Математическая логика, 2022

V. G.

Рис. 1: Критерий мудрости

Содержание

Введение. Предмет математической логики

Математическая логика (*символическая логика*) — раздел фундаментальной математики, в котором математическими методами исследуются законы человеческого мышления.
Современная математическая логика занимается проблемами математических доказательств и оснований математики.

Разделы математической логики:

1. Логика высказываний;
2. Логика предикатов;
3. Теория доказательств;
4. Теория моделей;
5. Теория вычислимости.

I. Логика высказываний

§1. Алгебра высказываний

1.1. Высказывания

Высказывание — утверждение, о котором можно определённо сказать, истинно оно или ложно.

Высказывание может принимать только два истинностных значения: истина или ложь.

Высказывания делятся на *простые* (*элементарные*) и сложные (*составные*). Простые высказывания представляют собой одно утверждение, сложные составлены из простых с помощью *операций над высказываниями*.

Назначение логики высказываний — определение истинностных значений сложных высказываний только на основе их структуры, т.е. безотносительно смысла высказывания.

1.2. Пропозициональные связки

Сложные высказывания строятся как истинностно-функциональные комбинации простых высказываний.

Простые высказывания будем обозначать строчными латинскими буквами: $a, b, c, \ldots, a_1, a_2, \ldots$, сложные — прописными латинскими буквами: $A, B, C, \ldots, A_1, A_2, \ldots$.

Операции над высказываниями:

1. Отрицание.

   Определение. *Отрицанием* высказывания A называется высказывание $\neg A$, ложное тогда и только тогда, когда A истинно.

   Истинностные значения высказываний удобно записывать в таблицы — *таблицы истинности* (*истинностные таблицы*).
   Таблица истинности для отрицания:

A	$\neg A$
И	Л
Л	И

   И — истина, Л — ложь

2. Конъюнкция.

   Определение. *Конъюнкцией* высказываний A и B называется высказывание $A \wedge B$, истинное тогда и только тогда, когда A и B истинны.

   Таблица истинности для конъюнкции:

A	B	$A \wedge B$
И	И	И
Л	И	Л
И	Л	Л
Л	Л	Л

3. Дизъюнкция.

   Определение. *Дизъюнкцией* высказываний A и B называется высказывание $A \vee B$, ложное тогда и только тогда, когда A и B ложны.

   Таблица истинности для дизъюнкции:

A	B	$A \vee B$
И	И	И
Л	И	И
И	Л	И
Л	Л	Л

4. Импликация.

   Определение. *Импликацией* высказываний A и B называется высказывание $A \supset B$, ложное тогда и только тогда, когда A истинно, а B ложно.

   Таблица истинности для импликации:

A	B	$A \supset B$	
И	И	И	
И	Л	Л	
Л	И	И	} Принцип материальной импликации
Л	Л	И	

   Определение. Высказывание A называется *антецедентом* (*посылкой*), B — *консеквентом* (*следствием*) импликации.

5. Эквиваленция.

   Определение. *Эквиваленцией* высказываний A и B называется высказывание $A \equiv B$, истинное тогда и только тогда, когда A и B принимают одинаковые истинностные значения.

   Таблица истинности для эквиваленции:

A	B	$A \equiv B$
И	И	И
Л	И	Л
И	Л	Л
Л	Л	И

Пропозициональными связками называются знаки операций $\neg$, $\wedge$, $\vee$, $\supset$, $\equiv$.

1.3. Формулы алгебры высказываний

Высказывания и операции над ними образуют *алгебру высказываний*.
Для записи формул этой алгебры используем алфавит, состоящий из:

1. строчных латинских букв $a, b, c, \ldots, a_1, a_2, \ldots$ — *пропозициональных букв*;
2. пропозициональных связок;
3. специальных символов (,).

Определение. *Формулой алгебры высказываний* (*пропозициональной формой*) называется слово в алфавите алгебры высказываний, построенное по правилам:

1. Любая пропозициональная буква есть формула.
2. Если A, B есть формулы, то слова $(\neg A)$, $(A \wedge B)$, $(A \vee B)$, $(A \supset B)$, $(A \equiv B)$ также являются формулами.
3. Слово является формулой в том и только том случае, когда оно получено по правилам 1 и 2.

Определение. *Подформулой* формулы называется её часть, сама являющаяся формулой.

Правила удаления лишних скобок:

1. Внешние скобки можно опускать.
2. Если формула содержит вхождения только одной бинарной связки $\wedge$, $\vee$, $\supset$ или $\equiv$, то для каждого вхождения можно опускать внешние скобки у подформулы слева.
3. Введём приоритет связок (по возрастанию): $\equiv$, $\supset$, $\vee$, $\wedge$, $\neg$. Можно опускать пары скобок, без которых возможно восстановление исходной формулы по следующим правилам. Каждое вхождение связки $\neg$ относится к наименьшей следующей за ним подформуле. После расстановки скобок, относящихся к $\neg$ каждое вхождение символа $\wedge$ связывает наименьшие окружающие его подформулы. После расстановки скобок, относящихся к $\wedge$, каждое вхождение $\vee$ относится к наименьшим подформулам слева и справа от него. Далее подобным образом расставляются скобки, относящиеся к символам $\supset$ и $\equiv$. При применении этого правила к одинаковым связкам движение по формуле происходит слева направо.

Формулы представляют собой формализованную математическую запись реальных высказываний. Поэтому для обозначения формул будем использовать прописные латинские буквы.

Каждому распределению истинностных значений пропозициональных букв, входящих в формулу, соответствует некоторое истинностное значение этой формулы, полученное по таблицам истинности пропозициональных связок. Таким образом, любая пропозициональная форма (слово, последовательность символов) определяет некоторую истинностную функцию (математическую функцию, функцию алгебры логики). Эта функция может быть графически представлена истинностной таблицей формулы.

Пример таблицы для формулы $\neg(A \wedge \neg B) \supset C$:

A	B	C	$\neg B$	$A \wedge \neg B$	$\neg(A \wedge \neg B)$	$\neg(A \wedge \neg B) \supset C$
И	И	И	Л	Л	И	И
И	И	Л	Л	Л	И	Л
И	Л	И	И	И	Л	И
И	Л	Л	И	И	Л	И
Л	И	И	Л	Л	И	И
Л	И	Л	Л	Л	И	Л
Л	Л	И	И	Л	И	И
Л	Л	Л	И	Л	И	Л

1.4. Тавтологии

Далее будем отождествлять форму и соответствующую ей истинностную функцию (не забывая при этом в чём их различие).

Определение. Формула называется *тождественно истинной* (*тавтологией*), если она истинна при любых наборах истинностных значений входящих в неё букв.

Определение. Формула называется *тождественно ложной* (*противоречием*), если она ложна при любых наборах истинностных значений входящих в неё букв.

Определение. Формула называется *выполнимой* (*опровержимой*), если она истинна (ложна) при некотором наборе истинностных значений входящих в неё букв.

Очевидно следующее утверждение.

Лемма 1.1. Формула A является тавтологией тогда и только тогда, когда $\neg A$ является противоречием.

Следующие важные теоремы служат основаниями для фундаментальных правил логического вывода.

Теорема 1.1. Если A, $A \supset B$ — тавтологии, то B — также тавтология.

Доказательство. От противного. Предположим, что B не является тавтологией. Тогда существует набор истинностных значений входящих в B букв, который реализует ложность B. В силу того, что A — тавтология, на указанном наборе A будет истинно. С другой стороны, импликация $A \supset B$ ложна в связи с истинностью A и ложностью B на указанному наборе, что вступает в противоречие с тем, что $A \supset B$ — тавтология.
Значит B является тавтологией. ■

Эта теорема обосновывает правило вывода по индукции modus ponens.

Теорема 1.2. Если A — тавтология, содержащая пропозициональные буквы $a_1, a_2, \ldots, a_n$, формула B получена подстановкой в A формул $A_1, A_2, \ldots, A_n$ вместо всех вхождений букв $a_1, a_2, \ldots, a_n$ соответственно. Тогда B также является тавтологией.

Доказательство. От противного. Пусть B не является тавтологией, тогда существует набор истинностных значений входящих в B букв, реализующий ложность этой формулы. Пусть этот набор доставляет формулам $A_1, A_2, \ldots, A_n$ истинностные значения $\alpha_1, \alpha_2, \ldots, \alpha_n$ соответственно. Присвоим буквам $a_1, a_2, \ldots, a_n$ формулы A истинностные значения $\alpha_1, \alpha_2, \ldots, \alpha_n$ соответственно. Ясно, что полученное ранее истинностное значение B совпадает с истинностным значением A, полученным в предыдущей подстановке. Такое совпадение порождает противоречие, ибо B, как показано ранее, ложно, а A — тавтология по условию.
Значит B является тавтологией. ■

Теорема 1.2 утверждает, что подстановка в тавтологию вместо всех вхождений букв (причём, не обязательно всех букв) произвольных формул даёт тавтологию. Таким образом, она обосновывает правило подстановки, используемое неявно в рассматриваемых далее исчислениях.

§2. Формальные аксиоматические теории

2.1. Определение формальной теории

Метод формальных теорий — другой, более мощный метод решения задачи логических исчислений. Но вместе с тем, это очень трудный метод.

Формальная аксиоматическая теория определена, если:

1. Задан *алфавит* теории (алфавит — не более чем счётное множество символов).
2. Задано подмножество слов в алфавите теории, которые считаются *формулами* теории.
3. Выделено некоторое подмножество формул — *аксиом* теории.
4. Задано конечное множество отношений между формулами теории, которые называются *правилами вывода*.

Введённые компоненты теории удовлетворяют следующим условиям:

1. Можно эффективно определить, является ли данная формула аксиомой теории или нет. Именно такие теории будем называть *аксиоматическими* (*аксиоматизируемыми*).
2. Правила вывода заданы эффективно. Это означает, что для каждого правила R_i существует такое число $j > 0$, что для любого набора j формул $A_1, \ldots, A_j$ и для любой формулы A можно эффективно определить, находятся ли эти формулы в отношении R_i с формулой A: $\langle A_1; \ldots; A_j; A\rangle \in R_i$. Если находятся, то говорят, что формула A является непосредственным следствием формул $A_1, \ldots, A_j$ по правилу вывода R_i:

$$\frac{A_1, \ldots, A_j}{A}.$$

2.2. Доказательства и теоремы

Определение. *Доказательством* (*выводом*) в теории называется такая последовательность формул $A_1, \ldots, A_m$, что для любого $i > 0$ A_i — либо аксиома, либо непосредственное следствие каких-либо предыдущих формул по одному из правил вывода.

Определение. Формула называется *теоремой* теории, если существует вывод, в котором эта формула последняя. Такой вывод называется *доказательством* (*выводом*) теоремы.

Определение. Теория называется *разрешимой*, если для любой формулы существует эффективный алгоритм определения, является ли она теоремой теории или нет.

В разрешимой теории доказательство можно автоматизировать (механизировать). В неразрешимой теории поиск доказательств — творческий процесс, посильный только человеку.

Определение. Формула A называется *следствием* в теории множества формул Γ, если существует последовательность формул $A_1, \ldots, A_m$, в которой A_m есть A, а для каждого $i > 0$ A_i — либо аксиома, либо непосредственное следствие каких-либо предыдущих формул по одному из правил вывода, либо формула из Γ. Такой вывод называется *доказательством* (*выводом*) формулы A из множества формул Γ. Формулы из множества Γ называются *гипотезами* (*посылками*).

Обозначается выводимость $\Gamma \vdash A$ или $A_1, \ldots, A_s \vdash A$. Если $\Gamma = \varnothing$, то $\Gamma \vdash A$ равносильно тому, что A — теорема, поэтому тот факт, что A является теоремой, записывают $\vdash A$.

Свойства выводимости из посылок:

1. Если $\Gamma \subseteq \Delta$ и $\Gamma \vdash A$, то $\Delta \vdash A$ (в множество гипотез можно добавлять любые формулы).
2. $\Gamma \vdash A$ тогда и только тогда, когда в Γ имеется такое конечное подмножество Δ, что $\Delta \vdash A$ (некоторые формулы можно удалять из множества гипотез без потери выводимости).
3. Если $\Delta \vdash A$ и $\Gamma \vdash B$ для каждой формулы $B \in \Delta$, то $\Gamma \vdash A$.

§3. Аксиоматическая теория исчисления высказываний

3.1. Определение теории исчисления высказываний

Зададим теорию исчисления высказываний.

Алфавит теории:

1. пропозициональные буквы $A, B, C, \ldots, A_1, A_2, \ldots$;
2. пропозициональные связки $\neg$, $\supset$;
3. специальные символы (,).

Формулы теории определяются рекуррентно по правилам:

1. Любая пропозициональная буква есть формула.
2. Если $\mathcal{A}$, $\mathcal{B}$ есть формулы, то слова $(\neg\mathcal{A})$, $(\mathcal{A} \supset \mathcal{B})$ также являются формулами.
3. Слово является формулой в том и только том случае, когда оно получено по правилам 1 и 2.

Используются те же правила удаления лишних скобок (см. п. 1.3.).

Аксиомы теории:

(A1) $A \supset (B \supset A)$;

(A2) $\big(A \supset (B \supset C)\big) \supset \big((A \supset B) \supset (A \supset C)\big)$;

(A3) $(\neg B \supset \neg A) \supset \big((\neg B \supset A) \supset B\big)$.

Единственное правило вывода: B — непосредственное следствие формул A, $A \supset B$, или

$$\frac{A,\ A \supset B}{B}.$$

Это правило называется *modus ponens* (*MP*). Его правомерность обосновывается теоремой 1.1.

Замечание 1. Аксиомы на самом деле являются *схемами аксиом*. Это означает, что подстановка в схему любых формул вместо всех вхождений букв (все вхождения одной буквы заменяются одной и той же формулой) даёт аксиому в силу теоремы 1.2. Таким образом, множество аксиом в нашем исчислении бесконечно.

Замечание 2. Остальные пропозициональные связки используются для сокращения формул по эквивалентным заменам:

$$A \wedge B \iff \neg(A \supset \neg B);$$
$$A \vee B \iff \neg A \supset B;$$
$$A \equiv B \iff (A \supset B) \wedge (B \supset A).$$

3.2. Доказательства в исчислении высказываний

Лемма 3.1. $\vdash A \supset A$.

Доказательство.

1. $\Big(A \supset \big((A \supset A) \supset A\big)\Big) \supset \Big(\big(A \supset (A \supset A)\big) \supset (A \supset A)\Big)$ (A2);
2. $A \supset \big((A \supset A) \supset A\big)$ (A1);
3. $\big(A \supset (A \supset A)\big) \supset (A \supset A)$ (из 1, 2 по MP);
4. $A \supset (A \supset A)$ (A1);
5. $A \supset A$ (из 3, 4 по MP).

■

Лемма 3.2. $\vdash (\neg A \supset A) \supset A$.

Доказательство.

1. $\neg A \supset \neg A$ (лемма 3.1);
2. $(\neg A \supset \neg A) \supset \big((\neg A \supset A) \supset A\big)$ (A3);
3. $(\neg A \supset A) \supset A$ (из 1, 2 по MP).

■

Лемма 3.3. $A \supset B,\ B \supset C \vdash A \supset C$.

Доказательство.

1. $B \supset C$ (гипотеза);
2. $(B \supset C) \supset \big(A \supset (B \supset C)\big)$ (A1);
3. $A \supset (B \supset C)$ (из 1, 2 по MP);
4. $A \supset B$ (гипотеза);
5. $\big(A \supset (B \supset C)\big) \supset \big((A \supset B) \supset (A \supset C)\big)$ (A2);
6. $(A \supset B) \supset (A \supset C)$ (из 3, 5 по MP);
7. $A \supset C$ (из 4, 6 по MP).

■

Лемма 3.4. $\vdash A \supset \big(B \supset (A \supset B)\big)$.

Доказательство.

1. $B \supset (A \supset B)$ (A1);
2. $\big(B \supset (A \supset B)\big) \supset \Big(A \supset \big(B \supset (A \supset B)\big)\Big)$ (A1);
3. $A \supset \big(B \supset (A \supset B)\big)$ (из 1, 2 по MP).

■

Лемма 3.5.

1) $\vdash A \supset (A \vee B)$;
2) $\vdash B \supset (A \vee B)$.

Доказательство.

1) Доказывается на основе $A, \neg A \vdash B$ (см. (1) в лемме 3.10) и применения теоремы дедукции (теорема 3.1):

$$A, \neg A \vdash B \Longrightarrow A \vdash \neg A \supset B \Longleftrightarrow A \vdash A \vee B.$$

2) Запись $B \supset (A \vee B)$ понимается как $B \supset (\neg A \supset B)$, что есть просто аксиома A1.

■

Лемма 3.6.

1) $A \wedge B \vdash A$;
2) $A \wedge B \vdash B$.

Доказательство.

1) Данная выводимость расшифровывается как $\neg(A \supset \neg B) \vdash A$. Для доказательства понадобятся результаты лемм 3.8 и 3.10, а также теорема дедукции. А именно,

$$\neg A, A \vdash \neg B \xRightarrow{\text{т. дедукции}} \neg A \vdash A \supset \neg B \xRightarrow{\text{контрапозиция}} \neg(A \supset \neg B) \vdash \neg\neg A \xRightarrow[\text{правило сечения}]{\neg\neg A \vdash A,} \neg(A \supset \neg B) \vdash A.$$

2) Выводимость $\neg(A \supset \neg B) \vdash B$ поясняется аналогично на основе выводимости $\neg B \vdash A \supset \neg B$:

   1. $\neg B$ (гипотеза);
   2. $\neg B \supset (A \supset \neg B)$ (A1);
   3. $A \supset \neg B$ (из 1, 2 по MP).

   Далее получаем

$$\neg B \vdash A \supset \neg B \xRightarrow{\text{контрапозиция}} \neg(A \supset \neg B) \vdash \neg\neg B \xRightarrow[\text{правило сечения}]{\neg\neg B \vdash B,} \neg(A \supset \neg B) \vdash B.$$

■

Лемма 3.7. $A \supset (B \supset C),\ B \vdash A \supset C$

Доказательство.

1. $A \supset (B \supset C)$ (гипотеза);
2. $\big(A \supset (B \supset C)\big) \supset \big((A \supset B) \supset (A \supset C)\big)$ (A2);
3. $(A \supset B) \supset (A \supset C)$ (из 1, 2 по MP);
4. $B \supset (A \supset B)$ (A1);
5. B (гипотеза);
6. $A \supset B$ (5, 4 по MP);
7. $A \supset C$ (из 6, 3 по MP).

■

Лемма 3.8.

1) $\vdash \neg\neg A \supset A$;
2) $\vdash A \supset \neg\neg A$;
3) $\neg\neg A \vdash A$;
4) $A \vdash \neg\neg A$.

Доказательство.

1) 1. $(\neg A \supset \neg\neg\neg A) \supset \big((\neg A \supset \neg A) \supset A\big)$ (A3);
   2. $\neg A \supset \neg A$ (лемма 3.1);
   3. $(\neg A \supset \neg\neg\neg A) \supset A$ (из 1, 2 по лемме 3.7);

4. $\neg\neg A \supset (\neg A \supset \neg\neg A)$ (A1);
5. $\neg\neg A \supset A$ (из 4, 3 по лемме 3.3).

2) 1. $(\neg\neg\neg A \supset \neg A) \supset \big((\neg\neg\neg A \supset A) \supset \neg\neg A\big)$ (A3);
2. $\neg\neg\neg A \supset \neg A$ (формула $\neg\neg A \supset A$ с подстановкой $A \leftrightharpoons \neg A$);
3. $(\neg\neg\neg A \supset A) \supset \neg\neg A$ (из 2, 1 по MP);
4. $A \supset (\neg\neg\neg A \supset A)$ (A1);
5. $A \supset \neg\neg A$ (из 4, 3 по лемме 3.3).

3) 1. $\neg\neg A$ (гипотеза);
2. $\neg\neg A \supset A$ (выведенная теорема в п. 1);
3. A (из 1, 2 по MP).

4) 1. A (гипотеза);
2. $A \supset \neg\neg A$ (выведенная теорема в п. 2);
3. $\neg\neg A$ (из 1, 2 по MP).

■

3.3. Теорема дедукции

Теорема 3.1 (*дедукция в ИВ*)**.** Если Γ — множество формул и $\Gamma, A \vdash B$, то $\Gamma \vdash A \supset B$.

Доказательство.

Пусть $B_1, B_2, \ldots, B_n$ — вывод $\Gamma, A \vdash B$. Тогда B_n совпадает с B.

Доказав индукцией по $i = 1, 2, \ldots, n$, что $\Gamma \vdash A \supset B_i$, мы получим утверждение теоремы при $i = n$.

База: $i \leqslant 2$.
Проверим $\Gamma \vdash A \supset B_1$. Имеются следующие варианты: B_1 — либо аксиома, либо совпадает с A, либо входит в Γ. Если B_1 совпадает с A, то $\Gamma \vdash A \supset A$ — справедливое утверждение (лемма 3.1). Если B_1 есть аксиома или $B_1 \in \Gamma$, то, написав первую аксиому $B_1 \supset (A \supset B_1)$, из B_1 и написанной аксиомы по MP выводим требуемую формулу $A \supset B_1$.
Очевидно, что для $i = 2$ допускаются точно такие же варианты и рассуждения, ибо вывод B_2 по MP невозможен — перед B_2 в выводе должно идти по меньшей мере две формулы.

Индукционное предположение: Пусть $\Gamma \vdash A \supset B_j$ для всех $j = 1, 2, \ldots, i-1$.

Индукционный шаг: Докажем $\Gamma \vdash A \supset B_i$.
Снова имеются варианты: B_i — аксиома, либо B_i совпадает с A, либо входит в Γ, либо выводится из каких-то предыдущих формул B_r, B_q по MP ($r, q < i$). Проверка первых трёх случаев дословно повторяет проверку в базе индукции. Пусть $r < q$. Тогда B_q имеет вид $B_r \supset B_i$. По предположению индукции верны $\Gamma \vdash A \supset B_r$ и $\Gamma \vdash A \supset B_q$. Запишем аксиому A2: $\big(A \supset (\underbrace{B_r \supset B_i}_{B_q})\big) \supset \big((A \supset B_r) \supset (A \supset B_i)\big)$. Дважды применяя MP ($A \supset B_q$ и написанная аксиома, а затем $A \supset B_r$ и $(A \supset B_r) \supset (A \supset B_i)$), получаем искомую формулу $A \supset B_i$.

Таким образом, по индукции доказано, что имеет место $\Gamma \vdash A \supset B_n$, то есть $\Gamma \vdash A \supset B$. ■

Следствие. Если $A \vdash B$, то $\vdash A \supset B$.

Замечание (*от автора конспекта*)**.** Теорема дедукции верна и в обратную сторону: если $\Gamma \vdash A \supset B$, то справедливо $\Gamma, A \vdash B$.

Доказательство. Напишем вывод $\Gamma \vdash A \supset B$, состоящий из формул $C_1, C_2, \ldots, C_n$, где C_n совпадает с $A \supset B$, а каждая из предыдущих формул либо аксиома, либо входит в Γ, либо выводится из некоторых предшествующих по MP. Далее допишем к написанному выводу формулу A как гипотезу (а это именно гипотеза для $\Gamma, A \vdash B$) и выведем B из A и C_n по MP. ■

3.4. Применение теоремы дедукции

Доказательство леммы 3.3.

Вывод $A \supset B,\ B \supset C,\ A \vdash C$:

1. $A \supset B$ (гипотеза);
2. A (гипотеза);
3. B (из 2, 1 по MP);
4. $B \supset C$ (гипотеза);
5. C (из 3, 4 по MP).

Теперь, применяя теорему дедукции, получаем $A \supset B, B \supset C \vdash A \supset C$. ■

Лемма 3.9. $A \supset (B \supset C) \vdash B \supset (A \supset C)$.

Доказательство.

Вывод $A \supset (B \supset C),\ B,\ A \vdash C$:

1. A (гипотеза);
2. $A \supset (B \supset C)$ (гипотеза);
3. $B \supset C$ (из 1, 2 по MP);
4. B (гипотеза);
5. C (из 4, 3 по MP).

Теперь, дважды применяя теорему дедукции, получаем требуемое: $A \supset (B \supset C) \vdash B \supset (A \supset C)$. ■

Лемма 3.10.

1) $\vdash \neg A \supset (A \supset B)$;
2) $\vdash (\neg B \supset \neg A) \supset (A \supset B)$ (*доказательство от противного*);
3) $\vdash (A \supset B) \supset (\neg B \supset \neg A)$ (*контрапозиция*);
4) $\vdash A \supset \big(\neg B \supset \neg(A \supset B)\big)$;
5) $\vdash (A \supset B) \supset \big((\neg A \supset B) \supset B\big)$.

Доказательство.

1) Доказательство $\neg A,\ A \vdash B$:
   1. $\neg A$ (гипотеза);
   2. A (гипотеза);
   3. $A \supset (\neg B \supset A)$ (A1);
   4. $\neg A \supset (\neg B \supset \neg A)$ (A1);
   5. $\neg B \supset A$ (из 2, 3 по MP);
   6. $\neg B \supset \neg A$ (из 1, 4 по MP);
   7. $(\neg B \supset \neg A) \supset \big((\neg B \supset A) \supset B\big)$ (A3);
   8. $(\neg B \supset A) \supset B$ (из 6, 7 по MP);
   9. B (из 5, 8 по MP).

   Теперь дважды применяем теорему дедукции и получаем искомую выводимость.

2) Доказательство $\neg B \supset \neg A,\ A \vdash B$:

   1. $\neg B \supset \neg A$ (гипотеза);
   2. A (гипотеза);
   3. $(\neg B \supset \neg A) \supset \big((\neg B \supset A) \supset B\big)$ (A3);
   4. $A \supset (\neg B \supset A)$ (A1);
   5. $(\neg B \supset A) \supset B$ (из 1, 3 по MP);
   6. $A \supset B$ (из 4, 5 по лемме 3.3);
   7. B (из 2, 6 по MP).

   Теперь дважды применяем теорему дедукции и получаем искомую выводимость.

3) Доказательство $A \supset B \vdash \neg\neg A \supset B$:

   1. $A \supset B$ (гипотеза);
   2. $(A \supset B) \supset \big(\neg\neg A \supset (A \supset B)\big)$ (A1);
   3. $\neg\neg A \supset (A \supset B)$ (из 1, 2 по MP);
   4. $\big(\neg\neg A \supset (A \supset B)\big) \supset \big((\neg\neg A \supset A) \supset (\neg\neg A \supset B)\big)$ (A2);
   5. $(\neg\neg A \supset A) \supset (\neg\neg A \supset B)$ (из 3, 4 по MP);
   6. $\neg\neg A \supset A$ (теорема, доказано в лемме 3.8 п.1);
   7. $\neg\neg A \supset B$ (из 6, 5 по MP).

   Далее проверим $A \supset B, \neg B \vdash \neg A$:

   1. $(\neg\neg A \supset \neg B) \supset \big((\neg\neg A \supset B) \supset \neg A\big)$ (A3);
   2. $\neg B$ (гипотеза);
   3. $\neg B \supset (\neg\neg A \supset \neg B)$ (A1);
   4. $\neg\neg A \supset \neg B$ (из 2, 3 по MP);
   5. $(\neg\neg A \supset B) \supset \neg A$ (из 4, 1 по MP);
   6. $A \supset B$ (гипотеза);
   7. $\neg\neg A \supset B$ (из 6 по $A \supset B \vdash \neg\neg A \supset B$);
   8. $\neg A$ (из 7, 5 по MP).

   Из полученной выводимости, дважды применяя теорему дедукции, получаем требуемое.

4) Ясно, что $A,\ A \supset B \vdash B$. Дважды используя теорему дедукции, получаем $\vdash A \supset \big((A \supset B) \supset B\big)$. Далее согласно 3) получаем $\vdash \big((A \supset B) \supset B\big) \supset \big(\neg B \supset \neg(A \supset B)\big)$. Наконец, задействуя лемму 3.3 на предыдущих двух выводимостях, получаем искомое $\vdash A \supset \big(\neg B \supset \neg(A \supset B)\big)$.

5) Доказательство $A \supset B,\ \neg A \supset B \vdash B$:

   1. $A \supset B$ (гипотеза);
   2. $\neg A \supset B$ (гипотеза);
   3. $(A \supset B) \supset (\neg B \supset \neg A)$ (доказанная формула контрапозиции);
   4. $\neg B \supset \neg A$ (из 1, 3 по MP);
   5. $(\neg A \supset B) \supset (\neg B \supset \neg\neg A)$ (доказанная формула контрапозиции);
   6. $\neg B \supset \neg\neg A$ (из 2, 5 по MP);
   7. $(\neg B \supset \neg\neg A) \supset \big((\neg B \supset \neg A) \supset B\big)$ (A3);
   8. $(\neg B \supset \neg A) \supset B$ (из 6, 7 по MP);
   9. B (из 4, 8 по MP).

   Теперь дважды применяем теорему дедукции и получаем искомую выводимость.

■

3.5. Полнота и непротиворечивость ИВ

Лемма 3.11 (*корректность ИВ*)**.** Всякая теорема теории ИВ есть тавтология.

Доказательство. Пусть $\vdash A$ в теории ИВ. Тогда существует вывод $B_1, B_2, \ldots, B_n$, где B_n совпадает с A. Первым делом нужно доказать, что все аксиомы теории ИВ являются тавтологиями. Это можно сделать с помощью составления таблиц истинности для соответствующих формул из схем аксиом, а затем применения теоремы 1.2.

Доказательство того, что B_n — тавтология, можно провести путём проверки по индукции по $j = 1, 2, \ldots, n$, что B_j — тавтологии. А именно, согласно определению вывода, B_1, B_2 — аксиомы, потому как эти формулы не могут быть выведены по MP из предшествующих (до них должно идти по крайней мере две формулы), а следующие формулы есть аксиомы (то есть тавтологии), либо выводятся из некоторых предшествующих по MP. Вспоминая теорему 1.1, получаем, что из тавтологичности B_j и $B_j \supset B_k$ $(j < k)$ вытекает тавтологичность B_k.
Таким образом, доказано, что если A — теорема теории ИВ, то в любом выводе A все формулы — тавтологии, в том числе сама A. ■

Теорема 3.2 (*полнота ИВ*)**.** Если формула в теории ИВ является тавтологией, то она является теоремой.

Следствие 1. Если слово $\mathcal{B}$ в алфавите ИВ содержит пропозициональные связки $\neg$, $\supset$, $\wedge$, $\vee$, $\equiv$ и является сокращением некоторой формулы $\mathcal{A}$ теории ИВ, то $\mathcal{B}$ является тавтологией тогда и только тогда, когда $\mathcal{A}$ есть теорема ИВ.

Определение. Теория называется *полной*, если для каждого её верного утверждения $\mathcal{A}$ либо $\mathcal{A}$, либо отрицание $\mathcal{A}$ есть теорема.

Таким образом, теорема 3.2 утверждает полноту теории ИВ.

Определение. Теория называется *противоречивой*, если в ней существует такое утверждение $\mathcal{A}$, что и $\mathcal{A}$, и отрицание $\mathcal{A}$ есть теоремы. Теория называется *непротиворечивой*, если в ней не существует такого утверждения.

Следствие 2. Теория ИВ непротиворечива.

Из непротиворечивости ИВ следует существование формулы, не являющейся теоремой (например, отрицание любой теоремы). С другой стороны, в силу леммы 3.10 (1) из существования формулы, не являющейся теоремой, следует непротиворечивость ИВ. Вообще, непротиворечивость и существование формулы, не являющейся теоремой, эквивалентны для любой теории с правилом вывода MP, в которой выводимо утверждение леммы 3.10 (1).

Определение. Теория называется *абсолютно непротиворечивой*, если в ней не все формулы являются теоремами.

Выше было показано, что для ИВ непротиворечивость и абсолютная непротиворечивость эквивалентны.

§4. Другие аксиоматические теории ИВ

4.1. Исчисление Гильберта–Аккермана

Примитивные связки: $\neg$, $\vee$, а $A \supset B$ — сокращение $\neg A \vee B$.

Схемы аксиом:

(A1) $A \vee A \supset A$;

(A2) $A \supset (A \vee B)$;

(A3) $(A \vee B) \supset (B \vee A)$;

(A4) $(B \supset C) \supset \big((A \vee B) \supset (A \vee C)\big)$.

Правило вывода: MP.

4.2. Исчисление Россера

Примитивные связки: $\neg$, $\wedge$, а $A \supset B$ — сокращение $\neg(A \wedge \neg B)$.

Схемы аксиом:

(A1) $A \supset A \wedge A$;

(A2) $A \wedge B \supset A$;

(A3) $(A \supset B) \supset \big(\neg(B \wedge C) \supset \neg(C \wedge A)\big)$.

Правило вывода: MP.

4.3. Исчисление секвенций

Примитивные связки: $\neg$, $\vee$, $\wedge$, $\supset$.

Специальный символ: $\vdash$.

Секвенциями называются слова следующих трёх видов, где $A_1, A_2, \ldots, A_n, B$ — произвольные формулы:

1. $A_1, A_2, \ldots, A_n \vdash B$ (из $A_1, A_2, \ldots, A_n$ следует B_n);
2. $\vdash B$ (B доказуема);
3. $A_1, A_2, \ldots, A_n \vdash$ (система $A_1, A_2, \ldots, A_n$ противоречива).

Схема аксиом: $A \vdash A$.

Правила вывода, где $\Gamma, \Gamma_1, \Gamma_2, \Gamma_3$ — произвольные конечные (может быть, пустые) последовательности формул, а A, B, C — произвольные формулы:

1) $\dfrac{\Gamma_1 \vdash A;\ \Gamma_2 \vdash B}{\Gamma_1, \Gamma_2 \vdash A \wedge B}$ (*введение* $\wedge$);
2) $\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}$ (*удаление* $\wedge$);
3) $\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$ (*удаление* $\wedge$);
4) $\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}$ (*введение* $\vee$);
5) $\dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$ (*введение* $\vee$);
6) $\dfrac{\Gamma_1 \vdash A \vee B;\ \Gamma_2, A \vdash C;\ \Gamma_3, B \vdash C}{\Gamma_1, \Gamma_2, \Gamma_3 \vdash C}$ (*удаление* $\vee$);
7) $\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}$ (*введение* $\supset$);
8) $\dfrac{\Gamma_1 \vdash A;\ \Gamma_2 \vdash A \supset B}{\Gamma_1, \Gamma_2 \vdash B}$ (*удаление* $\supset$);
9) $\dfrac{\Gamma, A \vdash}{\Gamma \vdash \neg A}$ (*введение* $\neg$);
10) $\dfrac{\Gamma_1 \vdash A;\ \Gamma_2 \vdash \neg A}{\Gamma_1, \Gamma_2 \vdash}$ (*сведение к противоречию*);
11) $\dfrac{\Gamma, \neg A \vdash}{\Gamma \vdash A}$ (*удаление* $\neg$);
12) $\dfrac{\Gamma \vdash}{\Gamma \vdash A}$ (*утончение*);
13) $\dfrac{\Gamma \vdash A}{\Gamma, B \vdash A}$ (*расширение*);
14) $\dfrac{\Gamma_1, A, B, \Gamma_2 \vdash C}{\Gamma_1, B, A, \Gamma_2 \vdash C}$ (*перестановка*);
15) $\dfrac{\Gamma, A, A \vdash C}{\Gamma, A \vdash C}$ (*сокращение*).

4.4. Исчисление Клини

Примитивные связки: $\neg$, $\wedge$, $\vee$, $\supset$.

Схемы аксиом:

(A1) $A \supset (B \supset A)$;

(A2) $(A \supset B) \supset \Big(\big(A \supset (B \supset C)\big) \supset (A \supset C)\Big)$;

(A3) $A \wedge B \supset A$;

(A4) $A \wedge B \supset B$;

(A5) $(A \supset B) \supset \big((A \supset C) \supset (A \supset B \wedge C)\big)$;

(A6) $A \supset (A \vee B)$;

(A7) $B \supset (A \vee B)$;

(A8) $(A \supset C) \supset \Big((B \supset C) \supset \big((A \vee B) \supset C\big)\Big)$;

(A9) $(A \supset \neg B) \supset (B \supset \neg A)$;

(A10) $\neg\neg A \supset A$.

Правило вывода: MP.

II. Логика предикатов первого порядка

§1. Кванторы и формулы логики предикатов первого порядка

Логика предикатов первого порядка представляет собой обобщение логики высказываний на такие логические рассуждения, которые не могут быть формализованы средствами последней.

Классический пример: все люди смертны, Сократ — человек, следовательно, Сократ смертен.

Пусть $P(x)$ означает, что объект x обладает свойством P (P — *предикат*). Посредством $\forall x P(x)$ будем обозначать утверждение «для всякого x выполнено свойство P», $\exists x P(x)$ — утверждение «существует x, для которого выполнено свойство P». Символ $\forall$ называется *квантором всеобщности*, а $\exists$ — *квантором существования*.

Пусть константный символ S означает Сократа, предикат $M(x)$ — «x смертен», $H(x)$ — «x — человек». Тогда приведённое выше рассуждение формализуется так:

$$\frac{\forall x\big(H(x) \supset M(x)\big),\ H(S)}{M(S)}.$$

Ещё пример: все боятся Дракулы, Дракула боится только меня, следовательно, я Дракула.
D — Дракула, $A(x, y)$ — «x боится y», I — я, $E(x, y)$ — «x есть y». Тогда указанное выше утверждение формализуется так:

$$\frac{\forall x A(x, D),\ \forall y\big(A(D, y) \supset E(y, I)\big)}{E(I, D)}$$

Алфавит теории ИП включает следующие символы:

1. предметные (индивидные) переменные: $x_1, x_2, \ldots$;
2. предметные (индивидные) константы: $a_1, a_2, \ldots$;
3. предикатные буквы $A_1^1, A_1^2, \ldots, A_1^j, \ldots$;
4. функциональные буквы $f_1^1, f_1^2, \ldots, f_1^j, \ldots$;
5. пропозициональные связки $\neg$, $\supset$;
6. квантор всеобщности $\forall$;
7. квантор существования $\exists$;
8. специальные символы (,), ,.

Верхний индекс предикатных и функциональных букв указывает число аргументов буквы, а нижний служит номером соответствующей буквы.

Определение. *Термом* называется слово в алфавите ИП, построенное по правилам:

1. Всякая предметная переменная или предметная константа — терм;
2. Если f_i^j есть функциональная буква, а $t_1, t_2, \ldots, t_j$ — термы, то $f_i^j(t_1, t_2, \ldots, t_j)$ — терм;
3. Слово является термом тогда и только тогда, когда оно может быть получено по правилам 1, 2.

Определение. Слово в алфавите ИП называется *элементарной формулой*, если оно имеет такой и только такой вид: $A_i^n(t_1, t_2, \ldots, t_n)$, где A_i^n — предикатный символ арности n, а $t_1, t_2, \ldots, t_n$ — термы.

Определение. Формулой теории ИП называется слово в алфавите ИП построенное по правилам:

1. Всякая элементарная формула является формулой;
2. Если A и B — формулы, а y — предметная переменная, то $(\neg A)$, $(A \supset B)$, $(\forall y A)$ также являются формулами. В последнем случае формула A называется *областью действия квантора* $\forall$.
3. Слово является формулой тогда и только тогда, когда оно может быть получено по правилам 1, 2.

Замечание.

1. Связки $\equiv$, $\wedge$, $\vee$ могут использоваться как сокращения по эквивалентностям

$$A \wedge B \iff \neg(A \supset \neg B);$$
$$A \vee B \iff \neg A \supset B;$$
$$A \equiv B \iff (A \supset B) \wedge (B \supset A).$$

2. Квантор $\exists$ можно использовать для сокращения по эквивалентности $\exists x A \iff \neg\big(\forall x(\neg A)\big)$.

3. Можно опускать лишние скобки по тем же правилам, что и в ИВ с учётом того, что кванторы по приоритету находятся между $\supset$ и $\vee$ (сильнее $\supset$, но слабее $\vee$).

4. Можно опускать скобки в (под)формулах вида $Q_1\Big(Q_2\big(\dots Q_{n-1}(Q_n A)\dots\big)\Big)$, где Q_i, $i = 1, 2, \dots, n$, есть кванторы, то есть допустимо писать $Q_1 Q_2 \dots Q_{n-1} Q_n A$.

Определение. Вхождение переменной x в формулу называется *связанным*, если x — переменная входящего в эту формулу квантора $\forall x$ или находится в области действия входящего в эту формулу квантора $\forall x$. В противном случае вхождение переменной x в формулу называется *свободным*.

Определение. Переменная x называется *свободной* (*связанной*) в формуле, если существует хотя бы одно её свободное (связанное) вхождение в эту формулу.

Вполне возможно, что одна и та же переменная может быть как связанной, так и свободной в одной и той же формуле.

Определение. Формула называется *замкнутой*, если она не содержит свободных переменных.

§2. Интерпретации и метод моделей

Определение. *Интерпретацией* называется непустое множество D (*область интерпретации*) и соответствие, относящее каждой предикатной букве A_i^n некоторое n-арное отношение в D, каждой функциональной букве f_i^n — некоторую n-местную функцию $D^n \to D$, каждой предметной константе — некоторый элемент D. Предметные переменные принимают значения в D, связки $\neg$, $\supset$ и квантор $\forall$ имеют обычный смысл.

При заданной интерпретации замкнутая формула переходит в истинное или ложное высказывание, формула со свободными переменными — в некоторое отношение на D, которое может быть выполнено для одних значений переменных из D и не выполнено для других.

Определение. Формула называется *истинной в данной интерпретации*, если она *выполнена* для всех элементов из D.

Определение. Формула называется *ложной в данной интерпретации*, если она *не выполнена* ни для одного элемента из D.

Определение. Интерпретация называется *моделью* для множество формул Γ, если каждая формула из Γ истинна в ней.

Определение. Формула называется *логически общезначимой*, если она истинна в любой интерпретации.

Логически общезначимые формулы также называются *логическими законами*.

Определение. Формула A называется *противоречием*, если $\neg A$ логически общезначима.

Определение. Формула называется *выполнимой*, если существует интерпретация, в которой она выполнена хотя бы на одном подмножестве элементов из D.

Метод моделей установления общезначимости (противоречивости, выполнимости) формула заключается в подборе моделей (интерпретаций) или доказательстве общезначимости (противоречивости) с помощью интерпретаций.

§3. Теории первого порядка

Для построения теории используем введённый в §1. алфавит. При этом положим, что множества предикатных букв и предметных переменных не пусты, множества функциональных символов и предметных констант могут быть пустыми.

Термы, элементарные формулы и формулы определяются так же.

Определение. Терм t называется *свободным для переменной* x_i *в формуле* A, если никакое свободное вхождение x_i в A не лежит в области действия никакого квантора $\forall x_j$, где x_j — переменная, входящая в терм t.

Иными словами, терм t свободен для переменной x_i в формуле A, если при подстановке t в A вместо всех свободных вхождений x_i никакая переменная в подставленном терме t не свяжется никаким квантором в формуле A. Ясно, что если в A нет свободных вхождений переменной x_i, то любой терм будет свободным относительно этой переменной. Также терм $t = x_i$, как нетрудно сообразить, будет свободным относительно x_i, какова бы ни была формула A.

Аксиомами теории будут следующие формулы:

(A1) $A \supset (B \supset A)$;

(A2) $\big(A \supset (B \supset C)\big) \supset \big((A \supset B) \supset (A \supset C)\big)$;

(A3) $(\neg B \supset \neg A) \supset \big((\neg B \supset A) \supset B\big)$;

(A4) $\forall x_i A(x_i) \supset A(t)$, где t — терм, свободный для x_i в формуле $A(x_i)$, а $A(t)$ — формула, в которой все вхождения переменной x_i заменены на t;

(A5) $\forall x_i(A \supset B) \supset (A \supset \forall x_i B)$, где A не содержит свободные вхождения переменной x_i.

Различные конкретные теории исчисления предикатов могут содержать ещё аксиомы в дополнение к приведённым выше (*собственные* аксиомы). Теория первого порядка без собственных аксиом называется *исчислением предикатов первого порядка* (*ИП*).
Первый порядок в названии выражается в том, что в предикаты можно подставлять исключительно термы, определённые в §1., а в кванторах могут записываться только индивидные переменные. В теориях более высокого порядка допускается взятие кванторов по предикатным символам, а так же подстановка в предикаты других предикатов.

Правила вывода:

1) MP
$$\frac{A,\ A \supset B}{B};$$

2) обобщение (Gen)
$$\frac{A}{\forall x_i A}.$$

Лемма 3.1. Если формула A произвольной теории первого порядка T есть частный случай тавтологии, то A есть теорема T и может быть выведена с применением одних только схем аксиом A1, A2, A3 и правила MP.

§4. Теорема дедукции в теории ИП

Теорема дедукции для пропозиционального ИВ не может быть перенесена без изменений на произвольные теории первого порядка. Однако некоторая ослабленная форма теоремы может быть доказана для них.

Пример: $A(x) \vdash \forall x A(x)$. Вывод состоит в применении к $A(x)$ правила Gen:

1. $A(x)$ (гипотеза);
2. $\forall x A(x)$ (из 1 по Gen).

Рассмотрим теперь интерпретацию с областью $D = \{a, b\}$. Предикат A возьмём таким, что $A(a)$ истинно, а $A(b)$ ложно. Тогда формула $A(x) \supset \forall x A(x)$ не является верной, если положить свободную переменную $x = a$. Действительно, ясно, что $\forall x A(x)$ ложно, а с другой стороны, взяв значение свободной переменной $x = a$, получим, что посылка импликации будет истинной ($A(a)$ истинно), что влечёт ложность импликации.

Пусть A — формула из множества формул Γ, а $B_1, B_2, \ldots, B_n$ — некоторый вывод из Γ. Будем говорить, что формула B_i *зависисит от* A *в этом выводе*, если для этой формулы выполнено какое-нибудь из условий:

1. формула B_i есть A;
2. формула B_i есть непосредственное следствие по одному из правил вывода некоторых предшествующих в этом выводе формул, из которых хотя бы одна зависит от A.

Лемма 4.1. Если формула B не зависит от формулы A в выводе $\Gamma, A \vdash B$, то $\Gamma \vdash B$.

Доказательство. Пусть $B_1, B_2, \ldots, B_n$ — произвольный вывод B из $\Gamma \cup \{A\}$, в котором B независит от A. Ясно, что B_n совпадает с B.

Докажем по индукции по $n \in \mathbb{N}$ (то есть по длине вывода), что $\Gamma \vdash B_n$, то есть $\Gamma \vdash B$. Так мы докажем, что утверждение леммы верно, каков бы ни был вывод $\Gamma, A \vdash B$.

База: $n = 1$. Вывод состоит всего из одной формулы — формулы B. Ясно, что B в таком случае не совпадает с A, поскольку в противном случае имела бы место зависимость B от A, противоречащая условию леммы. В таком случае очевидно, что написанный вывод, состоящий из одной формулы, по совместительству является ещё и выводом $\Gamma \vdash B$, что доказывает базу индукции.

Индукционное предположение: пусть утверждение доказано для всех выводов $\Gamma, A \vdash B$ всех длин $k \leqslant n-1$.

Индукционный шаг: докажем, что утверждение будет верно для вывода и длины n. Очевидно, что утверждение леммы будет верным, если окажется, что B входит в Γ или является одной из аксиом. Пусть теперь B_n в нашем произвольном выводе получено из каких-то предшествующих формул B_i и B_j $(i, j < n)$ по одному из двух правил вывода. Ясно, что поскольку B_n (то есть B) не зависит от A, то ни одна из формул B_i и B_j не зависит от A. Тогда согласно индукционному предположению и произвольности формулы B в формулировке леммы, получаем, что имеют место выводы $\Gamma \vdash B_i$ и $\Gamma \vdash B_j$. Тогда по правилу сечения извлекаем искомый вывод: $\Gamma \vdash B_n$. ■

Теорема 4.1 (*дедукция в ИП*)**.** Пусть $\Gamma, A \vdash B$ и существует вывод B из $\Gamma \cup \{A\}$, в котором ни при каком применении правила Gen к формулам, зависящим в этом выводе от A, не связывается квантором никакая свободная переменная формулы A. Тогда $\Gamma \vdash A \supset B$.

Доказательство. Пусть $B_1, B_2, \ldots, B_n$ — вывод B из $\Gamma \cup \{A\}$, удовлетворяющий условию теоремы. Проведём доказательство индукцией по $i = 1, 2, \ldots, n$ выводимостей $\Gamma \vdash A \supset B_i$. При $i = n$ получается утверждение теоремы.

База: $i = 1$. Возможны следующие варианты: B_1 — либо аксиома, либо формула из Γ, либо совпадает с A. В первых двух случаях запишем аксиому A1: $B_1 \supset (A \supset B_1)$. Далее выводем $A \supset B_1$ из написанной аксиомы и гипотезы B_1 по MP. Оставшийся вариант — B_1 совпадает с A. Ясно, что $A \supset A$ выводится так же, как в это делалось в лемме 3.1 (ИВ).

Индукционное предположение: пусть доказано для всех $j = 1, 2, \ldots, i-1$, что имеет место $\Gamma \vdash A \supset B_j$.

Шаг индукции: докажем утверждение для $j = i$. Доступны варианты: B_i — либо аксиома, либо формула из Γ, либо совпадает с A, либо B_i выводится из некоторых предшествующих формул по одному из правил вывода. Первые три варианта разбираются аналогично базе индукции.
Если B_i выводится из некоторых предшествующих по MP, то доказательство $\Gamma \vdash A \supset B_i$ аналогично доказательству в т. дедукции в ИВ. Действительно, если B_i выводится из B_r и B_q $(r < q < i)$, то B_q имеет вид $B_r \supset B_i$. Тогда

1. $\big(A \supset (\underbrace{B_r \supset B_i}_{B_q})\big) \supset \big((A \supset B_r) \supset (A \supset B_i)\big)$ (A2);
2. $A \supset (B_r \supset B_i)$ (по индукционному предположению $\Gamma \vdash A \supset B_q$);
3. $(A \supset B_r) \supset (A \supset B_i)$ (из 2, 1 по MP);
4. $A \supset B_r$ (по индукционному предположению $\Gamma \vdash A \supset B_r$);
5. $A \supset B_i$ (из 4, 3 по MP).

Пусть теперь B_i выводится из предшествующей формулы B_j $(j < i)$ по правилу Gen, то есть выполняется вывод $\dfrac{B_j}{\forall x_k B_j}$. Отсюда вытекает, что B_i имеет вид $\forall x_k B_j$. По индукционному предположению справедлива выводимость $\Gamma \vdash A \supset B_j$. Имеются два случая: B_j зависит от A и B_j не зависит от A.

- Пусть зависимости B_j от A нет. Тогда, согласно лемме 4.1, из выводиости $\Gamma, A \vdash B_j$ вытекает выводимость $\Gamma \vdash B_j$. Применяя правило Gen к B_j, получаем требуемое: $\Gamma \vdash \forall x_k B_j$, то есть $\Gamma \vdash B_i$.
- Пусть теперь имеет место зависимость B_j от A в данном выводе. Тогда по условию теоремы переменная x_k не является свободной переменной формулы A. Значит мы имеем право записать аксиому A5:

  $$\forall x_k (A \supset B_j) \supset (A \supset \forall x_k B_j).$$

  По индукционному предположению справедливо $\Gamma \vdash A \supset B_j$. Тогда, пользуясь правилом Gen, получаем $\Gamma \vdash \forall x_k (A \supset B_j)$, а значит из написанной аксиомы A5 и выведенного $\forall x_k (A \supset B_j)$ по MP извлекаем искомый вывод $\Gamma \vdash A \supset \forall x_k B_j$, то есть $\Gamma \vdash A \supset B_i$.

■

Следствие 1. Если $\Gamma, A \vdash B$ и существует вывод B из $\Gamma \cup \{A\}$, построенный без применения правила Gen к свободным переменным формулы A, то $\Gamma \vdash A \supset B$.

Следствие 2. Если формула A замкнута и $\Gamma, A \vdash B$, то $\Gamma \vdash A \supset B$.

Пример: $\vdash \forall x \forall y A(x, y) \supset \forall y \forall x A(x, y)$. Докажем вспомогательное утверждение $\forall x \forall y A(x, y) \vdash \forall y \forall x A(x, y)$:

1. $\forall x \forall y A(x, y)$ (гипотеза);
2. $\forall x \forall y A(x, y) \supset \forall y A(x, y)$ (A4, её можно применять, так как терм $t = x$ является свободным для переменной x в формуле $\forall y A(x, y)$);
3. $\forall y A(x, y)$ (из 1, 2 по MP);
4. $\forall y A(x, y) \supset A(x, y)$ (A4, так как терм $t = y$ свободен для переменной y в формуле $A(x, y)$);
5. $A(x, y)$ (из 3, 2 по MP);
6. $\forall x A(x, y)$ (из 5 по Gen);
7. $\forall y \forall x A(x, y)$ (из 6 по Gen).

В данном случае, в силу отсутствия свободных переменных в $\forall x \forall y A(x, y)$, применима теорема дедукции:

$$\forall x \forall y A(x, y) \vdash \forall y \forall x A(x, y)$$
$$\Downarrow$$
$$\vdash \forall x \forall y A(x, y) \supset \forall y \forall x A(x, y).$$

§5. Полнота и непротиворечивость теорий первого порядка

Лемма 5.1. Во всякой теории первого порядка любая теорема логически общезначима.

Полнота теории первого порядка должна означать доказуемость любой логически общезначимой формулы. Но логическая общезначимость определяется истинностью на интерпретациях. Поэтому установление полноты требует применения средств теории моделей.

Лемма 5.2. Всякая логически общезначимая формула теории первого порядка T является теоремой теории T.

Теорема 5.1 (*теорема Гёделя о полноте*)**.** Во всяком ИП первого порядка теоремами являются те и только те формулы, которые логически общезначимые.

Теорема 5.2 (*непротиворечивость ИП*)**.** Всякое ИП первого порядка непротиворечиво.

Доказательство. Поставим в соответствие каждой формуле A теории ИП первого порядка формулу $h(A)$, в которой опущены все кванторы и термы с соответствующими скобками и запятыми. В таком случае $h(A)$ станет пропозициональной формулой ИВ. Пример: $\forall x A\big(f(x), y\big) \supset \exists z \neg C(z) \xmapsto{h} A \supset \neg C$. Фактически $h(A)$ — интерпретация A на одноэлементной области интерпретации. Ясно, что верны следующие утверждения про h:

1. $h(\neg A)$ совпадает с $\neg h(A)$.
2. $h(A \supset B)$ совпадает с $h(A) \supset h(B)$ (то же самое верно для остальных связок).
3. Если A — аксиома A1–A5, то $h(A)$ — тавтология.
4. Если $h(A)$ и $h(A \supset B)$ — тавтологии, то и $h(B)$ — тавтология.
5. Если $h(A)$ — тавтология, то и $h(\forall x_i A)$ — тавтология, какова бы ни была переменная x_i.

Теорему теперь докажем от противного. Предположим, что существует утверждение A, для которого имеют место обе выводимости в теории ИП: $\vdash A$ и $\vdash \neg A$. Из перечисленных выше замечаний про h заключаем, что $h(B)$ для любой теоремы B суть тавтология. То есть $h(A)$ и $h(\neg A)$ являются тавтологиями, а значит $h(A)$ и $\neg h(A)$ тоже являются тавтологиями, что невозможно в силу непротиворечивости ИВ. Итак, для любой теории ИП первого порядка не существует утверждения A, для которого справедливы обе выводимости $\vdash A$ и $\vdash \neg A$, значит всякая теория ИП первого порядка непротиворечива. ■

§6. Некоторые дополнительные правила вывода в ИП

Для упрощения работы с конкретными теориями первого порядка полезно доказать некоторые дополнительные факты о них. Пусть далее T — произвольная теория первого порядка.

6.1. Правила индивидуализации и существования

Правило индивидуализации: если терм $\mathtt{t}$ свободен для $\mathtt{x}$ в формуле $\mathsf{A}(\mathtt{x})$, то $\forall \mathtt{x}\mathsf{A}(\mathtt{x}) \vdash \mathsf{A}(\mathtt{t})$.

Доказательство.

1. $\forall \mathtt{x}\mathsf{A}(\mathtt{x}) \supset \mathsf{A}(\mathtt{t})$ (A4, её использование правомерно, так как $\mathtt{t}$ свободен для $\mathtt{x}$ в $\mathsf{A}(\mathtt{x})$);
2. $\forall \mathtt{x}\mathsf{A}(\mathtt{x})$ (гипотеза);
3. $\mathsf{A}(\mathtt{t})$ (из 2, 1 по MP).

■

Лемма 6.1. Если A и B — формулы и предметная переменная $\mathtt{x}$ не свободна в A, то:

1) $\vdash \mathsf{A} \supset \forall \mathtt{x}\mathsf{A}$ (следовательно, по аксиоме A4 получается $\vdash \mathsf{A} \equiv \forall \mathtt{x}\mathsf{A}$);
2) $\vdash \exists \mathtt{x}\mathsf{A} \supset \mathsf{A}$ (следовательно, по нижеследующему правилу существования $\vdash \exists \mathtt{x}\mathsf{A} \equiv \mathsf{A}$);
3) $\vdash \forall \mathtt{x}(\mathsf{A} \supset \mathsf{B}) \equiv (\mathsf{A} \supset \forall \mathtt{x}\mathsf{B})$;
4) $\vdash \forall \mathtt{x}(\mathsf{B} \supset \mathsf{A}) \equiv (\exists \mathtt{x}\mathsf{B} \supset \mathsf{A})$.

Доказательство.

1) Ясно, что по правилу Gen справедлива выводимость $\mathsf{A} \vdash \forall \mathtt{x}\mathsf{A}$. Так как в данном случае переменная $\mathtt{x}$ не свободна в A и она не свяжется квантором $\forall \mathtt{x}$, правомерно использование теоремы дедукции, дающее искомое утверждение: $\vdash \mathsf{A} \supset \forall \mathtt{x}\mathsf{A}$.

2) Формула $\exists \mathtt{x}\mathsf{A} \supset \mathsf{A}$ расшифровывается как $\neg\forall \mathtt{x}(\neg\mathsf{A}) \supset \mathsf{A}$. Докажем вспомогательную выводимость $\neg\forall \mathtt{x}(\neg\mathsf{A}) \vdash \mathsf{A}$:

   1. $\big(\neg\mathsf{A} \supset \neg\forall \mathtt{x}(\neg\mathsf{A})\big) \supset \Big(\big(\neg\mathsf{A} \supset \forall \mathtt{x}(\neg\mathsf{A})\big) \supset \mathsf{A}\Big)$ (A3);
   2. $\neg\forall \mathtt{x}(\neg\mathsf{A}) \supset \big(\neg\mathsf{A} \supset \neg\forall \mathtt{x}(\neg\mathsf{A})\big)$ (A1);
   3. $\neg\forall \mathtt{x}(\neg\mathsf{A})$ (гипотеза);
   4. $\neg\mathsf{A} \supset \neg\forall \mathtt{x}(\neg\mathsf{A})$ (из 3, 2 по MP);
   5. $\big(\neg\mathsf{A} \supset \forall \mathtt{x}(\neg\mathsf{A})\big) \supset \mathsf{A}$ (из 5, 1 по MP);
   6. $\neg\mathsf{A} \supset \forall \mathtt{x}(\neg\mathsf{A})$ (доказанный п.1: ясно, что если $\mathtt{x}$ не свободна в A, то $\mathtt{x}$ не свободна и в $\neg\mathsf{A}$);
   7. A (из 6, 5 по MP).

   Ясно, что поскольку $\mathtt{x}$ не является свободной переменной в A, то в данной ситуации также можно применить теорему дедукции и получить требуемое: $\neg\forall \mathtt{x}(\neg\mathsf{A}) \supset \mathsf{A}$, то есть $\exists \mathtt{x}\mathsf{A} \supset \mathsf{A}$.

3) $\forall \mathtt{x}(\mathsf{A} \supset \mathsf{B}) \supset (\mathsf{A} \supset \forall \mathtt{x}\mathsf{B})$ — аксиома A5, поскольку $\mathtt{x}$ не свободна в A. Докажем вспомогательную выводимость $\mathsf{A} \supset \forall \mathtt{x}\mathsf{B}, \mathsf{A} \vdash \mathsf{B}$:

   1. $\mathsf{A} \supset \forall \mathtt{x}\mathsf{B}$ (гипотеза);
   2. A (гипотеза);
   3. $\forall \mathtt{x}\mathsf{B}$ (из 2, 1 по MP);
   4. $\forall \mathtt{x}\mathsf{B} \supset \mathsf{B}$ (A4, её использование законно, так как терм $\mathtt{t} = \mathtt{x}$ свободен для $\mathtt{x}$ в любой формуле);
   5. B (из 3, 4 по MP).

Так как в выводе выше ни разу не было использовано правило Gen, можно применить теорему дедукции и получить $A \supset \forall x B \vdash A \supset B$. По правилу Gen получаем, что $A \supset B \vdash \forall x(A \supset B)$, а значит по правилу сечения справедливо $A \supset \forall x B \vdash \forall x(A \supset B)$.
Ясно, исходя из предыдущих выводов и доказательства теоремы дедукции, что существует вывод $A \supset \forall x B \vdash \forall x(A \supset B)$, в котором правило Gen применяется только к переменной x, которая, во-первых, не свободна в A, во-вторых, не свободна в $\forall x B$, откуда x не свободна и в $A \supset \forall x B$, а значит мы снова имеем право применить теорему дедукции и получить желанное $\vdash (A \supset \forall x B) \supset \forall x(A \supset B)$.
Наконец, используя правило конъюнкции, доказываемое чуть дальше, и правило сечения, получаем, что

$$\vdash \big(\forall x(A \supset B) \supset (A \supset \forall x B)\big) \wedge \big((A \supset \forall x B) \supset \forall x(A \supset B)\big),$$

что равносильно искомому $\vdash \forall x(A \supset B) \equiv (A \supset \forall x B)$.

4) `ToDo...`

■

Правило существования (контрапозиция правила индивидуализации): если терм t свободен для x в $A(x)$, то $\vdash A(t) \supset \exists x A(x)$ и, следовательно, $A(t) \vdash \exists x A(x)$.

Доказательство. Формула $A(t) \supset \exists x A(x)$ является сокращением записи $A(t) \supset \neg\forall x\big(\neg A(x)\big)$. Предъявим вывод этой формулы:

1. $\forall x\big(\neg A(x)\big) \supset \neg A(t)$ (A4, её использование правомерно, так как терм t свободен для x в $A(x)$, а значит и в $\neg A(x)$);
2. $(\mathcal{A} \supset \neg\mathcal{B}) \supset (\mathcal{B} \supset \neg\mathcal{A})$ (теорема, являющаяся частным случаем тавтологии по лемме 3.1);
3. $A(t) \supset \neg\forall x\big(\neg A(x)\big)$ (из 1, 2 по MP, полагая $\mathcal{A} \leftrightharpoons \forall x\big(\neg A(x)\big)$ и $\mathcal{B} \leftrightharpoons A(t)$).

Так как доказано $A(t) \supset \exists x A(x)$, легко доказать и $A(t) \vdash \exists x A(x)$:

1. $A(t)$ (гипотеза);
2. $A(t) \supset \exists x A(x)$ (выведенная теорема);
3. $\exists x A(x)$ (из 1, 2 по MP).

■

Правило конъюнкции: $A, B \vdash A \wedge B$.

Доказательство. Вспомним, что $A \wedge B$ — сокращение записи $\neg(A \supset \neg B)$. Тем самым, требуется доказать выводимость $A, B \vdash \neg(A \supset \neg B)$. Доказательство имеет вид:

1. A (гипотеза);
2. B (гипотеза);
3. $A \supset \big(B \supset \neg(A \supset \neg B)\big)$ (тавтология, являющаяся теоремой по лемме 3.1);
4. $B \supset \neg(A \supset \neg B)$ (из 1, 3 по MP);
5. $\neg(A \supset \neg B)$ (из 2, 4 по MP).

■

Лемма 6.2. Для любых формул A и B справедливо $\vdash \forall x(A \equiv B) \supset (\forall x A \equiv \forall x B)$.

Доказательство. Вывод $\forall x(A \equiv B), \forall x A \vdash \forall x B$:

1. $\forall x(A \equiv B)$ (гипотеза);
2. $\forall x A$ (гипотеза);

3. $A \equiv B$ (из 1 по правилу индивидуализации, поскольку терм $t = x$ свободен относительно x в любой формуле);
4. A (из 2 по правилу индивидуализации);
5. $(A \equiv B) \supset (A \supset B)$ (тавтология, являющаяся теоремой согласно лемме 3.1);
6. $A \supset B$ (из 3, 5 по MP);
7. B (из 4, 6 по MP);
8. $\forall x B$ (из 7 по Gen).

Далее по теореме дедукции $\forall x(A \equiv B) \vdash \forall x A \supset \forall x B$. Аналогично доказывается $\forall x(A \equiv B) \vdash \forall x B \supset \forall x A$. По правилу конъюнкции и правилу сечения получаем $\forall x(A \equiv B) \vdash \forall x A \equiv \forall x B$. Теперь по теореме дедукции приходим к доказываемому утверждению. ■

6.2. Теорема эквивалентности

Теорема 6.1 (*теорема эквивалентности*)**.** Если B есть подформула A и A' есть результат замены каких-либо (может быть, ни одного) вхождений B формулой C и если всякая свободная переменная формулы B или C, являющаяся одновременно связанной переменной формулы A, встречается в списке $y_1, y_2, \ldots, y_k$, то

$$\vdash \forall y_1 \forall y_2 \ldots \forall y_k (B \equiv C) \supset (A \equiv A').$$

Доказательство. Рассмотрим тривиальные случаи:

- Пусть ни одно вхождение B не заменяется на C. Тогда A' просто совпадает с A. Требуется в таком случае доказать, что
$$\vdash \forall y_1 \forall y_2 \ldots \forall y_k (B \equiv C) \supset (A \equiv A).$$
Упомянутая теорема имеет вид $D \supset (A \equiv A)$, где $D \leftrightharpoons \forall y_1 \forall y_2 \ldots \forall y_k (B \equiv C)$. Ясно, что это тавтология, откуда по лемме 3.1 она является теоремой ИП.
- Пусть теперь B совпадает с A и это единственное вхождение заменяется на C. Тогда надо доказать
$$\vdash \forall y_1 \forall y_2 \ldots \forall y_k (B \equiv C) \supset (B \equiv C).$$
Это следует из более общего утверждения: $\vdash \forall y_1 \forall y_2 \ldots \forall y_k \mathcal{A} \supset \mathcal{A}$, следующего, в свою очередь, по индукции из правила индивидуализации. Взяв вместо $\mathcal{A}$ формулу $B \equiv C$, получаем требуемое.

Далее считаем, что хотя бы одно вхождение B заменяется, и B не совпадает с A (то есть B — собственная подформула A).

Доказательство проведём индукцией по числу связок и кванторов в формуле A.

База: в A одна связка или один квантор. Имеются варианты:

- В A всего один квантор всеобщности. Иными словами, A имеет вид $\forall x P$, где P — элементарная формула. Единственная собственная подформула A, как легко видеть, есть P, а значит P совпадает с B. Следовательно, A' имеет вид $\forall x C$. Тогда нужно доказать $\vdash \forall y_1 \forall y_2 \ldots \forall y_k (B \equiv C) \supset (\forall x B \equiv \forall x C)$.
Ясно, что поскольку x является связанной переменной в A, то она входит в список $y_1, y_2, \ldots, y_k$. Пусть x есть y_i. В таком случае от нас требуется доказать, что
$$\vdash \forall y_1 \forall y_2 \ldots \forall y_k (B \equiv C) \supset (\forall y_i B \equiv \forall y_i C). \tag{1}$$
Многократно используя доказанное в §4. утверждение $\forall x \forall y A(x, y) \vdash \forall y \forall x A(x, y)$, мы можем получить (1) из выводимости
$$\vdash \forall y_1 \forall y_2 \ldots \forall y_{i-1} \forall y_{i+1} \ldots \forall y_k \forall y_i (B \equiv C) \supset (\forall y_i B \equiv \forall y_i C). \tag{2}$$
Согласно лемме 6.2, справедливо $\vdash \forall y_i (B \equiv C) \supset (\forall y_i B \equiv \forall y_i C)$, а значит имеет место
$$\forall y_i (B \equiv C) \vdash \forall y_i B \equiv \forall y_i C. \tag{3}$$
Согласно уже упомянутому обобщённому правилу индивидуализации, имеем
$$\forall y_1 \forall y_2 \ldots \forall y_{i-1} \forall y_{i+1} \ldots \forall y_k \forall y_i (B \equiv C) \vdash \forall y_i (B \equiv C). \tag{4}$$
Тогда по правилу сечения из (3) и (4) получаем $\forall y_1 \forall y_2 \ldots \forall y_{i-1} \forall y_{i+1} \ldots \forall y_k \forall y_i (B \equiv C) \vdash \forall y_i B \equiv \forall y_i C$. Из полученной выводимости по теореме дедукции получаем (2), а из (2), как было уже замечено, получаем искомое (1). Законность применения теоремы дедукции здесь обусловлена тем, при выводе правило Gen применялось только к переменным $y_1, y_2, \ldots, y_k$, которые, с одной стороны, не свободны в A, и, с другой стороны, не свободны в $\forall y_1 \forall y_2 \ldots \forall y_{i-1} \forall y_{i+1} \ldots \forall y_k \forall y_i (B \equiv C)$.

- В A есть одна связка и только она, то есть A имеет вид $\neg\mathsf{P}$ или $\mathsf{P}\supset\mathsf{Q}$, где P,Q — элементарные формулы. Рассмотрим два этих подслучая отдельно:
  - A имеет вид $\neg\mathsf{P}$, тогда P совпадает с B, а A' есть $\neg\mathsf{C}$. Фактически требуется доказать, что
  $$\vdash \forall \mathsf{y}_1\forall \mathsf{y}_2\ldots\forall \mathsf{y}_\mathsf{k}(\mathsf{B}\equiv\mathsf{C})\supset(\neg\mathsf{B}\equiv\neg\mathsf{C}). \tag{5}$$
  Применяя обобщённое правило индивидуализации, получаем, что
  $$\forall \mathsf{y}_1\forall \mathsf{y}_2\ldots\forall \mathsf{y}_\mathsf{k}(\mathsf{B}\equiv\mathsf{C})\vdash \mathsf{B}\equiv\mathsf{C}. \tag{6}$$
  Записав далее очевидную тавтологию $(\mathsf{B}\equiv\mathsf{C})\supset(\neg\mathsf{B}\equiv\neg\mathsf{C})$, из которой вытекает $\mathsf{B}\equiv\mathsf{C}\vdash\neg\mathsf{B}\equiv\neg\mathsf{C}$, по правилу сечения из (6) и последовавшей из написанной тавтологии выводимости получаем, что
  $$\forall \mathsf{y}_1\forall \mathsf{y}_2\ldots\forall \mathsf{y}_\mathsf{k}(\mathsf{B}\equiv\mathsf{C})\vdash \neg\mathsf{B}\equiv\neg\mathsf{C}. \tag{7}$$
  Желанное (5) вытекает из (7) по теореме дедукции (правомерность её использования такая же, как в случае, когда A имеет вид $\forall\mathsf{x}\mathsf{P}$).
  - A имеет вид $\mathsf{P}\supset\mathsf{Q}$, где либо P совпадает с B, либо Q совпадает с B, либо выполнено и то, и другое. Доказательство для этого подслучая такое же, как для предудщего подслучая, только в качестве тавтологий нужно рассмотреть соответственно $(\mathsf{B}\equiv\mathsf{C})\supset\big((\mathsf{B}\supset\mathsf{Q})\equiv(\mathsf{C}\supset\mathsf{Q})\big)$, $(\mathsf{B}\equiv\mathsf{C})\supset\big((\mathsf{P}\supset\mathsf{B})\equiv(\mathsf{P}\supset\mathsf{C})\big)$ и $(\mathsf{B}\equiv\mathsf{C})\supset\big((\mathsf{B}\supset\mathsf{B})\equiv(\mathsf{C}\supset\mathsf{C})\big)$.

Тем самым, проверена база индукции.

Предположение индукции: пусть теорема верна для любой формулы с меньшим числом связок и кванторов, чем в A.

Шаг индукции: докажем утверждение для A. Ясно, что A не может быть атомарной формулой, поскольку тогда A не имела бы собственных подформул, среди которых по нашему предположению есть B. В таком случае имеются следующие варианты:

- A есть $\neg\mathsf{P}$. Тогда A' есть $\neg\mathsf{P}'$, где P' — результат подстановки в P некоторого числа (как минимум одной) формул C вместо вхождений подформулы B. Ясно, что в P содержится меньше связок и кванторов, чем в A, тогда для P применимо индукционное предположение:
  $$\vdash \forall \mathsf{y}_1\forall \mathsf{y}_2\ldots\forall \mathsf{y}_\mathsf{k}(\mathsf{B}\equiv\mathsf{C})\supset(\mathsf{P}\equiv\mathsf{P}')\Longrightarrow\forall \mathsf{y}_1\forall \mathsf{y}_2\ldots\forall \mathsf{y}_\mathsf{k}(\mathsf{B}\equiv\mathsf{C})\vdash\mathsf{P}\equiv\mathsf{P}'. \tag{8}$$
  Имея в виду тавтологию
  $$(\mathcal{A}\equiv\mathcal{B})\supset(\neg\mathcal{A}\equiv\neg\mathcal{B}),$$
  являющуюся теоремой согласно лемме 3.1, можем получить следующее:
  $$\vdash(\mathsf{P}\equiv\mathsf{P}')\supset(\neg\mathsf{P}\equiv\neg\mathsf{P}')\Longrightarrow\ \mathsf{P}\equiv\mathsf{P}'\vdash\neg\mathsf{P}\equiv\neg\mathsf{P}'. \tag{9}$$
  Из (1) и (2) по правилу сечения можно заключить, что
  $$\forall \mathsf{y}_1\forall \mathsf{y}_2\ldots\forall \mathsf{y}_\mathsf{k}(\mathsf{B}\equiv\mathsf{C})\vdash\neg\mathsf{P}\equiv\neg\mathsf{P}'\Longleftrightarrow\forall \mathsf{y}_1\forall \mathsf{y}_2\ldots\forall \mathsf{y}_\mathsf{k}(\mathsf{B}\equiv\mathsf{C})\vdash\mathsf{A}\equiv\mathsf{A}'.$$
  Искомая выводимость получается из предыдущей примененим теоремы дедукции:
  $$\vdash\forall \mathsf{y}_1\forall \mathsf{y}_2\ldots\forall \mathsf{y}_\mathsf{k}(\mathsf{B}\equiv\mathsf{C})\supset(\mathsf{A}\equiv\mathsf{A}').$$
  Правомерность применения теоремы дедукции обосновывается тем, что, согласно нашему доказательству, правило Gen использовалось только к переменным из списка $\mathsf{y}_1,\mathsf{y}_2,\ldots,\mathsf{y}_\mathsf{k}$ (свободные переменные $\mathsf{B}\equiv\mathsf{C}$), а они, как видно в выводимости выше, уже связаны кванторами.
- A есть $\mathsf{P}\supset\mathsf{Q}$. Тогда A' имеет вид $\mathsf{P}'\supset\mathsf{Q}'$, где P',Q' — результаты замены некоторых (как минимум одного) вхождений B на C в P и Q соответственно. Ясно, что в P и Q меньше связок и кванторов, чем в A. Тогда для этих формул применимо предположение индукции:
  $$\begin{cases}\vdash\forall \mathsf{y}_1\forall \mathsf{y}_2\ldots\forall \mathsf{y}_\mathsf{k}(\mathsf{B}\equiv\mathsf{C})\supset(\mathsf{P}\equiv\mathsf{P}')\Longrightarrow\forall \mathsf{y}_1\forall \mathsf{y}_2\ldots\forall \mathsf{y}_\mathsf{k}(\mathsf{B}\equiv\mathsf{C})\vdash\mathsf{P}\equiv\mathsf{P}',\\ \vdash\forall \mathsf{y}_1\forall \mathsf{y}_2\ldots\forall \mathsf{y}_\mathsf{k}(\mathsf{B}\equiv\mathsf{C})\supset(\mathsf{Q}\equiv\mathsf{Q}')\Longrightarrow\forall \mathsf{y}_1\forall \mathsf{y}_2\ldots\forall \mathsf{y}_\mathsf{k}(\mathsf{B}\equiv\mathsf{C})\vdash\mathsf{Q}\equiv\mathsf{Q}'.\end{cases} \tag{10}$$
  Запишем следующую тавтологию:
  $$(\mathcal{A}\equiv\mathcal{B})\wedge(\mathcal{C}\equiv\mathcal{D})\supset\big((\mathcal{A}\supset\mathcal{C})\equiv(\mathcal{B}\supset\mathcal{D})\big).$$

Пользуясь этой тавтологией и леммой 3.1, получаем следующее:

$$\vdash (P \equiv P') \wedge (Q \equiv Q') \supset \big((P \supset Q) \equiv (P' \supset Q')\big) \Longrightarrow (P \equiv P') \wedge (Q \equiv Q') \vdash (P \supset Q) \equiv (P' \supset Q'). \tag{11}$$

Теперь по правилу конъюнкции из (3) получаем выводимость:

$$\forall y_1 \forall y_2 \dots \forall y_k (B \equiv C) \vdash (P \equiv P') \wedge (Q \equiv Q'). \tag{12}$$

Далее из (5) и (4) и правила сечения заключаем

$$\forall y_1 \forall y_2 \dots \forall y_k (B \equiv C) \vdash (P \supset Q) \equiv (P' \supset Q') \Longleftrightarrow \forall y_1 \forall y_2 \dots \forall y_k (B \equiv C) \vdash A \equiv A'.$$

Теорема дедукции, применённая к полученной выше выводимости, даёт нужное утверждение. Правомерность применения теоремы дедукции обосновывается так же, как в предыдущем пункте.

- A имеет вид $\forall x_i P$. Тогда A' есть $\forall x_i P'$, где P' — результат замены некоторых вхождений B на C в формуле P. Ясно, что в P на один квантор меньше, чем в A, значит для P справедливо индукционное предположение:

$$\vdash \forall y_1 \forall y_2 \dots \forall y_k (B \equiv C) \supset (P \equiv P') \Longrightarrow \forall y_1 \forall y_2 \dots \forall y_k (B \equiv C) \vdash P \equiv P'. \tag{13}$$

Требуется показать, что

$$\vdash \forall y_1 \forall y_2 \dots \forall y_k (B \equiv C) \supset (\forall x_i P \equiv \forall x_i P').$$

Отметим, что переменная x_i не встречается свободно в $\forall y_1 \forall y_2 \dots \forall y_k (B \equiv C)$. Если бы она входила свободно в эту формулу, то она была бы свободной переменной B или C, но x_i одновременно с этим является связанной переменной в формуле A, а значит x_i входит в список $y_1, y_2, \dots, y_k$, согласно условию теоремы. Это значит, что она была бы связана в $\forall y_1 \forall y_2 \dots \forall y_k (B \equiv C)$.
Далее по правилу Gen $P \equiv P' \vdash \forall x_i (P \equiv P')$, что из леммы 6.2, правила сечения и (6) даёт

$$\forall y_1 \forall y_2 \dots \forall y_k (B \equiv C) \vdash \forall x_i P \equiv \forall x_i P' \Longleftrightarrow \forall y_1 \forall y_2 \dots \forall y_k (B \equiv C) \vdash A \equiv A'.$$

Поскольку правило обобщения здесь применялось к x_i, которая не является свободной в $\forall y_1 \forall y_2 \dots \forall y_k (B \equiv C)$, то можно применить теорему дедукции и заключить желаемое:

$$\vdash \forall y_1 \forall y_2 \dots \forall y_k (B \equiv C) \supset (A \equiv A').$$

Итак, все случаи разобраны, а значит индукционный шаг доказан. Тем самым, индукцией по числу связок и кванторов в формуле A доказана требуемая теорема. ■

Следствие 1 (*теорема о замене*)**.** Пусть формулы A, B, C и A' удовлетворяют условию теоремы эквивалентности. Тогда:

1. Если $\vdash B \equiv C$, то $\vdash A \equiv A'$.
2. Если $\vdash B \equiv C$ и $\vdash A$, то $\vdash A'$.

Определение. Формулы $A(x_i)$ и $A(x_j)$ (переменные x_i и x_j не совпадают, $A(x_j)$ получается из $A(x_i)$ подстановкой x_j вместо всех свободных вхождений x_i) называются *подобными*, если x_j свободна для x_i в $A(x_i)$ и $A(x_i)$ не имеет свободных вхождений x_j.

Если $A(x_i)$ и $A(x_j)$ подобны, то x_i свободна для x_j в $A(x_j)$, и $A(x_j)$ не имеет свободных вхождений x_i. Таким образом, подобие формул симметрично. Следовательно, $A(x_i)$ и $A(x_j)$ подобны тогда и только тогда, когда $A(x_j)$ имеет свободные вхождения x_j в точности в тех местах, в которых $A(x_i)$ имеет свободные вхождения x_i.

Лемма 6.3. Если формулы $A(x_i)$ и $A(x_j)$ подобны, то $\vdash \forall x_i A(x_i) \equiv \forall x_j A(x_j)$.

Следствие 2 (*переименование связанных переменных*)**.** Если $\forall x B(x)$ есть подформула формулы A, формула $B(y)$ подобна $B(x)$ и A' есть результат замены по крайней мере одного вхождения $\forall x B(x)$ в A на $\forall y B(y)$, то $\vdash A \equiv A'$.

6.3. Правило C

Пусть надо доказать $\exists x\big(B(x) \supset C(x)\big), \forall x B(x) \vdash \exists x C(x)$.
Интуитивное доказательство:

1. $\exists x\big(B(x) \supset C(x)\big)$ (гипотеза);
2. $\forall x B(x)$ (гипотеза);

3. $B(a) \supset C(a)$ (из 1, выбор некоторого a);
4. $B(a)$ (из 2, по правилу индивидуализации, терм $t = a$ свободен для любой переменной в любой формуле);
5. $C(a)$ (из 4, 3 по MP);
6. $\exists x C(x)$ (из 5 по правилу существования).

Можно то же самое доказать **без произвольного выбора** элемента на шаге 3.
Построим вывод $\forall x B(x), \forall x \neg C(x) \vdash \forall x \neg\big(B(x) \supset C(x)\big)$:

1. $\forall x B(x)$ (гипотеза);
2. $\forall x \neg C(x)$ (гипотезы);
3. $B(x)$ (из 1 по правилу индивидуализации);
4. $\neg C(x)$ (из 2 по правилу индивидуализации);
5. $B(x) \wedge \neg C(x)$ (из 3, 4 по правилу конъюнкции);
6. $B(x) \wedge \neg C(x) \supset \neg\big(B(x) \supset C(x)\big)$ (частный случай тавтологии $\mathcal{A} \wedge \neg\mathcal{B} \supset \neg(\mathcal{A} \supset \mathcal{B})$);
7. $\neg\big(B(x) \supset C(x)\big)$ (из 5, 6 по MP);
8. $\forall x \neg\big(B(x) \supset C(x)\big)$ (из 7 по Gen).

По теореме дедукции получаем

$$\forall x B(x) \vdash \forall x \neg C(x) \supset \forall x \neg\big(B(x) \supset C(x)\big).$$

Отсюда с помощью тавтологии $(\mathcal{A} \supset \mathcal{B}) \supset (\neg\mathcal{B} \supset \neg\mathcal{A})$ по правилу MP имеем

$$\forall x B(x) \vdash \exists x\big(B(x) \supset C(x)\big) \supset \exists x C(x).$$

Отсюда можно получить

$$\exists x\big(B(x) \supset C(x)\big), \forall x B(x) \vdash \exists x C(x).$$

Правило C (choice) позволяет переходить от $\exists x A(x)$ к $A(a)$.

Вывод с применением правила C.
$\Gamma \vdash_C A$ тогда и только тогда, когда существует вывод $B_1, B_2, \ldots, B_n$ формулы A, в котором:

1. Для любого i формула B_i есть либо аксиома, либо гипотеза из Γ, либо непосредственное следствие по MP или Gen из каких-либо предшествующих формул, либо $C(b)$, где b — новая предметная константа, и формуле B_i предшествует формула $\exists x C(x)$ (правило C).
2. В качестве аксиом в 1 допускаются также всевозможные логические аксиомы с новыми предметными константами, уже введёнными ранее по правилу C.
3. Не допускается применение правила Gen по переменным, свободным хотя бы в одной формуле вида $\exists x C(x)$, к которой ранее было применено правило C.
4. Формула A не содержит новых предметных констант, введённых с помощью правила C.

Пример вывода с применением правила C без п.3:

$$\forall x \exists y A_1^2(x, y) \vdash_C \exists y \forall x A_1^2(x, y) :$$

1. $\forall x \exists y A_1^2(x, y)$ (гипотеза);
2. $\exists y A_1^2(x, y)$ (из 1 по индивидуализации);
3. $A_1^2(x, b)$ (из 2 по правилу C);
4. $\forall x A_1^2(x, b)$ (из 3 по правилу Gen);
5. $\exists y \forall x A_1^2(x, y)$ (из 4 по правилу существования).

Между тем, данная выводимость не является верной: достаточно рассмотреть интерпретацию с областью $D = \mathbb{R}$ и $A_1^2(x, y) \iff x < y$.

Теорема 6.2. Если $\Gamma \vdash_C A$, то $\Gamma \vdash A$.

Доказательство. Пусть $\exists y_1 C_1(y_1), \ldots, \exists y_k C_k(y_k)$ — формулы (в порядке появления) в выводе $\Gamma \vdash_C A$, к которым применено правило C, а $a_1, a_2, \ldots, a_k$ — вводимые при этом новые предметные константы. Тогда

$$\Gamma, C_1(a_1), C_2(a_2), \ldots, C_k(a_k) \vdash A.$$

Применим теорему дедукции (что законно в силу п.3 в выводе с примененим правила C), получив в результате

$$\Gamma, C_1(a_1), C_2(a_2), \ldots, C_{k-1}(a_{k-1}) \vdash C_k(a_k) \supset A.$$

Заменим в полученном выводе все вхождения константы a_k на переменную z, не встречающуюся в этом выводе, и получим

$$\Gamma, C_1(a_1), C_2(a_2), \ldots, C_{k-1}(a_{k-1}) \vdash C_k(z) \supset A.$$

К полученному выводу применим правило обобщения и заключим

$$\Gamma, C_1(a_1), C_2(a_2), \ldots, C_{k-1}(a_{k-1}) \vdash \forall z\big(C_k(z) \supset A\big).$$

Из леммы 6.1 (п.4) вытекает следующее: $\forall x(B \supset A) \vdash \exists x B \supset A$. Из этого заключаем, что

$$\Gamma, C_1(a_1), C_2(a_2), \ldots, C_{k-1}(a_{k-1}) \vdash \exists z C_k(z) \supset A$$

Далее применяя правило переименования связанных переменных, получаем

$$\Gamma, C_1(a_1), C_2(a_2), \ldots, C_{k-1}(a_{k-1}) \vdash \exists y_k C_k(y_k) \supset A.$$

Затем учтём, что поскольку формула $\exists y_k C_k(y_k)$ уже встречалась в выводе, то

$$\Gamma, C_1(a_1), C_2(a_2), \ldots, C_{k-1}(a_{k-1}) \vdash \exists y_k C_k(y_k),$$

тогда по правилу MP и правилу сечения получаем

$$\Gamma, C_1(a_1), C_2(a_2), \ldots, C_{k-1}(a_{k-1}) \vdash A.$$

По аналогии избавляемся от $C_{k-1}(a_{k-1}), C_{k-2}(a_{k-2}), \ldots, C_1(a_1)$ и получаем требуемую выводимость: $\Gamma \vdash A$. ■

Пример: $\vdash \forall x\big(A(x) \supset B(x)\big) \supset \big(\exists x A(x) \supset \exists x B(x)\big)$.
Вывод $\forall x\big(A(x) \supset B(x)\big), \exists x A(x) \vdash_C \exists x B(x)$:

1. $\forall x\big(A(x) \supset B(x)\big)$ (гипотеза);
2. $\exists x A(x)$ (гипотеза);
3. $A(b)$ (из 2 по правилу C);
4. $A(b) \supset B(b)$ (из 1 по правилу индивидуализации);
5. $B(b)$ (из 3, 4 по MP);
6. $\exists x B(x)$ (из 5 по правилу существования).

Тогда по теореме 6.2 имеет место

$$\forall x\big(A(x) \supset B(x)\big), \exists x A(x) \vdash \exists x B(x).$$

Дважды применяя теорему дедукции, получаем требуемое:

$$\vdash \forall x\big(A(x) \supset B(x)\big) \supset \big(\exists x A(x) \supset \exists x B(x)\big).$$

§7. Теории первого порядка с равенством

Пусть K — теория первого порядка с предикатной буквой A_1^2:

$$A_1^2(x_1, x_2) \Longleftrightarrow x_1 = x_2, \quad \neg A_1^2(x_1, x_2) \Longleftrightarrow x_1 \neq x_2.$$

Определение. Теория K называется *теорией первого порядка с равенством*, если следующие формулы являются её теоремами (если точнее, дополнительными аксиомами):

A. $\forall x_1(x_1 = x_1)$ (рефлексивность равенства);

B. $x_1 = x_2 \supset \big(A(x_1, x_1) \supset A(x_1, x_2)\big)$ (подстановочность равенства), где x_1, x_2 — предметные переменные, $A(x_1, x_1)$ — произвольная формула, а $A(x_1, x_2)$ получается из $A(x_1, x_1)$ заменой некоторых (не обязательно всех, может быть, вообще ни одного) свободных вхождений x_1 переменной x_2, при этом x_2 свободно для заменяемых вхождений x_1.

Лемма 7.1. Во всякой теории первого порядка с равенством:

1) $\vdash t = t$, где t — произвольный терм;

2) $\vdash x_1 = x_2 \supset x_2 = x_1$;

3) $\vdash x_1 = x_2 \supset (x_2 = x_3 \supset x_1 = x_3)$.

Доказательство.

1) 1. $\forall x_1(x_1 = x_1)$ (рефлексивность равенства);
   2. $t = t$ (из 1 по правилу индивидуализации, любой терм t свободен для x_1 в элементарной формуле $x_1 = x_1$).

2) 1. $x_1 = x_1$ (доказанный п.1);
   2. $x_1 = x_2 \supset (x_1 = x_1 \supset x_2 = x_1)$ (подстановочность равенства с $A(x_1, x_1) \leftrightharpoons x_1 = x_1$ и $A(x_1, x_2) \leftrightharpoons x_2 = x_1$);
   3. $x_1 = x_1 \supset \Big(\big(x_1 = x_2 \supset (x_1 = x_1 \supset x_2 = x_1)\big) \supset \big(x_1 = x_2 \supset x_2 = x_1\big)\Big)$ (теорема, частный случай тавтологии $\mathcal{B} \supset \Big(\big(\mathcal{A} \supset (\mathcal{B} \supset \mathcal{C})\big) \supset \big(\mathcal{A} \supset \mathcal{C}\big)\Big)$)
   4. $\big(x_1 = x_2 \supset (x_1 = x_1 \supset x_2 = x_1)\big) \supset \big(x_1 = x_2 \supset x_2 = x_1\big)$ (из 1, 3 по MP);
   5. $x_1 = x_2 \supset x_2 = x_1$ (из 2, 4 по MP).

3) 1. $x_2 = x_1 \supset (x_2 = x_3 \supset x_1 = x_3)$ (подстановочность равенства с $A(x_2, x_2) \leftrightharpoons x_2 = x_3$ и $A(x_2, x_1) \leftrightharpoons x_1 = x_3$);
   2. $x_1 = x_2 \supset x_2 = x_1$ (симметричность равенства, доказанный п.2);
   3. $(x_1 = x_2 \supset x_2 = x_1) \supset \Big(\big(x_2 = x_1 \supset (x_2 = x_3 \supset x_1 = x_3)\big) \supset \big(x_1 = x_2 \supset (x_2 = x_3 \supset x_1 = x_3)\big)\Big)$ (теорема, частный случай тавтологии $(\mathcal{A} \supset \mathcal{B}) \supset \big((\mathcal{B} \supset \mathcal{C}) \supset (\mathcal{A} \supset \mathcal{C})\big)$);
   4. $\big(x_2 = x_1 \supset (x_2 = x_3 \supset x_1 = x_3)\big) \supset \big(x_1 = x_2 \supset (x_2 = x_3 \supset x_1 = x_3)\big)$ (из 2, 3 по MP);
   5. $x_1 = x_2 \supset (x_2 = x_3 \supset x_1 = x_3)$ (из 1, 4 по MP).

■

Упрощение условия для подстановочности равенства даёт следующее утверждение.

Лемма 7.2. Если теоремами теории первого порядка K является формула (A) и (B) для любой элементарной формулы A, то K есть теория первого порядка с равенством, то есть в K всякая формула (B) является теоремой.

Доказательство. Если A — элементарная формула, то доказывать нечего, (B) является теоремой по условию леммы. Пусть теперь A не является элементарной формулой. Доказываем лемму по индукции по n, где n — число связок и кванторов в A.

База: $n = 1$. Тогда формула A имеет один из трёх видов: $\forall x_i P$, $P \supset Q$ и $\neg P$, где P, Q — элементарные формулы. Доказательство для этих случаев такое же, как в индукционном шаге.

Индукционное предположение: пусть доказываемое нами утверждение верно для всех $k < n$.

Индукционный шаг: докажем утверждение для случая числа связок и кванторов, равного n. Имеют место три случая: A есть $P \supset Q$ или A есть $\neg P$, или A есть $\forall x_i P$, где P, Q — формулы с меньшим числом связок и кванторов, чем в A. Рассмотрим детально эти случаи:

1. $\underline{A(x_1, x_1) \leftrightharpoons \neg P(x_1, x_1)}$. Далее через $P(x_1, x_1)$ будем обозначать результат замены некоторых (необязательно всех) свободных вхождений x_2 в P на x_1. Для $P(x_1, x_1)$ верно индукционное предположение:

$$\vdash x_2 = x_1 \supset \big(P(x_1, x_2) \supset P(x_1, x_1)\big) \tag{1}$$

   Воспользуемся теоремой, являющейся частным случаем тавтологии: $\vdash \big(P(x_1, x_2) \supset P(x_1, x_1)\big) \supset \big(\neg P(x_1, x_1) \supset \neg P(x_1, x_2)\big)$ (формула контрапозиции). Применяя доказанную в лемме 7.1 (п.2) теорему $\vdash x_1 = x_2 \supset x_2 = x_1$, транзитивность импликации и выписанную контрапозицию, из (1) выводим требуемое:

$$\vdash x_1 = x_2 \supset \big(\neg P(x_1, x_1) \supset \neg P(x_1, x_2)\big) \Longleftrightarrow \vdash x_1 = x_2 \supset \big(A(x_1, x_1) \supset A(x_1, x_2)\big).$$

2. $\underline{A(x_1,x_1) \leftrightharpoons P(x_1,x_1) \supset Q(x_1,x_1)}$. Снова для P и Q верно индукционное предположение:

$$\vdash x_2 = x_1 \supset \big(P(x_1,x_2) \supset P(x_1,x_1)\big), \quad \vdash x_1 = x_2 \supset \big(Q(x_1,x_1) \supset Q(x_1,x_2)\big). \tag{2}$$

Применяя теорему $\vdash x_1 = x_2 \supset x_2 = x_1$ из первой выводимости в (2) получаем

$$\vdash x_1 = x_2 \supset \big(P(x_1,x_2) \supset P(x_1,x_1)\big). \tag{3}$$

Воспользуемся тавтологией:

$$\big(\mathcal{A} \supset (\mathcal{B}_1 \supset \mathcal{B})\big) \supset \Big(\big(\mathcal{A} \supset (\mathcal{C} \supset \mathcal{C}_1)\big) \supset \Big(\mathcal{A} \supset \big((\mathcal{B} \supset \mathcal{C}) \supset (\mathcal{B}_1 \supset \mathcal{C}_1)\big)\Big)\Big) \tag{4}$$

Запишем теорему, являющуюся частным случаем записанной тавтологии (4) ($\mathcal{A} \leftrightharpoons x_1 = x_2$, $\mathcal{B}_1 \leftrightharpoons P(x_1,x_2)$, $\mathcal{B} \leftrightharpoons P(x_1,x_1)$, $\mathcal{C}_1 \leftrightharpoons Q(x_1,x_2)$, $\mathcal{C} \leftrightharpoons Q(x_1,x_1)$):

$$\Big(x_1 = x_2 \supset \big(P(x_1,x_2) \supset P(x_1,x_1)\big)\Big) \supset \Bigg(\Big(x_1 = x_2 \supset \big(Q(x_1,x_1) \supset Q(x_1,x_2)\big)\Big) \supset \\ \supset \Big(x_1 = x_2 \supset \big(\big(P(x_1,x_1) \supset Q(x_1,x_1)\big) \supset \big(P(x_1,x_2) \supset Q(x_1,x_2)\big)\big)\Big)\Bigg) \tag{5}$$

Дважды применяя MP ((3) и (5), а затем вторая выводимость в (2) и результат предыдущего MP), получаем искомое

$$\vdash x_1 = x_2 \supset \big(\big(P(x_1,x_1) \supset Q(x_1,x_1)\big) \supset \big(P(x_1,x_2) \supset Q(x_1,x_2)\big)\big) \Longleftrightarrow \vdash x_1 = x_2 \supset \big(A(x_1,x_1) \supset A(x_1,x_2)\big).$$

3. $\underline{A(x_1,x_1) \text{ есть } \forall x_i P(x_1,x_1,x_i)}$. Для P верно индукционное предположение:

$$\vdash x_1 = x_2 \supset \big(P(x_1,x_1,x_i) \supset P(x_1,x_2,x_i)\big).$$

Применяем правило Gen:

$$\vdash \forall x_i \Big(x_1 = x_2 \supset \big(P(x_1,x_1,x_i) \supset P(x_1,x_2,x_i)\big)\Big). \tag{6}$$

Запишем аксиому A5 (правомерность её применения заключается в том, что в формуле $x_1 = x_2$ нет свободных вхождений x_i):

$$\vdash \forall x_i \Big(x_1 = x_2 \supset \big(P(x_1,x_1,x_i) \supset P(x_1,x_2,x_i)\big)\Big) \supset \Big(x_1 = x_2 \supset \forall x_i \big(P(x_1,x_1,x_i) \supset P(x_1,x_2,x_i)\big)\Big),$$

из этого и из (6) по MP заключаем

$$\vdash x_1 = x_2 \supset \forall x_i \big(P(x_1,x_1,x_i) \supset P(x_1,x_2,x_i)\big). \tag{7}$$

Затем запишем вспомогательное утверждение:

$$\vdash \forall x_i(\mathcal{A} \supset \mathcal{B}) \supset (\forall x_i \mathcal{A} \supset \forall x_i \mathcal{B}).$$

Поясним это утверждение. Докажем $\forall x_i(\mathcal{A} \supset \mathcal{B}), \forall x_i \mathcal{A} \vdash \forall x_i \mathcal{B}$:

1) $\forall x_i(\mathcal{A} \supset \mathcal{B})$ (гипотеза);
2) $\mathcal{A} \supset \mathcal{B}$ (из 1 по правилу индивидуализации, переменная x_i свободна для самой себя в любой формуле);
3) $\forall x_i \mathcal{A}$ (гипотеза);
4) $\mathcal{A}$ (из 3 по правилу индивидуализации, переменная x_i свободна для самой себя в любой формуле);
5) $\mathcal{B}$ (из 4, 2 по MP);
6) $\forall x_i \mathcal{B}$ (из 5 по Gen).

В выводе выше единственная переменная x_i, к которой применялось правило Gen, является связанной в обеих гипотезах выводимости, поэтому можно применить теорему дедукции (даже дважды) и получить искомое $\vdash \forall x_i(\mathcal{A} \supset \mathcal{B}) \supset (\forall x_i \mathcal{A} \supset \forall x_i \mathcal{B})$. Запишем проверенное утверждение при $\mathcal{A} \leftrightharpoons P(x_1,x_1,x_i)$ и $\mathcal{B} \leftrightharpoons P(x_1,x_2,x_i)$:

$$\vdash \forall x_i \big(P(x_1,x_1,x_i) \supset P(x_1,x_2,x_i)\big) \supset \big(\forall x_i P(x_1,x_1,x_i) \supset \forall x_i P(x_1,x_2,x_i)\big). \tag{8}$$

Применяя транзитивность импликации к (7) и (8), заключаем требуемое:

$$\vdash x_1 = x_2 \supset \big(\forall x_i P(x_1,x_1,x_i) \supset \forall x_i P(x_1,x_2,x_i)\big) \Longleftrightarrow \vdash x_1 = x_2 \supset \big(A(x_1,x_1) \supset A(x_1,x_2)\big).$$

Таким образом, индукцией по числу связок и кванторов в формуле A проверено утверждение леммы, это завершает доказательство. ■

Примеры:

1. Теория групп G: предикатная буква A_1^2 ($A_1^2(x_1, x_2) \leftrightharpoons x_1 = x_2$), функциональная буква f_1^2 ($f_1^2(x_1, x_2) \leftrightharpoons x_1 + x_2$), предметная константа a_1 (0). Собственные аксиомы:

   A. $x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$;
   B. $x_1 + 0 = x_1$;
   C. $\forall x_1 \exists x_2 (x_1 + x_2 = 0)$;
   D. $x_1 = x_1$;
   E. $x_1 = x_2 \supset x_2 = x_1$;
   F. $x_1 = x_2 \supset (x_2 = x_3 \supset x_1 = x_3)$;
   G. $x_1 = x_2 \supset (x_1 + x_3 = x_2 + x_3 \wedge x_3 + x_1 = x_3 + x_2)$.

   Можно показать, что G есть теория первого порядка с равенством.
   Если добавить аксиому

   H. $x_1 + x_2 = x_2 + x_1$,

   то получится теория G_C коммутативных (абелевых) групп.

2. Теория полей F: предикатная буква A_1^2 ($A_1^2(x_1, x_2) \leftrightharpoons x_1 = x_2$), функциональные буквы f_1^2 ($f_1^2(x_1, x_2) \leftrightharpoons x_1 + x_2$) и f_2^2 ($f_2^2(x_1, x_2) \leftrightharpoons x_1 \cdot x_2$), предметные константы a_1 (0) и a_2 (1). Собственные аксиомы:

   A. $x_1 + (x_2 + x_3) = (x_1 + x_2) + x_3$;
   B. $x_1 + 0 = x_1$;
   C. $\forall x_1 \exists x_2 (x_1 + x_2 = 0)$;
   D. $x_1 = x_1$;
   E. $x_1 = x_2 \supset x_2 = x_1$;
   F. $x_1 = x_2 \supset (x_2 = x_3 \supset x_1 = x_3)$;
   G. $x_1 = x_2 \supset (x_1 + x_3 = x_2 + x_3 \wedge x_3 + x_1 = x_3 + x_2)$;
   H. $x_1 + x_2 = x_2 + x_1$;
   I. $x_1 = x_2 \supset (x_1 \cdot x_3 = x_2 \cdot x_3 \wedge x_3 \cdot x_1 = x_3 \cdot x_2)$;
   J. $x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$;
   K. $x_1 \cdot (x_2 + x_3) = (x_1 \cdot x_2) + (x_1 \cdot x_3)$;
   L. $x_1 \cdot x_2 = x_2 \cdot x_1$;
   M. $x_1 \cdot 1 = x_1$;
   N. $x_1 \neq 0 \supset \exists x_2 (x_1 \cdot x_2 = 1)$.

   Можно показать, что F есть теория первого порядка с равенством. Аксиомы (A)–(M) определяют теорию R_C коммутативных колец с единицей.

§8. Предварённые нормальные формы

Определение. Формула $Q_1 x_1 \dots Q_n x_n A$, где $Q_i x_i$ — квантор всеобщности или существования, предметные переменные x_i и x_j различны при $i \neq j$ и формула A не содержит кванторов, называется формулой в *предварённой нормальной форме* или в *пренексной нормальной форме* (*ПНФ*) (случай $n = 0$ также включается в это определение).

Докажем, что для любой формулы можно построить эквивалентную ей формулу в ПНФ (формулы A и B называют *эквивалентными*, если $\vdash A \equiv B$).

Лемма 8.1. Во всякой теории первого порядка:

1) $\vdash (\forall x A(x) \supset B) \equiv \exists y (A(y) \supset B)$, если y не входит свободно ни в $A(x)$, ни в B.

2) $\vdash (\exists x A(x) \supset B) \equiv \forall y (A(y) \supset B)$, если y не входит свободно ни в $A(x)$, ни в B.

3) $\vdash (B \supset \forall x A(x)) \equiv \forall y (B \supset A(y))$, если y не входит свободно ни в $A(x)$, ни в B.

4) $\vdash (\mathsf{B} \supset \exists \mathsf{x}\mathsf{A}(\mathsf{x})) \equiv \exists \mathsf{y}(\mathsf{B} \supset \mathsf{A}(\mathsf{y}))$, если y не входит свободно ни в $\mathsf{A}(\mathsf{x})$, ни в B.

5) $\vdash \neg\forall \mathsf{x}\mathsf{A} \equiv \exists \mathsf{x}\neg\mathsf{A}$.

6) $\vdash \neg\exists \mathsf{x}\mathsf{A} \equiv \forall \mathsf{x}\neg\mathsf{A}$.

Доказательство.

1) Доказательство $\forall \mathsf{x}\mathsf{A}(\mathsf{x}) \supset \mathsf{B}, \neg\exists \mathsf{y}(\mathsf{A}(\mathsf{y}) \supset \mathsf{B}) \vdash \mathsf{B} \wedge \neg\mathsf{B}$:

   1. $\forall \mathsf{x}\mathsf{A}(\mathsf{x}) \supset \mathsf{B}$ (гипотеза);
   2. $\neg\neg\forall \mathsf{y}\neg(\mathsf{A}(\mathsf{y}) \supset \mathsf{B})$ (гипотеза, квантор $\exists$ заменён по эквивалентности);
   3. $\neg\neg\forall \mathsf{y}\neg(\mathsf{A}(\mathsf{y}) \supset \mathsf{B}) \supset \forall \mathsf{y}\neg(\mathsf{A}(\mathsf{y}) \supset \mathsf{B})$ (частный случай тавтологии $\neg\neg\mathcal{A} \supset \mathcal{A}$);
   4. $\forall \mathsf{y}\neg(\mathsf{A}(\mathsf{y}) \supset \mathsf{B})$ (из 2, 3 по MP);
   5. $\neg(\mathsf{A}(\mathsf{y}) \supset \mathsf{B})$ (из 4 по правилу индивидуализации, переменная y свободна для самой себя в любой формуле);
   6. $\neg(\mathsf{A}(\mathsf{y}) \supset \mathsf{B}) \supset \mathsf{A}(\mathsf{y}) \wedge \neg\mathsf{B}$ (частный случай тавтологии $\neg(\mathcal{A} \supset \mathcal{B}) \supset \mathcal{A} \wedge \neg\mathcal{B}$);
   7. $\mathsf{A}(\mathsf{y}) \wedge \neg\mathsf{B}$ (из 5, 6 по MP);
   8. $\mathsf{A}(\mathsf{y}) \wedge \neg\mathsf{B} \supset \mathsf{A}(\mathsf{y})$ (частный случай тавтологии $\mathcal{A} \wedge \mathcal{B} \supset \mathcal{A}$);
   9. $\mathsf{A}(\mathsf{y})$ (из 7, 8 по MP);
   10. $\forall \mathsf{y}\mathsf{A}(\mathsf{y})$ (из 9 по Gen);
   11. $\forall \mathsf{x}\mathsf{A}(\mathsf{x})$ (из 10 по лемме 6.3, так как $\mathsf{A}(\mathsf{x})$ и $\mathsf{A}(\mathsf{y})$, очевидно, подобны);
   12. B (из 1, 11 по MP);
   13. $\mathsf{A}(\mathsf{y}) \wedge \neg\mathsf{B} \supset \neg\mathsf{B}$ (частный случай тавтологии $\mathcal{A} \wedge \mathcal{B} \supset \mathcal{B}$);
   14. $\neg\mathsf{B}$ (7, 13 по MP);
   15. $\mathsf{B} \wedge \neg\mathsf{B}$ (из 12, 14 по правилу конъюнкции).

   Так как переменная y не является свободной ни в одной из гипотез, и только к этой переменной применялось правило Gen, то можно применить теорему дедукции и получить

   $$\forall \mathsf{x}\mathsf{A}(\mathsf{x}) \supset \mathsf{B} \vdash \neg\exists \mathsf{y}(\mathsf{A}(\mathsf{y}) \supset \mathsf{B}) \supset \mathsf{B} \wedge \neg\mathsf{B}.$$

   С учётом этого с помощью тавтологии $(\neg\mathcal{A} \supset \mathcal{B} \wedge \neg\mathcal{B}) \supset \mathcal{A}$, правила MP и последующего применения теоремы дедукции заключаем

   $$\vdash (\forall \mathsf{x}\mathsf{A}(\mathsf{x}) \supset \mathsf{B}) \supset \exists \mathsf{y}(\mathsf{A}(\mathsf{y}) \supset \mathsf{B}). \tag{1}$$

   Докажем $\exists \mathsf{y}(\mathsf{A}(\mathsf{y}) \supset \mathsf{B}), \forall \mathsf{x}\mathsf{A}(\mathsf{x}) \vdash_{\mathsf{C}} \mathsf{B}$:

   1. $\exists \mathsf{y}(\mathsf{A}(\mathsf{y}) \supset \mathsf{B})$ (гипотеза);
   2. $\mathsf{A}(\mathsf{a}) \supset \mathsf{B}$ (из 1 по правилу C);
   3. $\forall \mathsf{x}\mathsf{A}(\mathsf{x})$ (гипотеза);
   4. $\mathsf{A}(\mathsf{a})$ (из 3 по правилу индивидуализации, константа свободна для любой переменной в любой формуле);
   5. B (из 2, 4 по MP).

   Таким образом, показано $\exists \mathsf{y}(\mathsf{A}(\mathsf{y}) \supset \mathsf{B}), \forall \mathsf{x}\mathsf{A}(\mathsf{x}) \vdash_{\mathsf{C}} \mathsf{B}$, а из этого, согласно теореме 6.2, вытекает $\exists \mathsf{y}(\mathsf{A}(\mathsf{y}) \supset \mathsf{B}), \forall \mathsf{x}\mathsf{A}(\mathsf{x}) \vdash \mathsf{B}$. Так как в рассуждениях выше не применялось правило Gen, то можно использовать теорему дедукции (даже дважды):

   $$\vdash \exists \mathsf{y}(\mathsf{A}(\mathsf{y}) \supset \mathsf{B}) \supset (\forall \mathsf{x}\mathsf{A}(\mathsf{x}) \supset \mathsf{B}). \tag{2}$$

   Из полученных (1) и (2) по правилу конъюнкции заключаем искомое

   $$\vdash \big((\forall \mathsf{x}\mathsf{A}(\mathsf{x}) \supset \mathsf{B}) \supset \exists \mathsf{y}(\mathsf{A}(\mathsf{y}) \supset \mathsf{B})\big) \wedge \big(\exists \mathsf{y}(\mathsf{A}(\mathsf{y}) \supset \mathsf{B}) \supset (\forall \mathsf{x}\mathsf{A}(\mathsf{x}) \supset \mathsf{B})\big) \Longleftrightarrow \vdash (\forall \mathsf{x}\mathsf{A}(\mathsf{x}) \supset \mathsf{B}) \equiv \exists \mathsf{y}(\mathsf{A}(\mathsf{y}) \supset \mathsf{B}).$$

2) Докажем $\exists \mathsf{x}\mathsf{A}(\mathsf{x}) \supset \mathsf{B}, \mathsf{A}(\mathsf{y}) \vdash \mathsf{B}$:

   1. $\exists \mathsf{x}\mathsf{A}(\mathsf{x}) \supset \mathsf{B}$ (гипотеза);
   2. $\mathsf{A}(\mathsf{y})$ (гипотеза);
   3. $\exists \mathsf{x}\mathsf{A}(\mathsf{x})$ (из 2 по правилу существования, ясно, что x свободно для y в $\mathsf{A}(\mathsf{x})$ по условию);
   4. B (из 1, 3 по MP).

В выводе выше не использовалось правило Gen, поэтому допустимо применить теорему дедукции: $\exists x A(x) \supset B \vdash A(y) \supset B$. Применяя правило Gen к формуле $A(y) \supset B$, а также правило сечения, получаем $\exists x A(x) \supset B \vdash \forall y(A(y) \supset B)$. Так как применённое правило Gen связало переменную y, не входящую свободно в $\exists x A(x) \supset B$ по условию, можно снова применить теорему дедукции и получить $\vdash (\exists x A(x) \supset B) \supset \forall y(A(y) \supset B)$.
Поясним теперь $\forall y(A(y) \supset B), \exists x A(x) \vdash_C B$:

1. $\forall y(A(y) \supset B)$ (гипотеза);
2. $A(a) \supset B$ (из 1 по правилу индивидуализации, константа a свободна для любой переменной в любой формуле);
3. $\exists x A(x)$ (гипотеза);
4. $A(a)$ (из 3 по правилу C);
5. B (из 4, 2 по MP).

Тогда, применяя теорему 6.2, заключаем, что $\forall y(A(y) \supset B), \exists x A(x) \vdash B$. Так как правило Gen в нашем выводе не применялось, воспользуемся теоремой дедукции (даже дважды): $\vdash \forall y(A(y) \supset B) \supset (\exists x A(x) \supset B)$.
Применяя правило конъюнкции к двум полученным выводимостям, заключаем требуемое:

$$\vdash \big((\exists x A(x) \supset B) \supset \forall y(A(y) \supset B)\big) \wedge \big(\forall y(A(y) \supset B) \supset (\exists x A(x) \supset B)\big) \Longleftrightarrow \vdash (\exists x A(x) \supset B) \equiv \forall y(A(y) \supset B)\big).$$

3) Докажем $B \supset \forall x A(x), B \vdash A(y)$:

1. B (гипотеза);
2. $B \supset \forall x A(x)$ (гипотеза);
3. $\forall x A(x)$ (из 1, 2 по MP);
4. $A(y)$ (из 3 по правилу индивидуализации, y свободно для x в $A(x)$ по условию).

В силу того, что правило Gen в выводе выше не применялось, используем теорему дедукции: $B \supset \forall x A(x) \vdash B \supset A(y)$. Применяя правило Gen к формуле $B \supset A(y)$ и правило сечения, получаем выводимость $B \supset \forall x A(x) \vdash \forall y(B \supset A(y))$. Так как применённое правило Gen связало переменную y, не входящую свободно в $B \supset \forall x A(x)$, то можно снова применить теорему дедукции: $\vdash (B \supset \forall x A(x)) \supset \forall y(B \supset A(y))$.
Поясним $\forall y(B \supset A(y)), B \vdash \forall x A(x)$:

1. $\forall y(B \supset A(y))$ (гипотеза);
2. $B \supset A(x)$ (из 1 по правилу индивидуализации, x свободно для y в $A(x)$ по условию);
3. B (гипотеза);
4. $A(x)$ (из 3, 2 по MP);
5. $\forall x A(x)$ (из 4 по Gen).

Так как правило Gen в выводе выше связало переменную x, не входящую свободно в $\forall y(B \supset A(y))$ и B, то можно применить теорему дедукции (дважды): $\vdash \forall y(B \supset A(y)) \supset (B \supset \forall x A(x))$.
Применяя правило конъюнкции к полученным двум выводимостям, получаем требуемую теорему:

$$\vdash \big((B \supset \forall x A(x)) \supset \forall y(B \supset A(y))\big) \wedge \big(\forall y(B \supset A(y)) \supset (B \supset \forall x A(x))\big) \Longleftrightarrow \vdash (B \supset \forall x A(x)) \equiv \forall y(B \supset A(y)).$$

4) Докажем $B \supset \exists x A(x), B \vdash_C A(a)$, где a — константа, не входящая в $A(x)$ и B:

1. $B \supset \exists x A(x)$ (гипотеза);
2. B (гипотеза);
3. $\exists x A(x)$ (из 2, 1 по MP);
4. $A(a)$ (правило C).

По теореме 6.2 получаем $B \supset \exists x A(x), B \vdash A(a)$. Так как правило Gen не применялось к переменным, свободным в $B \supset \exists x A(x)$ и B, можно применить теорему дедукции: $B \supset \exists x A(x) \vdash B \supset A(a)$. Применяя правило существования и правило сечения (константа a свободна для любой переменной в любой формуле), получаем $B \supset \exists x A(x) \vdash \exists y(B \supset A(y))$. Понятно, что и в данном случае правило Gen не применялось к переменным, свободным в $B \supset \exists x A(x)$, поэтому можно снова применить теорему дедукции: $\vdash (B \supset \exists x A(x)) \supset \exists y(B \supset A(y))$.
Докажем теперь $\exists y(B \supset A(y)), B \vdash_C \exists x A(x)$:

1. $\exists y(B \supset A(y))$ (гипотеза);
2. $B \supset A(a)$ (из 1 по правилу C);

3. B (гипотеза);
4. $A(a)$ (из 3, 2 по MP);
5. $\exists x A(x)$ (из 4 по правилу существования, константа a свободна для любой переменной в любой формуле).

По теореме 6.2 получаем $\exists y(B \supset A(y)), B \vdash \exists x A(x)$. Правомерность применения теоремы дедукции аналогично предыдущим пунктам, применяем (дважды): $\vdash \exists y(B \supset A(y)) \supset (B \supset \exists x A(x))$.
Применяя правило конъюнкции к полученным двум выводимостям, получаем требуемую теорему:

$$\vdash \big((B \supset \exists x A(x)) \supset \exists y(B \supset A(y))\big) \wedge \big(\exists y(B \supset A(y)) \supset (B \supset \exists x A(x))\big) \iff \vdash (B \supset \exists x A(x)) \equiv \exists y(B \supset A(y)).$$

5) Докажем $\forall x \neg\neg A \vdash \forall x A$:

1. $\forall x \neg\neg A$ (гипотеза);
2. $\neg\neg A$ (из 1 по правилу индивидуализации, переменная x свободна для себя в любой формуле);
3. $\neg\neg A \supset A$ (частный случай тавтологии $\neg\neg\mathcal{A} \supset \mathcal{A}$);
4. A (из 2, 3 по MP);
5. $\forall x A$ (из 4 по Gen).

Так как правило Gen в выводе выше применялось к переменной x, которая связана в гипотезе $\forall x \neg\neg A$, можно воспользоваться теоремой дедукции и получить $\vdash \forall x \neg\neg A \supset \forall x A$. Далее имеем:

1. $\forall x \neg\neg A \supset \forall x A$ (доказанная выше теорема);
2. $(\forall x \neg\neg A \supset \forall x A) \supset (\neg\forall x A \supset \neg\forall x \neg\neg A)$ (частный случай тавтологии $(\mathcal{A} \supset \mathcal{B}) \supset (\neg\mathcal{B} \supset \neg\mathcal{A})$);
3. $\neg\forall x A \supset \neg\forall x \neg\neg A$ (из 1, 2 по MP).

Последняя формула в выводе выше по эквивалентной замене приводит нас к $\vdash \neg\forall x A \supset \exists x \neg A$.
Поясним теперь $\forall x A \vdash \forall x \neg\neg A$:

1. $\forall x A$ (гипотеза);
2. A (из 1 по правилу индивидуализации, переменная x свободна для себя в любой формуле);
3. $A \supset \neg\neg A$ (частный случай тавтологии $\mathcal{A} \supset \neg\neg\mathcal{A}$);
4. $\neg\neg A$ (из 2, 3 по MP);
5. $\forall x \neg\neg A$ (из 4 по Gen).

Так как правило Gen в выводе выше применялось к переменной x, которая связана в гипотезе $\forall x A$, можно воспользоваться теоремой дедукции и получить $\vdash \forall x A \supset \forall x \neg\neg A$. Далее имеем:

1. $\forall x A \supset \forall x \neg\neg A$ (доказанная выше теорема);
2. $(\forall x A \supset \forall x \neg\neg A) \supset (\neg\forall x \neg\neg A \supset \neg\forall x A)$ (частный случай тавтологии $(\mathcal{A} \supset \mathcal{B}) \supset (\neg\mathcal{B} \supset \neg\mathcal{A})$);
3. $\neg\forall x \neg\neg A \supset \neg\forall x A$ (из 1, 2 по MP).

Последняя формула в выводе выше по эквивалентной замене приводит нас к $\vdash \exists x \neg A \supset \neg\forall x A$. Имея в виду полученные две выводимости, по правилу конъюнкции получаем требуемое:

$$\vdash (\neg\forall x A \supset \exists x \neg A) \wedge (\exists x \neg A \supset \neg\forall x A) \iff \vdash \neg\forall x A \equiv \exists x \neg A.$$

6) Если заменить квантор $\exists$ на $\forall$ по эквивалентной замене, то получится формула $\neg\neg\forall x \neg A \equiv \forall x \neg A$, которая является частным случаем тавтологии $\neg\neg\mathcal{A} \equiv \mathcal{A}$.

■

Лемма 8.2. Существует эффективная процедура, преобразующая всякую формулу к эквивалентной ей формуле в предварённой нормальной форме.

Доказательство. Считаем, что все связанные переменные в формуле различные. Докажем лемму индукцией по числу связок и кванторов $n \geqslant 0$ в формуле A.

База: $n = 0$. В формуле A нет ни связок, ни кванторов — доказывать нечего, формула уже в ПНФ.

Индукционное предположение: пусть утверждение верно для всех формул всех значений $k = 0, 1, \ldots, n-1$ числа связок и кванторов, то есть для всех таких формул A существует эффективный алгоритм построения предварённой нормальной формы этих формул.

Индукционный шаг: докажем утверждение для произвольной формулы A с $k = n$ связками и кванторами. Имеется три случая.

1. A есть $\neg P$. В формуле P число связок и кванторов меньше, чем в A как минимум на 1. Тогда для P верно индукционное предположение: для P можно эффективно построить её ПНФ N: $\vdash P \equiv N$. Из упомянтой выводимости следует $\vdash \neg N \equiv \neg P$ (это выводится с помощью тавтологии $(\mathcal{A} \equiv \mathcal{B}) \supset (\neg\mathcal{B} \equiv \neg\mathcal{A})$), что равносильно $\vdash \neg N \equiv A$. Применяя эквиваленации 5, 6 из леммы 8.1, заносим связку $\neg$ в формуле $\neg N$ за кванторы до тех пор, пока эта формула не примет вид $Q_1x_1Q_2x_2\ldots Q_mx_m\neg R$, где R — бескванторная формула, что есть ПНФ. Это доказывает утверждение для первого случая.

2. A есть $P \supset Q$. По аналогичным п.1 причинам для P и Q верно индукционное предположение: существует эффективный алгоритм построения формул N_1 и N_2 в ПНФ таких, что $\vdash P \equiv N_1$ и $\vdash Q \equiv N_2$. Запишем частный случай тавтологии:

$$\vdash (P \equiv N_1) \wedge (Q \equiv N_2) \supset \big((P \supset Q) \equiv (N_1 \supset N_2)\big).$$

Правило конъюнкции из упомянутых индукционных предположений даёт выводимость $\vdash (P \equiv N_1)\wedge(Q \equiv N_2)$, что из записанного частного случая тавтологии по MP приводит к $\vdash (P \supset Q) \equiv (N_1 \supset N_2)$. Применяем лемму 8.1 (пп.1–4) к формуле $N_1 \supset N_2$, приводим её к виду $N_3 \leftrightharpoons Q_1x_1Q_2x_2\ldots Q_mx_mR$, где R — бескванторная формула. Это рассуждение, а также правило сечения, приводит нас к выводимости

$$\vdash (P \supset Q) \equiv N_3 \iff \vdash A \equiv N_3,$$

что и требовалось для данного случая.

3. A есть $\forall x_i P$. Для P снова верно индукционное предположение: существует эффективный алгоритм построения формулы N в ПНФ такой, что $\vdash P \equiv N$. Из этой выводимости, как нетрудно понять, следует $\vdash \forall x_i P \equiv \forall x_i N$, то есть $\vdash A \equiv \forall x_i N$. Ясно, что если N — формула в ПНФ, то и $\forall x_i N$ — формулой в ПНФ, что завершает доказательство последнего случая.

Все случаи разобраны, индукционный шаг доказан. Тем самым, по индукции доказана искомая лемма. ■

§9. Другие аксиоматические теории первого порядка

Исчисление предикатов Бернайса

К символам рассмотренного в лекциях ИП добавляется квантор существования. Соответственно меняется и определение формулы. К аксиомам (A1)–(A3) добавляются аксиомы:

(Б1) $\forall x A(x) \supset A(y)$;

(Б2) $A(y) \supset \exists x A(x)$,

где $A(x)$ — любая формула, содержащая свободные вхождения переменной x, причём ни одно из них не находится в области действия никакого квантора по y, если таковые имеются. Формула $A(y)$ получается из формулы $A(x)$ заменой всех свободных вхождений переменной x на переменную y. Эти аксиомы называются аксиомами Бернайса. К правилу вывода MP добавляются правила:

1. $\dfrac{A \supset B(x)}{A \supset \forall x B(x)}$ ($\forall$-правило, или обобщение);

2. $\dfrac{B(x) \supset A}{\exists x B(x) \supset A}$ ($\exists$-правило, или конкретизация),

где $B(x)$ может содержать, а A не содержит свободные вхождения x.
Для такого ИП справедлива теорема дедукции в формулировке для ИВ: если $\Gamma, A \vdash B$, то $\Gamma \vdash A \supset B$.

Секвенциональное исчисление предикатов

К алфавиту исчисления секвенций добавляются кванторы $\forall$, $\exists$. Понятия секвенции, вывода те же, что в исчислении секвенций. Терм, формула, свободные и связанные переменные, свободный терм определяются так же, как в §1.
Схема аксиом: $A \vdash A$.
Правила вывода (Γ, Γ_1, Γ_2, Γ_3 — произвольные множества формул, может быть, пустые, A, B, C — произвольные формулы; t — терм, свободный для x в $A(x)$; $A(t)$ получается из формулы $A(x)$ заменой всех свободных вхождений переменной x на t):

1) $\dfrac{\Gamma_1 \vdash A;\ \Gamma_2 \vdash B}{\Gamma_1, \Gamma_2 \vdash A \wedge B}$ (*введение* $\wedge$);

2) $\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash A}$ (*удаление* $\wedge$);

3) $\dfrac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$ (*удаление* $\wedge$);

4) $\dfrac{\Gamma \vdash A}{\Gamma \vdash A \vee B}$ (*введение* $\vee$);

5) $\dfrac{\Gamma \vdash B}{\Gamma \vdash A \vee B}$ (*введение* $\vee$);

6) $\dfrac{\Gamma_1 \vdash A \vee B;\ \Gamma_2, A \vdash C;\ \Gamma_3, B \vdash C}{\Gamma_1, \Gamma_2, \Gamma_3 \vdash C}$ (*удаление* $\vee$);

7) $\dfrac{\Gamma, A \vdash B}{\Gamma \vdash A \supset B}$ (*введение* $\supset$);

8) $\dfrac{\Gamma_1 \vdash A;\ \Gamma_2 \vdash A \supset B}{\Gamma_1, \Gamma_2 \vdash B}$ (*удаление* $\supset$);

9) $\dfrac{\Gamma, A \vdash}{\Gamma \vdash \neg A}$ (*введение* $\neg$);

10) $\dfrac{\Gamma_1 \vdash A;\ \Gamma_2 \vdash \neg A}{\Gamma_1, \Gamma_2 \vdash}$ (*сведение к противоречию*);

11) $\dfrac{\Gamma, \neg A \vdash}{\Gamma \vdash A}$ (*удаление* $\neg$);

12) $\dfrac{\Gamma \vdash}{\Gamma \vdash A}$ (*утончение*);

13) $\dfrac{\Gamma \vdash A}{\Gamma, B \vdash A}$ (*расширение*);

14) $\dfrac{\Gamma_1, A, B, \Gamma_2 \vdash C}{\Gamma_1, B, A, \Gamma_2 \vdash C}$ (*перестановка*);

15) $\dfrac{\Gamma, A, A \vdash C}{\Gamma, A \vdash C}$ (*сокращение*);

16) $\dfrac{\Gamma \vdash A(x)}{\Gamma \vdash \forall x A(x)}$, где x не входит свободно ни в одну из формул в Γ (*введение* $\forall$);

17) $\dfrac{\Gamma \vdash \forall x A(x)}{\Gamma \vdash A(t)}$ (*удаление* $\forall$);

18) $\dfrac{\Gamma \vdash A(t)}{\Gamma \vdash \exists x A(x)}$ (*введение* $\exists$);

19) $\dfrac{\Gamma, A(x) \vdash B}{\Gamma, \exists x A(x) \vdash B}$, где x не входит свободно ни в одну из формул из Γ, а также в B (*удаление* $\exists$).

Исчисление предикатов Клини

Примитивные связки: $\neg$, $\wedge$, $\vee$, $\supset$.
Схемы аксиом:

(A1) $A \supset (B \supset A)$;

(A2) $(A \supset B) \supset \Big((A \supset (B \supset C)) \supset (A \supset C)\Big)$;

(A3) $A \wedge B \supset A$;

(A4) $A \wedge B \supset B$;

(A5) $(A \supset B) \supset \big((A \supset C) \supset (A \supset B \wedge C)\big)$;

(A6) $A \supset (A \vee B)$;

(A7) $B \supset (A \vee B)$;

(A8) $(A \supset C) \supset \Big((B \supset C) \supset \big((A \vee B) \supset C\big)\Big)$;

(A9) $(A \supset \neg B) \supset (B \supset \neg A)$;

(A10) $\neg\neg A \supset A$;

(A11) $\forall x A(x) \supset A(t)$;

(A12) $A(t) \supset \exists x A(x)$.

В аксиомах (A11)–(A12) t — терм, свободный для x в $A(x)$, $A(t)$ получается из формулы $A(x)$ заменой всех свободных вхождений переменной x на t.
Правила вывода:

I. MP;

II. $\dfrac{C \supset A(x)}{C \supset \forall y A(y)}$;

III. $\dfrac{A(x) \supset C}{\exists y A(y) \supset C}$,

причём x не входит свободно в C, а y не входит свободно в $A(x)$ и свободна для x в $A(x)$.

III. Теория алгоритмов

§1. Понятие алгоритма

Алгоритм (от имени хорезмского учёного Абу Абдуллаха Мухаммеда ибн Мусы аль-Хорезми) — набор инструкций, описывающих порядок действий исполнителя для решения задачи.

Требования к (вычислительным) алгоритмам:

- приспособленность к работе с данными;
- *конечность*: число шагов должно быть конечно;
- *элементарность*: шаги алгоритма должны быть детализированы;
- *детерминированность*: после каждого шага точно определён следующий или определено окончание работы алгоритма;
- *направленность*: все шаги направлены на решение задачи;
- *результативность*: остановка после конечного числа шагов с указанием того, что считать результатом;
- *сходимость*: получение результата за конечное число шагов для набора исходных данных из некоторого множества (область сходимости);
- *конечность описания*: описание и механизм реализации (средства пуска, реализации элементарных шагов, остановки, выдачи результатов) конечны;
- *массовость*: приспособленность к решению классов задач при любых исходных данных из некоторого класса.

Итак, конкретизируем понятие алгоритма.
Алгоритм — предназначенная для решения некоторого класса задач конечная последовательность элементарных инструкций, каждая из которых имеет чёткий смысл и может быть выполнена с конечными вычислительными затратами.

При любых входных данных из области сходимости алгоритм завершается после конечного числа шагов и выдаёт результат (выходные данные).

Такое понимание алгоритма применялось математиками (и не только ими) в течение тысячелетий. Но на рубеже XIX–XX веков возникла потребность в строгой математической формализации алгоритма. Связано это было с пересмотром (вернее, строгим построением) оснований математики.

Кроме того, пересмотр оснований математики был связан с наличием большого числа логических парадоксов, возникших в связи с несовершенностью имеющихся на тот момент идей и принципов построения математических теорий. Известны, например, следующие парадоксы:

- *Парадокс лжеца*: является ли верным утверждение «Я лгу»?
- *Парадокс Рассела*: пусть определено множество $\mathsf{X} = \{\mathsf{Y} \mid \mathsf{Y} \notin \mathsf{Y}\}$, спрашивается, верно ли, что $\mathsf{X} \in \mathsf{X}$? (парадокс, возникший в наивной теории множеств Кантора).
  Парадокс брадобрея на ту же тему: в некоторой деревне живёт брадобрей, которому велено брить тех и только тех жителей деревни, кто не бреется сам, спрашивается, будет ли брадобрей брить сам себя?
- *Парадокс Банаха–Тарского* (или *парадокс удвоения шара*) говорит, что трёхмерный шар равносоставлен двум своим копиям. Более общо: любые два ограниченных подмножества Евклидова пространства с непустой внутренностью являются равносоставленными. Это парадокс, являющийся следствием знаменитой *аксиомы выбора*, входящей в аксиоматику ZFC (Zermelo–Fraenkel + axiom of Choice) Цермело–Френкеля с аксиомой выбора.

§2. Подходы к формализации алгоритма

Для формализации понятия алгоритма был выбран следующий подход. Выбирается конечный набор исходных объектов (элементов) и конечный набор правил построения из них новых объектов. Это означает, что определяется:

1) алфавит данных и алфавит алгоритмов (конечные наборы символов, которыми записываются обрабатываемые данные и команды алгоритма);
2) наборы объектов, над которыми производятся операции — слова в алфавите данных;

3) конечный набор элементарных операций;

4) ограничения на используемую память.

В зависимости от выбора этих атрибутов получается конкретная алгоритмическая модель. В теории алгоритмов сформировались три типа алгоритмических моделей.

Исторически первой была разработана формализация алгоритмов с помощью *рекурсивных числовых функций*. Теория рекурсивных функций была разработана Куртом Гёделем и Жаком Эрбраном. Поэтому этот подход к формализации алгоритмической вычислимости называется *вычислимость по Эрбрану–Гёделю*.

Основной результат этой теории: класс вычислимых с помощью алгоритмов в широком интуитивном смысле числовых функций совпадает с классом частично рекурсивных функций (тезис Чёрча). Иными словами, любая функция, которую можно вычислить известными человечеству методами, допускает представление через частично рекурсивные функции. Это утверждение называется тезисом, потому что его невозможно доказать в силу принципиальной неформализуемости понятия алгоритма.

Тезис Чёрча — это естественнонаучный факт, подтверждаемый опытом, накопленным в математике за всю её историю. Его можно опровергнуть, построив вычислимую функцию, не представимую с помощью частично рекурсивных функций.

Второй подход к формализации вычислимости связан с абстрактными вычислительными машинами — детерминированными устройствами, способными выполнять в каждый момент времени лишь примитивные операции. Первая машина была построена Аланом Тьюрингом (*машина Тьюринга*). Затем Эмиль Пост предложил свою машину (*машина Поста*), но позже было доказано, что машины Тьюринга и Поста эквивалентны, т.е. любая числовая функция, вычислимая машиной Тьюринга, вычисляется также и машиной Поста и наоборот.

Основной результат этой теории: класс вычислимых с помощью алгоритмов в широком интуитивном смысле числовых функций совпадает с классом вычислимых по Тьюрингу функций (*тезис Тьюринга*). Он также недоказуем, как тезис Чёрча. Впоследствии было доказано, что вычислимости по Эрбрану-Гёделю и Тьюрингу эквивалентны, поэтому тезис Тьюринга также называют *тезисом Чёрча–Тьюринга*.

Третий подход связан с преобразованиями слов в произвольных алфавитах с элементарными операциями подстановки. Алгоритмы преобразования слов были предложены Андреем Андреевичем Марковым (*нормальные алгорифмы Маркова*). Преимущество этого подхода в максимальной абстракции и применимости к объектам любой природы (не обязательно к числам).

Существование трёх различных подходов к формализации алгоритма не ведёт к утрате его универсальности. Доказано, что они сводятся друг к другу и в конечном счёте приводят к понятию вычислимой числовой функции — функции, для которой существует эффективный алгоритм вычисления. Это подтверждает тезис о единстве материального мира.

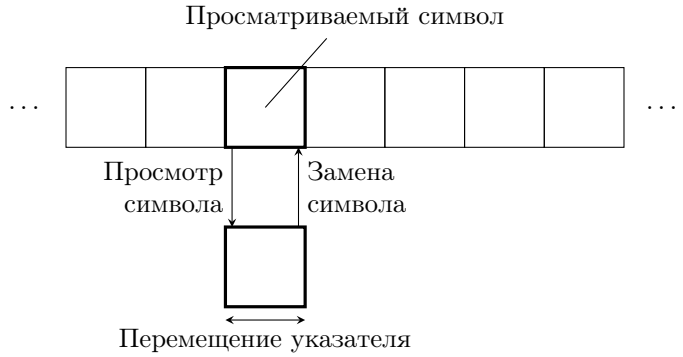
§3. Машина Тьюринга

3.1. Устройство машины Тьюринга

Машина Тьюринга представляет собой *абстрактное* устройство, состоящее из бесконечной ленты, считывающей (и печатающей) головки и управляющего устройства.

Лента разбита на ячейки (клетки); в каждой из них в произвольный дискретный момент времени находится ровно один символ *внешнего алфавита* $A = \{a_0, a_1, \ldots, a_{n-1}\}$, $n \geqslant 2$. Алфавит содержит символ, называемый *пустым* (обычно это a_0, и за него принимается 0 (нуль)). Клетка с пустым символом называется *пустой*. Бесконечность ленты означает, что в любой момент времени она конечна, но число клеток всегда можно увеличить в обе стороны насколько необходимо (потенциальная бесконечность).

Управляющее устройство в каждый момент времени находится в некотором состоянии q_j из внутреннего алфавита $Q = \{q_0, q_1, \ldots, q_{r-1}\}$, $r \geqslant 2$. Иногда в Q выделяются непересекающиеся подмножества Q_0 и Q_1 *заключительных* и *начальных состояний соответственно*. В дальнейшем $Q_0 = \{q_0\}$, $Q_1 = \{q_1\}$.



Головка перемещается вдоль ленты так, что в каждый момент времени она обозревает ровно одну ячейку, считывает содержимое обозреваемой ячейки, стирает находящийся в ней символ, записывает другой символ внешнего алфавита A (он может совпадать с прежним).

Управляющее устройство в зависимости от состояния, в котором оно находится, и обозреваемого головкой символа изменяет своё внутреннее состояние или остаётся в прежнем, выдаёт головке команду напечатать в ячейке определённый символ A и сдвинуться в следующий момент времени на одну клетку влево, вправо или остаться на месте.

Таким образом, работа управляющего устройства описывается тремя функциями:

$$G\colon Q \times A \to Q; \quad F\colon Q \times A \to A; \quad D\colon Q \times A \to \{S, L, R\}.$$

Символы S, L, R означают оставление головки на месте, движение на клетку влево и вправо соответственно. Функции G, F и D называются *функциями переходов*, *выходов* и *движения* соответственно. Их можно записать пятёркой вида $q_i a_j q_{ij} a_{ij} d_{ij}$, где $q_{ij} = G(q_i, a_j)$, $a_{ij} = F(q_i, a_j)$, $d_{ij} = D(q_i, a_j)$. Они называются *командами* машины Тьюринга. В общем случае команды определены не для каждой пары $\langle q_i, a_j \rangle$.

Список всех команд, определяющих работу машины Тьюринга, называется её *программой*. Программу можно записывать в таблицу. Если для пары $\langle q_i, a_j \rangle$ команда отсутствует, то в таблице ставится прочерк в соответствующей ячейке.

	q_0	$\dots$	q_i	$\dots$	q_{r-1}
a_0	—	$\dots$	—	$\dots$	—
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
a_j	—	$\dots$	$q_{ij}\ a_{ij}\ d_{ij}$	$\dots$	—
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
a_{n-1}	—	$\dots$	—	$\dots$	—

3.2. Конфигурации

Работу машины Тьюринга будем описывать на языке конфигураций.

Пусть в момент времени t самая левая непустая ячейка C_1 на ленте содержит символ a_{j_1}, а самая правая непустая ячейка C_s — символ a_{j_s} $(s \geqslant 2)$. Тогда будем говорить, что в момент времени t на ленте записано слово $P = a_{j_1} \dots a_{j_s}$.
При $s = 1$ на ленте записано слово $P = a_{j_1}$. Пустыми считаются клетки, содержащие пустой символ $a_0 \in A$. Далее пустой символ будем обозначать Λ.

Пусть в момент времени t управляющее устройство находится в состоянии q_i, а головка обозревает символ a_{j_ℓ} слова P $(\ell \geqslant 2)$. Тогда слово

$$a_{j_1} \dots a_{j_{\ell-1}} q_i a_{j_\ell} \dots a_{j_s}$$

называется *конфигурацией машины в момент времени* t.

При $\ell = 1$ конфигурация имеет вид $q_i P$. Если головка обозревает пустую ячейку, находящуюся слева (справа) от слова P, и между ней и первым (последним) непустым символом слова находятся $\nu \geqslant 0$ пустых ячеек, то конфигурацией называется слово

$$q_i \Lambda^{\nu+1} P \quad (P \Lambda^{\nu} q_i \Lambda),$$

где a^{ν} — сокращённая запись слова, состоящего из ν символов a. Если в момент t лента пуста, то конфигурацией будет слово $q_i \Lambda$.

Пусть в момент t машина имеет конфигурацию $a_{j_1} \dots a_{j_{\ell-1}} q_i a_{j_\ell} \dots a_{j_s}$ и выполняется команда $q_i a_{j_\ell} q_{ij_\ell} a_{ij_\ell} d_{ij_\ell}$. Тогда при $d_{ij_\ell} = L$ в следующий момент машина будет иметь конфигурацию:

1. $q_{ij_1}\Lambda a_{ij_1}a_{j_2}\dots a_{j_s}$, если $\ell = 1$;
2. $q_{ij_2}a_{j_1}a_{ij_2}a_{j_3}\dots a_{j_s}$, если $\ell = 2$;
3. $a_{j_1}\dots a_{j_{\ell-2}}q_{ij_\ell}a_{j_{\ell-1}}a_{ij_\ell}a_{j_{\ell+1}}\dots a_{j_s}$, если $\ell > 2$.

Если в какой-то момент времени управляющее устройство приходит в заключительное состояние q_0, машина прекращает работу, и её конфигурация в этот момент называется *заключительной*.

Если для пары $\langle q_i, a_j\rangle$ команда отсутствует, то машина прекращает работу и текущая конфигурация также считается заключительной. Конфигурация, соответствующая началу работы, называется *начальной*.

Пусть K — конфигурация в некоторый момент времени, K' — конфигурация в следующий момент. Тогда говорят, что конфигурация K' *непосредственно выводима* из K (обозначение $K \models K'$). Если K_1 — начальная конфигурация, то последовательность $K_1, \dots, K_m$, где $K_i \models K_{i+1}$, $1 \leqslant i < m$, называется *тьюринговым вычислением*. При этом конфигурация K_m *выводима из конфигурации* K_1: $K_1 \vdash K_m$. Если к тому же K_m является заключительной конфигурацией, то говорят, что K_m *заключительно выводима из* K_1: $K_1 \Vdash K_m$.

Слово на ленте в начальный момент времени называется *исходным* (*начальным*). Если P_1 — исходное слово, то машина T, начав с него, либо остановится через конечное число шагов, либо никогда не остановится. В первом случае говорят, что машина T *применима к слову* P_1, и результатом применения является слово P, соответствующее заключительной конфигурации (обозначение $P = T(P_1)$). Во втором случае говорят, что машина T *не применима* к слову P_1.

В дальнейшем предполагаем, что:

1. Исходное слово не пусто.
2. В начальный момент головка находится на самой левой непустой ячейке ленты.
3. Начальное состояние машины q_1.
4. Внешний алфавит двоичный, т.е. $A = \{0, 1\}$, 0 — пустой символ.

Зоной работы машины T (на исходном слове P_1) называется множество всех ячеек, которые за время работы машина хотя бы один раз обозревала.

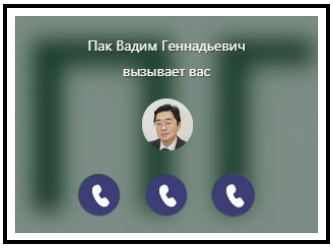


Рис. 2: «IV курс! Приглашаю на консультацию по МЛ».