\theta]] = [(a \& b)[x=[\theta]]]$
     (b) аналогично, TODO
  2. ◎y.a, ◎y.a

(a) [◎y.a]$^{(x:=[\theta])}$ =? [◎y.a[x:=θ]] Если x входит в ◎y.a связанно, то вообще никакой роли наша подстановка в оценке не играет. Значит пусть входит свободно. Поскольку θ свободна для подстановки вместо x в a, то в θ не входит свободно y - оценка θ не меняется. По предположению индукции [a]$^{(x:=[\theta])}$ = [a[x:=θ]]. Из свободности для подстановки θ следует еще и [a]$^{(x:=[\theta],\ y:=v)}$ = [a[x:=θ]]$^{(y:=v)}$, значит оценки полных формул с кванторами тоже будут совпадать

(b) ◎ аналогично, TODO

С помощью леммы проводим аналогичные рассуждения, как для ИВ. Рассматриваем только новые аксиомы и правила вывода:

1. ◎x.a ◎ a[x:=θ] Пусть это не тавтология, тогда ◎x.a = *И*, a[x:=θ] = *Л*. При любом x выполнено a, но с x=θ нет. Противоречие

2. a[x:=θ] ◎ ◎x.a аналогично, TODO

3. a ◎ b; a ◎ ◎x.b a ◎ b истинно по предположению индукции. Пусть a ◎ ◎x.b ложь, тогда a = *И*, ◎x.b = *Л*, но b = (◎x.b)@θ, значит это есть частный случай, а он верен. противоречие

4. a ◎ b; ◎x.a ◎ b аналогично, TODO

8 Ticket 6: полнота исч. пред.

А почему собственно наше множество Γ какое-то отношение имеет к предикатам?

8.1 Свойства противоречивости

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

- *Лемма*: теория противоречива ◎ в ней выводится a & ¬a ◎ если выводится a & ¬a, то противоречива – очевидно через аксиомы & ◎ если противоречива, то выводится a & ¬a a ¬a a ◎ ¬a ◎ (a & ¬a)

Заметим, что всякое подмножество непрот 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).

8.2 *Лемма 1:* о дополнении непр. мн-ва до полного

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

Для не более чем счетных сигнатур: Давайте добавлять недостающие формулы в Γ - если есть формула a, добавим a или ¬a в зависимости от того, является ли Γ∪a или Γ∪¬a противоречивым или нет (выберем непротиворечивый вариант). Одно всегда верно, потому что:

1. Γ∪a, Γ∪¬a противоречивы обе. Тогда Γ противоречиво.

2. Γ∪a, Γ∪¬a непротиворечивы обе. a ꩜ ¬a ꩜ a&¬a. ꩜꩜

Общий случай: *Лемма Цорна* гласит, что частично упор. мн-во, в котором каждая цепь имеет верхнюю грань, содержит максимальный элемент. Рассмотрим частично упорядоченное множество с элементами непротиворечивыми множествами, а отношение ≤ - это быть подмножеством. Тогда в силу не более чем счетности любой цепи по предыдущему случаю каждая цепь имеет верхнюю границу. По лемме Цорна наше множество содержит максимальный элемент. Этот элемент полон (если нет, то можем в него добавить a или ¬a

8.3 Условие о интерпретации непротиворечивого мн-ва

Будем называть интерпретацией непротиворечивого множества формул функцию оценки, тождественно равную 1 на элементах из этого множества. Будем говорить, что Γ ꩜ a, если она тождественна в любой модели Γ.

8.4 *Лемма 2:* если Γ ⚜ a, то Γ ⚜ a

Механическая проверка аксиом

8.5 *Лемма 3:* если у Γ есть модель, то Γ непротиворечиво

Пусть Γ имеет модель, но противоречиво, тогда из Γ выводится a, ¬a, по корректности Γ ꩜ a, ¬a, но формула и ее отрицание не могут быть общезначимыми одновременно.

8.6 Лемма 4: о модели бескванторного непротив. мн-ва формул

Пусть Г - полное непротиворечивое множество **бескванторных** формул. Тогда существует модель для Г.

Построим модель структурной индукцией по формулам. Предметное множество - строки, содержащие выражения. То есть какое-нибудь $f_1(c, b, f_5(c_5))$ = ”$f_1(c, b, f_5(c_5))$” Мы не хотим заниматься подсчетом, а предпочитаем оставлять то, что нужно вычислить как отдельную функцию. Рассмотрим формулу - предикат. Его оценка истина, если он принадлежит носителю, ложна если его отрицание в носителе (в предметном множестве). Элементы всегда входят противоречиво (элемент не вдохит со своим отрицанием. Связки определим естественным образом. Докажем, что γ ⊚ Г <=> γ истинна (Г - предметное множество)

- База Если атомарная формула лежит в Г, то она истинна по опр. Если атомарная формула истинна, то лежит в Г
- Переход
    1. a & b если a & b лежит в Г, то оно истинно по определению. если [a & b] = 1
        (a) [a & b] = И, покажем a & b ⊚ Г Пусть [a & b] = И, тогда по таблице истинности [a] = [b] = И, тогда a, b лежат в Г по предполож. тогда a ⊚ b ⊚ a & b лежит в модели
        (b) [a & b] = Л, покажем !(a & b) ⊚ Г a ложь или b ложь по таблице истинности. Пусть a ложь, тогда ¬a ⊚ Г. (a & b) ⊚ ¬a, (a & b) ⊚ a, 9 акс.
    2. a V b
        (a) [a V b] = И [a] = И, [b] = И, они лежат в множестве, a ⊚ a V b
        (b) [a V b] = Л ¬a, ¬b лежат в множестве, тогда 9 акс.
    3. Аналогично

8.7 Теорема Гёделя о полноте исчисления предикатов

Г - непротиворечивое множество формул, тогда Г имеет модель

8.7.1 Построение Г*

Нам нужно построить из нашего множества формул множество безкванторных формул, для этого определим такую операцию избавления от 1 квантора: Построим новый язык, отличающийся от нашего контантами, там будут d◎◎, где первый индекс - это поколение, второй – нумерационный. Возьмем непротиворечивое множество формул Г◎ и пополним его, получив непротиворечивое множество формул $Г_{◎+1}$, такое что Г◎ ◎ $Г_{◎+1}$. Возьмем формулу γ ◎ Г◎.

1. Не содержит кванторов. Ничего не делаем
2. γ = ◎x.a. Возьмем все константы, использующиеся в Г◎ - это будут c◎ и d◎◎, где a ≤ i, занумеруем их θ_1, θ_2,… и добавим формулы a_1=a[x:=θ_1],… к $Г_{◎+1}$
3. γ = ◎x.a. Возьмем новую константу $d_{◎+1}$◎ и добавим a[x:=$d_{◎+1}$,◎]

Заметим, что сами формулы с кванторами мы не выкидываем - ведь в будущем появятся новые формулы, и процесс для уже использованных кванторных формул нужно будет повторить. Покажем, что полученные множества остаются непротиворечивыми. Г◎ непротиворечиво, а $Г_{◎+1}$ противоречиво, тогда $Г_{◎+1}$ ◎ a&¬a, тогда выпишем конечное доказательство, найдем посылки, новые в $Г_{◎+1}$, которых нету в Г◎, выпишем их и впихнем направо по теореме о дедукции: Г◎ ◎ γ_1 ◎ γ_2 ◎ γ_3 ◎ …◎ γ◎ ◎ b&¬b Новые посылки у нас получаются только из пунктов 2 и 3.

1. γ_1 = a[x:=θ] из ◎x.a ◎x.a ◎ a[x:=θ] ◎x.a a[x:=θ] … a[x:=θ]◎(γ_2 ◎ …γ◎ ◎ b&¬b) γ_2 ◎ … ◎ b&¬b
2. γ_1 = a[x:=$d_{◎+1}$,◎] из ◎x.a выберем переменную, не участвующую в выводе противоречия - z. заменим все вхождения $d_{◎+1}$,◎ в д-ве на z. поскольку d◎ - константа, мы можем делать такие замены. Поскольку z - константа, специально введенная для замены и раньше не встречавшаяся, то она отсутствует в γ_2,… + мы можем правильно выбрать b, чтобы она в нем отсутствовала. Значит мы можем применить правило вывода c ◎ a[x:=z] ◎ (γ_2 ◎ … ◎ b&¬b) ◎z.a[x:=z] ◎ … правило вывода ◎x.a из Г◎ ◎z.a[x:=z] γ_2 ◎ … ◎ b&¬b

Возьмем $Г_0$ = Г. Г* = ∪Г◎. Г* также не противоречиво, потому что д-во использует конечное количество предположений, добавленных на каком-то шаге j максимум, значит множество Г◎ тоже противоречиво, что невозможно по условию.

8.7.2 Доказательство того, что дополненное бескв.подмн-во Г* - модель для Г

Выделим в Г* бескванторное подмножество G. Пополним его по лемме 1 (там где лемма цорна, можем дополнить) модель сделаем из него по лемме о бескванторной модели. Покажем, что это модель для всего Г*, а значит и для Г. Рассмотрим γ ◎ Г*, покажем, что [γ] = И.

- База Формула не содержит кванторов. Истинность гарантируется леммой о бескванторном множестве.
- Переход Пусть G это модель для любой формулы из Г* с r кванторами, покажем что она остается моделью для r+1 квантора.
  1. γ = ◎x.a Покажем, что формула истинна для любого t ◎ D. По построению подели есть такое θ, что t = ”θ” (string). По построению Г* начиная с шага p+1 мы добавляем формулы вида a[x:=k], где k - конструкция из констант и ф.симв. Также каждая константа (c◎ или d◎◎) из θ добавлена на некотором шаге s◎. То есть будет шаг l=max(max(s◎), p), на котором θ обретет смысл и в $Г_{◎+1}$ будет присутствовать a[x:=θ]. В формуле a на один квантор меньше, значит она истинна по предположению индукции.
  2. γ = ◎x.a По построению Г* как только добавили a к Г◎, так сразу в следующем мире $Г_{◎+1}$ появляется a[x:=$d_{◎+1}$,◎]. Значит формула истинна на значении ”$d_{◎+1}$,k”, то есть истинна.

8.8 Следствие – если ⚜a, то ⚜a

- Пусть Г◎a, тогда по полноте множества Г, Г◎¬a, но у Г есть модель, в которой Г◎¬a. То есть Г◎a. Но Г по построению то же, что и модель теории, то есть все рассуждения Г ◎ a равноценны в предикатах ◎ a.
- Пусть ◎a, тогда пусть Г={¬a}
  1. Г непротиворечиво Пусть Г противоречиво, значит ◎b Г ◎ b, Г ◎ ¬b;
     (a) ¬a ◎ b, ¬a ◎ b;
     (b) ¬a ◎ a, ¬a ◎ ¬a;
     (c) ◎ ¬a ◎ a, ¬a ◎ ¬a

(d) ⊚ (¬a ⊚ a) ⊚ (¬a ⊚ ¬a) ⊚ ¬¬a

(e) ⊚ ¬¬a ⊚ a

(f) ⊚ a ⊚⊚ a недоказуемо по условию.

2. Г подходит под условие теоремы Гёделя о полноти исчисления предикатов, то есть у Г есть модель. Тогда в ней оценка [¬a] = 1, значит оценка [a] = 0, то есть ⊚a. Мы доказали мета-контрпозицию ⊚a => ⊚a.

9 Ticket 7: ФА

9.1 Структуры и модели, теория первого порядка

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

Структура по ДГ: Структурой теории первого порядка мы назовем упорядоченную тройку <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).

9.2 Аксиомы Пеано

Множество N удовлетворяет аксиоматике Пеано, если:

1. 0 ⊚ N

2. x ◎ N, succ(x) ◎ N

3. ◎ x ◎ N : (S(x) = 0)

4. (succ(a) = c & succ(b) = c) ◎ a = b

5. P(0) & ◎n.(P(n) ◎ P(succ(n))) ◎ ◎n.P(n)

9.3 Формальная арифметика – аксиомы, схемы, правила вывода

Формальная арифметика - это теория первого порядка, у которой сигнатура определена как: (циферки, логические связки, алгебр. связки, ′), а интерпретацию сейчас будем определять. Интерпретация определяет два множества - V, P - истинностные и предметные значения. На самом деле нет никакого множества P, мы определяем только V, потому что оно нужно для оценок. Все элементы, которые мы хотели бы видеть, выражаются в сигнатуре. Пусть множество V = {0, 1} по-прежнему. Определим оценки логических связок естественным образом. Определим алгебраические связки так: +(a, 0) = a +(a, b′) = (a + b)′ *(a, 0) = 0 *(a, b′) = a * b + a

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

9.3.1 Аксиомы

1. a = b ◎ a′ = b′

2. a = b ◎ a = c ◎ b = c

3. a′ = b′ ◎ a = b

4. ¬(a′ = 0)

5. a + b′ = (a + b)′

6. a + 0 = a

7. a * 0 = 0

8. a * b′ = a * b + a

9. φ[x:=0] & ◎x.(φ ◎ φ[x:=x′]) ◎ φ

1. a = a Тут цифры в кавычках - д-во на i-й строке a = b ◎ a = c ◎ b = c акс a2 ◎ ваша любимая аксиома ″1″ ◎ ◎ ◎ ″1″ ◎ ◎ ″1″ ◎ ◎ ◎a.″1″ ◎ ◎ ◎a◎b.″1″ ◎ ◎ ◎a◎b◎c.″1″ ◎a◎b◎c.″1″ MP ◎a◎b◎c.(a = b ◎ a = c ◎ b = c) ◎ ◎b◎c.(a + 0 = b ◎ a + 0 = c ◎ b = c) схема по ◎ ◎b◎c.(a + 0 = b ◎ a + 0 = c ◎ b = c) MP ◎c.(a + 0 = a ◎ a + 0 = c ◎ a = c) схема ◎, MP a + 0 = a ◎ a + 0 = a ◎ a = a схема ◎, MP a + 0 = a акс a6 a ◎ a 2 MP

10 Ticket 8: рекурс, Аккерман

10.1 Рекурсивные функции

Z(x) = 0 N(x) = x + 1 U◎◎($x_1 \ldots x$◎) = x◎ S<f, $g_1 \ldots g$◎>($x_1 \ldots x$◎) = f(g_1($x_1 \ldots x$◎),…g◎($x_1 \ldots x$◎))
R<f, g>($x_1 \ldots x$◎, n) = if n = 0 f($x_1 \ldots x$◎) else g($x_1 \ldots x$◎, n, R<f, g>($x_1 \ldots x$◎, n - 1))
μ<f>($x_1 \ldots x$◎) - минимальное k, такое что f($x_1 \ldots x$◎, k) = 0

Пример: a + b = R<U_1, S<N, U_{33}»(a, b)

10.2 Характеристическая функция и рекурсивное отношение

- Характеристическая фукнция от выражения возвращает 1 если

выражение истинно, 0 иначе.

- Рекурсивное отношение - отношение, характеристическая функция

которого рекурсивна.

10.3 Аккерман не примитивно-рекурсивен, но рекурсивен (второе)

i: A(0, n) = n + 1 ii: A(m, 0) = A(m - 1, 1) iii: A(m, n) = A(m - 1, A(m, n - 1))

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

10.3.1 A(m, n) ≥ 1

A(m, n) определена только на натуральных числах, A(0, 0) = 1, A(1, 0) = A(0, 1) = 2, A(0, 1) = 2, все остальное еще больше

10.3.2 *Лемма 1а:* A(1, n) = n + 2

A(1, n) = A(0, A(1, n - 1)) = A(0, A(0, A(1, n - 2))) = A(0, A(0, A(0, … A(1, 0)))) = A(0, A(0, A(0, … 2))) = n + 2 (n раз инкрементируем двойку)

10.3.3 *Лемма 1b:* $A(2, n) = 2n + 3$

$A(2, n) = A(1, A(1, \ldots A(2, 0))) = A(1, A(1, \ldots 3)) = 2n + 3$ (n раз к тройке прибавляем $A(0, 1) = 2$)

10.3.4 *Лемма 2:* $A(m, n) \geq n + 1$

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

10.3.5 *Лемма 3a:* $A(m, n) < A(m, n + 1)$

индукция по m:

- база $A(0, n) = n + 1 < n + 2 = A(0, n + 1)$
- переход: $A(k + 1, m) < A(k + 1, m) + 1 \leq A(k, A(k + 1, m))$ (по лемме 2) $\leq A(k + 1, m + 1)$ (iii)

10.3.6 *Лемма 3b:* $A(m, n + 1) \leq A(m + 1, n)$

индукция по n:

- база $A(m, 0 + 1) = A(m, 1) = A(m + 1, 0)$ (ii)
- переход, предположение: $A(m, j + 1) \leq A(m + 1, j)$ по лемме 2 $(j + 1) + 1 \leq A(m, j + 1)$ $A(m, (j + 1) + 1) \leq A(m, A(m, j + 1))$ (по монотонности) $A(m, A(m, j + 1)) \leq A(m, A(m + 1, j))$ (по монотонности + предположение) $A(m, (j + 1) + 1) \leq A(m, A(m + 1, j)) = A(m + 1, j + 1)$ (iii)

10.3.7 *Лемма 3c:* $A(m, n) < A(m + 1, n)$

$A(m, n) < A(m, n + 1) \leq A(m + 1, n)$ (3a, 3b)

10.3.8 *Лемма 4:* A(m_1, n) + A(m_2, n) < A(max(m_1, m_2) + 4, n)

A(m_1, n) + A(m_2, n) ≤ A(max(m_1, m_2), n) + A(max(m_1, m_2), n) = 2 * A(max(m_1, m_2), n) < 2 * A(max(m_1, m_2), n) + 3 = A(2, A(max(m_1, m_2), n)) *лемма* 1 < A(2, A(max(m_1, m_2) + 3, n)) строгая монотоннасть по обоим арг. < A(max(m_1, m_2) + 2, A(max(m_1, m_2) + 3, n)) *лемма* 3c = A(max(m_1, m_2) + 3, n + 1) (iii) ≤ A(max(m_1, m_2) + 4, n) *лемма* 3b

10.3.9 *Лемма 5:* A(m, n) + n < A(m + 4, n)

A(m, n) + n < A(m, n) + n + 1 = A(n, m) + A(0, n) < A(m + 4, n)

10.3.10 Аккерманн не примитивно-рекурсивен

Пусть f(n_1…n◎) - примитивная рекурсинвная функция, k ≥ 0. ◎J:f(n_1…n◎)<A(J, ∑(n_1,…n◎))

]n~ = (n_1…n◎) Индукция по рекурсивным функциям

- База: f(n~) - N *или* Z *или* U◎◎
  1. f(n~) = N, k = 1; Пусть J=1, по (i) и *лемме* 3c f(n) = N(n) = n + 1 = A(0, n) < A(1, n) = A(J, n) = A(J, ∑(n~))
  2. f(n~) = Z, k = 1; f(n) = 0 < A(J, n) (потому что A ≥ 1) = A(J, ∑(n~))
  3. f(n~) = U◎◎; k = k; Пусть J=1 f(n_1…n◎) = U◎◎(n_1…n◎) = n◎ Пусть n◎ = 0, тогда f(n) = 0 < A(J, ∑(n~)) *для любого нормального* J Пусть n◎ > 0, тогда f(n) = (n◎ - 1) + 1 = A(0, n◎ - 1) < A(1, n) = A(J, ∑(n~))
- Переход
  1. Предположим, что f(n~) = S<h, g_1…g◎>(n~) = h(g_1(n~),…g◎(n~)) По предположению индукции существует J_0 для h, J_1…J◎ для g_1…g◎. f(n~) = h(g_1(n~),..) < A(J_0, ∑{i=1..m}(n~)) по выбору J_0 < A(J_0, ∑(A(J◎, ∑(n~)))) по выбору J◎ и строгой монотонности // J* = max(J_1..J◎) + 4(m - 1) < A(J_0, A(J*, ∑(n~))) по *лемме* 4 примененной m-1 раз < A(J_0, A(J*+1, ∑(n~))) по монотонности ≤ A(J_0, A(max(J_0, J*) + 1, ∑(n~))) по монотонности ≤ A(max(J_0, J*) + 1, ∑(n~) + 1) (iii) = A(max(J_0, J*) + 2, ∑(n~)) по *лемме* 3b Тогда пусть j=max(J_0, J*) + 2

2. Пусть f(n~) = R<h,g>(n~) f(n_1…n⊚, 0) = h(n_1…n⊚) f(n_1…n⊚, m+1) = g(n_1…n⊚, m, f(n_1…n⊚, m)) По предположению имеем J_0 (h), J_1 (g).] J = max(J_0, J_1) + 4
   (a) f(n~, 0) ≤ f(n~, 0) + ∑(n~) = h(n~) + ∑(n~) < A(J_0, ∑(n~)) + ∑(n~) < A(J_0 + 4, ∑(n~)) по лемме 5 < A(J, ∑(n~)) по монотонности = A(J, ∑(n~) + 0)
   (b) f(n~, k + 1) = g(n~, k, f(n~, k)) < A(J_1, ∑(n~) + k + f(n~, k)) по выбору J_1 < A(J_1, ∑(n~) + k + 1 + f(n~, k)) по монотонности = A(J_1, A(0, ∑(n~) + k) + f(n~, k)) (i) < A(J_1, A(0, ∑(n~) + k) + H(J, ∑(n~)+k)) по предположению < A(J_1, A(J, ∑(n~)+k)+A(J, ∑(n~) + k)) по монотонности (J > 0) = A(J_1, 2 * [A(J, ∑(n~) + k)]) < A(J_1, 2 * [A(J, ∑(n~) + k)] + 3) = A(J_1, A(2, A(J, ∑(n~) + k))) по лемме 1 < A(J_1, A(J_1 + 1, A(J, ∑(n~) + k))) по строгой монотонности (J_1 > 2) = A(J_1 + 1, A(J, ∑(n~) + k) + 1) (iii) ≤ A(J_1 + 2, A(J, ∑(n~) + k)) < A(J - 1, A(J, ∑(n~) + k)) по монот. J > max(..) + 4 = A(J, ∑(n~) + (k + 1)) (iii), J != 0

10.3.11 Аккерманн рекурсивен

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

11 Ticket 9: представимость

11.1 Функции, их представимость

Арифметическая функция - это отображение f: N_0^n ⊚ N_0 Арифметическое отношение - это P ⊚ N_0^n Если k ⊚ N_0, то k~ = 0′′′′…, где количество штрихов есть k.

- Арифметическое отношение R ⊚ N_0^n выразимо в ФА, если ⊚a с n свободными переменными: a(x_1…x⊚), такая что
  1. Если R(k_1…k⊚), то ⊚ a(k_1~…k⊚~)
  2. Если ¬R(k_1..k⊚), то ⊚ ¬a(k_1~…k⊚~)
- C_R - функция, равная 1, если R, и равная 0, если ¬R
- ⊚!y.φ(y) = ⊚y.φ(y) & ⊚a⊚b(φ(a) & φ(b) ⊚ a = b)
- f: N_0^n ⊚ N_0 представима в ФА, если ⊚a(x_1…x⊚₊₁), что ⊚x_1…x⊚+$_1$:

1. $f(x_1 \ldots x_{◎}) = x_{◎+1} \Leftarrow\Rightarrow$ ◎$a(x_1\sim, \ldots x_{◎+1}\sim)$
2. ◎$!b(a(x_1\sim \ldots x_{◎}\sim, b))$

11.2 Теорема о связи представимости и выразимости

R выразимо <=> C◎ представимо ◎ a выражает R (a ◎ ($x_{◎+1}$=0′)) & (¬a ◎ ($x_{◎+1}$=0)) представляет C◎ По выразимости R ◎ a; тогда ◎◎a◎◎ => a◎◎ По 10i, перенесенной к нам a ◎ (¬a ◎ ◎) правило с единственностью вроде понятно (хотя руками помахал, да) ◎ C◎ представимо ◎ R выразимо Пусть представлять C◎ будет $a(x_1 \ldots . x_{◎}, x_{◎+1})$ Тогда определим, какая формула выражает R: a(…., 1) Из представимости:

- ◎$b.a(x_1 \ldots x_{◎+1})$
- ◎x◎y(a(…x) & a(… y) ◎ x = y)
- если C◎$(x_1 \ldots x_{◎})$ = 1, то ◎ $a(x_1 \ldots x_{◎}, 1)$
- если C◎(…) = 0, то ◎ a(..,0)

Докажем выводимость

1. Покажем, что если $R(x_1 \ldots x_{◎})$, то ◎ $a(x_1 \ldots x_{◎}, 1)$ Из представимости прямо ровно.
2. Покажем, что если ¬$R(x_1 \ldots . x_{◎})$, то ◎ ¬$a(x_1 \ldots x_{◎}, 1)$ по единственности

   ◎x◎y($a(x_1 \ldots x_{◎}, x)$ & $a(x_1 \ldots x_{◎}, y)$ ◎ x = y) $a(x_1 \ldots x_{◎}, 0)$ & $a(x_1 \ldots x_{◎}, 1)$ ◎ (0 = 1) (спустя две акс. и 2 MP) дедукцию $a(x_1 \ldots x_{◎}, 0)$ & $a(x_1 \ldots x_{◎}, 1)$ ◎ ◎ $a(x_1 \ldots x_{◎}, 0)$ & $a(x_1 \ldots x_{◎}, 1)$ ◎ $a(x_1 \ldots x_{◎}, 0)$ $a(x_1 \ldots x_{◎}, 0)$ ¬$a(x_1 \ldots x_{◎}, 0)$ по представимости $a(x_1 \ldots x_{◎}, 0)$ ◎ (¬$a(x_1 \ldots x_{◎}, 0)$ ◎ ¬$a(x_1 \ldots x_{◎}, 1)$) (10i в ИИВ, доказуема в предикатах) ¬$a(x_1 \ldots x_{◎}, 1)$ хотим ¬$a(x_1 \ldots x_{◎}, 1)$

11.3 beta-функция Гёделя, китайская теорема об остатках

$\beta(b,c,i) = b \% (1 + c(1 + i))$, где %(a, b) = d, ◎m.(d + m * b = a), $m \geq 0$, $0 \leq d \leq b$

11.3.1 Китайская теорема об остатках

$n_1 \ldots n_{◎}$ - попарно взаимно простые инты $r_1 \ldots r_{◎}$ - любые целые, что 0 ≤ $r_{◎} < n_{◎}$ ◎i◎b $r_{◎} = b \% n_{◎}$

11.3.2 Гёделева Г-последовательность

Г◎ = (i + 1) * c + 1 Г(c) = 1*c + 1, 2*c + 1, 3*c + 1,…(n+1)*c + 1

Докажем, что Г(c) подходит на роль n_1…n◎ в китайской теореме об остатках. Выделим последовательность размера n: k_1…k◎. Чтобы это выполнялось возьмем c = (max(k_1…k◎))!

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

2. Каждое k◎ < Г◎ k◎ ≤ c < 1 + c * (i + 1) = Г◎

11.3.3 *Лемма о β-функции*

Увидим, что β(b,c,i) считает остаток от деления b на (i + 1) * c + 1 - элемент Геделевой последовательности.

- <a_0…a◎>◎N ◎ ◎b◎c(a◎=β(b,i,c)) - β-функция кодирует последовательность натуральных чисел и может доставать по индексу i

  a_0…a◎ - последовательность натуральных чисел тогда существует такое c, что Г = 1*c+1, 2*c+1,… если c ≥ max(a_0…a◎), то a◎ < (i+1)*c+1 Но по свойству Г элементы попарно взаимно просты тогда сравнения a_0 % (0+1)*c+1 a_1 % (1+1)*c+1 ………… a◎ % (n+1)*c+1 имеют общее решение b по китайской теореме об остатках тогда a◎ = b % (i+1)*c + 1 но это и есть β-функция a◎ = β(b,c,i)

11.3.4 Представимость β-функции Гёделя в ФА

β-функция представима в ФА отношением B(b,c,i,d) = ◎q((b = q * (1 + c * (i + 1)) + d) & (d < 1 + c * (i + 1))) Пусть 1 + c * (i + 1) = z Докажем условия представимости:

1. Эквивалентность

   (a) β(b,c,i) = d, тогда ◎ B(b,c,i,d) b = z * (1 + c * (i + 1)) (это и следующее - из леммы о β) P d < 1 + c * (i + 1) Q P ◎ Q ◎ P & Q P & Q P & Q ◎ ◎q.(P & Q) [z:= q] ◎q.(P & Q)

(b) Пусть ◎ B(b,c,i,d), тогда ◎q.(P & Q) подберем такое q (по лемме) P & Q ◎ P P & Q ◎ Q P Q значит $\beta(b,c,i) = d$

2. Единственность Следует из леммы.

11.4 Теорема о представимости рекурсивных функций Z, N, U

1. Z Z(a, b) = (b = 0)
   - Z(a) = b верно, тогда b = 0 b = 0
   - (b = 0) b = 0 тогда Z(0) = 0, все ок
   - ◎y.φ(y) & ◎a◎b(φ(a) & φ(b) ◎ a = b) Тоже как-то несложно
2. N N(a, b) = (a = b′)
   - N(a) = b, тогда a = b′ a = b′
   - a = b′, тогда N(a) = b
   - Третье не хочу
3. U◎◎ U◎◎(x_1…x◎) = (x_1 = x_1) & (x_2 = x_2) & … & ($x_{◎+1}$ = x◎)
   - U(..) = x◎, тогда $x_{◎+1}$ = x_1 x_1 = x_1 доказывается … x◎ = x◎ доказывается $x_{◎+1}$ = x_1 по условию объединяем все &
   - (x_1 = x_1) & …. вытаскиваем каждый элемент и тогда видим, что проекция делает ровно то, что должна.
   - ◎q.($x_{◎+1}$ = q) ХЗ
   - ◎a◎b(x(…a)&x(….b) ◎ a = b) Для конкретных a, b обявляем a = b - ◎, тогда выводим из него конъюнкцию и навешиваем два квантора

11.5 Теорема о представимости S

Если f и g_1…g◎ представимы, то S<f, g_1…g◎> представима Пусть F, G_1…G◎ представляют их. S(a_1…a◎, b) = ◎b_1…◎b◎(G_1(a_1…a◎, b_1) & … & Gn(a_1…a◎, b◎) & F(b_1…b◎, b))

- Пусть S(a_1…a◎) = b, тогда существуют такие b_1…b◎, что #каждый аргумент# Поскольку f,g_1…g◎ представимы, то доказуемы по представимости f(b_1…b◎, b) g_1(a_1…a◎, b_1) … g◎(a_1…a◎, b◎) g_1 & g_2 & … & g◎ & f объединили & ″P″ ″P″ ◎ ◎b_1.″P[b_1:=b_1]″ + MP … Ну и навесили кванторы, да.

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

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

11.6 Теорема о представимости R

Пусть f, g представимы F, G. Тогда R<f,g> представима. f: $N^n \circledcirc N$, g:$N^{n+2} \circledcirc N$ $r(x_1 \ldots x_\circledcirc, k, a) = \circledcirc b \circledcirc c(\circledcirc k(\beta(b, c, 0, k)\ \&\ \varphi(x_1 \ldots x_\circledcirc, k))\ \&\ B(b, c, x_{\circledcirc+1}, a)\ \&\ \circledcirc k(k < x_{\circledcirc+1} \circledcirc \circledcirc d \circledcirc e(B(b,c,k,d) \& B(b,c,k',e) \& G(x_1 \ldots x_\circledcirc,k,d,e))))$ Единственная возможность осознать – внимательно прочесть формулу. Тут β-функция используется в качестве функии отображения нашего шага вычисления рекурсии в результат, типа 0 - F(…) 1 - G(…) … n - G(…)

11.7 Теорема о представимости μ

f: $N^{n+1} \circledcirc N$ представима F, тогда μ<f> представима M $M<F>(x_1 \ldots x_{\circledcirc+1}) = F(x_1 \ldots x_\circledcirc, x_{\circledcirc+1}, 0)\ \&\ \circledcirc y((y < x_{\circledcirc+1}) \circledcirc \neg F(x_1 \ldots x_\circledcirc, y, 0))$

- $\mu<f>(x_1 \ldots x_\circledcirc) = x_{\circledcirc+1}$, тогда $x_{\circledcirc+1}$ - минимальное k, такое что $f(x_1 .. x_\circledcirc, k) = 0$ то есть имеем $F(x_1 \ldots x_\circledcirc, x_{\circledcirc+1}, 0) \circledcirc x.(k < x \circledcirc \neg F(x_1 \ldots x_\circledcirc, k, 0))$ Просто объединим конъюнкцией

- обратно ей же и разъединим

12 Ticket 10: Тьюринг

12.1 Арифметические отношения, их выразимость

- Арифметическое отношение $R \circledcirc N_0^n$ выразимо в ФА, если ◎a с n свободными переменными: $a(x_1 \ldots x_\circledcirc)$, такая что

  1. Если $R(k_1 \ldots k_\circledcirc)$, то $\circledcirc\ a(k_1\sim \ldots k_\circledcirc\sim)$
  2. Если $\neg R(k_1 .. k_\circledcirc)$, то $\circledcirc\ \neg a(k_1\sim \ldots k_\circledcirc\sim)$

12.2 Гёделева нумерация

a	‘a	описание
(	3	
)	5	
,	7	
¬	9	
◎	11	
V	13	
&	15	
◎	17	
◎	19	
x◎	$21 + 6 * k$	переменные
f^n◎	$23 + 6^{*k} * 3^n$	n-местные функцион. символы (’, +, *)
P^n◎	$25 + 6^{*k} * 3^n$	n-местные предикаты (=)

Последовательность значков будем составлять так: $a_1 \ldots a_{◎}$ - наши простые числа, соответствующие char’ам, тогда $p_1^{(a_1)} * p_2^{(a_2)}, \ldots p_{◎}^{(a_{◎})}$ - геделев нумерал стринга, составленного из чаров.

Если a - выражение, то ‘a - выражение в Геделевой форме (на практике пишут квадратные скобочки без нижних их половинок) Тогда если a - выражение, ‘a~ - это элемент предметного множества ФА, соответствующий нолику с количеством черточек, равным ‘a.

Доказательство - это последовательность простых чисел, возведенная в геделевы нумералы выражений, являющихся составляющими док-ва, по порядку. Аналогично с составлением строки из символов.

Тогда определим следующие функции операций с нумералами:

- $plog(a, b) = \max n : a \% b^n = 0$ Иногда вместо b стоит P_b, где P_b - простое число с индексом b. Функция берет геделев нумерал и достает у него i-й элем. последов.

- $len = \max n : a \% p_{◎}$ Возвращает длину строки\д-ва

- $s@t = p_1^{(plog(s, 1))} * \ldots * p_{◎◎◎(◎)}^{(plog(s, len(s)))} * p_{◎◎◎(◎)+1}^{(plog(t, 1))} * \ldots * p_{◎◎◎(◎)+◎◎◎(◎)}^{(plog(t, len(t)))}$ Конкатенация строк

12.3 Машина Тьюринга

Машина тьюринга состоит из ленты, головки, регистра состояния и конечной таблицы состояний Более формально, это 7-кортеж: <Q, Г,

b, ∑, δ, q_0, F> Конечный список состояний, конечный алфавит, пустой символ из алфавита, символы, которые мы можем писать (из Γ \ b), функция таблицы состояний, начальное состояние из Q, конечное состояние из Q.

- Лента - бесконечный двусвязный список, в каждой ячейке которого содержится символ из конечного алфавита, в котором также есть пустой символ (тут и далее), которым изначально заполнена вся лента
- Головка может находиться над элементом, писать в него и читать из него символ. Может двигаться влево-вправо (или двигать ленту, неважно)
- Регистр состояния хранит состояние - элемент из конечного множества состояний машины. Есть особые состояния - стартовое и конечные.
- Таблица состяний - таблица, хранящая данные о функции смены состояния - foo: Γ × Q ⊚ Γ × Q × {left, this, right}. Функция берет текущее состояние, читает символ на головке, потом получает тройку, пишет новый символ, перемещается по третьему элементу, выставляет новое состояние. Если состояние конечное, то она останавливается.

Мы будем придерживаться нотации <␣, ␣ , ␣, ␣ S, F>.

12.4 Проблема останова

Дано описание процедуры и входные данные. Функция P(a, b) определяет, остановится ли a на входных данных b. Существует ли P?

- Проблема останова неразрешима на машине Тьюринга: Пусть P существует. Тогда S(x) = P(x, x) остановится ли функция на своем же коде MyProg(x) = if S(x) then while(true){} else 1 Рассмотрим MyProg('MyProg) Если оно остановится, то первое условие выполнено, тогда оно не остановится И наоборот. Значит, P не существует.

12.5 Выводимость и рек. функции - Тьюринг

12.5.1 Выражение машин Тьюринга через рекурсивные функции

Мы хотим доказать, что если у нас есть какая-нибудь процедура, которую можно выразить в Тьюринге, то мы можем ее сделать и в формальной арифметике (рекурсивные функции представимы). Введем обозначение $<st,tape,pos> = 2^{(st)}*3^{(tape)}*5^{(pos)}$ Такая тройка – основная характеристика машины в данный момент. Будем называеть ее текущим полным состоянием, например. st, tape, pos - геделевы нумералы, st - нумерал из 1 элемента с состоянием, tape - string, обозначающий ленту (бесконечные слева и справа не входят), pos - позиция в ленте.

- p: <st, a> ◎ <st, a, dir> принимает <st, a>, декодит, лезет в δ машины тьюринга, достает новые значения, делает из них <,,>, отдает.
- t: <st> ◎ 0 | 1 Определяет, терминально ли наше состояние (0 если терминально)
- ε - пустой символ (у нас)
- pb, pc кодируют β-функцией последовательность инпутов в последовательность аутпутов. $\beta(p_b, p_c, x) = p(x)$
- tb, tc аналогично кодируют t
- $R<f,g>(<s_{st}, s_{tape}, s_{pos}>, \varepsilon, pb, pc, tb, tc, y)$ Запускает машину Тьюринга от стартового состояния, заранее говоря ей, сколько шагов (y) она должна сделать. Возвращает тройку <st, tape, pos>
- Определим f, g
  1. Дополнительные функции
     - os(prev) = plog(prev, 1) Текущее состояние
     - ot(prev) = plog(prev, 2) Лента
     - op(prev) = plog(prev, 3) Позиция головки в ленте
     - $nextstate(pb, pc, prev) = \beta(pb, pc, 2^{(os(prev))} * 3^{(plog(ot(prev), op(prev)))}$ Реализует функцию p
     - st(pb, pc, prev) = plog(nextstate(pb, pc, prev), 1) Новое состояние.
     - sym(pb, pc, prev) = plog(nextstate(pb, pc, prev), 2) Символ который нужно писать
     - dir(pb, pc, prev) = plog(nextstate(pb, pc, prev), 3) Направление для перехода головки
     - $repl(pb, pc, prev) = (ot(prev) / (P_{op})^{(plog(ot(..), op(..)))}) * (P_{op})^{sym}(..)$ Возвращает ленту, в которой удален символ в позиции op, и добавлен новый символ в эту же позицию.

2. f - возвращает полное состояние машины f(<$start_{state}$>, ε, pb, pc, tb, tc) = <$start_{state}$>
3. g - возвращает новое полное состояние из машины после перехода (пометка: 0 - nothing, 1 - right, 2 - left все фукнции вызываются с аргументом prev, <$start_{state}$> не используется) g(<$start_{state}$>, ε, pb, pc, tb, tc, y, prev) =

Condition	Result	Desrc
dir = 0	<st, repl, op>	nothing
dir = 1 & len(repl) = op	<st, repl@$2^{(\varepsilon)}$, op + 1>	tape end
dir = 1	<st, repl, op + 1>	move right
dir = 2 & op = 0	<st, $2^{(\varepsilon)}$@repl, op - 1>	tape start
dir = 2	<st, repl, op - 1>	move left

- Определим steps - функцию, определяющую необх. кол-во шагов steps(<$start_{state}$>, ε, pb, pc, tb, tc) = μ<β(tb, tc, plog(R<f,g>, 1))>(<$start_{state}$>, ε, pb, pc, tb, tc) Она найдет такое минимальное к, что состояние plog(R<f, g>(args, k), 1) терминально.

12.5.2 Выражение программы по проверке доказательства в машине тьюринга

- Emulate(input, prog) = plog(R<f,g>(<'S, input, 0>, , pb, pc, tb, tc, steps(-//-)), 1) == F Функция проверяет, правда ли получившееся терминальное состояние - ок. Можем давать программу такую, что она заканчивается в терминальном F(inish) или в терминальном FAIL Дает в качестве аргумента функцию перехода, pb, pc выражают prog

- Proof(term, proof) = Emulate(proof, $MY_{PROOFCHECKER}$) && (plog(proof, len(proof)) = term) Проверяет, что доказательство p заканчивается корректно и его последний элемент - то, что мы доказываем.

- *Л*юбая представимая в ФА ф-я является рекурсивной Пусть f представима Пусть $f(x_1 \ldots x_{\circledcirc}) = b$, тогда $\circledcirc$ $\varphi(x_1\tilde{}\ldots x_{\circledcirc}\tilde{}, b\tilde{})$ Всегда можно построить рекурсивную функцию $G_\varphi(x_1 \ldots x_{\circledcirc}, b, p)$, утверждающую, что p - гёделев номер вывода предиката $\varphi(x_1\tilde{}\ldots x_{\circledcirc}\tilde{}, b\tilde{})$ Мы делаем это обычным перебором чисел, проверяем вывод нашей программой из домашнего задания, выраженную в тьюринге, а потом в рекурсивных функциях. Тогда f в рекурсивных функциях выражается так: $f(x_1 \ldots x_{\circledcirc}) = plog(\mu<S<G_\varphi, U_{\circledcirc+1,1}, \ldots U_{\circledcirc+1,\circledcirc}, plog(U_{\circledcirc+1,\circledcirc+1}, 1), plog(U_{\circledcirc+1,\circledcirc+1},$

2)»($x_1 \ldots x$⊚), 1) Такая функция берет plog(1) от первого такого минимального геделева номера k (геделева пара из двух элементов - <b, p>)), что S<G_φ, U....>($x_1 \ldots x$⊚, k) = 0. Это значит, что G_φ($x_1 \ldots x$⊚, plog(k, 1), plog(k, 2)) = 0, это значит, что G_φ($x_1 \ldots x$⊚, b, p) = 0, то есть p - вывод φ(x_1~...x⊚~, b~). Этот геделев номер - b

13 Ticket 11: 1т о неполноте

13.1 Непротиворечивость, ω-непротиворечивость

- Теория непротиворечива, если в ней нельзя вывести одновременно a и ¬a (что аналогично невозможности вывести a&¬a).
- Теория ω-непротиворечива, если из ⊚φ(x) ⊚φ(x~) следует ⊚ ⊚p¬φ(p). Проще говоря, если мы взяли формулу, то невозможно вывести одновременно ⊚x¬A(x) и A(0), A(1), ...
- Лемма о w-# и обычной непротиворечивости Если теория w-непротиворечива, то она непротиворечива φ = x=x ⊚ x=x Такая формула очевидно доказуема (A ⊚ A) ⊚φ[x:=k] k ⊚ N_0 Но недоказуемо ⊚x¬(x=x⊚x=x) A в противоречивой теории доказуемо все

13.2 Прервая теорема о неполноте

Определим отношение W_1(x, p), истинное тогда и только тогда, когда x - геделев номер формулы φ с единственным свободным аргументом x, a p - геделев номер доказательства φ(”φ”). Это отношение выразимо в ФА, потому что мы просто пихаем это в наш Proof, а его мы выразили через рекурсивные функции, а они представимы. Пусть его выражает w_1(x, p); Рассмотрим формулу σ = ⊚p¬w_1(x, p) - для любого доказательства оно не является доказательством самоприменения φ, то есть самоприменение φ недоказуемо. То есть если σ(‘a~) истинно, то a(‘a~) недоказуемо. В нашем случае если σ(‘a~) истинно, то σ(‘σ~) недоказуемо.

1. Если формальная арифметика непротиворечива, то недоказуемо σ(‘σ~)
   (a) Пусть ⊚ σ(‘σ~), тогда найдется геделев номер ее док-ва p, тогда W_1(‘σ, p), то есть ⊚ w_1(‘σ~, p~).
   (b) С другой стороны, ⊚ σ(‘σ~) ⊚ ⊚p¬w_1(’σ~, p) ⊚p¬w_1(‘σ~, p) ⊚ ¬w_1(‘σ~, p~) ¬w_1(‘σ~, p~) Тогда ФА противоречива.

2. Если формальная арифметика w-непротиворечива, то недоказуемо ¬σ(‘σ~) Пусть ◎ ¬σ(‘σ~), то есть ◎ ¬◎p¬w_1(‘σ~, p), что значит ◎p.w_1(‘σ~, p) Найдется такой q, что ◎ w_1(‘σ~, q~), потому что если бы не нашелся, это бы значило доказуемость для каждого q ¬w_1(‘σ~, q~), тогда по ω-непротиворечивости было бы не доказуемо ◎p¬¬w_1(‘σ~, p) То q, что мы нашли - это номер доказательства σ(‘σ~), что и утверждает выражение ◎ w_1(‘σ~, q~). Но мы предполагали, что ◎ ¬σ(‘σ~). Противоречие.

Нормальное доказательство общезначимости: Я не знаю, зачем нам второй пункт, но из первого следует, что если наша теория w-непротиворечива, то она непротиворечива (по лемме выше), значит в ней недоказуемо σ(‘σ~), то есть ◎p¬w_1(‘σ~, p), то есть по корректности последнее выражение И, но это и есть в точности определение σ(‘σ~).

Ненормальное д-во общезначимости: Итого мы доказали, что если формальная арифметика ω-непротиворечива, то в ней не доказуемо ни σ(‘σ~) ни ¬σ(‘σ~). Одно из них точно тавтология (в формуле нет свободных переменных). Тогда ФА неполна при условии ω-непротиворечивости.

Другое доказательство общезначимости: ¬σ(‘σ~) недоказуема [σ(‘σ~)] = [◎p¬w_1(‘σ~, p)] =

1. И если [¬w_1(‘σ~, a)] = И для какого-то a
2. *Л* иначе

Это значит, что И если [w_1(‘σ~, a)] = *Л* [w_1(‘σ~, a)] = *Л*, докажем от противного Пусть [σ(‘σ~)] = *Л*, [◎p¬w_1(‘σ~, p)] = *Л* [¬◎p¬w_1(‘σ~, p)] = *И* [◎p.w_1(‘σ~, p)] = *И* [w_1(‘σ~, a)] = И для какого-то a то есть a доказывает σ(‘σ~) ???

тогда по определению w_1 существует доказательство σ(‘σ~),

13.3 Пример w-противоречивой, но непротиворечивой теории (при усл. непрот. ФА)

Добавим в ФА аксиому Г: ¬σ(‘σ~) Тогда по контрпозиции 1п2 она w-противоречива. Если бы мы могли доказать противоречивость нашей системы, то ФА была бы противоречива, тогда хз ¬σ(‘σ~) ◎ σ(‘σ~)&¬σ(‘σ~) ◎ σ(‘σ~) Но мы предположили что ¬σ(‘σ~)

13.4 Форма Россера

Если формальная арифметика непротиворечива, то в ней найдется такая формула φ, что ⊚φ и ⊚¬φ

14 Ticket 12: 2т о неполноте

14.1 Consis, Условия выводимости Гильберта-Бернайса

Определим Consis как утверждение, показывающее непротиворечивость ФА - отсутствие φ : ⊚ φ, ¬φ. Поскольку в противоречивой теории выводится что угодно, возьмем что-то недоказуемое, типа 1=0. Consis = ⊚p(¬Proof(’(1=0)~, p))

Определим отношение Sub(a, b, c) истинно, если a, b - ‘a, ‘b & c = ‘a[x:=b] или a V b не геделев номер и c = 0

Пусть Sub(a, b, c) выражает τ(a, b, c)

- *Лемма о самоприменении* a(x) - формула, тогда ⊚b такой что
  1. ⊚ a(‘b~) ⊚ b
  2. ⊚ β ⊚ a(‘b~)

  b_0(x) = ⊚t(τ(x, x, t) ⊚ a(t)) b = b_0(‘b_0~)

  1. a(‘b~) ⊚ a(‘b~) a(‘b~) ⊚ τ(‘b_0~, ‘b_0~, ‘b~) ⊚ a(‘b~) акс 1 + MP a(‘b~) ⊚ ⊚ ⊚ (τ(‘b_0~, ‘b_0~, ‘b~) ⊚ a(‘b~)) a(‘b~) ⊚ ⊚ ⊚ ⊚t(τ(‘b_0~, ‘b_0~, t) ⊚ a(t)) a(‘b~) ⊚ ⊚t(τ(‘b_0~, ‘b_0~, t) ⊚ a(t)) a(‘b~) ⊚ b
  2. b ⊚ ⊚t(τ(‘b_0~, ‘b_0~, t) ⊚ a(t)) тут почти a ⊚ a написано b ⊚ τ(‘b_0~, ‘b_0~, ‘b~) по выразимости b ⊚ τ(‘b_0~, ‘b_0~, ‘b~) ⊚ a(‘b~) сняли квантор с 1 b ⊚ a(‘b~)

- Условия Гильберта-Бернайса

Пусть πg(x, p) выражает Proof(x, p) πr(x) = ⊚t πg(x, t) тогда если

1. ⊚ a , то ⊚πr(‘a~)
2. ⊚ πr(‘a~) ⊚ πr(‘πr(‘a~)~)
3. ⊚ πr(‘a~) ⊚ πr(‘(a ⊚ b)~) ⊚ πr(‘b~)

14.2 Вторая теорема о неполноте

14.2.1 Рукомашеское доказательство без условий Г-Б

- Если арифметика непротиворечива, в ней нет д-ва Consis рассмотрим Consis ⊚ σ('σ~). Тогда если Consis доказуемо, то σ('σ~) недоказуемо. То есть это формулировка 1.1 Гёделя о неполноте. Тогда если у нас будет Consis, мы сможем доказать σ('σ), тогда 1.1 фейлится. Значит Consis недоказуемо.

- Доказательство того, что Consis недостаточно формален Заменим Consis в д-ве на Proof1(a, x) = Proof(a, x)&¬Proof('(1=0),x) Consis1 = ⊚x¬Proof1('(1=0),x) Если арифметика непротиворечива, то Proof1(a, x) = Proof(a, x) Если арифметика противоречива, то Consis1 доказуема как и все остальное. Ну давайте менять.

  Поменяли. Смотрим. хехехе, давайте докажем Consis1: ¬(π(x) & ¬π(x)) доказуемо в ИВ ⊚ ⊚ ⊚ ¬(π(x) & ¬π(x)) 1 акс, МР ¬(π(x) & ¬π(x)) ⊚x(¬(π(x) & ¬π(x)))

  Тогда выходит, что мы можем доказать противоречивость арифметики. Но это не так, бага вот в чем: Замена consis на consis1 неоправдана - в consis1 есть формула 1=0, на которой ее результат не вычисляется, а постулируется. Чтобы выражать Consis абстрактно, существуют условия выводимости Гильберта-Бернайса.

  Докажем, что consis1 не удовлетворяет 3 свойству Г-Б Пусть Proof1(x,p) выражает π1. ⊚ π1('a~) ⊚ π1('a⊚b~) ⊚ π1('b~) оценим при a=(2=0), b=(1=0) ? ⊚ (true ⊚ false) ? ⊚ false Если эта формула верна, то ⊚ π1('a~) Тогда если π1('a~), то Proof(2=0, x)&¬Proof('1=0, x) = И Это значит что теория противоречива, потому что в ней выводимо 2=0, но она непротиворечива, потому что недоказуемо 1=0. ⊚⊚

14.2.2 Доказательство 2 теоремы Гёделя о неполноте

Пусть π удовлетворяет условиям Г-Б Consis = ¬π(1=0) ФА непротиворечива Тогда ⊚ Consis

1. По лемме о самоприменении
   (a) ¬$\pi(\gamma)$ ⊚ γ
   (b) γ ⊚ ¬$\pi(\gamma)$
   (c) ¬γ ⊚ $\pi(\gamma)$ контрпозиция

(d) $\pi(\gamma)$ ◎ $\neg\gamma$

2. $\pi(\gamma)$ ◎ $\pi(\neg\gamma)$

   (a) $\pi(\gamma)$ ◎ π(‘$\pi(\gamma)$~) ГБ2

   (b) ◎ $\pi(\pi(\gamma)$ ◎ $\neg\gamma)$ ГБ1 от 1.4

   (c) ◎ $\pi(\pi(\gamma))$ ◎ $\pi(\pi(\gamma)$ ◎ $\neg\gamma)$ ◎ $\pi(\neg(\gamma))$ ГБ3

   (d) $\pi(\gamma)$ ◎ $\pi(\neg\gamma)$ 2MP (2.1, 2.2)

3. ◎ $\pi(\alpha$ ◎ β ◎ $\gamma)$ and ◎ $\pi(\alpha)$ ◎ $\pi(\beta)$ => ◎ $\pi(\alpha)$ ◎ $\pi(\gamma)$

   (a) $\pi(\alpha$ ◎ β ◎ $\gamma)$ ◎ $\pi(\alpha)$ ◎ π(b ◎ γ) ГБ3

   (b) $\pi(\beta$ ◎ $\gamma)$ ◎ $\pi(\beta)$ ◎ $\pi(\gamma)$ ГБ3

   (c) $\pi(\alpha)$ ◎ $\pi(\beta$ ◎ $\gamma)$ MP 1, given

   (d) $\pi(\alpha)$ ◎ $\pi(\beta)$ given

   (e) $\pi(\alpha)$ ◎ $\pi(\gamma)$ занести под дедукцию, ГБ3

4. ◎ $\pi(\gamma)$ ◎ $\pi(1{=}0)$

   (a) γ ◎ $\neg\gamma$ ◎ (1=0) 10i в ИИВ, выводима в предикатах

   (b) ◎ $\pi(\gamma$ ◎ $\neg\gamma$ ◎ (1=0)) ГБ1

   (c) $\pi(\gamma)$ ◎ $\pi(\neg\gamma)$ 2

   (d) ◎ $\pi(\gamma)$ ◎ $\pi(1{=}0)$ MP 4.2 4.3

5. ◎ Consis ◎ $\neg\pi(1{=}0)$ ◎ $\neg\pi(\gamma)$ контрапозиция 4 ◎ Consis ◎ $\neg\pi(\gamma)$ the same] ◎ Consis, тогда ◎ $\neg\pi(\gamma)$ ◎ $\neg\pi(\gamma)$ ◎ γ => ◎ γ => ◎ $\pi(\gamma)$ 1.1, ГБ1 ◎ $\neg\pi(\gamma)$, ◎ $\pi(\gamma)$ ◎◎

15 Ticket 13: TM

15.1 Теория множеств

Значит это такая теория первого порядка. В сигнатуре модели есть один пред.символ - ◎ Добавляем связку a ◎◎ b = (a ◎ b) & (b ◎ a) σ ◎ Θ => ◎x(x ◎ σ ◎ x ◎ Θ) o $\sigma = \Theta$ => σ ◎ Θ & Θ ◎ σ ◎ : ◎x(¬x ◎ ◎) x ∩ y = z, тогда ◎t(t ◎ z ◎◎ t ◎ x & t ◎ y) Dj(x) ◎a◎b(a ◎ x & b ◎ x & a ≠ b ◎ a ∩ b = ◎) X(a) - мн-во всех x пересекающихся ровно в одном эл-те с каждым из a и содержащих элементы из ∪a. X({{1, 2}, {2′, 3}}) = {{2, 3}, {1, 2′}}

15.1.1 Если существует мн-во, то существует пустое мн-во

Аксиома выделения: ◎x◎b◎y(y ◎ b ◎◎ (y ◎ x & φ(y))) Возьмем наше существующее мн-во x ◎b◎y(y ◎ b ◎◎ (y ◎ x & φ(y))) Пусть φ(y) = ◎ тогда подставим ◎ вместо b: ◎y(y ◎ ◎ ◎◎ (y ◎ x & ◎)) Это выполняется вроде.

15.1.2 Если x, то найдется {x}

◎x◎{x}◎y(y ◎ {x} ◎ y = x)

1. Пусть x ≠ ◎ {x} = {y | y ◎ {x, y} & y ≠ ◎} по аксиоме объединения ◎p◎y(y ◎ p ◎◎ ◎s(y ◎ s & s ◎ x)) ◎y(y ◎ {x, ◎} ◎◎ ◎s(y ◎ s & s ◎ x))

   или по аксиоме пары ◎p(x ◎ p & ◎ ◎ p & ◎z(z ◎ p ◎ (x = z V y = z))) x ◎ {x, ◎} & ◎ ◎ {x, ◎} & ◎z(z ◎ {x, ◎} ◎ …}

   ДГ руками помахал тут, ну и я помахаю по причине отсутствия времени доказывать

   А, нет, вот, кажется: По аксиоме степени ◎x◎{x, ◎}◎y(y ◎ {x, ◎} ◎◎ y ◎ x) ◎x◎{x, ◎}◎y((y ◎ {x, ◎} ◎ y ◎ x)&(y ◎ x ◎ y ◎ {x, ◎})) ¬y ◎ ◎, значит (y ◎ x ◎ y ◎ x) = ◎ ◎x◎{x, ◎}◎y((y ◎ {x, ◎} ◎ y ◎ x)&◎) ◎x◎{x, ◎}◎y(y ◎ {x, ◎} ◎ y = x) более слабое условие

2. x = ◎ P(◎) = {◎}

15.1.3 ⚜!x(⚜y.¬(y ⚜ x))

◎x(◎y.¬(y ◎ x)) & ◎a◎b((◎y.¬(y ◎ a)) & (◎y.¬(y ◎ b)) ◎ a = b) Первое по определению пустого множества и аксиоме выделения с ◎ ◎y.(¬y ◎ {}) & ◎y.(¬y ◎ {}) ◎ ◎p((p◎x ◎ p◎y) & (p◎y ◎ p◎x)) Второе как-то через ◎$_1$ ◎ ◎$_2$ и обратное включение На основании того, что мы подставляем наши пустые множества, импликация вырождается в ◎ ◎ ◎

15.1.4 x ∩ y существует

по теореме выделения ◎x◎b◎y(y ◎ b ◎◎ (y ◎ x & φ(y))) ◎y(y ◎ x ∩ y ◎◎ (y ◎ x & t ◎ y))

15.2 Аксиоматика ZFC

15.2.1 Аксиома равенства

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

15.2.2 Аксиома пары

◎x◎y(¬(x=y) ◎ ◎p(x ◎ p & y ◎ p & ◎z(z ◎ p ◎ (x = z V y = z)))) x ≠ y, тогда сущ. {x, y}

15.2.3 Аксиома объединений

◎x(◎y(y◎x) ◎ ◎p◎y(y ◎ p ◎◎ ◎s(y ◎ s & s ◎ 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

15.2.4 Аксиома степени

◎x◎p◎y(y ◎ p ◎◎ y ◎ 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.

15.2.5 Схема аксиом выделения

◎x◎b◎y(y ◎ b ◎◎ (y ◎ x & φ(y))) Для нашего множества x мы можем подобрать множество побольше, на котором для всех элементов, являющихся подмножеством x выполняется предикат.

15.2.6 Аксиома выбора (не входит в ZF по дефолту)

Если a = Dj(x) и a ≠ 0, то x ◎ a ≠ 0

15.2.7 Аксиома бесконечности

◎N(◎ ◎ N & ◎x(x ◎ N ◎ x ∪ {x} ◎ N))

15.2.8 Аксиома фундирования

◎x(x = ◎ V ◎y(y ◎ x & y ∩ x = ◎)) ◎x(x ≠ ◎ ◎ ◎y(y ◎ x & y ∩ x = ◎)) Равноценные формулы.

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

15.2.9 Схема аксиом подстановки

◎x◎!y.φ(x,y) ◎ ◎a◎b◎c(c ◎ b ◎◎ (◎d.(d ◎ a & φ(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.

16 Ticket 14: ординалы

16.1 Ординальные числа

- Определение вполне упорядоченного множества (фундированное с линейныи порядком).
- Определение транзитивного множества Множество X транзитивно, если ◎a◎b((a ◎ b & b ◎ x) ◎ a ◎ x)
- Ординал - транзитивное вполне упорядоченное отношением ◎ мн-во
- Верхняя грань множества ординалов S C | {C = min(X) & C ◎ X | X = {z | ◎(y◎S)(z ≥ y)}} C = Upb(S) Upb({◎}) = {◎}
- 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 $\varepsilon = w^{\varepsilon}$ $\varepsilon_0 = Upb(w, w^{w}, w^{w^{w}}, w^{w^{w^{w}}}, \ldots)$ - 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 ⊚ N) пишут a раз w^b. В канторовой форме приятно заниматься сложениями и прочим, потому что всякие upb - слишком ниочем.

16.2 Операции над ординальными числами

16.2.1 Стабилизация убывающей последовательности

Допустим, что есть убывающая последовательность ординалов $x_1,x_2\ldots$ Возьмем ординал $x_1 + 1 = x_0$. Тогда $\{x_1, x_2, \ldots\}$ ⊚ x_0. x_0 не пусто, значит там есть минимальный элемент по определению порядка на ординале. Пусть этот элемент - m. Тогда поскольку m ⊚ x_0, то m = x⊚ для какого-то i нашей убывающей последовательности.

1. Последовательность убывает нестрого. Тогда все x⊚ ≤ m, для k > i. Это выполняется, если x⊚ = x⊚, тогда последовательность стабилизируется в m.

2. Последовательность убывает строго. Тогда все x⊚ < m для k > i, но m - минимум множества. Противоречие. Убывающей строго последовательности ординалов не существует.

16.2.2 Арифметические операции через Upb

Пусть lim(a) = предельный ординал a

x + 0 = x x + c′ = (x + c)′ x + lim(a) = Upb{x + c | c < a}

x * 0 = 0 x * c′ = x * c + x x * lim(a) = Upb{x * c | c < a}

x ^ 0 = 1 x ^ c′ = x⊚ * x x ^ lim(a) = Upb{x⊚ | c < a}

Ну вот короче можно так, только приходится много думать как реализовывать Upb. Или только у меня так.

2^w = Upb(2, 4, 8, …) = w

16.2.3 Арифметические операции через Канторову форму

Хорошо описано в этой статье: Algorithms for Ordinal Arithmetic Переписывать довольно громоздко, учитывая количество вспомогательных функций.
Есть в моем гитхабе (*volhovm/mathlogic*) реализованное

17 Ticket 15: кардиналы

17.1 Кардинальные числа

Будем называть множества равномощными, если найдется биекция. Будем называть A не превышающим по мощности B, если найдется инъекция A ◎ 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 ◎ $x \leq a$ $|x| \leq |a|$ $◎_0 = w$ по определению; $◎_1$ = минимальный кардинал, следующий за $◎_0$ Кардинальное число ◎ - это ординальное число a, такое что ◎◎ = P(◎$◎_{-1}$) $◎_0 = ◎_0$ Континуум-гипотеза формулируется таким образом: $|P(◎_0)| = ◎_1$ или $◎_1 = ◎_1$ В 40 году Гёдель доказал недоказуемость отрицания Континуум-гипотезы в терминах ZFC, в 60 Коэн сделал то же самое но без отрицания. Это все в условиях непротиворечивости ФА. То есть в ZFC нельзя доказать или опровергнуть континуум-гипотезу. Сложение кардинальных чисел - $|A| + |B| = |A \cup B|$ если в них нету общих элементов, иначе max(|A|, |B|), поскольку мы можем построить двумерную таблицу из перес. элементов. Остальное есть на вики и вряд ли нужно вообще.

17.2 Диагональный метод Кантора

Докажем, что для любого множества $|x| < |P(x)|$ Воспользуемся диагональным методом Кантора Пусть $|x|=|P(x)|$ Выпишем таблицу, в которой столбцу p и строке q соответствует 1, если в множестве X лежит p, а в множестве P(X) лежит множество, содержащее в себе p. Построим ключевое мн-во t: элемент лежит в t, если на i-й диагональной позиции не стоит 1 и наоборот. То есть это множество всех таких элементов из X, которым по биекции соответствует множество о чем угодно, но не о самом элементе (не включающее элемент). t состоит из подмножеств X, тогда оно должно лежать в P(X). Докажем, что строка t не присутствует в таблице, сравнив ее с каждой другой строкой - от каждой n-й строки отличается в n-й столбце по построению. Противоречие - t нет в таблице, но t ◎ P(X).

17.3 Теорема Лёвингейма-Скулема

- Назовем мощностью модели мощность ее носителя (V или P или V∪P). M - модель, |M| - ее мощность, ну ясно.

- Элементарная подмодель Пусть M - модель фс первого порядка с носителем D. Пусть определено D_1 ◎ D, тогда структура M_1 построенная на D_1 так, что в ее интерпретации лежит все, что и в интерпретации M, кроме элементов, взаимодействующих с M \ M_1 (сужение области определения на D_1), называется **элементарной подмоделью**, если:

    1. Любая функция ФС, над которой рассматривается M, замкнута на D_1 (то есть если a ◎ D_1, b ◎ D_1, … то f(a, b, …) ◎ D_1)
    2. Любая формула A(x_1…x◎) теории при любых аргументах из D_1, истинная в M истинна и в M_1.

- Элементарная подмодель теории - модель теории Рассмотрим формулу A, она общазначима в M, значит и в M_1, тогда M_1 корректна.

- Счетно-аксиоматизируемая теория - множество аксиом ФС имеет мощность ◎$_0$

- ФА и ТМ счетно-аксоиматизируемые

- Пусть M - модель, T - мн-во формул теории. Тогда ◎M_1 : |M_1| = max(|T|, ◎$_0$) Нужно построить необходимое предметное множество и доказать, что модель на нем - это подмодель.

    1. Построение множества Пусть у нас есть множество D′, тогда D″ = D′ ∪ P, где P - некоторое множество формул добавленное при рассмотрении формул D′ по одной. A(y, x_1…x◎) - n-местная формула из T. Фиксируем x_1…x◎ из D′.
        - Если A = И или A = Л (тождественно) при любом y ◎ D - пропустим формулу
        - Если A = И или A = Л при каких-то y ◎ D′ - пропустим формулу
        - ◎y: A(y,..) = И, но при этом ◎y◎D′ A(y,..) = Л - тогда добавим один из тех y, на которых формула истинна, в D″. Добавим еще констант, которые нужны для вычисления A. Типа если В D′ не хватает переменных для того, чтобы показать что A может принимать истинностное значение, сгенерим и добавим такое.

    Переход от предыдущего множества к текущему увеличивает его не более чем на ◎$_0$ * |T| * |D′| - max(◎$_0$, T) Рассмотрим

D_0, D_0 ◎ D такое, что в него входят те элементы носителя, соответствующие константам, упоминающимся в T. Если оно пустое – добавим какую-нибудь константу из D. Оно ляжет в начало счетной последовательности D_0 ◎ D_1 ◎ … (каждый переход описан выше). D* = ∪D◎. D* - нужное нам множество. |D*| = max(◎$_0$, T)

2. Проверка структуры Индукция по структуре.
   - База. Предикат. P(f_1(x_1…x◎), …, f◎(x_1…x◎)). Если x_1…x◎ взяты из D*, то они были добавлены на некотором шаге, значит ◎t | x◎ ◎ D◎. Тогда на шаге D◎$_{+1}$ лежат результаты функций f_1…f◎. по построению. Тогда оценка формулы сохраняется.
   - Переход Связки X&Y, XVY, X◎Y, ¬X работают на сужении модели и оценка сохр.
     * ◎yB(y, x_1…x◎). Фиксируем x_1…x◎ из D*.
     (a) A была тождественно истинна или ложна - все OK
     (b) A принимала значения разных знаков Каждый x◎ добавлен на каком-то шаге, тогда возьмем максимальный шаг t, в D◎$_{+1}$ уже лежат все эти x◎. Тогда по построению D◎$_{+1}$ мы добавили нужный y такой что B(y, x_1…x◎) определено и выполнено в M. Значит B выполнено в M* по индукции, тогда A истинна в M*.
   - ◎yB(y, x_1…x◎).
     (a) Тождественно - OK
     (b) Принимает значения разных знаков Если оно истинно в M, тогда оно истинно в M* по 1 пункту перехода. Если ◎yB(y, x_1…x◎) было ложно на t-шаге, тогда на t+1 шаге мы здоровски исправили ситуацию, положив в мир y на котором оно истинно. Если оно было истинно, то по пункту 2 пошло дальше.

   Таким образом, D* - подмодель нашего множества, |D*| = ◎$_0$ + |T|

17.4 Парадокс Скулема

Мнимый парадокс Сколема формулируется так: Возьмем теорию, прикрутим модель с аксиоматикой ZF. Модель будет счетно-аксиоматизируемой потому что ZF. Утверждается, что в ZF ◎ ◎x(|x| = ◎$_1$) - это доказывает диагон. метод Кантора. Тогда получается что по теореме Лёвингейма-Скулема у нашей модели есть подмодель размером ◎$_0$ + ◎$_0$(счетно-акс) = ◎$_0$, но мы можем взять то самое x | |x| = ◎$_1$, и его занумеровать, выходит.

Формальный подход не допускает этого конфликта ввиду одного простого факта: Рассмотрим отношение существования несчетного мн-ва в R. ZF ◎ ¬◎f(f - биецкия между w и P(w)) & ◎f(f - биецкия между w и w∪w) // второе гарантирует счетность Первый аргумент конъюнкции - ¬◎f(◎x◎y(<x,y>◎f ◎◎ x◎A&x◎B)) <x,y> - пара (типа {x, y, {x}}) Тогда это значит, что в носителе модели нет такого f, что он бы представлял собой объединение пар. Собственно, по теореме Лёвингейма-Скулема у нас любая подмодель будет иметь счетный носитель. Нет никакого противоречия, потому что мы все еще работаем со счетным количеством множеств, а отсутствие биекции все так же выражается отсутствием множества в носителе.

18 Ticket 16: неполнота ФА

18.1 Теорема о трансфинитной индукции

Пусть есть формула с одной свободной переменной a(x) a истинна, если

1. a(0)
2. Если для любого конечного p - ординала мы можем показать следование { q < p => a(p) }, то a(p) истинно.

Без док-ва, не требуется.

18.2 Построение S∞

Мы строим еще одну теорию I порядка. По сути, мы вкладываем ФА в нашу теорию так, что любое доказательство ФА работает в S∞ и мы можем доказать доказать непротиворечивость любого "импортированного" д-ва

1. Формулы: Оставим связки ◎x, V, ¬ Заметим, что {V, ¬} полно для {0, 1}.
2. Доказательство Доказательством является дерево утверждений, в узлах которого правли, причем если дерево растет вверх, то правила действуют сверху вниз.

3. Аксиомы:

   (a) все термы ФА без переменных типа $\theta_1=\theta_2$ (корректные)

   (b) все термы вида $\neg(\theta_1=\theta_2)$ если $[\theta_1]\neq[\theta_2]$ (некорректные, все остальн.)

4. Правила: Примечание: в правилах используются боковые формулы, они могут отсутствовать. Это сделано для формализации того факта, что мы можем применять правило для двух любых элементов нашей дизъюнкции или вроде того. Примечание: org-mode подчеркивает a, если "$_{\text{a}}$_"

   (a) Структурные

      i. Перестановка $\underline{aVbV\gamma V\sigma}$ $aV\gamma VbV\sigma$

      ii. Сокращение $\underline{aVbVbV\gamma}$ $aVbV\gamma$

   (b) Сильные

      i. Ослабление $\underline{\gamma}$ $aV\gamma$

      ii. Де-Морган $\underline{(\neg a)V\gamma_{(\neg b)}V\gamma}$ $\neg(aVb)V\gamma$

      iii. Отрицание $\underline{aV\gamma\_\_}$ $(\neg\neg a)V\gamma$

      iv. Квантификация $\underline{\neg a(t)V\gamma}$ $\neg⊚x.a(x)V\gamma$

      v. Бесконечная индукция $\underline{a(0\sim)V\gamma_a(1\sim)V\gamma}$ … $\underline{a(r\sim)V\gamma}$… $⊚xa(x)V\gamma$

   (c) Сечение (для облегчения жизни) $\underline{\gamma Va_{\neg aV\delta}}$ $\gamma V\delta$

5. Порядки Каждой формуле в дереве соответствует порядок, причем посылке и заключению (выше и ниже _) слабого правила вывода соответствует один порядок, а порядковое число, отнесенное заключению сильного правила или сечения, больше порядковых чисел, отнесенных соотвтетствующим посылкам. Порядковые числа - это ординалы, они могут быть достижимыми, но не конечными - пусть формула какая-нибудь околорекурсивная типа $\Phi(x)$: $\Phi(0) = A ⊚ A$, $\Phi(1) = A ⊚ A ⊚ A$, $\Phi(2) = A ⊚ A ⊚ A ⊚ A$. Тогда пусть мы хотим доказать $⊚x.\Phi(x)$ - по бесконечной индукции порядок термов будет увеличиваться, а порядок $⊚x.\Phi(x)$ будет w. Именно из-за этого факта мы используем в доказательстве теоремы об устранении сечений трансфинитную индукцию по порядку - ведь обычной индукции мало для порядков больших w.

6. Степень Степень сечения - количество связок в $\neg a$. Степень доказательства - наибольшая степень сечения в дереве. Степень всегда конечна

- любая формула в ФА содержит конечное число связок, а при трансляции нет возможности увеличить их количество. Тогда трансфинитная индукция по термам, в которых в сечении количество связок растет до бесконечности, невозможно.

7. Нитью называется последовательность формул от начальной до конечной. Все нити в доказательстве конечны, поскольку если в начальной формуле стоит ординал, последовательность в нити не возрастает, а эти числа убывают с применением строгого правила или сечения. Мы знаем, что строго убывающая бесконечная последовательность ординалов не существует. Добавим правило, что последовательность применения слабых правил подряд была всегда конечна

8. Теорема в S∞ - выражение, которое может стоять в заключительной формуле вывода

18.3 Теоремы об эквивалентности ФА и S∞

18.3.1 *Лемма* 1: В S∞ выводимо AV¬A

A либо корректна, либо некорректна, тогда $\underline{A}$ ¬AVA ослабление
$\underline{\neg A}$ $\underline{A V \neg A}$ ослабление $\underline{\neg A V A}$ перестановка

18.3.2 *Лемма* 2: В S∞ выводимо s≠tV¬A(s)VA(t)

Если выводимо A(s), s = t, то выводимо A(t) (все вхождения меняем) если s=t, то выводимо ¬A(t)VA(t), потом сделаем ослабление если s≠t, то она аксиома (некорректная) и ослабим.

18.3.3 *Лемма* 3: всякая выводимая в S замкнутая формула A является теоремой S∞

Докажем, что если что-то доказуемо в ФА, то его эквивалент доказуем и в S∞. ◎◎◎A => ◎◎A′ Схема док-ва Рассмотрим доказательство в ФА, оно состоит из β_1′…β◎′, оттранслируем каждое в β◎ ◎ S∞ (по полноте {¬, V} это возможно) Тогда можно сделать дерево, в котором начальные формулы - аксиомы S, а правила вывода - MP, GEN.

Рассмотрим формулу A = β◎

1. B ◎ C ◎ B, те ¬B V (¬ C V B) Из замкнутости A следует замкнутость B ¬B V B выводима по *Л*1, тогда ослабим с ¬C, переставим.

2. (B ◎ C) ◎ (B ◎ C ◎ D) ◎ B ◎ D ¬(¬B V C) V (¬(¬B V (¬C V D)) V (¬B V D)) По Л1 выводимо ¬(¬B V C) V (¬B V C), (¬B V ¬C V D) V ¬(¬B V ¬C V D) Тогда можно по перестановке, сечению (с C) и сокращению доказать (B ◎ C ◎ D) ◎ (B ◎ C) ◎ (B ◎ D) что одно и то же, см дедукцию в предикатах

3. (B ◎ C) ◎ (B ◎ ¬C) ◎ ¬B ¬(¬B V C) V ¬(¬B V ¬C) V ¬B

   (a) ¬B V B л1
   (b) ¬¬¬B V B отрицание
   (c) ¬(¬¬B V C) V ¬¬¬B V B ослабление
   (d) ¬¬¬B V ¬(¬¬B V C) V B перестановка
   (e) ¬¬¬B V B V ¬¬C аналогично + еще перестановка
   (f) ¬C V ¬¬C лемма
   (g) ¬C V B V ¬¬C ослабление + перестановка
   (h) ¬(¬¬B V C) V B V ¬¬C де-морган от 6 и 8
   (i) ¬¬C V ¬(¬¬B V C) V B перестановка 8
   (j) ¬(¬¬B V ¬C) V ¬(¬¬B V C) V B де-морган от 4 и 9

   Ну вот мы доказали что-то очень похожее на то, что нужно было. Там контрпозиция, шмяк шмяк, готово.

4. Видимо, примерно все формулы так доказываются.

5. ◎x.B(x) ◎ B(t) ¬◎x.B(x) V B(t) По л1 ¬B(t) V B(t), потом квантификация по 1 элем.

6. B(t) ◎ ◎x.B(x) B(t) ◎ ¬◎x.B(x) (что заметно отличается от ◎x.¬B(x)) ¬B(t) V ¬◎x.B(x) Не, я не знаю. Но точно можно! По бесконечной индукции мож как-то. Или там сечение хитрое.

А еще есть аксиомы ФА

1. a = b ◎ a′ = b′ ¬(a = b) V a′ = b′

   - если a = b, то a′ = b′, это аксиома S∞, тогда по ослаблению добавим ¬(a = b)
   - если a ≠ b, то она же и аксиома

2. a = b ◎ a = c ◎ b = c a ≠ b V a ≠ c V b = c a ≠ b V ¬(x = c) @ b V (x = c) @ c по лемме 2

3. a′ = b′ ⊚ a = b Аналогично 1
4. ¬(a′ = 0) Аксиома, поскольку a′ всегда имеет с 0 разные значения
5. a + b′ = (a + b)′ TODO
6. a + 0 = a Аксиома, поскольку это вседа равенство
7. a * 0 = 0 аналогично 6
8. a * b′ = a * b + a TODO
9. φ[x:=0] & ⊚x.(φ ⊚ φ[x:=x′]) ⊚ φ ¬B(0) V ¬⊚x(¬B(x)VB(x′)) V B(0) лемма 1 и перестановка ¬B(0) V ¬(¬B(0) V B(1)) V … можно показать по индукции … V ¬(¬B(k) V B(k′)) V B(k′) (ослабление, перестановка, де-морган) ¬B(0) V ¬(⊚x(¬B(x) V B(x′))) V B(k′) k раз квантификация, перестановки, сокращ. Применим бесконечную индукцию относительно первого и третьего терма и получим что надо.

Окей, с аксиомами разобрались. И еще есть два правила вывода

1. MP B условие ¬B V A условие A сечение
2. GEN B(x) условие Продвигаясь от этой формулы вверх можно поменять все x на k, тогда верно ⊚ B(k) На основании принципа бесконечной индукции доказываем ⊚xB(x)
3. A ⊚ B(t) => A ⊚ ⊚x.B(x) ¬A V B Заменим все вхождения перменной в доказательстве в ФА формулы ¬A V B на 0, 1, 2…, тогда по бесконечной индукции: ¬A V B(0), ¬A V B(1), … ⊚ ¬A V ⊚x.B (только B(0) V ¬A везде)
4. A(t) ⊚ B => ⊚x.A(x) ⊚ B ¬A V B ⊚ ¬¬⊚x.(¬A(x)) ⊚ B Заменим все вхождения свободной перменной t в ФА на конкретные. Получим счетное мн-во д-в ¬A(0) V B, ¬A(1) V B, … по беск. индукции ⊚x.¬A(x) V B ¬¬⊚x.¬A(x) V B - навесили двойное отрицание

18.3.4 Следствие: непротиворечивость S∞ влечет непротиворечивость S

Пусть в S доказуемо ¬(0=0), тогда оно доказуемо и в S∞, тогда AV0=0¬(0=0)VA
Аргументы получаются по ослаблению AVA A

18.4 Теорема Генцена об устранении сечений

18.4.1 Лемма: сильные правила 2, 3, 5 обратимы

Правила обратимы и их д-во имеет порядок и степень не больше, чем первоначальное Нам дают доказательство формулы, мы строим новое дерево, в котором из результата следуют посылки.

1. Правило Де-Моргана ¬(B V E) V D Рассмотрим вывод формулы. Проследим вхождения подформул ¬(B V E) вормулы, которые соответствуют вхождению в конечную формулу (то есть не те, которые исчезают в сечении). Мы пройдем через всякий случай применения слабого правила и сильные, когда ¬(B V E) является боковой формулой. Остановка произойдет либо в ослаблении (F ◎ ¬(B V E) V F) либо в Де-Моргане (¬B V F, ¬E V F ◎ ¬(B V E) V F). Совокупность таких вхождений формулы назовем ее **историей**. Если все вхождения формулы ¬(B V E) в ее истории заменить на ¬B, то в результате получится вывод ¬B V D. Аналогично можем вывести ¬E V D.

2. Правило отрицания ¬¬B V D Заменим все вхождения ¬¬B в ее истории на B, получим вывод B V D

3. Бесконечная индукция ◎xB(x) V D Заменим все вхождения ◎xB(x) в ее истории (1 элемент) на B(k) (причем если мы уткнулись в бесконечную индукцию, выберем только ту ветку, которая соответствует B(k)) Тогда для любого k получим вывод B(k)

18.4.2 Теорема: устранение сечения

Если для A в S∞ существует вывод (m, a), то существует вывод в S∞ (n, 2^a), где n < m Докажем через трансфинитную индукцию по порядку a вывода A

- База: порядок вывода 0 Вывод не содержит сечений и его степень 0

- Переход: пусть теорема верна для выводов порядков меньших a Будем продвигаться вверх по выводу, пока не встретим первое применение сильного правила или сечения.

  1. Сильное правило Пусть его посылки занумерованы порядковыми числами a◎ Согласно индуктивному предположению, для

этих посылок существует дерево вывода F со степенью < m и порядком $2^{(a_{\circledcirc})}$. Заменим таким деревом то поддерево данного дерева вывода, заключительной формулой которого служит рассматриваемое вхождение F. Сделав так со всеми посылками мы получим новое дерево для A, отнесем ему порядковое число $2^{a} > 2^{(a_{\circledcirc})}$ (пояснение от меня, потому что я чет долго доганял - каждую посылку заменяем по индукции на ее модное новое дерево от нее самой же).

2. Сечение Значит имеем что-то на уровне $\underline{CVB\_{\neg BVD}}$ CVD Согласно индуктивному предположению для CVB и ¬BVD существуют выводы степеней меньших m и порядков 2^{a_1}, 2^{a_2}. Рассмотрим разные случаи строения B:

   (a) B - это элементарная формула. Одна из формул B и ¬B есть аксиома. Пусть K - та, которая не аксиома. По предположениию поддерево основного дерева вывода с K может быть заменено другим со степенью n и порядка $2^{(a_i)}$ (i = 1 или 2, смотря в какой посылке K). В этом новом дереве расмотрим историю K, начальные формулы в которой могут возникнуть только по ослаблению (а исчезать по сечению). Поэтому удаление всех вхождений K из истории приводит к построению дерева вывода для D или C порядка $2^{a_{\circledcirc}}$. Отсюда с помощью ослабления получаем дерево вывода для C V D порядка 2^{a}. Степень меньше m (одно сечение убрали).

   (b) B - это ¬E, тогда посылки выглядят как CV¬E, ¬¬EVD Существует дерево вывода для ¬¬EVD степени < m и порядка 2^{a_2} В силу леммы об обратимости можно построить дерево вывода EVD порядка 2^{a_2} степени < m Кроме того существует дерево вывода степени < m и порядка 2^{a_1} для левой посылки, тогда построим из них новое дерево вывода $\underline{EVD}$ $\underline{CV\neg E}$ $\underline{DVE\_{\neg EVC}}$ $\underline{DVC}$ CVD Степень выделенного здесь сечения на единицу меньше общего числа связок и кванторов в ¬E, которое само по себе ≤ m. Формуле CVD можно присвоить порядковое число C V D по свойству посылок новог сечения.

   (c) B - это EVF, посылки: CVEVF, ¬(EVF)VD Существует дерево вывода для правой посылки < m и порядка 2^{a_2}, по лемме об обратимости существуют выводы степеней < m и порядка 2^{a_2} для ¬EVD и ¬FVD (по Де-Моргану).

По предположению индукции есть еще дерево вывода для левой посылки. Из последних трех построим такое: CVEVF_¬FVD CVEVD CVDVE___¬EVD CVDVD CVD Степень сечения уменьшили (в каждом на 1), в формуле CVEVD можно дать порядок $2^{max}(a_1, a_2)+1$, а остальным - 2^a

(d) B - это ◎xE, посылки: CV◎xE (¬◎xE)VD По индуктивному предположению для левой посылки можно построить дерево вывода (< m,2^{a_1}). В силу указания в начале 2 леммы о эквивалентности S∞ и ФА (если ◎A(t), t=s, то ◎A(s)) и леммы об обратимости для любого постоянного терма z существует вывод CVE(z). Можем и правую посылку заменить (< m, 2^{a_2}) по инд.предположению Тогда в правой посылке история ¬(◎xE) может начинаться либо с ослабления либо с квантификации. Заменим на C все такие начала - если это ослабление, то просто подменим вместо ¬(◎xE) новое C, если квантификация, то ¬E(t)VF__ CVE(t)_¬E(t)VF //первое мы взяли из левой посылки ¬(◎xE(x))VF => CVF В результате мы получили дерево вывода CVD Степень меньше m, поскольку связку мы одну убрали **тут еще ОЧЕНЬ АДОВЫЕ оценки порядка CVD, но он 2^a**

18.4.3 Следствие: устранение всех сечений

Воспользуемся леммой об устранении сечения, пока степень вывода не станет равна нулю. Тогда порядок будет что-то на уровне степенной башни из двоек, в вершине которой первоначальная степень, а количество двоек – количество применения леммы.

18.4.4 Следствие: S∞ непротивроечива

Если S∞ противоречива, в ней докажется 0≠0V0≠0V…V0≠0. В ее истории появление 0≠0 может быть только из-за ослабления, но тогда посылкой ослабления тоже будет 0≠0. Если в д-ве есть сечения, мы можем перестроить его, устранив все сечения, а затем провести рассуждения вновь и увидеть, что такая формула недоказуема, а значит S∞ непротиворечива, значит и ФА тоже непротиворечива.

19 Ключевые фигуры

- Станислав Яськовски - 1906 Алгебра Яськовского, один из первых исследователей ИИВ
- Герхард Генцен - 1909 Теорема об устранении сечения (1935)
- Курт Гёдель - 1906 Теоремы о непротиворечивости - 1930 Чуть ли не все остальное
- Сол Крипке - 1940 Семантика Крипке - 1960-1970
- Дэвид Гильберт - 1862, Пауль Бернайс - 1888 Основания математики - 1934, 39
- Их достаточно много, а времени мало.