Лекции по Математической логике N5-8

Профессор, член-корреспондент РАН С.С.Гончаров

Новосибирский государственный университет, Новосибирск, Россия

gonchar@math.nsc.ru

L 5

Лекция 5. Исчисление Высказываний.

Для анализа доказательств и определения основных законов логики, лежащих в основе как логических обоснований. так и нашей повседневной логики, используемой в общении людей мы построим вначале язык исчисления высказываний и выделим основные логические формы, которые лежат в основе правильных рассуждений. Этот фрагмент логики базируется на силлогизмах Аристотеля и является достаточным для анализа большей части, встречающихся в рассуждениях, которые не используют идеализаций бесконечного характера, и носят дедуктивный характер. Мы рассмотрим также ограничение и на способ построения более сложных высказываний из заданных, допуская для таких построений только логические связки: & ($\wedge$) — конъюнкция, $\vee$ — дизъюнкция, $\longrightarrow$ — импликация, $\neg$ — отрицание. Эти связки соответствуют соответственно союзам "и", "или", утверждению типа "если ..., то ..."и отрицанию высказывания. Естественно это соответствие неполное. После построения истинностной семантики для нашего исчисления высказываний мы обсудим некоторые особенности и ограничения в понимании таких связок, отличающие их от причинно - следственных связей в естественном языке.

Определим алфавит нашего формального языка из трех типов символов:

1. Множество $\mathcal{P}$, состоящее из символов пропозициональных переменных $P_0, P_1, \ldots, Q_0, Q_1, \ldots, R_0, R_1 \ldots, \ldots$

2. Множество логических связок: & — конъюнкция, $\vee$ — дизъюнкция, $\rightarrow$ — импликация, $\neg$ — логические связки.

3. Множество вспомогательные символы: (,), которые задают левую и правую скобки, для определения структуры наших выражений.

Конечный последовательности символов из алфавита называются словами этого алфавита. Но не все слова осмысленны. Обычно определяется индуктивная процедура определения осмысленных слов данного формального языка. Мы хотим таким образом в нашем фиксированном алфавите определить понятие высказывания или пропозициональной формулы представляющими слова специального вида, с которыми мы и будем работать в нашем формальном языке .

Индуктивное определение высказываний (пропозициональной формулы)и их подформул.

1.(базис индукции) Пропорциональная переменная является высказыванием и единственной ее подформулой.

2.(шаг индукции) Если φ, ψ — высказывания, то $(\varphi\&\psi)$, $(\varphi\vee\psi)$, $(\varphi\to\psi)$, $\neg\varphi$ — высказывания, а подформулами будут сами формулы, а также все подформулы формул из которых они определены логическими связками.

3.Других способов построения высказываний нет.

Обозначим через $Form(\mathcal{P})$ множество всех высказываний (пропозициональных формул), построенных из пропозициональных переменных $\mathcal{P}$. В дальнейшем мы будем использовать вместо термина пропозициональная формула термин формула, если из контекста ясно, что мы рассматриваем пропозициональные формулы.

Семантики высказываний.

Построим вначале теоретико–множественную семантику. В теоретико - множественной семантике каждое высказывание трактуется как некоторое свойство объектов из произвольно выбранного универсума, относительно которых выполнены естественные свойства, связывающие выполнимость более сложно определенных выражений через их составные части.

Пусть задано множество объектов $\mathcal{U}$. Рассмотрим множество всех его подмножеств $P(\mathcal{U})$. Мы рассматриваем множество всех пропозициональных переменных $\mathcal{P}$ для наших высказываний в качестве имен простейших свойств, из

которых с помощью логических связок строятся уже более сложные свойства элементов. Мы будем рассмотривать в качестве означиваний в $\mathcal{U}$ пропозициональных переменных функции $\gamma\colon \mathcal{P} \to P(\mathcal{U})$. Любое такое означивание может быть естественным образом продолжено до функции $Int_\gamma\colon \mathcal{P} \to P(\mathcal{U})$ на все множество пропозициональных формул, построенных из множества пропозициональных переменных $\mathcal{P}$, которое будем называть интерпретацией в $\mathcal{U}$ для означивания γ.

Для любой пропозициональной переменной Q из нашего множества пропозициональных переменных определяем $Int_\gamma(Q) \rightleftharpoons \gamma(Q)$. Если высказывание φ имеет вид $(\varphi_1 \bigtriangledown \varphi_2$, где $\bigtriangledown$ одна из логических связок &, $\vee$ или $\to$, то полагаем для конъюнкции $Int_\gamma(\varphi_1 \& \varphi_2) \rightleftharpoons Int_\gamma(\varphi_1) \cap Int_\gamma(\varphi_1)$, для дизъюнкции $Int_\gamma(\varphi_1 \vee \varphi_2) \rightleftharpoons Int_\gamma(\varphi_1) \cup Int_\gamma(\varphi_1)$ и для импликации $Int_\gamma(\varphi_1 \to \varphi_2) \rightleftharpoons (\mathcal{U} \backslash Int_\gamma(\varphi_1)) \cup Int_\gamma(\varphi_2)$. Для формулы φ вида $\neg\varphi_1$ полагаем $Int_\gamma(\neg\varphi_1) \rightleftharpoons (\mathcal{U} \backslash Int_\gamma(\varphi_1))$.

Заметим, что $\gamma(\varphi) \subseteq \mathcal{U}$ и мы говорим, что на элементе a из $\mathcal{U}$ те, которые попадают в подмножество $\gamma(\varphi)$ обладают этим свойством φ, остальные нет.

Определим теперь отношение теоретико-множественного следования:

Из гипотез $\varphi_1, \ldots, \varphi_n$ следует в теоретико–множественной семантике φ ($\varphi_1, \ldots, \varphi_n \vdash_{TM} \varphi$), если для любого множества $\mathcal{U}$ и для любого означивания γ в $\mathcal{U}$ интерпретация Int_γ удовлетворяет следующему свойству:

$\gamma(\varphi_1) \cap \gamma(\varphi_2) \cap \ldots \cap \gamma(\varphi_n) \subseteq \gamma(\varphi)$,

то есть любой элемент из $\mathcal{U}$, удовлетворяющий при заданной интерпретации всеми свойствами из гипотез удовлетворяет также свойству φ.

Набор свойств $\varphi_1, \ldots, \varphi_n$ совместен в теоретико - множественной семантике, если существуют множество $\mathcal{U}$ и означивание γ в $\mathcal{U}$ и хотя бы один элемент обладает всеми свойствами $\varphi_1, \ldots, \varphi_n$ при интерпретации для данного означивания. В противном случае этот набор формул называется несовместным и обозначим это условие через $\gamma(\varphi_1), \ldots, \gamma(\varphi_n) \vdash_{TM}$. Формулу φ исчисления высказываний назовем тождственно истинной в теоретико-множественной семантике, если для любого множества U и любого означивания γ в $\mathcal{U}$ все элементы из $\mathcal{U}$ обладают

свойством φ при интерпретации для этого означивания, то есть выполняется $\models_{TM} \varphi$.

Определим теперь истинностную семантику. При этой семантике мы про каждое высказывание сможем сказать истинно оно или ложно, если заданы соответствующие ответы про простые высказывания соответствующие пропозициональным переменным.

Рассмотрим двухэлементное множество $\{0,1\}$. Мы будем трактовать 0 как значение истинности "истинно"и 1 как "ложно". При истиностной семантике мы также будем рассматривать означивания для пропозициональных переменных и в зависимости от него определять для любого высказывания ложно оно ил истинно. И так означиваниями в истинностной семантике будут функции $\gamma\colon \mathcal{P} \to \{0,1\}$. Любое такое означивание может быть естественным образом продолжено до функции $Int_\gamma\colon \mathcal{P} \to \{0,1\}$ на все множество пропозициональных формул, построенных из множества пропозициональных переменных $\mathcal{P}$, которое будем называть интерпретацией в $\mathcal{U}$ для означивания γ.

Для любой пропозициональной переменной Q из нашего множества пропозициональных переменных определяем $Int_\gamma(Q) \rightleftharpoons \gamma(Q)$. Если высказывание φ имеет вид $(\varphi_1 \bigtriangledown \varphi_2$, где $\bigtriangledown$ одна из логических связок $\&$, $\vee$ или $\to$, то полагаем для конъюнкции $Int_\gamma(\varphi_1 \& \varphi_2) \rightleftharpoons \min\{Int_\gamma(\varphi_1), Int_\gamma(\varphi_1)\}$, для дизъюнкции $Int_\gamma(\varphi_1 \vee \varphi_2) \rightleftharpoons \max\{Int_\gamma(\varphi_1), Int_\gamma(\varphi_1)\}$ и для импликации $Int_\gamma(\varphi_1 \to \varphi_2) \rightleftharpoons \max\{(1 - Int_\gamma(\varphi_1)), Int_\gamma(\varphi_1)\}$. Для формулы φ вида $\neg\varphi_1$ полагаем $Int_\gamma(\neg\varphi_1) \rightleftharpoons (1 - Int_\gamma(\varphi_1))$.

Заметим, что $\gamma(\varphi) \in \{0,1\}$.

Определим теперь отношение следования в истинностной семантике:

Из гипотез $\varphi_1, \ldots, \varphi_n$ следует в истинностной семантике φ $(\varphi_1, \ldots, \varphi_n \vdash_I \varphi)$, если для любого истинностного означивания γ в $\{0,1\}$ интерпретация Int_γ удовлетворяет следующему свойству:

если все формулы из $\varphi_1, \ldots, \varphi_n$ при этой интерпретации Int_γ истинны, то и формула φ при этой интерпретации истинна.

Набор свойств $\varphi_1, \ldots, \varphi_n$ совместен в теоретико - множественной семантике, если существует истинностное означивание γ в $\mathcal{U}$ такое, что все формулы из $\varphi_1, \ldots, \varphi_n$ при этой интерпретации истинны. В противном случае этот набор формул называется несовместным и обозначим это условие через $\varphi_1, \ldots, \varphi_n \vdash_I$.

Если в формулу φ входят только пропозициональные переменные из набора $P_1, ..., P_n$, то для того чтобы определить на этой формуле интерпретацию достаточно знать интерпретации только символов из этого набора пропозициональных переменных $P_1, ..., P_n$. В таком случае мы можем обозначить в качестве означивания упорядоченный набор $\varepsilon_1, ..., \varepsilon_n$ значений из $\{0, 1\}$. В таком случае функция f_φ из $\{0, 1\}^n$ в $\{0, 1\}$ такая, что $f_\varphi(\varepsilon_1, ..., \varepsilon_n) \rightleftharpoons Int_{\varepsilon_1,...,\varepsilon_n}(\varphi)$ для любого набора $\varepsilon_1, ..., \varepsilon_n$ из $\{0, 1\}^n$, называется таблицей истинности формулы φ. Обычно функция являющаяся таблицей истинности некоторой формулы записывается в табличном виде. Заметим, что формула называется тождественно истинной, если ее таблица истинности тождественно равна единице, и тождественно ложной, если она тождественно равна нулю. Функции из $\{0, 1\}^n$ в $\{0, 1\}$ называются булевыми функциями. Нетрудно заметить, что любая булева функция может быть представлена в виде таблицы истинности некоторой формулы.

Покажем, что две эти семантики тесно взаимосвязаны.

Пусть задано произвольное множество $\mathcal{U}$ и некоторое истинностное означивание пропозициональных переменных γ. Определим для него теоретико-множественное означивание $\overline{\gamma}$ в универсум $\mathcal{U}$, определив для любой пропозициональной переменной Q из заданного набора

1. $\overline{\gamma}(Q) \rightleftharpoons \mathcal{U}$, если $\gamma(Q) = 1$, и
2. $\overline{\gamma}(Q) \rightleftharpoons \emptyset$, если $\gamma(Q) = 0$.

Теперь мы можем определить две интерпретации высказываний: теоретико-множественную $Int_{\overline{\gamma}}$ и истиностную Int_γ.

Лемма. Для любой формулы φ и любого истинностного означивания γ выполняются следующие эквивалентности:

1. $\overline{\gamma}(\varphi) \rightleftharpoons \mathcal{U}$, **если** $\gamma(\varphi) = 1$, **и**

2. $\overline{\gamma}(\varphi) \rightleftharpoons \emptyset$, **если** $\gamma(\varphi) = 0$.

Доказательство следует из определений индукцией по сложности формулы φ.

Непосредственно из этой леммы и определения следования получаем следующую связь между следованиями в различных семантиках.

Теорема о связи семантик.

1. **Если** $\varphi_1, \ldots, \varphi_n \vdash_{TM} \varphi$, **то** $\varphi_1, \ldots, \varphi_n \vdash_I \varphi$,

2. **Если** $\varphi_1, \ldots, \varphi_n \vdash_{TM}$, **то** $\varphi_1, \ldots, \varphi_n \vdash_I$

Секвенциальное Исчисление Высказываний .

Определим теперь секвенциальное исчисление высказываний. Введем в наш формальный язык еще один новый символ $\vdash$ **— символ секвенции. Этот символ мы добавим к алфавиту высказываний, чтобы построить формальные выражения — секвенции. Для любых последовательности высказываний** Γ **и высказывания** A **выражения вида:**

$\Gamma \vdash A$, $\Gamma \vdash$, $\vdash A$ **назовем секвенциями.**

Чтобы иметь некоторое интуитивное представление о значении этого символа, мы можем сформулировать в качестве цели построения этого исчисления $\Gamma \vdash A$ **— формализацию доказуемости из гипотез** Γ **формулы** A, $\Gamma \vdash$ **— формализацию противоречивости набора высказываний** Γ.

Секвенциальное исчисление высказываний

Чтобы определить исчисление нам нужно определить в нем аксиомы и правила вывода (правила преобразований).

Определим теперь Секвенциальное Исчисление Высказываний (СИВ).

Аксиомы СИВ: $\varphi \vdash \varphi$ **— для любого высказывания (пропозициональной формулы)** φ**.**

Пусть Γ **и** Γ' **— наборы высказываний, а** A, B, C **— высказывания. Определим теперь правила вывода секвенциального исчисления высказываний.**

Правила вывода СИВ:

1. Правила вывода с коньюнкцией—$(\&)$**:**

$\frac{\Gamma\vdash A \;\; \Gamma\vdash B}{\Gamma\vdash(A\&B)}$ $\frac{\Gamma\vdash(A\&B)}{\Gamma\vdash A}$ $\frac{\Gamma\vdash(A\&B)}{\Gamma\vdash B}$

2. Правила вывода с дизъюнкцией — $(\vee)$**:**

$\frac{\Gamma\vdash A}{\Gamma\vdash(A\vee B)}$ $\frac{\Gamma\vdash B}{\Gamma\vdash(A\vee B)}$ $\frac{\Gamma\vdash(A\vee B) \;\; \Gamma,A\vdash C \;\; \Gamma,B\vdash C}{\Gamma\vdash C}$**. (правило разбора случаев).**

3. Правила вывода с импликацией — $(\to)$**:**

$\frac{\Gamma\vdash A \;\; \Gamma\vdash(A\to B)}{\Gamma\vdash B}$ $\frac{\Gamma,A\vdash B}{\Gamma\vdash A\to B}$**.**

4. Правила вывода с отрицанием —$(\neg)$**:**

$\frac{\Gamma\vdash A \;\; \Gamma\vdash\neg A}{\Gamma\vdash}$ $\frac{\Gamma,A\vdash}{\Gamma\vdash\neg A}$ $\frac{\Gamma,\neg A\vdash}{\Gamma\vdash A}$

5. Структурные правила вывода:

$\frac{\Gamma\vdash A}{\Gamma,B\vdash A}$ **(правило утончения).**

$\frac{\Gamma,A,A,\Gamma'\vdash B}{\Gamma,A,\Gamma'\vdash B}$**.**

$\frac{\Gamma,A,B,\Gamma'\vdash C}{\Gamma,B,A,\Gamma'\vdash C}$**.**

Линейный вывод

Будем говорить, что секвенция γ **доказуема (выводима), если существует последовательность секвенций** $\gamma_0, \ldots, \gamma_n$ **такая, что** $\gamma_n = \gamma$ **и для каждого** $i \leq n$ **секвенция** γ_i **аксиома или получается из предыдущих секвенций по одному из правил вывода. Последовательность секвенций** $\gamma_0, \ldots, \gamma_n$ **будем называть в этом случае доказательством (выводом) секвенции** γ**.**

Заметим, что начальный кусок $\gamma_0, \ldots, \gamma_i$ **для** $i \leq n$ **из доказательства** $\gamma_0, \ldots, \gamma_n$ **секвенции** γ_n **будет доказательством секвенции** γ_i**.**

Последовательность секвенций называется квазивыводом, если наряду с аксиомами мы можем использовать в доказательстве доказуе-

мые секвенции. Ясно, что любой квазивывод мы можем дополнить до вывода.

Древовидный вывод

Определим вначале понятие дерева секвенций и его основных элементов.

Дерево секвенций определяется индуктивно по числу переходов в нем.

1.(базис индукции).Любая секвенция γ является деревом с основанием и вершиной γ, а переходов в этом дереве нет.

2.(шаг индукции). Если $\mathcal{D}_0, \mathcal{D}_1, \ldots, \mathcal{D}_n$ — деревья с основаниями $\gamma_0, \gamma_1, \ldots, \gamma_n$, а γ секвенция, то выражение $\frac{\mathcal{D}_0, \mathcal{D}_1, \ldots, \mathcal{D}_n}{\gamma}$ является деревом с основанием γ, вершинами этого дерева являются все вершины деревьев $\mathcal{D}_0, \mathcal{D}_1, \ldots, \mathcal{D}_n$, а переходы состоят из переходов деревьев $\mathcal{D}_0, \mathcal{D}_1, \ldots, \mathcal{D}_n$ и перехода $\frac{\gamma_0, \gamma_1, \ldots, \gamma_n}{\gamma}$.

Дерево секвенций называется деревом вывода или древовидным выводом, если все переходы в нем являются правилами вывода в секвенциальном исчислении высказываний,а вершины дерева являются аксиомами нашего исчисления.

Аналогично линейному выводу мы можем определить для деревьев понятия квазивывода, допустив в качестве вершин доказуемые секвенции. Ясно, что и в этом случае квазивывод легко дополняется до вывода.

Покажем, что линейный вывод и древовидный вывод определяют одни и те же доказуемые секвенции.

Предложение. Секвенция γ доказуема, если и только если существует дерево вывода с основанием γ.

Доказательство. Докажем необходимость ($\Longrightarrow$) индукцией по длине вывода секвенции. Если вывод состоит из одной секвенции, то она является и деревом вывода. Таким образом базис индукции доказан.

Предположим, что для секвенций с доказательствами длины меньшей $n+1$ наше утверждение справедливо. Пусть секвенция γ имеет доказательство $\gamma_0, \gamma_1, ..., \gamma_n$ длины $n+1$. В таком случае секвенция γ либо является аксиомой, но тогда она имеет доказательство длины 1 и по ранее доказанному имеет дерево вывода, либо она получается из предыдущих $\gamma_{s_0}, \gamma_{s_1}, ..., \gamma_{s_k}$ по одному из правил вывода. Но тогда по индукционному предположению эти секвенции уже имеют дерево вывода $D_{s_0}, D_{s_1}, ..., D_{s_k}$. Но тогда дерево $\frac{D_{s_0}, D_{s_1}, ..., D_{s_k}}{\gamma}$ будет деревом вывода для секвенции γ.

Докажем теперь достаточность ($\Longleftarrow$) индукцией по числу переходов в дереве вывода. Если дерево вывода не имеет переходов, то секвенция является вершиной и следовательно аксиомой, но тогда последовательность из одной этой секвенции является ее линейным выводом. Это доказывает базис индукции. Докажем индукционный переход. Предположим, что для секвенций с деревьями вывода счислом переходов меньшим $n+1$ наше утверждение справедливо. Пусть секвенция γ имеет дерево вывода $\frac{D_{s_0}, D_{s_1}, ..., D_{s_k}}{\gamma}$ с числом переходов $n+1$. Рассмотрим основания $\gamma_{s_0}, \gamma_{s_1}, ..., \gamma_{s_k}$ деревьев вывода $D_{s_0}, D_{s_1}, ..., D_{s_k}$. В таком случае по индукционному предположению для секвенций $\gamma_{s_0}, \gamma_{s_1}, ..., \gamma_{s_k}$ существуют последовательности линейных доказательств $L_{s_0}, L_{s_1}, ..., L_{s_k}$, так как деревья $D_{s_0}, D_{s_1}, ..., D_{s_k}$ очевидно имеют уже по крайней мере на один переход меньше чем все дерево вывода. Но тогда последовательность формул $L_{s_0}, L_{s_1}, ..., L_{s_k}, \gamma$, составленная из объединения всех доказательств и добавленной секвенции γ в конце последовательности будет линейным выводом этой секвенции. Предложение об эквивалентности двух способов построения доказательств таким образом закончено.

Докажем теперь, что построенное нами исчисление двузначно. Определим для этого понятие формулы доказуемой в секвенциальном ис-

числении высказываний. Мы будем говорить, что формула A доказуема в секвенциальном исчислении высказываний, если секвенция $\vdash A$ доказуема в нашем исчислении СИВ.

Теорема о двузначности СИВ. Для любой формулы A формула $A \vee \neg A$ доказуема в секвенциальном исчислении высказываний.

Доказательство. Построим для секвенции $\vdash (A \vee \neg A)$ дерево вывода.

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\neg A \vdash \neg A}{\neg A \vdash (A \vee \neg A)}}{\neg (A \vee \neg A), \neg A \vdash}}{\neg (A \vee \neg A) \vdash A} \quad \dfrac{\dfrac{\dfrac{A \vdash A}{A \vdash (A \vee \neg A)}}{\neg (A \vee \neg A), A \vdash}}{\neg (A \vee \neg A) \vdash \neg A}}{\neg (A \vee \neg A) \vdash}}{\vdash (A \vee \neg A)}.$$

Нетрудно проверить, что представленное дерево является деревом вывода и теорема доказана.

L 6

Лекция 6. Основные эквивалентности формул в Секвенциальном Исчислении Высказываний .

Мы назовем формулы A и B эквивалентными $(A \equiv B)$, если секвенциии $A \vdash B$ и $B \vdash A$ доказуемы в секвенциальном исчислении высказываний.

Определим теперь бинарное отношение "A и B эквивалентные формулы"на множестве формул. Мы назовем формулы A и B эквивалентными (будем писать в этом случае $(A \equiv B)$), если секвенциии $A \vdash B$ и $B \vdash A$ доказуемы в секвенциальном исчислении высказываний. Заметим прежде всего, что это отношение действительно эквивалентность, то есть для него выполнены свойства рефлексивности, симметричности и транзитивности.

Лемма 1 об эквивалентности. Для отношения $A \equiv B$ выполнены следующие три свойства для любых высказываний A, B, C:

1. $A \equiv A$;

2. если $A \equiv B$, **то** $B \equiv A$;

3. если $A \equiv B$ **и** $B \equiv C$, **то** $A \equiv C$.

Доказательство непосредственно следует из определения.

Докажем теперь, что эквивалентность согласована и с логическими операциями.

Лемма 2 о конгруентности. Для любых высказываний A, A', B, B', если $A \equiv A'$ и $B \equiv B'$, то справедливы следующие свойства:

1. $A\&B \equiv A'\&B'$,

2. $A \vee B \equiv A' \vee B'$,

3. $\neg A \equiv \neg A'$; $\neg B \equiv \neg B'$,

4. $A \to B \equiv A' \to B'$.

Доказательство. Так как условия симметричны, то достаточно доказать для каждой эквивалнтности только одну из требуемых секвенций.

Докажем для конъюнкции.

$$\dfrac{\dfrac{\dfrac{(A\&B)\vdash(A\&B)}{(A\&B)\vdash B}\ \dfrac{B\vdash B'}{\vdash(B\to B')}}{(A\&B)\vdash A'}\ \dfrac{\dfrac{(A\&B)\vdash(A\&B)}{(A\&B)\vdash B}\vdash(B\to B')}{(A\&B)\vdash B'}}{(A\&B)\vdash(A'\&B')}$$

Докажем лемму для дизъюнкции, то есть $A \vee B \vdash A' \vee B'$.

$$\dfrac{(A\vee B)\vdash(A\vee B)\ \dfrac{A\vdash A'}{A\vdash(A'\vee B')}\ \dfrac{B\vdash B'}{B\vdash(A'\vee B')}}{(A\vee B)\vdash(A'\vee B')}$$

3. Докажем эквивалентность для импликации, то есть $(A \to B) \vdash (A' \to B')$.

$$\dfrac{\dfrac{A'\vdash A\ (A\to B)\vdash(A\to B)}{(A\to B),A'\vdash B},\ \dfrac{B\vdash B'}{\vdash(B\to B')}}{\dfrac{(A\to B),A'\vdash B'}{(A\to B)\vdash(A'\to B')}}$$

4. Докажем последнее утверждение для отрицания, то есть $\neg A \vdash \neg A'$.

$$\dfrac{\dfrac{\neg A\vdash\neg A\ A'\vdash A}{\neg A,A'\vdash}}{\neg A\vdash\neg A'}$$

Лемма доказана.

Из этой леммы о конгруентности следует непосредственно индукцией по сложности формулы B **следующая теорема.**

Теорема о замене. Если формула A **является подформулой формулы** B**, а формулы** A **и** A' **эквивалентны, то подставив в** B **вместо подформулы** A **формулу** A' **в результате этой замены мы получим формулу** $B^A_{A'}$ **эквивалентную формуле** B.

Докажем теперь основные свойства эквивалентности, которые будут использоваться при нахождении специальных нормальных форм высказываний аналогичных преобразованиям многочленов в алгебре.

Теорема об основных эквивалентностях. Следующие эквивалентности справедливы для всех высказываний A, B, C**:**

1. $A\&A \equiv A$ **и** $A \vee A \equiv A$ **(идемпотентность),**

2. $(A\&B) \equiv (B\&A)$ **и** $(A \vee B) \equiv (B \vee A)$ **(симметричность),**

3. $((A\&B)\&C) \equiv (A\&(B\&C))$ **и** $((A \vee B) \vee C) \equiv (A \vee (B \vee C)$ **(ассоциативность),**

4. $(A\&(B \vee C)) \equiv ((A\&B) \vee (B\&C))$ **и** $(A \vee (B\&C)) \equiv ((A \vee B)\&(A \vee C)$ **(дистрибутивность),**

5. $(A \to B) \equiv (\neg A \vee B)$**,**

6. $\neg\neg A \equiv A$ **(двойное отрицание),**

7. $\neg(A \vee B) \equiv (\neg A\&\neg B)$**, и** $\neg(A\&B) \equiv (\neg A \vee \neg B)$ **(двойственность).**

Доказательство остается читателям в качестве упражнения.

Докажем 4–ю эквивалентность. Для этого построим вначале дерево вывода для первой секвенции из определения эквивалентности.

$$\dfrac{\dfrac{(A\&(B\vee C))\vdash(A\&(B\vee C))}{(A\&(B\vee C))\vdash(B\vee C)},\ \dfrac{\dfrac{\dfrac{(A\&(B\vee C))\vdash(A\&(B\vee C))}{(A\&(B\vee C))\vdash A}\,B\vdash B}{(A\&(B\vee C)),B\vdash(A\&B)}}{(A\&(B\vee C)),B\vdash((A\&B)\vee(A\&C))}\ \dfrac{\dfrac{\dfrac{(A\&(B\vee C))\vdash(A\&(B\vee C))}{(A\&(B\vee C))\vdash A}\,C\vdash C}{(A\&(B\vee C)),C\vdash(A\&C)}}{(A\&(B\vee C)),C\vdash((A\&B)\vee(A\&C))}}{(A\&(B\vee C)),\vdash((A\&B)\vee(A\&C))}.$$

Построим дерево вывода для второй секвенции из определения эквивалентности формул.

$$\dfrac{((A\&B)\vee(A\&C))\vdash((A\&B)\vee(A\&C))\ \dfrac{(A\&B)\vdash(A\&B)}{(A\&B)\vdash A}}{((A\&B)\vee(A\&C))\vdash(A\&(B\vee C))}\ \dfrac{\dfrac{\dfrac{(A\&C)\vdash(A\&C)}{(A\&C)\vdash C}}{(A\&C)\vdash(B\vee C)}}{(A\&C)\vdash(A\&(B\vee C))}$$

На этом доказательство теоремы завершено.

L 7

Гильбертовское Исчисление Высказывания.

Определим еще одно исчисление, в котором основными объектами являются пропозициональные формулы (высказывания) и преобразования определены непосредственно на формулах. Таким образом определенные правила преобразования в большей мере отвечают нашему привычному интуитивному понятию доказательства. Однако, как мы покажем позднее, эти два исчисления эквивалентны. Тем не менее для построения конкретных доказательств оказывается более легко оперировать с доказательствами в секвенциальной форме, а для применения свойств доказуемых формул и различных их свойств оказывается более удобным использовать исчисление на высказываниях, которое традиционно называется Гильбертовским Исчислением Высказываний (ГИВ).

Как и раньше для задания формального исчисления нам нужно определить четыре типа конструкций для исчисления:

1. Высказывания (формулы)в заданном алфавите Гильбертовского исчисления высказываний.

2. Аксиомы Гильбертовского исчисления высказываний.

3. Правила вывода Гильбертовского исчисления высказываний.

4. Понятие доказательства Гильбертовского исчисления высказываний.

Как уже было замечено формулами Гильбертвского исчисления будут ранее определенны высказывания в том же самом алфавите без значка секвенции.

Правило вывода только одно:

$\frac{A,\ \ A \to B}{B}$,

где A и B пропозициональные формулы (высказывания).

Это правило называется правилом отделения (rule of modus ponens).

Аксиомами гильбертовского исчисления высказываний являются все формулы, имеющие оддну из следующих форм:

1. $A \to (B \to A)$
2. $(A \to B) \to ((A \to (B \to C)) \to (A \to C))$
3. $(A\&B) \to A$
4. $(A\&B) \to B$
5. $(C \to A) \to ((C \to B) \to (C \to (A\&B)))$
6. $A \to (A \vee B)$.
7. $B \to (A \vee B)$.
8. $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$
9. $(A \to B) \to ((A \to \neg B) \to \neg A)$.
10. $\neg\neg A \to A$.

Заметим, что часто эти формы называют схемами аксиом, так как каждая форма задает целый класс формул, являющихся аксиомами.

Формула A доказуема из множества формул Γ ($\Gamma \vdash A$), если существует последовательность формул $B_0, B_1, \ldots, B_n$ с $B_n = A$ такая, что

для любого $i \leq n$ формула B_i является аксиомой, или $B_i \in \Gamma$, или существуют формулы B_p, B_q с индексами $p < i, q < i$ такие, что формула B_i получается из формул B_p и B_q по правилу отделения. В этом случае последовательность формул $B_0, B_1, \ldots, B_n$ называется доказательством из множества формул Γ формулы A или просто доказательством. Часто в этом случае говорят, что формула A доказуема из множества гипотез Γ.

Формула называется доказуемой в гильбертовском исчислении высказываний, если она доказуема из пустого множества формул.

Множество формул Γ называется противоречивым ($\Gamma \Vdash$), если существует формула A такая, что она A и ее отрицание $\neg A$ доказуемы из множества формул Γ.

Лемма 1. Формула $A \to A$ доказуема в гильбертовском исчислении высказываний.

Доказательство. Построим требуемую последовательность формул.

1. $A \to (A \to A)$ — **первая аксиома при** $B \rightleftharpoons A$.
2. $(A \to (A \to A)) \to ((A \to ((A \to A) \to A)) \to (A \to A))$ — **вторая аксиома при** $B \rightleftharpoons (A \to A)$, $C \rightleftharpoons A$.
3. $(A \to ((A \to A) \to A)) \to (A \to A)$ — **формула получается по правилу отделения из первой и второй формул.**
4. $A \to ((A \to A) \to A)$ — **первая аксиома при** $B \rightleftharpoons (A \to A)$.
5. $A \to A$ — **получается из третьей и четвертой формул по правилу отделения.**

Лемма доказана.

Как уже раньше было замечено, строить доказательства в гильбертовском исчислении довольно трудоемкая задача. Следующая важная

теорема позволяет для обоснования доказуемости использовать метаконструкции, которые значительно облегчают эту деятельность.

Теорема о дедукции. Если $\Gamma, A \Vdash B$, **то** $\Gamma \Vdash A \to B$.

Доказательство. Воспользуемся индукцией по длине кратчайшего доказательства формулы B **из последовательности формул** Γ, A.

Пусть $\Gamma, A \Vdash B$ **и рассмотрим кратчайшее доказательство** $\Psi_0, \ldots, \Psi_n$ **формулы** B **из** Γ, A. **Докажем справедливость базиса индукции. При** $n = 0$ **доказательство состоит из одной формулы** B **и в этом случае по определению доказательства из формул** Γ, A **выполняется одна из следующих возможностей для этой формулы:** $B \in \Gamma$ **или** $B = A$ **или** B **— аксиома.**

Если $B \in \Gamma$ **или** B **— аксиома, то следующая последовательность формул**

1. B

2. $B \to (A \to B)$ **(аксиома 1).**

3. $A \to B$.

будет доказательством из множества формул Γ **формулы** $A \to B$ **и базис индукции выполнен в этом случае, т. е.** $\Gamma \Vdash A \to B$.

Если $B = A$**,то нужно доказать формулу** $A \to A$, **но по лемме формула** $A \to A$ **доказуема и, следовательно, получаем, что** $\Rightarrow \Gamma \Vdash A \to A$. **Докажем теперь индуктивный переход.**

Пусть для доказательств длины меньшей n **теорема верна. Докажем для длины** $n+1$. **Пусть** $\Psi_0, \ldots, \Psi_{n+1}$ **доказательство формулы формулы** B **из** Γ, A. **По определению** $\Psi_{n+1} = B$.

Для последней формулы Ψ_{n+1} **имеется по определению следующие возможности:**

1) $\Psi_{n+1} \in \Gamma$,

2) Ψ_{n+1} — **аксиома,**

3) $\Psi_{n+1} = A$,

4) Ψ_{n+1} **получается из** $\Psi_i \quad \Psi_j = (\Psi_i \to \Psi_{n+1})$ **для** $(i, j < n+1)$.

Так как мы взяли кратчайшее доказательство и оно имеет длину большую 1, **то первые три случае не возможны. Таким образом выполняется четвертый случай. Но последовательность формул** $\Psi_0, \ldots, \Psi_m$ **любого** $m \leq n+1$ **также является доказательством из множества формул** Γ, A. **При этом длина доказательств уже меньше** $n+1$. **Отсюда по индукционному предположению получаем, что** $\Gamma \Vdash A \to \Psi_i$, $\Gamma \Vdash A \to \Psi_j$.

Рассмотрим последовательность формул $\rho_1, \rho_2, ..., \rho_m$ **являющуюся доказательством формулы** $(A \to \Psi_i)$ **из** Γ **и** $\sigma_1, \sigma_2, ..., \sigma_k$ **являющуюся доказательством формулы** $(A \to \Psi_j)$ **из** Γ.

Построим теперь доказательство формулы $(A \to B)$**из** Γ, **взяв следующую последовательность формул:**

$\rho_1, \rho_2, ..., \rho_m, (A \to \Psi_i) \to ((A \to (\Psi_i \to \Psi_{n+1})) \to (A \to \Psi_{n+1}))$**(аксиома 2)**, $(A \to (\Psi_i \to \Psi_{n+1})) \to (A \to \Psi_{n+1})), \sigma_1, \sigma_2, ..., \sigma_k$, $A \to \Psi_{n+1}$.

Заметим, что

$\rho_m = (A \to \Psi_i)$ **и** $\sigma_k = (A \to \Psi_j)$, **а** $\Psi_j = (\Psi_i \to \Psi_{n+1})$ **и** $B = \Psi_{n+1}$. **Отсюда следует, что построенная последовательность формул является доказательством из** Γ **формулы** $(A \to B)$. **Теорема доказана.**

Докажем теперь утверждение о связи двух исчислений.

Теорема о связи исчислений.

1. **Если секвенция** $\varphi_1, \ldots, \varphi_n \vdash \varphi$ **доказуема, то в гильбертовском исчислении высказываний мы имеем выводимость** $\varphi_1, \ldots, \varphi_n \Vdash \varphi$,
2. **Если секвенция** $\varphi_1, \ldots, \varphi_n \vdash$ **доказуема, то в гильбертовском исчислении высказываний мы имеем выводимость** $\varphi_1, \ldots, \varphi_n \Vdash$.

Доказательство проведем индукцией по длине доказательства в секвенциальном исчислении высказываний. Пусть

$$\gamma_0, \ldots, \gamma_n = \gamma$$

доказательство длины $n+1$.

Если $n = 0$, **то** γ_n **аксиома и** $\gamma_n = A \vdash A$, **но тогда очевидно, что** $A \Vdash A$. **Таким образом базис индукции доказан.**

Докажем шаг индукции. Пусть для доказательств длины меньшей $n+1$ **наша теорема уже доказана. Покажем ее справедливость и для доказательств длины** $n+2$. **Пусть**

$$\gamma_0, \ldots, \gamma_{n+1} = \gamma$$

доказательство секвенции γ. **В таком случае секвенция** γ_{n+1} **либо аксиома, либо получается из предыдущих секвенций по одному из правил вывода.Если** γ_{n+1} **аксиома, то** $\gamma_n = A \vdash A$, **но тогда как и раньше очевидно, что** $A \Vdash A$. **Остается рассмотреть теперь все возможности для правил вывода. Однако любой кусок доказательства есть доказательство, а поэтому все секвенции** γ_i **для** $i \leq n$ **имеют доказательства длины меньшей** $n+2$ **и к ним применимо предположение индукции. Рассмотрим здесь доказательство только для двух правил, оставляя разбор остальных в качестве упражнения.**

Рассмотрим правило с конъюнкцией. Пусть наша секвенция γ_{n+1} **получается по правилу**

$$\frac{\Gamma \vdash A \;\; \Gamma \vdash B}{\Gamma \vdash A\&B}$$

,

где $\gamma_{n+1} = \Gamma \vdash (A\&B)$, $\gamma_i = \Gamma \vdash A \gamma_j = \Gamma \vdash B$, **а** $i, j \leq n$.

Отсюда по индукционному предположению получаем, что $\Gamma \Vdash A$ **и** $\Gamma \Vdash B$.

Построим теперь квазивывод формулы $(A\&B)$.

1. $(C \to A) \to ((C \to B) \to (C \to (A\&B))$ — **пятая аксиома ГИВ, где** C **любая аксиома ГИВ.**

2. C — **аксиома ГИВ .**

3. $A \to (C \to A)$ — **первая аксиома ГИВ.**

4. A — **по индукционному предположению доказуема из** Γ.

5. $C \to A$ — **получается из третьей и четвертой формулы по правилу отделения.**

6. $((C \to B) \to (C \to (A\&B))$ — **получается из первой и пятой формулы по правилу отделения.**

7. $B \to (C \to B)$ — **первая аксиома ГИВ.**

8. B — **по индукционному предположению доказуема из** Γ.

9. $C \to B$ — **получается из седьмой и восьмой формулы по правилу отделения.**

10. $(C \to (A\&B))$ — **получается из девятой и шестой формулы по правилу отделения.**

11. $(A\&B)$ — **получается из второй и десятой формулы по правилу отделения.**

Разберем еще случай трех-посылочного правила разбора случаев. Пусть наша секвенция γ_{n+1}**получается по правилу**

$$\frac{\Gamma \vdash (A \vee B)\ \ \Gamma, A \vdash C\ \ \Gamma, B \vdash C}{\Gamma \vdash C}$$

,

где $\gamma_{n+1} = \Gamma \vdash C$, $\gamma_i = \Gamma \vdash (A \vee B)$, $\gamma_k = \Gamma, A \vdash C$ **и** $\gamma_j = \Gamma, B \vdash C$, **а** $i, j, k \leq n$.

Отсюда по индукционному предположению получаем, что $\Gamma \Vdash (A \vee B)$, $\Gamma, A \Vdash C$ **и** $\Gamma, B \Vdash C$. **По теореме о дедукции мы можем заключить теперь, что** $\Gamma \Vdash (A \to C)$ **и** $\Gamma \Vdash (B \to C)$.

Построим теперь квазивывод формулы C.

1. $(A \vee B)$— **по индукционному предположению доказуема из** Γ.
2. $(A \to C)$—**по индукционному предположению и теореме о дедукции доказуема из** Γ.
3. $(B \to C)$—**по индукционному предположению и теореме о дедукции доказуема из** Γ.
4. $.(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$—**восьмая аксиома ГИВ.**
5. $((B \to C) \to ((A \vee B) \to C))$ — **получается из второй и четвертой формулы по правилу отделения.**
6. $((A \vee B) \to C)$ — **получается из третьей и пятой формулы по правилу отделения.**
7. C — **получается из первой и шестой формулы по правилу отделения.**

Разбор для остальных правил вывода проводится аналогично и ключевая роль принадлежит теореме о дедукции. Теорема доказана.

Установим теперь связь наших исчислений с теоретико-множественной семантикой. Прежде всего мы покажем, что любая формула доказуемая в гильбертовском исчислении высказываний будет тождественно истинной формулой.

Лемма 2. Любая аксиома гильбертовского исчисления высказываний тождественно истинна в теоретико-множественной семантике, то есть для любой аксиомы φ **выполняется** $\models_{TM} \varphi$.

Доказательство. Рассмотрим произвольное множество U **произвольное означивание** γ**. Определим для этого означивания интерпретацию** Int_γ **и покажем, что для любой аксиомы** φ **гильбертовского исчисления высказываний** $Int_\gamma(\varphi) = U$**, то есть для любого элемента из** U **выполнено свойство** φ**. Для доказательства этой леммы нам нужно рассмотреть аксиомы всех десяти форм и убедиться, что для них указанное свойство выполняется. Мы будем доказывать это от противного, предполагая, что для некоторого элемента** s **не выполнено свойство** φ**. Для доказательства мы рассмотрим только восьмую и девятую аксиомы:** $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$ **и** $(A \to B) \to ((A \to \neg B) \to \neg A)$.

И так пусть вначале $\varphi = ((A \to C) \to ((B \to C) \to ((A \vee B) \to C)))$ **и** $s \notin Int_\gamma(\varphi)$**. Тогда по определению интерпретации** $s \in Int_\gamma(A \to C)$ **и** $s \notin Int_\gamma((B \to C) \to ((A \vee B) \to C))$**. Вновь воспользуемся определением интерпретаций для второй формулы и получим:** $s \in Int_\gamma(B \to C)$ **и** $s \notin Int_\gamma((A \vee B) \to C)$**. А теперь получаем, что** $s \in Int_\gamma(A \vee B)$ **и** $s \notin Int_\gamma C$**. Из условий** $s \notin Int_\gamma C$ **и** $s \in Int_\gamma(A \to C)$ **заключаем, что** $s \notin Int_\gamma A$**. Аналогично из** $s \notin Int_\gamma C$ **и** $s \in Int_\gamma(B \to C)$ **получаем** $s \notin Int_\gamma B$**. Но в таком случае** $s \notin Int_\gamma(A \vee B)$**. Но мы уже заметили, что** $s \in Int_\gamma(A \vee B)$**. Полученное противоречие показывает, что наше предположение неверно и для восьмой аксиомы требуемое условие выполнено всегда.**

Докажем теперь требуемое условие в случае девятой аксиомы, то есть в случае $\varphi = (A \to B) \to ((A \to \neg B) \to \neg A)$**. Предполагаем как и в предыдущем случае, что** $s \notin Int_\gamma(\varphi)$**. Тогда по определению интерпретации** $s \in Int_\gamma(A \to B)$ **и** $s \notin Int_\gamma((A \to \neg B) \to \neg A)$**. Вновь воспользуемся определением интерпретаций для второй формулы и получим:** $s \in Int_\gamma(A \to \neg B)$ **и** $s \notin Int_\gamma \neg A$**. А теперь получаем, что** $s \in Int_\gamma A$**. Из условий** $s \in Int_\gamma(A \to B)$ **и** $s \in Int_\gamma A$ **заключаем, что** $s \notin Int_\gamma B$**. Аналогично из** $s \in Int_\gamma A$ **и** $s \in Int_\gamma(A \to \neg B)$ **получаем** $s \in Int_\gamma \neg B$**. Но в таком случае** $s \notin Int_\gamma B$**. Но мы уже заметили, что** $s \in Int_\gamma B$**. Получен-**

ное противоречие показывает, что наше предположение неверно и для девятой аксиомы требуемое условие выполнено всегда. Мы оставляем разбор остальных случаев читателям в качестве упражнения. Лемма доказана.

Лемма 3. Если формулы A и $(A \to B)$ тождественно истинны в теоретико-множественной семантике, то и формула B тождественно истинна для теоретико-множественной семантики.

Доказательство следует непосредственно из определения теоретико-множественной интерпретации для импликации.

Из этих двух лемм индукцией по длине доказательств мы получаем следующее важное соотношение доказуемости и теоретико-множественной семантики.

Теорема о корректности доказуемости. Любая формула доказуемая в гильбертовском исчислении высказываний тождественно истинна в теоретико-множественной семантике.

Следствие 1. Если в гильбертовском исчислении высказываний из гипотез $\varphi_1, \varphi_2, ..., \varphi_n$ выводима формула φ, то есть $(\varphi_1, \varphi_2, ..., \varphi_n \Vdash \varphi)$, то $\varphi_1, \varphi_2, ..., \varphi_n \models_{TM} \varphi$.

Доказательство получаем n–кратным применением теоремы о дедукции и затем теоремы о корректности доказательств.

Следствие 2. Если в гильбертовском исчислении высказываний гипотезы $\varphi_1, \varphi_2, ..., \varphi_n$ противоречивы, то есть $(\varphi_1, \varphi_2, ..., \varphi_n \Vdash)$, то $\varphi_1, \varphi_2, ..., \varphi_n \models_{TM}$.

Следствие 3. Выполнены следующие следствия:

1. **Если секвенция $\Gamma \vdash A$ доказуема, то $\Gamma \Vdash A$,**
2. **Если $\Gamma \Vdash A$, то $\Gamma \models_{TM} A$,**
3. **Если $\Gamma \models_{TM} A$, то $\Gamma \models_I A$.**

Следствие 4. Выполнены следующие следствия:

1. **Если секвенция** $\Gamma \vdash$ **доказуема, то** $\Gamma \Vdash$,
2. **Если** $\Gamma \Vdash$, **то** $\Gamma \models_{TM}$,
3. **Если** $\Gamma \models_{TM}$, **то**$\Gamma \models_{I}$

L 8

Нормальные формы.

В этой лекции мы найдем для любой формулы эквивалентные ей формулы в форме, которая более явно позволяет распознавать доказуемость формул, а на основе этой характеризации доказать теорему Геделя о полноте исчисления высказываний.

Определим вначале понятия элементарной дизъюнкции и элементарной конъюнкции, которые определяются индуктивно.

Определение. Элементарная дизъюнкция определяется индуктивно:

Базис индукции. Любая пропозициональная переменная или ее отрицание являются элементарными дизъюнкциями.

Шаг индукции. Если высказывания A, B являются элементарными дизъюнкциями, то и формула $(A \vee B)$ является элементарной дизъюнкцией.

Определение. Элементарная конъюнкция определяется индуктивно:

Базис индукции. Любая пропозициональная переменная или ее отрицание являются элементарными конъюнкциями.

Шаг индукции. Если высказывания A, B являются элементарными конъюнкциями, то и формула $(A \& B)$ является элементарной конъюнкцией.

Заметим, что из теоремы об основных эквивалентностей об ассоциативности конъюнкции и дизъюнкции следует, индукцией по числу

соответственно дизъюнкций или конъюнкций, что элементарные дизъюнкции (и соответственно конънкции) отличающиеся только расстановкой скобок в формулах будут эквивалентны. Нетрудно заметить, что и порядок пропозициональных переменных и отрицаний пропозициональных переменных в силу эквивалентности для коммутативности конъюнкции и дизъюнкции не нарушает эквивалентности.

Конъюнктивная нормальная форма (к.н.ф) для высказываний определятся также индуктивно.

Базис индукции. Любая элементарная дизъюнкция является к.н.ф. и она является единственной элементарной дизъюнкцией этой к.н.ф.

Шаг индукции. Если K_1, K_2 — к.н.ф., то и формула $K_1 \& K_2$ находится в к.н.ф.,а их элементарные дизъюнкции являются в точности элементарными дизъюнкциями нашей к.н.ф.

Дизъюнктивная нормальная форма (д.н.ф) для высказываний определятся также индуктивно.

Базис индукции. Любая элементарная конъюнкция является д.н.ф. и она является единственной элементарной конъюнкцией этой д.н.ф.

Шаг индукции. Если D_1, D_2 — д.н.ф., то и формула $D_1 \vee D_2$ находится в д.н.ф.,а их элементарные конъюнкции являются в точности элементарными конъюнкциями нашей д.н.ф.

Покажем, что любая формула эквивалентна в Секвенциальном исчислении высказываний формулам в к.н.ф. и д.н.ф.. Для этого мы последовательно будем определять эквивалентные преобразования формул.

Сначала избавимся в нашей формуле от импликаций. Для этого докажем следующее утверждение.

Теорема (об устранении импликации). Для любого высказывания существует эквивалентное ему высказывание не содержащее символа импликации $\to$.

Докажем эту теорему индукцией по числу логических связок в формуле.

Базис индукции. Если A — пропозициональная переменная, то $A \equiv A$ и A не содержит импликаций $\to$.

Шаг индукции. Пусть для формул с числом логических связок меньшем n наше утверждение верно. Рассмотрим формулу A с n логическими связками. Если A не пропозициональная переменная тогда по опрередлению формула A имеет вид $(B\&C)$, $(B \vee C)$, $\neg B$ или $(B \to C)$ для высказываний B, C, для которых выполнено индукционное предположение, то есть существуют формулы B', C' не содержащие импликаций $\to$ и такие, что $B \equiv B'$ и $C \equiv C'$. Отсюда, если A имеет вид $(B\&C)$, то A эквивалентно формуле $(B'\&C')$, если A имеет вид $(B \vee C)$, то A эквивалентно формуле $(B' \vee C')$, если A имеет вид $\neg B$, то A эквивалентно формуле $\neg B'$, если A имеет вид $(B \to C)$, то A эквивалентно формуле $(\neg B' \vee C')$. Теорема доказана.

Теорема (об устранении импликации и отрицания). Для любой формулы A существует формула B без импликаций $\to$, о отрицания $\neg$ могут стоять только перед пропозициональными переменными, которая эквивалентна формуле A.

В силу теоремы об элиминации импликации достаточно доказать, что для для любой формулы A без импликаций существует формула D эквивалентная A без импликаций и с отрицаниями только перед пропозициональными переменными.

Доказательство проведем индукцией по числу логических связок в формуле без импликаций A.

1. Базис индукции. Если A — пропозициональная переменная, то $A \equiv A$ и A — искомая формула.

2. Шаг индукции. Пусть для формул с числом логических связок меньшем n наше утверждение верно. Рассмотрим формулу A с n логическими связками. Если A не пропозициональная переменная тогда по определению формула A имеет вид $(B\&C)$, $(B \vee C)$, $\neg B$ для высказываний B, C, для которых выполнено индукционное предположение, то есть существуют формулы B', C' не содержащие импликаций $\rightarrow$ и такие, что $B \equiv B'$ и $C \equiv C'$. Отсюда, если A имеет вид $(B\&C)$, то A эквивалентно формуле $(B'\&C')$, если A имеет вид $(B \vee C)$, то A эквивалентно формуле $(B' \vee C')$. Остается рассмотреть последний случай, когда если A имеет вид $\neg B$. В этом случае формула B имеет вид $(B_1\&B_2)$, $(B_1 \vee B_2)$, $\neg B_1$ или Q, где Q — пропозициональная переменная, а B_1 и B_2 — формулы, у которых по крайней мере на две логических связки меньше, чем в формуле A. Если формула B имеет вид Q, где Q — пропозициональная переменная, то сама формула A имеет искомый вид $\neg Q$. Если формула B имеет вид $(B_1\&B_2)$, $(B_1 \vee B_2)$, $\neg B_1$, тогда формулы B_1 и B_2 содержат по крайней мере на две логических связки меньше, чем формула A. В этом случае наша формула A в силу теоремы об основных эквивалентностях эквивалентна формуле $(\neg B_1 \vee \neg B_2)$, $(\neg B_1 \& \neg B_2)$, B_1. Заметим, что формулы $\neg B_1$, $\neg B_2$, B_1 имеют меньше логических связок, чем наша формула A, но тогда по индукционному предположению существуют формулы C_1, C_2 и C эквивалентные соответственно формулам $\neg B_1$, $\neg B_2$ и B_1, которые без импликаций и с отрицаниями только перед пропозициональными переменными. Но в таком случае наша формула A эквивалентна соответственно формуле $(C_1 \vee C_2)$, $(C_1\&C_2)$ или C, которые без импликаций и с отрицаниями только перед пропозициональными переменными. Теорема доказана.

Теорема (о д.н.ф. и к.н.ф.) Для любой формулы A существуют формулы K в к.н.ф. и D в д.н.ф. такие, что

$$A \equiv K \text{ и } A \equiv D.$$

Доказательство. Достаточно доказать теорему для формул без импликаций и с отрицаниями только перед пропозициональными переменными.

Докажем это индукцией по числу логических связок в формуле A.

1. **Базис индукции. Если A — пропозиционная переменная, то в силу эквивалентности $A \equiv A$ определим $K \leftrightharpoons A$ и $D \leftrightharpoons A$ и искомые формулы получены.**

2. **Шаг индукции. Пусть для формул с числом логических связок меньшем n наше утверждение верно. Рассмотрим формулу A с n логическими связками. В этом случае она имеет вид: $A = B \vee C$, или $A = B\&C$ или $A = \neg Q$, где Q — пропозициональная переменная, а B и C подформулы меньшей сложности.**

В случае $A = \neg Q$, где Q — пропозициональная переменная, мы определим $K \leftrightharpoons \neg Q$ и $D \leftrightharpoons \neg Q$.

Построим K для A в случае $A = (B\&C)$. По индуктивному предположению для B и C существуют к.н.ф. K_B и K_C соответственно. В таком случае $(B\&C) \equiv (K_B\&K_C)$. По определению в этом случае формула $(K_B\&K_C)$ уже находится в конъюктивной нормальной форме. Построим теперь для $A = (B\&C)$ дизъюнктивную нормальную форму D. По индуктивному предположению для B и C существуют д.н.ф. D_B и D_C соответственно. Индукцией по числу конъюнкции в формулах A, B мы можем доказать следующую лемму, которая доказывает существование эквивалентной д.н.ф. в данном случае.

Лемма. Если A, B —д.н.ф., то $(A\&B)$ также эквивалентна дизъюнктивной нормальной форме.

Доказательство индукцией по числу конъюнкций $(\vee)$ в A и B.

Базис: Если дизъюнкций нет, тогда A, B — элементарные конъюнкции и формула $(A\&B)$ является элементарной конъюнкции и следовательно является конъюнктивной нормальной формой.

Пусть мы имеем $n+1$ дизъюнкцию в формулах A и B, тогда A или B не элементарная конъюнкция. По коммутативности можем считать, что хотя бы одна дизъюнкция есть в A. В таком случае $A = (D_1 \vee D_2)$, где D_1, D_2 — д.н.ф. Из основных эквивалентностей по правилу дистрибутивности мы получаем, что

$(A\&B) = ((D_1 \vee D_2)\&B) \equiv ((K_1\&B) \vee (K_2\&B))$. По индукционному предположению существуют дизъюнктивные нормальные формы D_1' и D_2' такие, что $D_1' \equiv (D_1\&B)$, $D_2' \equiv (D_2\&B)$. Отсюда $(A\&B) \equiv (D_1' \vee D_2')$ и лемма доказана.

Построим искомые д.н.ф. D и к.н.ф. K для A в случае $A = (B \vee C)$. Аналогично предыдущему случаю для B и C для этих по индукционному предположению существуют эквивалентные дизъюнктивные нормальные формы D_B и D_C.В таком случае $(B\&C) \equiv (D_B \vee D_C)$. По определению в этом случае формула $(D_B \vee D_C)$ уже находится в дизъюнктивной нормальной форме. Построим теперь для $A = (B \vee C)$ конъюнктивную нормальную форму D. По индуктивному предположению для B и C существуют к.н.ф. K_B и K_C соответственно. Индукцией по числу дизъюнкции в формулах A, B мы можем доказать следующую лемму, которая доказывает существование эквивалентной к.н.ф. в данном случае.

Лемма. Если A, B — к.н.ф., то формула $(A \vee B)$ эквивалентна конъюнктивной нормальной форме .

Доказательство (1) индукцией по сумме числа конъюнкций $(\&)$ в A и B.

Базис: Если конъюнкций нет, тогда A, B — элементарные дизъюнкции и формула $(A \vee B)$ является элементарной конъюнкции и следовательно является дизъюнктивной нормальной формой.

Пусть мы имеем $n+1$ конъюнкцию в формулах A и B, тогда A или B не элементарная дизъюнкция. По коммутативности можем считать, что хотя бы одна конъюнкция есть в A. В таком случае $A = (K_1 \& K_2)$, где K_1, K_2 — к.н.ф. Из основных эквивалентностей по правилу дистрибутивности мы получаем, что

$(A \vee B) = ((K_1 \& K_2) \vee B) \equiv ((K_1 \vee B) \& (K_2 \vee B))$. **По индукционному предположению существуют конъюнктивные нормальные формы K_1' и K_2' такие, что $K_1' \equiv (K_1 \vee B)$, $K_2' \equiv (K_2 \vee B)$. Отсюда $(A \vee B) \equiv (K_1' \& K_2')$ и лемма доказана.**