Исчисление высказываний
лекция 3

Лев Дмитриевич Беклемишев
http://lpcs.math.msu.su/vml2008

lbekl@yandex.ru

28 февраля 2008 г.

Консультации

У каждой группы один раз в две недели.

Гр.	Нед.	Д.	Время	Ауд.	Преп.	Первая конс.
101	верх.	пт	16:45—18:20	13-27	асс. Бабенко	22.02.08
102	верх.	пт	16:45—18:20	13-27	асс. Бабенко	22.02.08
103	ниж.	пт	16:45—18:20	13-27	асс. Бабенко	29.02.08
104	ниж.	пт	16:45—18:20	13-27	асс. Бабенко	29.02.08
105	верх.	пн	16:45—18:20	16-24	доц. Плиско	03.03.08
106	верх.	пн	16:45—18:20	16-24	доц. Плиско	03.03.08
107	ниж.	чт	16:45—18:20	16-10	проф. Пентус	28.02.08
108	ниж.	чт	16:45—18:20	16-10	проф. Пентус	28.02.08
109	верх.	чт	16:45—18:20	16-10	доц. Крупский	06.03.08
110	верх.	чт	16:45—18:20	16-10	доц. Крупский	06.03.08
111	ниж.	пн	16:45—18:20	16-24	доц. Плиско	25.02.08
112	ниж.	пн	16:45—18:20	16-24	доц. Плиско	25.02.08

Дизъюнктивные и конъюнктивные нормальные формы

Опр.

Литералами называются переменные и их отрицания.

Пример.

$P_3, \ \neg P_5$ — литералы;
$P_3 \vee P_1$ и $\neg\neg P_3$ — не литералы.

Опр.

Элементарной конъюнкцией называем формулу вида $\bigwedge_{i=1}^{n} L_i$, где L_i — литералы.

Пример.

$(P \wedge \neg Q) \wedge \neg P$ — элементарная конъюнкция;
$P \wedge (\neg Q \wedge \neg P)$ — не элементарная конъюнкция.

Опр.

Дизъюнктивной нормальной формой (ДНФ) называем формулу вида $\bigvee_{j=1}^{m} C_j$, где C_j — элементарные конъюнкции.

Пример.

$(P \wedge \neg R) \vee (Q \wedge R)$ и $(P \wedge Q \wedge R) \vee \neg P \vee \neg R$ — дизъюнктивные нормальные формы.

Опр.

Элементарной дизъюнкцией называем формулу вида $\bigvee_{i=1}^{n} L_i$, где L_i — литералы.

КНФ называем формулу вида $\bigwedge_{j=1}^{m} D_j$, где D_j — элементарные дизъюнкции.

Упражнение

Привести к КНФ формулу $(P \vee Q) \to R$. *Ответ:* $(\neg P \vee R) \wedge (\neg Q \vee R)$.

Опр.

Элементарной дизъюнкцией называем формулу вида $\bigvee_{i=1}^{n} L_i$, где L_i — литералы.

КНФ называем формулу вида $\bigwedge_{j=1}^{m} D_j$, где D_j — элементарные дизъюнкции.

Упражнение

Привести к КНФ формулу $(P \vee Q) \to R$. *Ответ:* $(\neg P \vee R) \wedge (\neg Q \vee R)$.

Теорема о ДНФ и КНФ

Теорема.

Каждая пропозициональная формула равносильна некоторой ДНФ и некоторой КНФ.

Доказательство.

(первый вариант) *Достаточно заметить, что формула, построенная в доказательстве теоремы о функциональной полноте, является ДНФ.*

Теорема о ДНФ и КНФ

Теорема.

Каждая пропозициональная формула равносильна некоторой ДНФ и некоторой КНФ.

Доказательство.

(первый вариант) *Достаточно заметить, что формула, построенная в доказательстве теоремы о функциональной полноте, является ДНФ.*

Доказательство.

(второй вариант)

Применяем основные эквивалентности.

$A \wedge B$	$\equiv$	$B \wedge A$	$A \vee B$	$\equiv$	$B \vee A$
$A \wedge (B \wedge C)$	$\equiv$	$(A \wedge B) \wedge C$	$A \vee (B \vee C)$	$\equiv$	$(A \vee B) \vee C$
$A \wedge A$	$\equiv$	A	$A \vee A$	$\equiv$	A
$A \wedge (B \vee C)$	$\equiv$	$(A \wedge B) \vee (A \wedge C)$	$A \vee (B \wedge C)$	$\equiv$	$(A \vee B) \wedge (A \vee C)$
$A \vee (A \wedge B)$	$\equiv$	A	$A \wedge (A \vee B)$	$\equiv$	A
$\neg(A \wedge B)$	$\equiv$	$\neg A \vee \neg B$	$\neg(A \vee B)$	$\equiv$	$\neg A \wedge \neg B$
$\neg\neg A$	$\equiv$	A	$A \rightarrow B$	$\equiv$	$\neg A \vee B$

Доказательство.

(второй вариант)

Применяем основные эквивалентности.

$A \wedge B$	$\equiv$	$B \wedge A$	$A \vee B$	$\equiv$	$B \vee A$
$A \wedge (B \wedge C)$	$\equiv$	$(A \wedge B) \wedge C$	$A \vee (B \vee C)$	$\equiv$	$(A \vee B) \vee C$
$A \wedge A$	$\equiv$	A	$A \vee A$	$\equiv$	A
$A \wedge (B \vee C)$	$\equiv$	$(A \wedge B) \vee (A \wedge C)$	$A \vee (B \wedge C)$	$\equiv$	$(A \vee B) \wedge (A \vee C)$
$A \vee (A \wedge B)$	$\equiv$	A	$A \wedge (A \vee B)$	$\equiv$	A
$\neg(A \wedge B)$	$\equiv$	$\neg A \vee \neg B$	$\neg(A \vee B)$	$\equiv$	$\neg A \wedge \neg B$
$\neg\neg A$	$\equiv$	A	$A \rightarrow B$	$\equiv$	$\neg A \vee B$

1. Выразим $\to$ через $\neg$ и $\vee$;
2. Проносим все отрицания максимально вглубь формулы по правилам де Моргана;
3. Удаляем многократные отрицания.
4. Выносим все дизъюнкции максимально наружу, пользуясь дистрибутивностью;
5. Пользуясь ассоциативностью $\wedge$ и $\vee$ расставляем правильно скобки.

1. Выразим $\rightarrow$ через $\neg$ и $\vee$;
2. Проносим все отрицания максимально вглубь формулы по правилам де Моргана;
3. Удаляем многократные отрицания.
4. Выносим все дизъюнкции максимально наружу, пользуясь дистрибутивностью;
5. Пользуясь ассоциативностью $\wedge$ и $\vee$ расставляем правильно скобки.

1. Выразим $\longrightarrow$ через $\neg$ и $\vee$;
2. Проносим все отрицания максимально вглубь формулы по правилам де Моргана;
3. Удаляем многократные отрицания.
4. Выносим все дизъюнкции максимально наружу, пользуясь дистрибутивностью;
5. Пользуясь ассоциативностью $\wedge$ и $\vee$ расставляем правильно скобки.

1. Выразим $\to$ через $\neg$ и $\vee$;
2. Проносим все отрицания максимально вглубь формулы по правилам де Моргана;
3. Удаляем многократные отрицания.
4. Выносим все дизъюнкции максимально наружу, пользуясь дистрибутивностью;
5. Пользуясь ассоциативностью $\wedge$ и $\vee$ расставляем правильно скобки.

1. Выразим $\to$ через $\neg$ и $\vee$;
2. Проносим все отрицания максимально вглубь формулы по правилам де Моргана;
3. Удаляем многократные отрицания.
4. Выносим все дизъюнкции максимально наружу, пользуясь дистрибутивностью;
5. Пользуясь ассоциативностью $\wedge$ и $\vee$ расставляем правильно скобки.

Пример.

$$(\neg R \to P) \wedge P \equiv (\neg\neg R \vee P) \wedge P \equiv (R \vee P) \wedge P \equiv P$$

Другой вариант: $(R \vee P) \wedge P \equiv (R \wedge P) \vee (P \wedge P)$

Пример.

$$(\neg R \to P) \land P \equiv (\neg\neg R \lor P) \land P \equiv (R \lor P) \land P \equiv P$$

Другой вариант: $(R \lor P) \land P \equiv (R \land P) \lor (P \land P)$

Замечание.
Если A — ДНФ, то $\neg A$ превращается в КНФ после переноса всех отрицаний вглубь и удаления двойных отрицаний.

Для того чтобы получить КНФ формулы A, достаточно применить этот алгоритм к ДНФ формулы $\neg A$.

Опр.

Формула A от переменных $P_1, \ldots, P_n$ называется *совершенной ДНФ*, если A — ДНФ и

- Каждая элем. конъюнкция имеет вид $A_{\vec{x}} \rightleftharpoons \bigwedge_{i=1}^{n} P_i^{x_i}$ для некоторого $\vec{x} \in \mathbb{B}^n$.
- $A = \bigvee_{j=1}^{m} A_{\vec{x}_j}$, где $\vec{x}_1, \ldots \vec{x}_m \in \mathbb{B}^n$ попарно различны и взяты в лексикографическом порядке.

Замечание.

Удобно расширить множество формул константой $\perp$ (ложь) и считать её совершенной ДНФ.

Опр.

Формула A от переменных $P_1, \dots, P_n$ называется *совершенной ДНФ*, если A — ДНФ и

- Каждая элем. конъюнкция имеет вид $A_{\vec{x}} \rightleftharpoons \bigwedge_{i=1}^{n} P_i^{x_i}$ для некоторого $\vec{x} \in \mathbb{B}^n$.
- $A = \bigvee_{j=1}^{m} A_{\vec{x}_j}$, где $\vec{x}_1, \dots \vec{x}_m \in \mathbb{B}^n$ попарно различны и взяты в лексикографическом порядке.

Замечание.

Удобно расширить множество формул константой $\perp$ (ложь) и считать её совершенной ДНФ.

Теорема.

Всякая формула A равносильна некоторой совершенной ДНФ.

Доказательство.

Воспользуемся равносильностями:

1. $A \wedge \neg A \equiv \bot, \quad \bot \wedge A \equiv \bot, \quad \bot \vee A \equiv A$ (удаляем противоречивые конъюнкции)
2. $A \wedge A \equiv A$ (удаляем повторы литералов)
3. $A \equiv (A \wedge B) \vee (A \wedge \neg B)$ (добавляем недостающие переменные)

Теорема.

Всякая формула A равносильна некоторой совершенной ДНФ.

Доказательство.

Воспользуемся равносильностями:

1. $A \wedge \neg A \equiv \bot, \quad \bot \wedge A \equiv \bot, \quad \bot \vee A \equiv A$ (удаляем противоречивые конъюнкции)
2. $A \wedge A \equiv A$ (удаляем повторы литералов)
3. $A \equiv (A \wedge B) \vee (A \wedge \neg B)$ (добавляем недостающие переменные)

Теорема.

Совершенные ДНФ эквивалентных формул (относительно одного набора переменных) графически совпадают.

Доказательство.

Для совершенной ДНФ каждая элем. конъюнкция определяет выполняющую оценку, а сама ДНФ — все такие оценки.

Следствие.

Совершенная ДНФ любой формулы A единственна.

Другие варианты формальной семантики

- Теоретико-множественная семантика.

Пусть U — непустое множество; $\mathcal{P}(U)$ — множество всех его подмножеств.

Оценка $f : \mathrm{Var} \to \mathcal{P}(U)$.

Значение $f(A) \subseteq U$ формулы A при оценке f определяется по правилам:

- $f(\neg A) \rightleftharpoons U \setminus f(A)$
- $f(A \wedge B) \rightleftharpoons f(A) \cap f(B)$
- $f(A \vee B) \rightleftharpoons f(A) \cup f(B)$
- $f(A \to B) \rightleftharpoons (U \setminus f(A)) \cup f(B)$

Значение $f(A) \subseteq U$ формулы A при оценке f определяется по правилам:

- $f(\neg A) \rightleftharpoons U \setminus f(A)$
- $f(A \wedge B) \rightleftharpoons f(A) \cap f(B)$
- $f(A \vee B) \rightleftharpoons f(A) \cup f(B)$
- $f(A \to B) \rightleftharpoons (U \setminus f(A)) \cup f(B)$

Значение $f(A) \subseteq U$ формулы A при оценке f определяется по правилам:

- $f(\neg A) \rightleftharpoons U \setminus f(A)$
- $f(A \wedge B) \rightleftharpoons f(A) \cap f(B)$
- $f(A \vee B) \rightleftharpoons f(A) \cup f(B)$
- $f(A \to B) \rightleftharpoons (U \setminus f(A)) \cup f(B)$

Значение $f(A) \subseteq U$ формулы A при оценке f определяется по правилам:

- $f(\neg A) \rightleftharpoons U \setminus f(A)$
- $f(A \wedge B) \rightleftharpoons f(A) \cap f(B)$
- $f(A \vee B) \rightleftharpoons f(A) \cup f(B)$
- $f(A \to B) \rightleftharpoons (U \setminus f(A)) \cup f(B)$

Значение $f(A) \subseteq U$ формулы A при оценке f определяется по правилам:

- $f(\neg A) \rightleftharpoons U \setminus f(A)$
- $f(A \wedge B) \rightleftharpoons f(A) \cap f(B)$
- $f(A \vee B) \rightleftharpoons f(A) \cup f(B)$
- $f(A \to B) \rightleftharpoons (U \setminus f(A)) \cup f(B)$

Замечание.

Если взять $U = \{0\}$, теоретико-множественная семантика сводится к стандартной двузначной: $Л = \varnothing$, $И = U$.

Замечание.

Если взять $U = \mathbb{R}^2$ и если для $P \in \mathrm{Var}\ f(P)$ — круги на плоскости, получаем *диаграммы Венна*, известные из школы.

- Алгебраическая семантика.

Опр.

Множество **B** с заданными на нём константами 0, 1 и операциями $\neg$, $\wedge$, $\vee$, $\rightarrow$, которые удовлетворяют равенствам

$$a \wedge \neg a = 0, \quad a \vee \neg a = 1$$

и равенствам, соответствующим таблице основных эквивалентностей, называется *булевой алгеброй*.

(Читаем $\equiv$ как $=$; a, b, c означают элементы множества **B**.)

$a \wedge b = b \wedge a$	$a \vee b = b \vee a$
$a \wedge (b \wedge c) = (a \wedge b) \wedge c$	$a \vee (b \vee c) = (a \vee b) \vee c$
$a \wedge a = a$	$a \vee a = a$
$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$	$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
$a \vee (a \wedge b) = a$	$a \wedge (a \vee b) = a$
$\neg(a \wedge b) = \neg a \vee \neg b$	$\neg(a \vee b) = \neg a \wedge \neg b$
$\neg\neg a = a$	$a \rightarrow b = \neg a \vee b$
$a \wedge \neg a = 0$	$a \vee \neg a = 1$

Пример.

$$a \vee 1 = a \vee (a \vee \neg a) = (a \vee a) \vee \neg a = a \vee \neg a = 1$$

$$a \wedge 1 = a \wedge (a \wedge 1) = a \wedge (a \vee (a \wedge \neg a)) = a \wedge (a \vee 0) = a$$

$a \wedge b$	$=$	$b \wedge a$	$a \vee b$	$=$	$b \vee a$
$a \wedge (b \wedge c)$	$=$	$(a \wedge b) \wedge c$	$a \vee (b \vee c)$	$=$	$(a \vee b) \vee c$
$a \wedge a$	$=$	a	$a \vee a$	$=$	a
$a \wedge (b \vee c)$	$=$	$(a \wedge b) \vee (a \wedge c)$	$a \vee (b \wedge c)$	$=$	$(a \vee b) \wedge (a \vee c)$
$a \vee (a \wedge b)$	$=$	a	$a \wedge (a \vee b)$	$=$	a
$\neg(a \wedge b)$	$=$	$\neg a \vee \neg b$	$\neg(a \vee b)$	$=$	$\neg a \wedge \neg b$
$\neg\neg a$	$=$	a	$a \to b$	$=$	$\neg a \vee b$
$a \wedge \neg a$	$=$	0	$a \vee \neg a$	$=$	1

Пример.

$$a \vee 1 = a \vee (a \vee \neg a) = (a \vee a) \vee \neg a = a \vee \neg a = 1$$

$$a \wedge 1 = a \wedge (a \wedge 1) = a \wedge (a \vee (a \wedge \neg a)) = a \wedge (a \vee 0) = a$$

Примеры булевых алгебр

- $\mathbb{B}$
- $\mathcal{P}(U)$ для любого U
- $\mathrm{Fm}/\equiv$ (*алгебра Линденбаума*), то есть множество классов равносильных формул с синтаксически определёнными операциями $\wedge$, $\vee$, $\rightarrow$, $\neg$.

Примеры булевых алгебр

- $\mathbb{B}$
- $\mathcal{P}(U)$ для любого U
- $\mathrm{Fm}/\equiv$ (*алгебра Линденбаума*), то есть множество классов равносильных формул с синтаксически определёнными операциями $\wedge$, $\vee$, $\to$, $\neg$.

Примеры булевых алгебр

- $\mathbb{B}$
- $\mathcal{P}(U)$ для любого U
- $\mathrm{Fm}/\equiv$ (*алгебра Линденбаума*), то есть множество классов равносильных формул с синтаксически определёнными операциями $\wedge$, $\vee$, $\rightarrow$, $\neg$.

Оценка $f : \mathrm{Var} \to \mathbf{B}$.
Значение $f(A) \in \mathbf{B}$ формулы A вычисляется в соответствии с заданными на $\mathbf{B}$ операциями.

Каждая из указанных семантик задаёт одно и то же множество тавтологий, то есть имеет место следующая теорема (без доказательства).

Теорема.

Для любого множества U и любой булевой алгебры $\boldsymbol{B}$ равносильны следующие утверждения.

1. *A — тавтология;*
2. *$f(A) = U$ для любой оценки $f : \mathrm{Var} \to \mathcal{P}(U)$;*
3. *$f(A) = 1$ для любой оценки $f : \mathrm{Var} \to \boldsymbol{B}$.*

Исчисление высказываний

Аксиомы:

1. $A \to (B \to A)$,
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$,
3. $A \wedge B \to A, \quad A \wedge B \to B$,
4. $A \to (B \to A \wedge B)$,
5. $A \to A \vee B, \quad B \to A \vee B$,
6. $(A \to C) \to ((B \to C) \to (A \vee B \to C))$,
7. $(A \to B) \to ((A \to \neg B) \to \neg A)$,
8. $\neg\neg A \to A$.

Правило вывода (*modus ponens*):

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

Опр.

Выводом называется конечная последовательность формул, каждая из которых является аксиомой или получается из некоторых предыдущих формул по правилу вывода.

Правило вывода (*modus ponens*):

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

Опр.

Выводом называется конечная последовательность формул, каждая из которых является аксиомой или получается из некоторых предыдущих формул по правилу вывода.

Пример.

$P \to Q \vee P$ (аксиома 5)

$Q \to Q \vee P$ (аксиома 5)

$(P \to Q \vee P) \to ((Q \to Q \vee P) \to (P \vee Q \to Q \vee P))$

$(Q \to Q \vee P) \to (P \vee Q \to Q \vee P)$ (MP)

$P \vee Q \to Q \vee P$ (MP)

Пример.

$P \to Q \vee P$ (аксиома 5)

$Q \to Q \vee P$ (аксиома 5)

$(P \to Q \vee P) \to ((Q \to Q \vee P) \to (P \vee Q \to Q \vee P))$

$(Q \to Q \vee P) \to (P \vee Q \to Q \vee P)$ (MP)

$P \vee Q \to Q \vee P$ (MP)

Пример.

$P \to Q \vee P$ (аксиома 5)

$Q \to Q \vee P$ (аксиома 5)

$(P \to Q \vee P) \to ((Q \to Q \vee P) \to (P \vee Q \to Q \vee P))$

$(Q \to Q \vee P) \to (P \vee Q \to Q \vee P)$ (MP)

$P \vee Q \to Q \vee P$ (MP)

Пример.

$P \to Q \vee P$ (аксиома 5)

$Q \to Q \vee P$ (аксиома 5)

$(P \to Q \vee P) \to ((Q \to Q \vee P) \to (P \vee Q \to Q \vee P))$

$(Q \to Q \vee P) \to (P \vee Q \to Q \vee P)$ (MP)

$P \vee Q \to Q \vee P$ (MP)

Пример.

$P \to Q \vee P$ (аксиома 5)

$Q \to Q \vee P$ (аксиома 5)

$(P \to Q \vee P) \to ((Q \to Q \vee P) \to (P \vee Q \to Q \vee P))$

$(Q \to Q \vee P) \to (P \vee Q \to Q \vee P)$ (MP)

$P \vee Q \to Q \vee P$ (MP)

Опр.

Формула A называется *выводимой* в исчислении высказываний или *теоремой* исчисления высказываний (обозначение $\vdash A$), если существует вывод, в котором последняя формула есть A.

Пример.

$\vdash P \vee Q \to Q \vee P$.

Пример.

$\vdash A \to A$.

Доказательство.

В аксиоме 2 возьмём $B = (A \to A)$ и $C = A$.

$(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$ (2)

$A \to ((A \to A) \to A)$ (1)

$(A \to (A \to A)) \to (A \to A)$ (MP)

$A \to (A \to A)$ (1)

$A \to A$ (MP)

Пример.

$\vdash A \to A$.

Доказательство.

В аксиоме 2 возьмём $B = (A \to A)$ и $C = A$.

$(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$ (2)

$A \to ((A \to A) \to A)$ (1)

$(A \to (A \to A)) \to (A \to A)$ (MP)

$A \to (A \to A)$ (1)

$A \to A$ (MP)

Пример.

$\vdash A \to A$.

Доказательство.

В аксиоме 2 возьмём $B = (A \to A)$ и $C = A$.

$(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$ (2)

$A \to ((A \to A) \to A)$ (1)

$(A \to (A \to A)) \to (A \to A)$ (MP)

$A \to (A \to A)$ (1)

$A \to A$ (MP)

Пример.

$\vdash A \to A$.

Доказательство.

В аксиоме 2 возьмём $B = (A \to A)$ и $C = A$.

$$(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A)) \quad (2)$$

$$A \to ((A \to A) \to A) \quad (1)$$

$$(A \to (A \to A)) \to (A \to A) \quad (\mathrm{MP})$$

$$A \to (A \to A) \quad (1)$$

$$A \to A \quad (\mathrm{MP})$$

Пример.

$\vdash A \to A$.

Доказательство.

В аксиоме 2 возьмём $B = (A \to A)$ и $C = A$.

$(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$ (2)

$A \to ((A \to A) \to A)$ (1)

$(A \to (A \to A)) \to (A \to A)$ (MP)

$A \to (A \to A)$ (1)

$A \to A$ (MP)

Пример.

$\vdash A \to A$.

Доказательство.

В аксиоме 2 возьмём $B = (A \to A)$ и $C = A$.

$$(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A)) \quad (2)$$

$$A \to ((A \to A) \to A) \quad (1)$$

$$(A \to (A \to A)) \to (A \to A) \quad (\mathrm{MP})$$

$$A \to (A \to A) \quad (1)$$

$$A \to A \quad (\mathrm{MP})$$

Выводимость из гипотез

Опр.

Пусть Γ — некоторое множество формул, называемых *гипотезами*.

Выводом из Γ называется конечная последовательность формул, каждая из которых либо принадлежит множеству Γ, либо является аксиомой, либо получается из предыдущих формул по правилу вывода.

Пример.

Вывод из множества гипотез $\{P \wedge Q\}$:

$$
\begin{array}{ll}
P \wedge Q & \text{(гипотеза)} \\
P \wedge Q \to P & \\
P & \text{(MP)} \\
P \wedge Q \to Q & \\
Q & \text{(MP)} \\
Q \to (P \to Q \wedge P) & \\
P \to Q \wedge P & \text{(MP)} \\
Q \wedge P & \text{(MP)}
\end{array}
$$

Опр.

Формула A называется *выводимой из множества формул* Γ (обозначение $\Gamma \vdash A$), если существует вывод из Γ, в котором последняя формула есть A.

Замечание.

Вместо $\{B_1, \ldots, B_n\} \vdash A$ обычно пишут $B_1, \ldots, B_n \vdash A$. Выражение $\Gamma \vdash A, B$ означает $\Gamma \vdash A$ и $\Gamma \vdash B$.

Пример.

$P \wedge Q \vdash Q \wedge P$.

Опр.

Формула A называется *выводимой из множества формул* Γ (обозначение $\Gamma \vdash A$), если существует вывод из Γ, в котором последняя формула есть A.

Замечание.

Вместо $\{B_1, \ldots, B_n\} \vdash A$ обычно пишут $B_1, \ldots, B_n \vdash A$. Выражение $\Gamma \vdash A, B$ означает $\Gamma \vdash A$ и $\Gamma \vdash B$.

Пример.

$P \wedge Q \vdash Q \wedge P$.

Опр.

Формула A называется *выводимой из множества формул* Γ (обозначение $\Gamma \vdash A$), если существует вывод из Γ, в котором последняя формула есть A.

Замечание.

Вместо $\{B_1, \ldots, B_n\} \vdash A$ обычно пишут $B_1, \ldots, B_n \vdash A$. Выражение $\Gamma \vdash A, B$ означает $\Gamma \vdash A$ и $\Gamma \vdash B$.

Пример.

$P \wedge Q \vdash Q \wedge P$.

Свойства выводимости из гипотез

- Если $\Delta \subseteq \Gamma$ и $\Delta \vdash A$, то $\Gamma \vdash A$ (*монотонность*).
- Если $\Gamma \vdash A$, то существует такое конечное множество $\Delta \subseteq \Gamma$, что $\Delta \vdash A$ (*компактность*).
- Если $\Gamma \vdash A$ и для каждой формулы $B \in \Gamma$ имеет место $\Delta \vdash B$, то $\Delta \vdash A$ (*транзитивность*).

Свойства выводимости из гипотез

- Если $\Delta \subseteq \Gamma$ и $\Delta \vdash A$, то $\Gamma \vdash A$ (*монотонность*).
- Если $\Gamma \vdash A$, то существует такое конечное множество $\Delta \subseteq \Gamma$, что $\Delta \vdash A$ (*компактность*).
- Если $\Gamma \vdash A$ и для каждой формулы $B \in \Gamma$ имеет место $\Delta \vdash B$, то $\Delta \vdash A$ (*транзитивность*).

Свойства выводимости из гипотез

- Если $\Delta \subseteq \Gamma$ и $\Delta \vdash A$, то $\Gamma \vdash A$ (*монотонность*).
- Если $\Gamma \vdash A$, то существует такое конечное множество $\Delta \subseteq \Gamma$, что $\Delta \vdash A$ (*компактность*).
- Если $\Gamma \vdash A$ и для каждой формулы $B \in \Gamma$ имеет место $\Delta \vdash B$, то $\Delta \vdash A$ (*транзитивность*).

Корректность исчисления высказываний

Предложение.

Всякая выводимая формула является тавтологией.

Доказательство.

Индукция по длине вывода формулы A.

Предложение.

Если $\Gamma \vdash A$, то $\Gamma \models A$.

Корректность исчисления высказываний

Предложение.

Всякая выводимая формула является тавтологией.

Доказательство.

Индукция по длине вывода формулы A.

Предложение.

Если $\Gamma \vdash A$, то $\Gamma \models A$.

Теорема о дедукции для исчисления высказываний

Теорема.
Если $\Gamma \cup \{A\} \vdash B$, *то* $\Gamma \vdash (A \to B)$.

Упрощает построение выводов в исчислении высказываний.

Доказательство.

Индукция по длине вывода формулы B из множества гипотез $\Gamma \cup \{A\}$.

Если B является аксиомой или принадлежит Γ, то:

$$\begin{array}{ll} B & \\ B \to (A \to B) & (1) \\ A \to B & \text{(MP)} \end{array}$$

Если $B = A$, то используем вывод $A \to A$.

Доказательство.

Индукция по длине вывода формулы B из множества гипотез $\Gamma \cup \{A\}$.

Если B является аксиомой или принадлежит Γ, то:

$$\begin{array}{ll} B & \\ B \to (A \to B) & (1) \\ A \to B & (\mathrm{MP}) \end{array}$$

Если $B = A$, то используем вывод $A \to A$.

Доказательство.

Индукция по длине вывода формулы B из множества гипотез $\Gamma \cup \{A\}$.

Если B является аксиомой или принадлежит Γ, то:

$$
\begin{array}{ll}
B & \\
B \to (A \to B) & (1) \\
A \to B & \text{(MP)}
\end{array}
$$

Если $B = A$, то используем вывод $A \to A$.

Пусть B получена из C и $C \to B$ по modus ponens.

Имеем $\Gamma \vdash (A \to C)$ и $\Gamma \vdash (A \to (C \to B))$ по предположению индукции.

Соединяем эти два вывода и достраиваем так:

$$(A \to (C \to B)) \to ((A \to C) \to (A \to B)) \quad (2)$$

$$(A \to (C \to B)) \to (A \to B) \quad \text{(MP)}$$

$$A \to B \quad \text{(MP)}$$

Пусть B получена из C и $C \to B$ по modus ponens.

Имеем $\Gamma \vdash (A \to C)$ и $\Gamma \vdash (A \to (C \to B))$ по предположению индукции.

Соединяем эти два вывода и достраиваем так:

$$(A \to (C \to B)) \to ((A \to C) \to (A \to B)) \quad (2)$$

$$(A \to (C \to B)) \to (A \to B) \quad \text{(MP)}$$

$$A \to B \quad \text{(MP)}$$

Пусть B получена из C и $C \to B$ по modus ponens.

Имеем $\Gamma \vdash (A \to C)$ и $\Gamma \vdash (A \to (C \to B))$ по предположению индукции.

Соединяем эти два вывода и достраиваем так:

$$(A \to (C \to B)) \to ((A \to C) \to (A \to B)) \qquad (2)$$
$$(A \to (C \to B)) \to (A \to B) \qquad \text{(MP)}$$
$$A \to B \qquad \text{(MP)}$$

Замечание.

Вместо $\Gamma \cup \{A\} \vdash B$ обычно пишут $\Gamma, A \vdash B$.

Следствие.

$\Gamma, A \vdash B \iff \Gamma \vdash A \to B$

Полезные выводимые правила

Пример.
(*силлогизм*) $A \to B,\ B \to C \vdash A \to C$.

Доказательство.
Дважды по правилу modus ponens выводим

$$A, A \to B, B \to C \vdash C.$$

Применяем теорему о дедукции.

Полезные выводимые правила

Пример.

(*силлогизм*) $A \to B,\ B \to C \vdash A \to C$.

Доказательство.

Дважды по правилу modus ponens выводим

$$A, A \to B, B \to C \vdash C.$$

Применяем теорему о дедукции.

Пример.

(*контрапозиция*) $A \to B \vdash \neg B \to \neg A$.

Доказательство.

Достаточно вывести $A \to B,\ \neg B \vdash \neg A$.

$A \to B$	
$\neg B$	
$(A \to B) \to ((A \to \neg B) \to \neg A)$	
$(A \to \neg B) \to \neg A$	(MP)
$\neg B \to (A \to \neg B)$	
$A \to \neg B$	(MP)
$\neg A$	(MP)

Пример.

(*контрапозиция*) $A \to B \vdash \neg B \to \neg A$.

Доказательство.

Достаточно вывести $A \to B,\ \neg B \vdash \neg A$.

$A \to B$

$\neg B$

$(A \to B) \to ((A \to \neg B) \to \neg A)$

$(A \to \neg B) \to \neg A$ (MP)

$\neg B \to (A \to \neg B)$

$A \to \neg B$ (MP)

$\neg A$ (MP)

Пример.

(*контрапозиция*) $A \to B \vdash \neg B \to \neg A$.

Доказательство.

Достаточно вывести $A \to B,\ \neg B \vdash \neg A$.

$$
\begin{array}{ll}
A \to B & \\
\neg B & \\
(A \to B) \to ((A \to \neg B) \to \neg A) & \\
(A \to \neg B) \to \neg A & (\mathrm{MP}) \\
\neg B \to (A \to \neg B) & \\
A \to \neg B & (\mathrm{MP}) \\
\neg A & (\mathrm{MP})
\end{array}
$$

Пример.

(*контрапозиция*) $A \to B \vdash \neg B \to \neg A$.

Доказательство.

Достаточно вывести $A \to B,\ \neg B \vdash \neg A$.

$$
\begin{array}{ll}
A \to B & \\
\neg B & \\
(A \to B) \to ((A \to \neg B) \to \neg A) & \\
(A \to \neg B) \to \neg A & \text{(MP)} \\
\neg B \to (A \to \neg B) & \\
A \to \neg B & \text{(MP)} \\
\neg A & \text{(MP)}
\end{array}
$$

Пример.

(*контрапозиция*) $A \to B \vdash \neg B \to \neg A$.

Доказательство.

Достаточно вывести $A \to B,\ \neg B \vdash \neg A$.

$$
\begin{array}{ll}
A \to B & \\
\neg B & \\
(A \to B) \to ((A \to \neg B) \to \neg A) & \\
(A \to \neg B) \to \neg A & \text{(MP)} \\
\neg B \to (A \to \neg B) & \\
A \to \neg B & \text{(MP)} \\
\neg A & \text{(MP)}
\end{array}
$$

Пример.

(*контрапозиция*) $A \to B \vdash \neg B \to \neg A$.

Доказательство.

Достаточно вывести $A \to B,\ \neg B \vdash \neg A$.

$A \to B$

$\neg B$

$(A \to B) \to ((A \to \neg B) \to \neg A)$

$(A \to \neg B) \to \neg A$ (MP)

$\neg B \to (A \to \neg B)$

$A \to \neg B$ (MP)

$\neg A$ (MP)

Пример.

(*контрапозиция*) $A \to B \vdash \neg B \to \neg A$.

Доказательство.

Достаточно вывести $A \to B,\ \neg B \vdash \neg A$.

$$
\begin{array}{ll}
A \to B & \\
\neg B & \\
(A \to B) \to ((A \to \neg B) \to \neg A) & \\
(A \to \neg B) \to \neg A & \text{(MP)} \\
\neg B \to (A \to \neg B) & \\
A \to \neg B & \text{(MP)} \\
\neg A & \text{(MP)}
\end{array}
$$

Пример.

(*контрапозиция*) $A \to B \vdash \neg B \to \neg A$.

Доказательство.

Достаточно вывести $A \to B,\ \neg B \vdash \neg A$.

$$A \to B$$
$$\neg B$$
$$(A \to B) \to ((A \to \neg B) \to \neg A)$$
$$(A \to \neg B) \to \neg A \qquad \text{(MP)}$$
$$\neg B \to (A \to \neg B)$$
$$A \to \neg B \qquad \text{(MP)}$$
$$\neg A \qquad \text{(MP)}$$

Пример.

(*контрапозиция*) $A \to B \vdash \neg B \to \neg A$.

Доказательство.

Достаточно вывести $A \to B,\ \neg B \vdash \neg A$.

$$A \to B$$

$$\neg B$$

$$(A \to B) \to ((A \to \neg B) \to \neg A)$$

$$(A \to \neg B) \to \neg A \qquad \text{(MP)}$$

$$\neg B \to (A \to \neg B)$$

$$A \to \neg B \qquad \text{(MP)}$$

$$\neg A \qquad \text{(MP)}$$

Пример.

(*ex falso*) $A, \neg A \vdash B$.

ex falso sequitur quodlibet (лат.) «из ложного следует всё, что угодно»

Доказательство.

Выводим, опираясь на аксиомы 1 (дважды), 7 и 8:

$$A, \neg A \vdash \neg B \to A, \neg B \to \neg A \vdash \neg\neg B \vdash B.$$

Пример.

(*ex falso*) $A, \neg A \vdash B$.

ex falso sequitur quodlibet (лат.) «из ложного следует всё, что угодно»

Доказательство.

Выводим, опираясь на аксиомы 1 (дважды), 7 и 8:

$$A, \neg A \vdash \neg B \to A, \neg B \to \neg A \vdash \neg\neg B \vdash B.$$