Mathematical Logic Questions

1. Исчисление высказываний. Общезначимость, следование, доказуемость, выводимость. Корректность, полнота, непротиворечивость. Теорема о дедукции для исчисления высказываний.

- **Общезначимость($\models \alpha$) .** Общезначимое высказывание - высказывание, которое истинно при любой оценке пропозициональных переменных.

- **Следование($\Gamma \models \alpha$).** Пусть $\Gamma = \gamma_1, \gamma_2, \ \dots, \gamma_n$. Тогда α следует из Γ, если при любой оценке пропозициональных переменных, входящих в высказывания Γ и α, на которых все высказывания из Γ истинны, α также истинна.
- **Выполнимость.** Формула истинна при какой-нибудь оценке.
- **Невыполнимость.** Формула не истинна ни при какой оценке.
- **Опровержимость.** Формула ложна при какой-нибудь оценке.
- ▶ Схемы аксиом и правило вывода

  $1.\ \alpha \to \beta \to \alpha$

  $2.\ (\alpha \to \beta) \to (\alpha \to \beta \to \gamma) \to (\alpha \to \gamma)$

  $3.\ \alpha \to \beta \to \alpha \& \beta$

  $4.\ \alpha \& \beta \to \alpha$

  $5.\ \alpha \& \beta \to \beta$

  $6.\ \alpha \to \alpha \vee \beta$

  $7.\ \beta \to \alpha \vee \beta$

  $8.\ (\alpha \to \gamma) \to (\beta \to \gamma) \to (\alpha \vee \beta \to \gamma)$

  $9.\ (\alpha \to \beta) \to (\alpha \to \neg \beta) \to \neg \alpha$

  $10.\ \neg\neg\alpha \to \alpha$

  $ModusPonens:$
  $\frac{\alpha, \alpha \to \beta}{\beta}$

- **Доказуемость($\vdash \alpha$) .** Высказывание α доказуемо, если существует доказательство $\alpha_1, \alpha_2 \dots \alpha_k$ и α_k совпадает с α

  Доказательство. Доказательство в исчислении высказываний — это некоторая конечная последовательность выражений (высказываний) $\alpha_1, \alpha_2 \dots \alpha_k$, что каждое из высказываний α_i либо является аксиомой, либо получается из других утверждений $\alpha_{P_1}, \alpha_{P_2}, \dots, \alpha_{P_n}$ $(P_1 \dots P_n < i)$ по правилу вывода.
- **Выводимость($\Gamma \vdash \alpha$).** Высказывание α выводимо из списка гипотез Γ, если существует вывод $\alpha_1, \alpha_2 \dots \alpha_k$ и α_k совпадает с α.

  Вывод. Доказательство, в котором могут использоваться гипотезы.
  Ака. Вывод в исчислении высказываний — это некоторая конечная последовательность выражений (высказываний) $\alpha_1, \alpha_2 \dots \alpha_k$, что каждое из высказываний α_i либо является аксиомой, либо получается из других утверждений $\alpha_{P_1}, \alpha_{P_2}, \dots, \alpha_{P_n}$ $(P_1 \dots P_n < i)$ по правилу вывода, либо является гипотезой из списка Γ.
- **Корректность($\vdash \alpha \ \Rightarrow \ \models \alpha$).** Если высказывание доказуемо, то оно общезначимо
- **Полнота($\models \alpha \ \Rightarrow \ \vdash \alpha$).** Если высказывание общезначимо, то оно доказуемо.
- **Непротиворечивость.** Теория непротиворечива если не существует формулы α такой, что $\vdash \alpha$ и $\vdash \neg\alpha$
- **Противоречивость.** Если теория противоречива, то в ней доказуема любая формула
- **Теорема о дедукции.** Пусть имеется Γ, α, β. Утверждение $\Gamma \vdash \alpha \to \beta$ тогда и только тогда, когда $\Gamma, \alpha \vdash \beta$

  (если из списка высказываний Γ выводится импликация α и β, то можно перестроить вывод таким образом, что из Γ, α выводимо β и наоборот)

2. Теорема о полноте исчисления высказываний.

- Классическое исчисление высказываний полно.

  Полнота($\models \alpha \ \Rightarrow \ \vdash \alpha$). Если высказывание общезначимо, то оно доказуемо.

  ▶ Вспомогательные утверждения
  - *Лемма 1.* Если $\Gamma, \Sigma \vdash \alpha$, то $\Gamma, \Sigma, \Delta \vdash \alpha$. Если $\Gamma, \Sigma, \Delta, \Phi \vdash \alpha$, то $\Gamma, \Delta, \Sigma, \Phi \vdash \alpha$.
  - *Лемма 2.* Если справедливы три утверждения: $\Gamma \vdash \gamma, \ \Delta \vdash \delta, \ \gamma, \delta \vdash \alpha$, то справедливо и $\Gamma, \Delta \vdash \alpha$
  - *Лемма 3.* (Правило контрапозиции). Каковы бы ни были формулы α, β, справедливо, что $\vdash (\alpha \to \beta) \to (\neg\beta \to \neg\alpha)$
  - *Лемма 4.* Правило исключенного третьего. Какова бы ни была формула $\alpha, \vdash \alpha \vee \neg\alpha$
  - *Лемма 5.* Каждое из построенных по таблицам истинности утверждений доказуемо.
  - *Лемма 6.* Пусть пропозициональные переменные $X_1, X_2 \ldots X_N$ - все переменные, которые используются в формуле α. И пусть задана некоторая оценка переменных. Тогда $X_1^{(\neg)}, X_2^{(\neg)} \ldots X_N^{(\neg)} \vdash \alpha^{(\neg)}$.
  -
  - *Лемма 7.* Исключение допущения. Пусть справедливо $\Gamma, \rho \vdash \alpha$ и $\Gamma, \neg\rho \vdash \alpha$. Тогда также справедливо $\Gamma \vdash \alpha$.
  - *Лемма 8.* Пусть при всех оценках переменных $X_1^{(\neg)}, X_2^{(\neg)} \ldots X_N^{(\neg)} \vdash \alpha$, тогда $\vdash \alpha$
- Классическое исчисление высказываний корректно.

3. Интуиционистское исчисление высказываний. BHK-интерпретация. Решётки. Булевы и псевдобулевы алгебры. Теорема Гливенко.

- **Интуиционистское исчисление высказываний.** Чтобы получить **ИИВ** (Интуиционистское исчисление высказываний) нужно в **КИВ** (Классическое исчисление высказываний) заменить 10-ю аксиому ($\neg\neg\alpha \to \alpha$) на $\alpha \to \neg\alpha \to \beta$
  - В интуиционистском исчислении высказываний невозможно доказать правило исключенного третьего: $\alpha \vee \neg\alpha$
  - Существует множество способов построить модель для интуиционистской логики: BHK-интерпретация, Модели Крипке, Топологическая интерпретация...
  - ▶ Топологическая интерпретация.

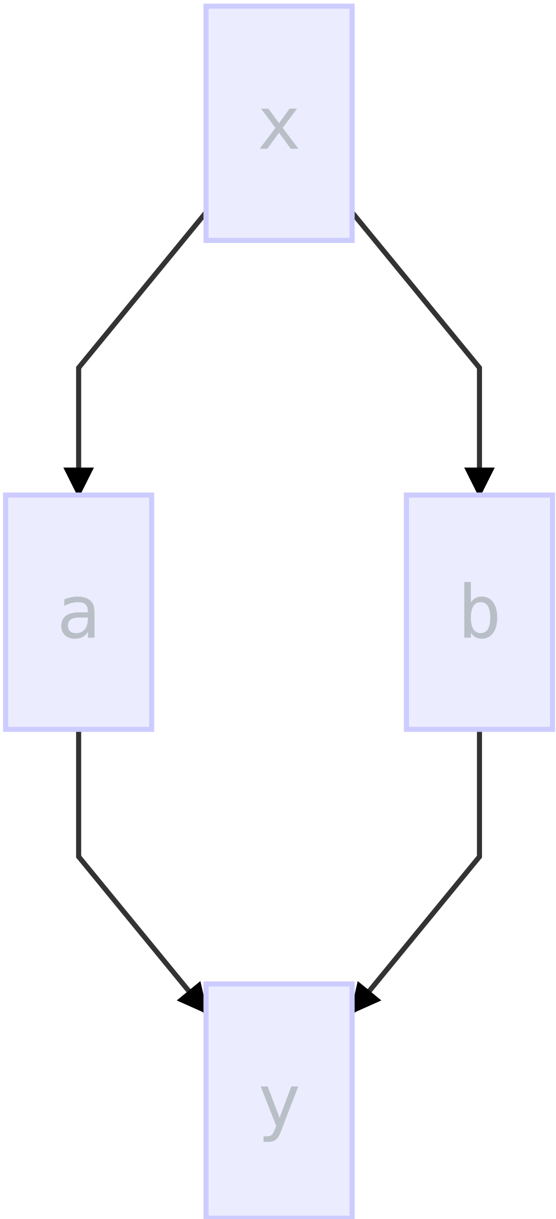
    Начнем с множества истинностных значений. Возьмем в качестве этого множества все открытые множества некоторого заранее выбранного топологического пространства. Определим оценку для связок интуиционистского исчисления высказываний следующим образом:
    - $[A \& B] = [A] \cap [B]$
    - $[A \vee B] = [A] \cup [B]$
    - $[A \to B] = (c[A] \cup [B])^{\circ}$
    - $[\neg A] = (c[A])^{\circ}$

    Будем считать, что формула истинна в данной модели, если её значение оказалось равно всему пространству.
    * Example: возьмем пространство R, и вычислим значение формулы $A \vee \neg A$ при A равном (0,1):
    $[A \vee \neg A] = (0,1) \cup [\neg A] = (0,1) \cup (c(0,1))^{\circ} = (0,1) \cup ((-\infty, 0) \cup (1, \infty)) = (-\infty, 0) \cup (0,1) \cup (1, \infty)$

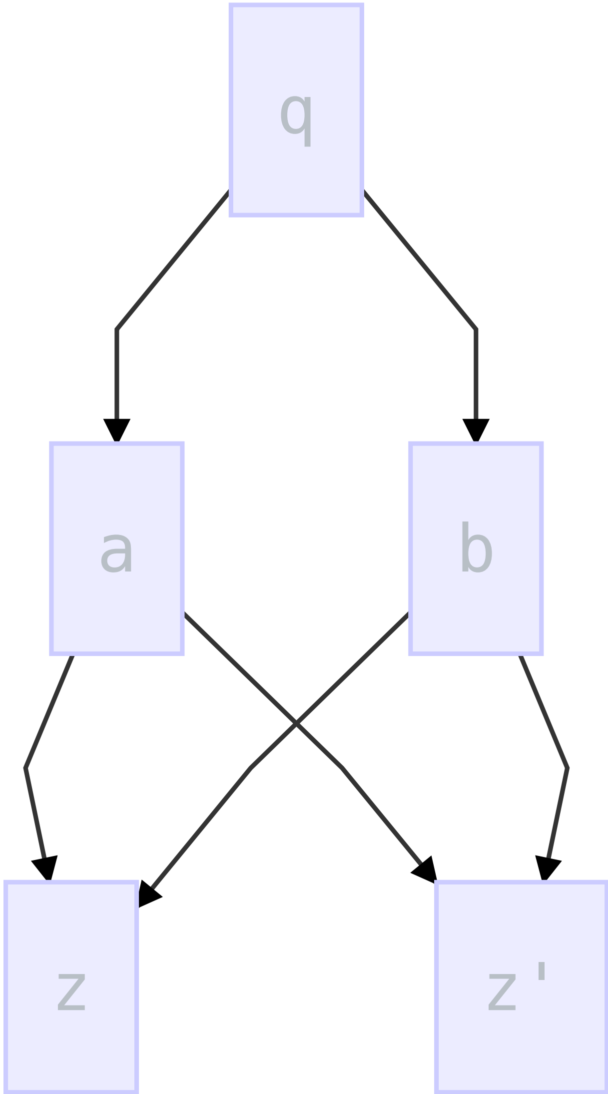
- **BHK-интерпретация (Brouwer-Heyting-Kolmogorov interpretation).** Пусть заданы высказывания α, β, тогда:

- мы считаем $\alpha \& \beta$ доказанным, если у нас есть доказательство α и есть доказательство β
- мы считаем $\alpha \vee \beta$ доказанным, если у нас есть доказательство α или доказательство β, и мы точно знаем какое
- мы считаем $\alpha \to \beta$ доказанным, если из доказательства α мы можем построить доказательство β
- мы считаем $\perp$ (aka 0) утверждением не имеющим доказательства
- $\neg\alpha$ есть сокращение $\alpha \to \perp$. Мы считаем $\neg\alpha$ доказанным, если мы умеем из доказательства α получить противоречие

- **Решётка.** Частично-упорядоченное(рефлексивно, транзитивно, антисимметрично) множество $\langle M, \sqsubseteq \rangle$, в котором, для любых a, b определены две операции:
  - верхняя грань a, b: $a + b = c$, наименьший c, что $a \sqsubseteq c, b \sqsubseteq c$
  - нижняя грань a, b: $a * b = c$, наибольший c, что $c \sqsubseteq a, c \sqsubseteq b$
  - example: $a + b = x, a * b = y$



- наименьший и минимальный:\
  z-наименьший в M, если для всех $t \in M: \ z \sqsubseteq t$\
  z-минимальный в M, если нет такого $t \in M: \ t \sqsubseteq z$
  example: z, z' : никакой не наименьший, но оба минимальные



- **Дистрибутивная решетка.** Для любых a, b, c: $(a+b)*c = a*c+b*c$
    - Решетка дистрибутивна т. и т. т., когда при любых $a, b, c : a*b+c = (a+c)*(b+c)$
- **Импликативная решётка.** Решетка с псевдодополнением, определённым для любых двух элементов этой решетки
    - Операция псевдодополнения. $c = a \to b$, c - это такой наибольший t, что $t*a \sqsubseteq b$
    - В импликативной решетке есть наибольший элемент
- **Псевдобулева алгебра (алгебра Гейтинга).** Импликативная решетка с 0
    - 0 - наименьший элемент решетки
- **Булева алгебра.** Псевдобулева алгебра, в которой для любых a: $a + (a \to 0) = 1.$ \
  Булева алгебра - пример классической логики:
  a + (a -> 0) = 1 - Закон исключенного третьего, который читается как "Либо альфа, либо не альфа выполнено"

- **Теорема Гливенко.** $\vdash_{\text{к и в}}\ \alpha$, то $\vdash_{\text{и и в}}\ \alpha$.Если формула α выводима в классическом исчислении высказываний, то $\neg\alpha$ выводима в интуиционистком исчислении высказываний.

4. Алгебра Линденбаума. Полнота интуиционистского исчисления высказываний в псевдобулевых алгебрах.

- **Алгебра Линденбаума.** Множество множеств (классов) факторизованных по отношению эквивалентности.
  - Определение. Возьмем множество всех формул ИИВ, тогда:
  1. $\alpha \sqsubseteq \beta$, если $\alpha \vdash \beta$
  2. $\alpha \approx \beta$, если $\alpha \sqsubseteq \beta$ и $\beta \sqsubseteq \alpha$
- Полнота ИИВ TODO()

5. Модели Крипке. Сведение моделей Крипке к псевдобулевым алгебрам. Нетабличность интуиционистского исчисления высказываний.

- **Вообще, очень полезно посмотреть видосики на степике**
- **Определение**
  1. Пусть W - множество миров. (миры - это какие-то множества;
  2. $(\preceq) \subseteq W \times W$ - отношение частичного порядка на W;
  3. $(\Vdash) \subseteq W \times P$ - отношение вынужденности, причём если $W_x \preceq W_y$ и $W_x \Vdash X$, то $W_y \Vdash X$, где X - переменная. (*Мы требуем, чтобы если некоторый мир наследует нашему, то все переменные, которые вынуждены в нашем мире в нем тоже были бы вынуждены*)

     Тогда $< W, (\preceq), (\Vdash) >$ - **модель Крипке**

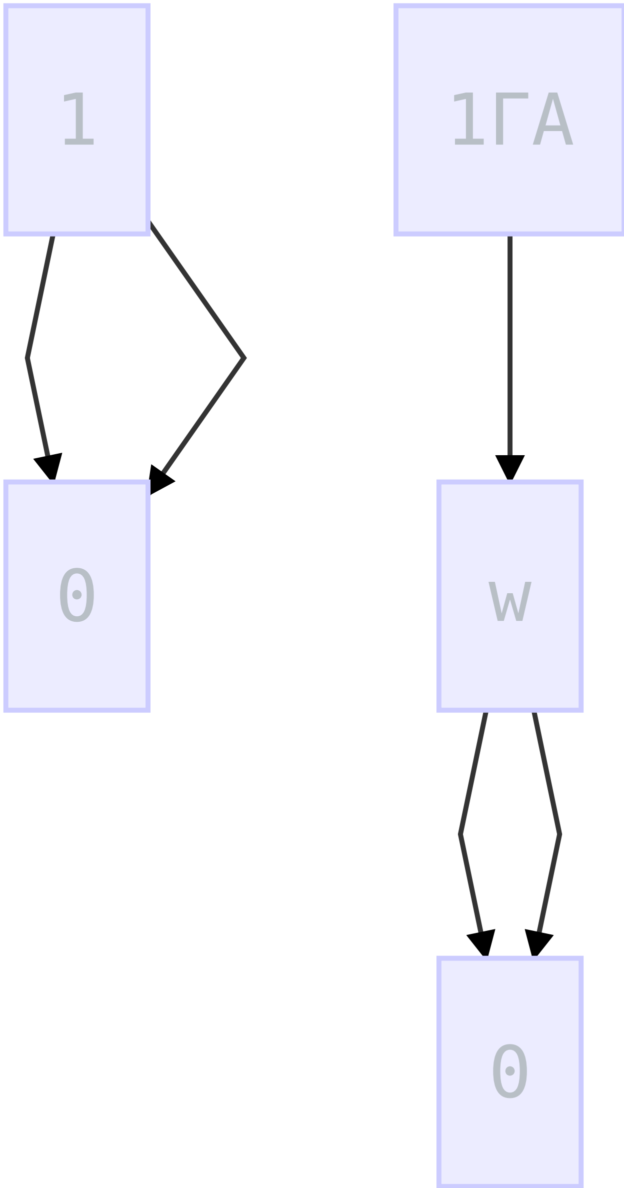
     Как оценить высказывание в модели Крипке?
- **Определение**
  1. $W_k \Vdash P$ - задано в модели.
  2. $W_k \Vdash \phi \& \psi$ - если $W_k \Vdash \phi$ и $W_k \Vdash \psi$
  3. $W_k \Vdash \phi \vee \psi$ - если $W_k \Vdash \phi$ или $W_k \Vdash \psi$
  4. $W_k \Vdash \phi \rightarrow \psi$ - если в любом W_i : $W_k \preceq W_i$ из $W_i \Vdash \phi$ следует $W_i \Vdash \psi$
  5. $W_k \Vdash \neg\phi$ - если в любом W_i : $W_k \preceq W_i$ выполнено $W_i \nVdash \phi$
  6. $W_k \nVdash \perp$

- **Определение**
  - $\Vdash \phi$ в модели W (иначе: $W \models \phi$), если $W_i \Vdash \phi$ при всех $W_i \in W$ (*Будем говорить, что формула ϕ **истинна** в данной модели, если она вынуждена в каждом мире этой модели*)
  - $\models \phi$, если $\Vdash \phi$ во всех моделях W (*Будем говорить, что формула ϕ **общезначима**, если она вынуждена во всех моделях*)
- **Теорема**
  - Модель Крипке это **алгебра Гейтинга**
- **Табличная модель.** Будем говорить, что модель исчисления - табличная, если:
  1. Задано множество истинностных значений V.
  2. Для каждой связки задана функция оценки: $f_\star$: $V * V \rightarrow V$ и $f_\neg : V \rightarrow V$
  3. Среди V выделены некоторые истинные значения $\top$. Мы считаем, что $\models \alpha$, если $[\alpha] \in \top$ при любых оценках пропозициональных переменных.

    4. Модель корректна
        - классическая оценка для исчисления высказываний - табличная модель
- TODO картинки?, ...
- **Теорема** В интуиционистской логике нет полной табличной модели

6. Гёделева алгебра. Операция $\Gamma(A)$. Дизъюнктивность интуиционистского исчисления высказываний.

- **Гёделева алгебра** Алгебра A - гёделева, если для любых $a, b \in A$ если $a + b = 1$, то $a = 1$ и $b = 1$.
- **Гёделизация ($\Gamma(A)$)** Добавление элемента, который больше всех



Алгебра с добавлением ω и $1_{\Gamma(A)}$. Причем если $a \in A$, то $\omega \geqslant a, 1_\Gamma(A) \geqslant a$ и $1_\Gamma(A) > \omega$

- Утв. если A - алгебра Гейтинга, то $\Gamma(A)$ - алгебра Гейтинга
- Дизъюнктивность ИИВ. Если $\vdash \alpha \vee \beta$, то $\vdash \alpha$ или $\vdash \beta$

7. Исчисление предикатов. Общезначимость, следование, выводимость. Теорема о дедукции в исчислении предикатов.

- **Определение**
    - ***Терм*** исчисления предикатов (или *предметное выражение*) это:
        - *Предметная переменная* - маленькая буква начала или конца лат. алфавита, (возможно с индексами или апострофом)
        - Применение функции: если $(\theta_1, \dots \theta_n)$ - термы и f - *функциональный символ* (некая функция), то $f(\theta_1, \dots \theta_n)$ тоже терм. (Например константы - нульместные функции)
- **Определение**
    - **Формула** исчисления предикатов - это:
        - Если α и β - формулы исчисления предикатов, то $\neg\alpha, \alpha \& \beta, \alpha \vee \beta, \alpha \to \beta$ - также формула
        - Если α - формула, и x - предметная переменная, то $\forall x.\ \alpha$ и $\exists x.\ \alpha$ - также формулы
        - Применение предиката: если $(\theta_1, \dots \theta_n)$ - термы, и P - предикатный символ, то $P(\theta_1, \dots \theta_n)$ - формула.
- **Определение**
    - Дана некоторая формула s. Будем говорить, что подстрока s_1 строки s является подформулой если она в точности соответствует какому-то одному нетерминалу в дереве разбора строки s.
- **Определение**
    - Если в формулу входит подформула, полученная по правилам для кванторов $(\forall x.\ \alpha, \exists x.\ \alpha)$, то мы будем говорить, что формула α находится в области действия данного квантора по переменной x. Также будем говорить, что любая подформула формулы α находится в области действия данного квантора.
- **Определение**
    - Если некоторое вхождение переменной x находится в области действия квантора по переменной x, то такое вхождение мы назовем **связанным**. Вхождение x непосредственно рядом с квантором назовём **связывающим**. Те вхождения переменных, которые не являются связанными или связывающими назовём **свободными**. Формула не имеющая свободных вхождений переменных называется **замкнутой**.
- **Определение**
    - Будем говорить, что терм θ **свободен для подстановки** в формулу ψ вместо x, если после подстановки вместо свободных вхождений x ни одно вхождение свободной переменной в θ не станет связанным.
- В исчислении предикатов к схемам аксиом из исчисления высказываний добавляется две схемы аксиом:

  Пусть θ свободно для подстановки вместо x в ψ

  1. $(\forall x.\ \psi) \to (\psi[x := \theta])$
  2. $\psi[x := \theta] \to \exists x.\ \psi$
- Правила вывода:

  Пусть x не входит свободно в ϕ, тогда имеют место следующие правила вывода:

  $\frac{\phi \to \psi}{\phi \to \forall x. \psi}$
  $\frac{\psi \to \phi}{(\exists x. \psi) \to \phi}$
- **Определения**
    - Формула в исчислении предикатов **общезначима**, если она истинна на любом предметном множестве D, при любой оценке предикатных и функциональных символов, и при любых оценках свободных предметных переменных.
    - Пусть имеется некоторое исчисление предикатов с множеством аксиом A, и пусть дан некоторый список Γ формул исчисления предикатов. Тогда **вывод** формулы α в исчислении с аксиомами $A \cup \Gamma$ мы назовем выводом из допущений Γ и будем записывать как $\Gamma \vdash \alpha$

- Пусть имеется какое-то предметное множество D, список формул Γ и высказывание α, тогда **следованием** из Γ в α назовем следующее утверждение: если при всех оценках (предикатных, функциональных и т.д.) в предметном множестве D, где формулы Γ истинны, истинна и α. (мб можно понятнее написать TODO)

- **Теорема о дедукции**

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

- *Исчисление предикатов* **корректно**, т.е. любое доказуемое утверждение общезначимо

8. Непротиворечивые множества формул. Доказательство существования моделей у непротиворечивых множеств формул в бескванторном исчислении предикатов.

- **Непротиворечивое множество формул.** Назовем Γ - множество замкнутых формул - непротиворечивым, если ни для какой формулы α невозможно показать, что $\Gamma \vdash \alpha$ и $\Gamma \vdash \neg\alpha$
  - *Альтернативное определение.* Γ - непротиворечивое множество формул, если $\Gamma \nvdash \alpha \& \neg\alpha$ при некотором α
- **Пример замкнутых и бескванторных.**
  - Бескванторная = не содержащая кванторов.\
    Замкнутая = не содержащая свободных переменных.

    Возможны все 4 варианта:\
    ЗБ: $0 = 1$

    З: $\forall x. x = 1$

    Б: $x = 1$

    : $\forall x. x = y$

- **Def.** Полным непротиворечивым множеством замкнутых (замкнутых и бескванторных) формул назовем такое множество Γ, что для любой замкнутой (замкнутой и бескванторной) формулы α либо $\alpha \in \Gamma$, либо $(\neg\alpha) \in \Gamma$

▶ Некоторые теоремы.

- **Теорема.** Пусть Γ - непротиворечивое множество замкнутых (замкнутых и бескванторных) формул. Тогда какова бы ни была замкнутая (замкнутая и бескванторная) формула ϕ, хотя бы $\Gamma \cup \{\phi\}$ или $\Gamma \cup \{\neg\phi\}$ - непротиворечиво
- **Теорема.** Пусть Γ - непротиворечивое множество замкнутых (замкнутых и бескванторных) формул. Тогда найдется полное непротиворечивое множество замкнутых (замкнутых и бескванторных) формул Δ, что $\Gamma \in \Delta$.

- **Def.** Моделью для множества формул F назовем такую модель M, что при всяком $\phi \in F$ выполнено $[\phi]_M = \text{и}$
  - **Альтернативное обозначение.** $M \models \phi$
- **Теорема.** Любое непротиворечивое множество замкнутых бескванторных формул имеет модель.
- **Def.** Пусть M - полное непротиворечивое множество замкнутых формул. Тогда модель M задается так:

  1. D - множество всех бескванторных формул и дополнительная строка "ошибка!"
  2. $[f(\theta_1, \ldots, \theta_n)] =" f(" + + [\theta_1] + + "," ++ \ldots ++ "," + + [\theta_n] + + ")"$
  3.

$$[P(\theta_1, \ldots, \theta_n)] = \begin{cases} И, если & "f(" ++ [\theta_1] ++ "," ++ \ldots ++ "," ++ [\theta_n] ++ ")" \in M \\ Л, иначе & \end{cases}$$

1. $[x]=$"ошибка!", т.к. формулы замкнуты

- *Лемма.* Пусть ϕ - бескванторная формула, тогда $M \models \phi$ тогда и только тогда, когда $\phi \in \mathrm{M}$
- **Lemma.** Пусть Γ - полное непротиворечивое множество бескванторных формул. Тогда существует модель для Γ.

9. Теорема Гёделя о полноте исчисления предикатов. Доказательство полноты исчисления предикатов.

- **Определение**
  - Назовём формулу α **формулой с поверхностными кванторами**, если существует такой узел в дереве разбора формула, не являющийся квантором, ниже которого нет ни одного квантора, а выше - нет ничего кроме кванторов. (Например: $\forall x \exists y \forall z (P(x, y, z) \& P(z, y, x))$)
- **Лемма**

  Для любой формулы исчисления предикатов найдётся эквивалентная ей формула с поверхностными кванторами.

- **Теорема Гёделя о полноте исчисления предикатов.**

  Пусть Γ - непротиворечивое множество формул исчисления предикатов. Тогда существует модель для Γ.

- **Теорема**

  Если $\models \alpha$, то $\vdash \alpha$

10. Теории первого порядка, структуры и модели. Аксиоматика Пеано. Арифметические операции. Формальная арифметика.

- **Теория первого порядка.** Теорией первого порядка назовем исчисление предикатов с дополнительными ("нелогическими" или "математическими")
  - предикатными и функциональными символами
  - аксиомами\
    сущности, взятые из исходного исчисления высказываний, назовём логическими.
- **Структура.** Структурой теории первого порядка мы назовем упорядоченную тройку $\langle D, F, P \rangle$, где $F = \langle F_0, F_1 \ldots \rangle$ - списки оценок для 0-местных, 1-местных и т.д. функций, и $P = \langle P_0, P_1 \ldots \rangle$ - списки оценок для 0-местных, 1-местных и т.д. предикатов, D - предметное множество.

  ▶ Небольшое пояснение
- **Def.** Назовем структуру корректной, если любая доказуемая формула истинна в данной структуре.
- **Модель.** Модель теории - любая корректная структура
- **Аксиоматика Пеано.** Рассмотрим некоторое множество N. Будем говорить, что оно удовлетворяет аксиомам Пеано, если выполнено:
  - В нем существует некоторый выделенный элемент 0 ($0 \in N$)
  - Для каждого элемента определена операция $'$, результат ее также принадлежит множеству N ($N \to N$)

  Кроме того, эти элементы и операция к этим элементам должны удовлетворять следующим требованиям:
  - Не существует такого $x \in N$, что $x' = 0$ (Нет предшественника у минимального элемента)

- Если при x и y из N верно, что $x' = y'$, то $x = y$. Если $x = y'$, то x назовем следующим за y, а y - предшествующим x (определение операции $'$)
- Каково бы ни было свойство ("предикат") $P : N \to V$, если:
  - выполнено $P(0)$
  - при любом $x \in N$ из $P(x) \Rightarrow P(x')$\
    то при любом $x \in N$ выполнено $P(x)$\
    (Индукция)

- **Формальная арифметика.** (формализация аксиоматики Пеано) формальная арифметика - теория первого порядка, со следующими добавленными нелогическими:
  - двуместными функциональными символами $(+)$,$(*)$, одноместным функциональным символом $(')$, нульместным функциональным символом 0;
  - двуместным предикатным символом $(=)$;
  - восемью аксиомами:
    - $(A1)$ $a = b \to a = c \to b = c$ (транзитивность равенства)
    - $(A2)$ $a = b \to a' = b'$ (инъективность штриха)
    - $(A3)$ $a' = b' \to a = b$ (инъективность штриха)
    - $(A4)$ $\neg a' = 0$ (у нуля нет предшественников)
    - $(A5)$ $a + 0 = a$ (определение сложения)
    - $(A6)$ $a + b' = (a + b)'$ (определение сложения)
    - $(A7)$ $a * 0 = 0$ (определение умножения)
    - $(A8)$ $a * b' = a * b + a$ (определение умножения)
  - схемой аксиом индукции\
    $\psi[x := 0] \& (\forall x. (\psi \to \psi[x := x'])) \to \psi$

- Еще один пример теории первого порядка.

  Теория групп. К исчислению предикатов добавим двуместный предикат $(=)$, двуместную функцию $(*)$, одноместную функцию x^{-1}, нульместную функцию 1 и следующие аксиомы:

  - $(E1)$ $a = b \to a = c \to b = c$
  - $(E2)$ $a = b \to (a * c = b * c)$
  - $(E3)$ $a = b \to (c * a = c * b)$
  - $(G1)$ $a * (b * c) = (a * b) * c$
  - $(G2)$ $a * 1 = a$
  - $(G3)$ $a * a^{-1} = 1$

11. Примитивно-рекурсивные и рекурсивные функции. Функция Аккермана. Примитивная рекурсивность арифметических функций, функций вычисления простых чисел, частичного логарифма.

- **Примитивы:**

  1. Ноль. $Z : \mathbb{N}_0 \to \mathbb{N}_0, Z(x) = 0$
  2. Инкремент. $N : \mathbb{N}_0 \to \mathbb{N}_0, N(x) = x'$
  3. Проекция. $V_i^n : \mathbb{N}_0^n \to \mathbb{N}_0, V_i^n(x_1, \ldots, x_n) = x_i$
  4. Подстановка. Если $f : \mathbb{N}_0^n \to \mathbb{N}_0$ и $g_1, \ldots, g_n : \mathbb{N}_0^m \to \mathbb{N}_0$, то $S\langle f, g_1, \ldots, g_n \rangle : \mathbb{N}_0^m \to \mathbb{N}_0$, при этом:

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

  5. Примитивная рекурсия. Если $f : \mathbb{N}_0^n \to \mathbb{N}_0$ и $g : \mathbb{N}_0^{n+2} \to \mathbb{N}_0$, то $R\langle f, g \rangle : \mathbb{N}_0^{n+1} \to \mathbb{N}_0$, при этом

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

6. Минимизация. Если $f:\mathbb{N}_0^{n+1}\to\mathbb{N}_0$, то $\mu\langle f\rangle:\mathbb{N}_0^n\to\mathbb{N}_0$, при этом

$$\mu\langle f\rangle(x_1,\ldots,x_n)=\text{такое минимальное число } y, \text{ что } f(x_1,\ldots,x_n,y)=0.$$

$$\text{Если такого } y \text{ нет, то результат примитива неопределён}$$

- **Примитивно-рекурсивная функция.** Функция называется примитивно-рекурсивной, если возможно построить выражение только из первых пяти примитивов, такое, что оно при всех аргументах возвращает значение, равно значению требуемой функции.
- **Рекурсивная функция.** Если функция может быть выражена только из 6 примитивов, то она называется рекурсивной.
- **Функция Аккермана.** Рекурсивна, но не примитивно-рекурсивна

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

- **Простые арифметические операции.**
  - Сложение
  - Умножение
  - Вычитание
  - Остальные арифметические операции
- **Проверка числа на простоту.** Функция проверки числа на простоту примитивно-рекурсивна.
- **Частичный логарифм.** Частичный логарифм примитивно-рекурсивен.

12. Выразимость отношений и представимость функций в формальной арифметике. Представимость примитивов N, Z, S, U в формальной арифметике.

- **Выразимое отношение.** Отношение R называется выразимым (в формальной арифметике), если существует такая формула $\alpha(x_1,\ldots x_n)$ с n свободными переменными, что для любых натуральных чисел $k_1,\ldots,k_n$
  1. если $(k_1,\ldots,k_n)\in R$, то доказуемо $\alpha(\overline{k_1},\ldots,\overline{k_n})$
  2. если $(k_1,\ldots,k_n)\notin R$, то доказуемо $\neg\alpha(\overline{k_1},\ldots,\overline{k_n})$
- **Представимость.** Функция f от n аргументов называется представимой в формальной арифметике, если существует такая формула $\alpha(x_1,\ldots,x_{n+1})$ с $n+1$ свободной переменной, что для любых натуральных $k_1,\ldots,k_n$:
  1. $f(k_1,\ldots,k_n)=k_{n+1}$ тогда и только тогда, когда доказуемо $\alpha(\overline{k_1},\ldots,\overline{k_{n+1}})$
  2. Доказуемо $\exists!b.\,\alpha(\overline{k_1},\ldots,\overline{k_n},\overline{b})$,

     где $\exists!y.\,\alpha(y)=(\exists y.\,\alpha(y))\&\forall a.\,\forall b.\,\alpha(a)\&\alpha(b)\to a=b$
- **Вспомогательные утверждения.**

  ▶ Spoiler

  Для любого выводимого выражения мы можем составить этот же вывод с другими переменными, пусть $T\ :=\ 0=0\to 0=0\to 0=0$ (sch.ax.1) : \
  $Lemma\ 1)\vdash P[x:=\Theta]$\
  $1.\ P\to T\to P$ (sch.ax.1)\
  $1.5\ P$ (т.к. это выводимое утверждение) \
  $2.\ T\to P$ (MP 1, 1.5) \
  $3.\ T\to\forall x.\,(P)$ (по правилу вывода(2) можно ввести кванторы по переменным внутри P, если эти переменные не входят свободно в T, что верно по построению) \
  $3.5\ T$ (sch.ax.1) \

$4. \forall x. (P)$ (MP 3.5, 3) \
$5. (\forall x. (P)) \to (P[x := \Theta])$ (по sch.ax.11 можно заменить переменные по кванторам внутри P) \
$6. (P[x := \Theta])$ (MP 4,5)

$Lemma\ 2)\ a = b \vdash b = a$

$1.\ a = b\ (Hypothesis\ 1)$

$2.\ a = a\ (\text{нетрудно показать по Лемме}\ 1)$

$3.\ a = b \to a = a \to b = a\ (Ax.\ 2\ (FA))$

$4.\ b = a\ (2\ MP\ from\ 3)$

- **Представимость примитива Z (Ноль).** Примитив Z представим в ФА
$\psi(x_1, x_2) := x_1 = x_1 \& x_2 = 0$
- **Представимость примитива N (Инкремент).** Примитив N представим в ФА.
$\alpha(x_1, x_2) := x_2 = x_1'$
- **Представимость примитива U (Проекция).** Примитив U представим в ФА
$\beta(x_1, \ldots, x_{n+1}) := (\&_{i \neq k} x_i = x_i) \& x_k = x_{n+1}$
- **Представимость примитива S (Подстановка).** Пусть функции $f, g_1, .., g_k$ представимы в ФА. Тогда $S\langle f, g_1, .., g_k \rangle$ представим в ФА
$\exists g_1 \ldots \exists g_k. \phi(g_1, \ldots, g_k, x_{n+1}) \& \gamma_1(x_1, \ldots, x_n, g_1) \& \ldots \& \gamma_k(x_1, \ldots x_n, g_k)$

13. Бета-функция Гёделя. Представимость примитивов R и M и рекурсивных функций в формальной арифметике.

- **β-функция Гёделя.** $\beta(b, c, i) := b\%(1 + (i + 1) * c)$

  Здесь b, c параметры, а i - какой-то элемент последовательности. Ака b, c определяют что за массив, а i говорит о каком-то индексе.

  ▶ Представление бета-функции в ФА

  β-функция Гёделя представима в ФА формулой:
  $\beta(c, d, i, d) := \exists q. (b = q * (1 + c * (i + 1)) + d) \& (d < 1 + c * (i + 1))$\
  Деление b на x с остатком: найдутся частное (q) и остаток (d), что $b = q * x + d$ и $0 \leq d < x$

  Доказать формально???

  Теорема. Китайская теорема об остатках (вариант формулировки):

  если $u_0, \ldots, u_n$ - попарно взаимно-просты, и $0 \leq a_i < u_i$, то существует такой b, что $a_i = b\%u_i$

  Теорема. Главное свойство β-функции.

  Если $a_0, \ldots, a_n \in \mathbb{N}_0$, то найдутся такие $b, c \in \mathbb{N}_0$, что $a_i = \beta(b, c, i)$

- **Представимость примитива R (Примитивная рекурсия).** Примитив R представим в ФА. примитив $R\langle f, g \rangle$ представим в ФА формулой $\rho(x_1, \ldots, x_n, y, a)$:

  $\exists b. \exists c. (\exists a_0. \beta(b, c, 0, a_0) \& \phi(x_1, \ldots, x_n, a_0))$

  $\& \forall k. k < y \to \exists d. \exists e. \beta(b, c, k, d) \& \beta(b, c, k', e) \& \gamma(x_1, \ldots, x_n, k, d, e)$

  $\& \beta(b, c, y, a)$

- **Представимость примитива M (Минимизация).** Примитив M представим в ФА. Пусть функция $f : \mathbb{N}_0^{n+1} \to \mathbb{N}_0$ представима в ФА формулой $\phi(x_1, \ldots, x_n, y)$. Тогда примитив $M\langle f \rangle$ представим в ФА формулой:

$\mu(x_1, \dots, x_n, y) := \neg\phi(x_1, \dots, x_n, y, 0) \& \forall u.\, u < y \to \phi(x_1, \dots, x_n, u, 0)$

- **Представимость рекурсивных в формальной арифметике.** Рекурсивные функции представимы в формальной арифметике (индукция по длине док-ва)

14. Гёделева нумерация. Рекурсивность представимых в формальной арифметике функций.

- **Гёделева нумерация (Способ представления доказательств в виде натуральных чисел).** Будем называть Гёделевой нумераций следующую конструкцию. Пусть $\langle a_0, \dots, a_{n-1}\rangle$-некоторый список положительных натуральных чисел. Пусть p_i-простое число номер i, тогда Гёделева нумерация этого списка:

  $\ulcorner\langle a_0, \dots, a_{n-1}\rangle\urcorner = 2^{a_0} * 3^{a_1} * \dots * p_{n-1}^{a_{n-1}}$
- Также мы можем составить Гёделеву нумерацию для всей программы, в т.ч. для отдельных символов:

Номер	Символ
3	(
5	)
7	'
9	.
11	$\neg$
13	$\to$
15	$\vee$
17	$\&$
19	$\forall$
21	$\exists$
23	$\vdash$
$25 + 6k$	x_k
$27 + 6 * 2^k * 3^n$	f_k^n
$29 + 6 * 2^k * 3^n$	p_k^n

  Формула. $\phi \equiv s_0 s_1 \dots s_{n-1}$. Гёделев номер $\ulcorner\phi\urcorner = 2^{\ulcorner s_1\urcorner} * \dots * p_{n-1}^{\ulcorner s_{n-1}\urcorner}$

  Доказательство. $\text{п} = \delta_0 \delta_1 \dots \delta_{k-1}$, его Гёделев номер: $\ulcorner\text{п}\urcorner = 2^{\ulcorner\delta_1\urcorner} * \dots * p_{n-1}^{\ulcorner\delta_{k-1}\urcorner}$
- **Рекурсивность функций представимых в ФА.** Функции, представимые в ФА, рекурсивны. То есть, если мы можем про функцию доказать, что эта функция действительна равна такому значению, то значит мы можем написать программу, которая ее вычисляет.

  Более формально. Если $f : \mathbb{N}_0^n \to \mathbb{N}_0$, и f представима в ФА формулой ϕ, то f - рекурсивна.

15. Непротиворечивость и ω-непротиворечивость. Первая теорема Гёделя о неполноте арифметики, её неформальный смысл.

▶ Некоторые определения

- **Проблема останова.** Не существует функции `bool p (std::string source, std::string arg)`, возвращающей $true$ тогда и только тогда, когда функция с исходным кодом $source$ (имеющая аргумент типа `std::string`) оканчивает работу, если ей передать на вход значение arg

  Ее полный исходный код - в переменной s_source

  Что вернет `p (s_source, s_source)`? Если возвращаемое p истинно, то s должна остановиться, но по ее исходному коду она зациклиться. Если возвращаемое p ложна, то s должна зациклиться, но по ее исходному коду она должна остановиться. Противоречие.\
  Из этого получаем, что такой функции p не существует.

- **Самоприменимость.** $W_1 : W_1(x,p) = 1$, если $x = \ulcorner\xi\urcorner$, где ξ - формула с единственной свободной переменной x_1, а p - доказательство самоприменения ξ:

  $\vdash \xi(\overline{\ulcorner\xi\urcorner})$

  $W_1(x,p) = 0$, если это не так.

Теорема. Существует формула ω_1 со свободными переменными x_1, x_2, такая, что:

1. $\vdash \omega_1(\overline{\ulcorner\phi\urcorner}, \overline{p})$, если p - гёделев номер доказательства самоприменения ϕ;
2. $\vdash \neg\omega_1(\overline{\ulcorner\phi\urcorner}, \overline{p})$, иначе

Док-во. W_1 рекурсивна, то есть представима в ФА формулой o_1. Функция такая же как и $proof$ (add ref to proof TODO()).

Возьмем $\omega_1(x_1, x_2) := o_1(x_1, x_2, \overline{1})$.

- **Непротиворечивость.** Формальная арифметика непротиворечива, если нет формулы α, что $\vdash \alpha$ и $\vdash \neg\alpha$
- **ω-непротиворечивость.** Формальная арифметика ω-непротиворечива, если для любой формулы $\phi(x)$, что
  - $\vdash \phi(\overline{p})$ при всех $p \in \mathbb{N}_0$ выполнено $\nvdash \exists p. \neg\phi(p)$
  - (менее формально) пусть $\vdash \phi(\overline{0}), \vdash \phi(\overline{1})$... Значит, нет p, что $\vdash \neg\phi(p)$
- **Теорема.** Если формальная арифметика ω-непротиворечива, то она непротиворечива.

- **Первая теорема Гёделя о неполноте арифметики.**

  Def. $\sigma(x) := \forall p. \neg\omega_1(x,p)$. Не существует доказательства p для самоприменения x.

  Теорема Гёделя

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

```
$\sigma(x):=\forall p.\neg\omega_1(x,p)$:
$\sigma(\overline{\ulcorner\sigma\urcorner})$ означает "я не доказуема". При этом мы
показали, что она не доказуема, значит она истинна? Покажем это формально.

**Теорема** $\models\sigma(\overline{\ulcorner\sigma\urcorner})$ В стандартной
интерпретации формальной арифметики: $D=\N_0,a'=a+1$ и т.д.
```

16. Формулировка первой теоремы Гёделя о неполноте арифметики в форме Россера, её неформальный смысл. Формулировка второй теоремы Гёделя о неполноте арифметики, $Consis$. Неформальное пояснение метода доказательства.

- **Первая теорема Гёделя в форме Россера.**
  - **Def.** $W_2(x,p) = 1$, если p-доказательство отрицания самоприменения.
  - **Лемма.** Существует формула ω_2, что $\vdash \omega_2(\overline{x}, \overline{p})$, если $W_2(x,p) = 1$, иначе $\vdash \neg\omega_2(\overline{x}, \overline{p})$
  - **Теорема**. Пусть $\rho(x) := \forall p.\, \omega_1(x,p) \to \exists q.\, q < p \& \omega_2(x,q)$, тогда $\nvdash \rho(\overline{\ulcorner \rho \urcorner})$ и $\nvdash \neg\rho(\overline{\ulcorner \rho \urcorner})$

    Описание. Мы говорим, что если p является доказательством самоприменения x, то найдется доказательство q, причем, с меньшим Гёделевым номером, чем p, который является док-вом отрицания самоприменения x. Тогда не доказуемо ни самоприменение ρ, ни отрицание самоприменения.

    Менее формальное определение теоремы. Если существует доказательство самоприменения ρ, то существует и доказательство отрицания самоприменения ρ, причем с меньшим номером
- **Формула $Consis$.**
  - **Теорема.** Существует формула $\pi(x,p)$ - доказуемая тогда и только тогда, когда $proof(x,p) = 1$. Проверка, что p является доказательством x
  - **Def.** Формула *"доказуемо"*: $\pi_r(x) := \exists p.\, \pi(x,p)$. Если найдется p - гёделев номер доказательства x
  - **Def.** $Consis := \neg\pi_r(\overline{\ulcorner \overline{1} = 0 \urcorner})$. Если формальная арифметика непротиворечива, то ожидаем, что формула $Consis$ истинна.

- **Вторая теорема Гёделя о неполноте арифметики.**

  $\vdash Consis \to \sigma(\overline{\ulcorner \sigma \urcorner})$

  "Если непротиворечивость формальной арифметики может быть доказана в формальной арифметике, то формальная арифметика противоречива"