ИСЧИСЛЕНИЕ ВЫСКАЗЫВАНИЙ

1. Формальные теории

Одним из основных понятий математической логики является понятие формальной теории или исчисления. Это понятие было первоначально разработано для формализации логики и теории доказательств. Формальная теория является эффективным механизмом получения новых теорем. Кроме того, аппарат формальной теории позволяет решать задачи, связанные с математическим моделированием различных явлений и процессов.

Формальная теория считается заданной, если известны следующие четыре составляющих:

1. *Алфавит* – конечное или счетное множество символов.
2. *Формулы*, которые по специальным правилам строятся из символов алфавита. Формулы, как правило, составляют счетное множество.
   Алфавит и формулы определяют язык или сигнатуру формальной теории.
3. *Аксиомы* – выделенное из множества формул специальное подмножество. Множество аксиом может быть конечным или бесконечным. Бесконечное множество аксиом задается с помощью конечного множества *схем аксиом* и правил порождения конкретных аксиом из схемы аксиом. Различают два вида аксиом: *логические* (общие для класса формальных теорий) и *собственные* (определяющие содержание конкретной теории).
4. *Правила вывода* – множество отношений (как правило, конечное) на множестве формул, позволяющие из аксиом получать теоремы формальной теории.

Обратите внимание, что здесь аксиомы – это необязательно утверждения, не требующие доказательства.

Определение. *Выводом* формальной теории называется последовательность формул A_1, A_2, …, A_n, в которой все формулы – либо аксиомы, либо получаются из предыдущих по правилам вывода.

Говорят, что формула A *выводима* из множества формул Γ (обозначение: $\Gamma \vdash A$), если существует вывод A_1, A_2, …, A_n, где $A_n = A$, и есть три возможности:

- $A_i \in \Gamma$;
- A_i - аксиома;
- A_i получаются из предыдущих формул по правилам вывода.

Формулы из множества Γ называются *посылками* или *гипотезами* вывода.

Примеры выводов мы рассмотрим в определенных формальных теориях.

В частном случае, когда $\Gamma = \varnothing$, имеет место обозначение: $\vdash A$, и формула Γ называется *выводимой* в данной теории (или *теоремой* данной теории). Иногда значок $\vdash$ записывается так: $\vdash_K$, где K – обозначение данной теории.

2. Исчисление высказываний

Исчисление высказываний (теория L) определяется следующими компонентами.

1. Алфавит составляют:

- Пропозициональные переменные (от англ. proposition – высказывание) – заглавные буквы латинского алфавита (иногда с индексами – натуральными числами): $A, B, C, \ldots$, $A_1, B_1, C_1, \ldots$
- Логические связки: $\neg, \to$.
- Скобки: (,).

Иногда в исчислении высказываний допускаются формулы с другими логическими связками, но при этом учитывается, как они выражаются через инверсию и импликацию. Так, $A \wedge B = \neg(A \to \neg B)$, $A \vee B = \neg A \to B$. Такие записи являются удобными сокращениями.

2. Формулы определяются так же, как в главе 1.

Определение. 1) Всякая пропозициональная переменная есть формула.
2) Если A, B – формулы, то формулами являются также $\neg A$, $A \to B$.
3) Никаких других формул нет.

3. Аксиомы задаются тремя схемами аксиом:

А1. $A \to (B \to A)$.

А2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$.

А3. $(\neg B \to \neg A) \to ((\neg B \to A) \to B)$.

Существуют исчисления высказываний с другим набором логических связок и другими схемами аксиом, но в данном пособии они не рассматриваются.

4. Правило вывода Modus ponens (сокращенно MP) – правило отделения (лат.).

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

Здесь A, B – любые формулы. Таким образом, множество аксиом исчисления высказываний, заданное тремя схемами аксиом, бесконечно. Множество правил вывода задано одной схемой, и также бесконечно.

Теорема. Все теоремы исчисления высказываний – тавтологии.

Доказательство. Докажем сначала, что аксиомы А1 – А3 являются тавтологиями.

Предположим, что

$$|A \to (B \to A)| = 0 \Leftrightarrow \begin{cases} |A| = 1, \\ |B \to A| = 0, \end{cases} \Leftrightarrow \begin{cases} |A| = 1, \\ |B| = 1, \\ |A| = 0. \end{cases}$$

Полученное противоречие доказывает, что аксиома А1 – тавтология.

Предположим, что

$$|(A \to (B \to C)) \to ((A \to B) \to (A \to C))| = 0 \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} |A \to (B \to C)| = 1, \\ |(A \to B) \to (A \to C)| = 0, \end{cases} \Leftrightarrow \begin{cases} |A \to (B \to C)| = 1, \\ |A \to B| = 1, \\ |A \to C| = 0, \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} |A \to (B \to C)| = 1, \\ |A \to B| = 1, \\ |A| = 1, \\ |C| = 0, \end{cases} \Leftrightarrow \begin{cases} |A \to (B \to C)| = 1, \\ |B| = 1, \\ |A| = 1, \\ |C| = 0, \end{cases} \Leftrightarrow \begin{cases} |B \to C| = 1, \\ |B| = 1, \\ |A| = 1, \\ |C| = 0, \end{cases} \Leftrightarrow \begin{cases} |C| = 1, \\ |B| = 1, \\ |A| = 1, \\ |C| = 0. \end{cases}$$

Полученное противоречие доказывает, что аксиома А2 – тавтология.

Предположим, что

$$|(\neg B \to \neg A) \to ((\neg B \to A) \to B)| = 0 \Leftrightarrow \begin{cases} |\neg B \to \neg A| = 1, \\ |(\neg B \to A) \to B| = 0, \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} |\neg B \to \neg A| = 1, \\ |\neg B \to A| = 1, \\ |B| = 0, \end{cases} \Leftrightarrow \begin{cases} |\neg B| = 1, \\ |\neg B \to \neg A| = 1, \\ |\neg B \to A| = 1, \\ |B| = 0, \end{cases} \Leftrightarrow \begin{cases} |\neg A| = 1, \\ |A| = 1, \\ |B| = 0, \end{cases} \Leftrightarrow \begin{cases} |A| = 0, \\ |A| = 1, \\ |B| = 0. \end{cases}$$

Полученное противоречие доказывает, что аксиома А3 – тавтология.

Таким образом, все аксиомы исчисления высказываний представляют собой тавтологии. Теоремы выводятся по правилу вывода МР, следовательно, по ранее полученным результатам, также являются тавтологиями, что и требовалось доказать.

Следствие. Исчисление высказываний непротиворечиво.

Доказательство. Предположим противное, то есть в исчислении есть теоремы A и $\neg A$. По доказанной теореме, A и $\neg A$ являются тавтологиями (тождественно истинными формулами), следовательно, формула A одновременно является тождественно истинной и тождественно ложной, что является противоречием.

3. Теорема дедукции

Теорема тождества. $\vdash A \to A$.

Доказательство. Построим вывод формулы $A \to A$.

1. $A \to (A \to A)$. А1 с подстановкой вместо B – A.
2. $A \to ((A \to A) \to A)$. А1 с подстановкой вместо B – $A \to A$.
3. $(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$

   А2 с подстановкой вместо C – A, а вместо B – $A \to A$.
4. $((A \to A) \to A) \to (A \to A)$. МР 2,3.
5. $A \to A$. МР 1,4.

Что и требовалось доказать.

Теорема дедукции. Пусть Γ – множество формул, A, B – формулы. Тогда Γ, $A \vdash B \Rightarrow \Gamma \vdash A \to B$.

В частности, если $\Gamma = \varnothing$, то если $A \vdash B \Rightarrow \vdash A \to B$.

Доказательство. Пусть B_1, B_2, …, $B_n = B$, – вывод из Γ и A. Методом математической индукции докажем, что $\Gamma \vdash A \to B_i$, $i = 1,2,\ldots,n$.

1) Проверим, что утверждение $\Gamma \vdash A \to B_i$ справедливо при $i = 1$, то есть $\Gamma \vdash A \to B_1$.

Для B_1 возможны три варианта: $B_1 \in \Gamma$, B_1 – аксиома, $B_1 = A$.

а) Пусть $B_1 \in \Gamma$ или B_1 – аксиома. Построим вывод:

1. B_1.
2. $B_1 \to (A \to B_1)$. A1 с подстановкой вместо A – B_1, вместо B – A.
3. $A \to B_1$. MP 1, 2.

Таким образом, $\Gamma \vdash A \to B_1$.

б) Пусть $B_1 = A$. По лемме, $\vdash A \to A = A \to B_1$. Таким образом, $\Gamma \vdash A \to B_1$.

2) Пусть утверждение $\Gamma \vdash A \to B_i$ верно при $i = 1,2,\ldots,k$, $k \le n$. Докажем утверждение для $i = k+1$, то есть $\Gamma \vdash A \to B_{k+1}$.

Для формулы B_{k+1} есть следующие возможности: $B_{k+1} \in \Gamma$, B_{k+1} – аксиома, $B_{k+1} = A$, которые рассматриваются аналогично предыдущему пункту, и новая возможность: B_{k+1} получается из предыдущих формул B_1, B_2, …, B_k, по правилу Modus ponens. Последний случай рассмотрим подробно.

Среди формул B_1, B_2, …, B_k есть формулы (может быть, и не одна) вида B_j, $1 \le j \le k$, такие, что имеет место формула $B_j \to B_{k+1}$ (которая также присутствует в выводе), поэтому и возможно применение правила Modus ponens.

По предположению индукции, $\Gamma \vdash A \to B_j$, $\Gamma \vdash A \to (B_j \to B_{k+1})$.

Построим вывод:

1. $A \to B_j$.
2. $A \to (B_j \to B_{k+1})$.
3. $(A \to (B_j \to B_{k+1})) \to ((A \to B_j) \to (A \to B_{k+1}))$. A2 с подстановкой вместо B – B_j, вместо C – B_{k+1}.
4. $(A \to B_j) \to (A \to B_{k+1})$. MP 2, 3.
5. $A \to B_{k+1}$.

Таким образом, доказано, что $\Gamma \vdash A \to B_{k+1}$, следовательно, по методу математической индукции, $\Gamma \vdash A \to B_n$, то есть $\Gamma \vdash A \to B$. Теорема доказана.

Справедлива и обратная теорема.

Теорема. $\Gamma \vdash A \to B \Rightarrow \Gamma, A \vdash B$.

Доказательство. Построим вывод:

1. Γ.
2. A.
3. $A \to B$. По условию теоремы, эта формула выводима из Γ.
4. B. MP 2, 3.

Теорема доказана.

На основании теоремы дедукции получена теорема о полноте исчисления высказываний.

Теорема о полноте. Всякая тавтология является теоремой исчисления высказываний.

Следствие. Множество всех теорем исчисления высказываний совпадает с множеством всех тавтологий.

Теорема дедукции позволяет строить выводы многих формул в исчислении высказываний.

4. Построение вывода в логике высказываний

Теорема о контрапозиции. Выводима формула $(\neg B \to \neg A) \to (A \to B)$. Сокращенно это записывается так: $\vdash (\neg B \to \neg A) \to (A \to B)$.

Доказательство. По теореме, обратной теореме дедукции, посылку можно перенести в левую часть:
$\neg B \to \neg A \vdash A \to B$.

Проделаем эту операцию еще раз:
$\neg B \to \neg A,\ A \vdash B$.

Таким образом, нам нужно доказать, что из формул $\neg B \to \neg A$ и A выводима формула B. Составим вывод формулы B. В каждой строке вывода записывается только одна формула. В правой части страницы удобно указывать комментарий, – что собой эта формула представляет. Возможны варианты:

- гипотеза,
- аксиома (может быть, с какими-то подстановками),
- ранее доказанная теорема,
- формула получена из предыдущих формул по правилу Modus ponens.

Вначале мы запишем гипотезы.

1. $\neg B \to \neg A$ – гипотеза.
2. A – гипотеза.

Формулу B удобно получить из аксиомы А3. Поэтому запишем эту аксиому:

3. $(\neg B \to \neg A) \to ((\neg B \to A) \to B)$ А3.

К формулам 1 и 3 можно применить правило вывода Modus ponens (что мы и отметим в комментарии). Порядок номеров формул существенен (первой указывается посылка).

4. $(\neg B \to A) \to B$. MP 1, 3.

Посылку в формуле 4 можно получить из аксиомы А1, если заменить B на $\neg B$:

5. $A \to (\neg B \to A)$. А1 с подстановкой вместо B – $\neg B$.

Далее дважды применяем правило Modus ponens:

6. $\neg B \to A$. MP 2, 5.
7. B. MP 6, 4.

Вывод построен, и применением теоремы дедукции мы доказали выводимость первоначальной формулы.

Отметим, что вывод может быть неединственным, в частности, формулы могут быть записаны в другом порядке. Решение данной задачи может быть оформлено следующим образом:

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

По теореме, обратной теореме дедукции,

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

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

1. $\neg B \to \neg A$ – гипотеза.	
2. A – гипотеза.	
3. $A \to (\neg B \to A)$.	A1, $B : \neg B$.
4. $\neg B \to A$.	MP 2, 3.
5. $(\neg B \to \neg A) \to ((\neg B \to A) \to B)$.	A3.
6. $(\neg B \to A) \to B$.	MP 1, 5.
7. B.	MP 4, 6.

Следующая теорема более проста, но достаточно показательна. Обратите внимание, что здесь не используются ни аксиомы, ни теоремы.

Теорема о силлогизме. $\vdash (C \to A) \to ((A \to B) \to (C \to B))$

Доказательство строится только на основании правила MP.

По теореме, обратной теореме дедукции,

$C \to A \vdash (A \to B) \to (C \to B)$.

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

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

1. $A \to B$ – гипотеза.	
2. $C \to A$ – гипотеза.	
3. C – гипотеза.	
4. A.	MP 3,2.
5. B.	MP 4,1.

5. Метод резолюций в логике высказываний

Метод резолюций – это метод автоматического доказательства теорем – основы логического программирования. Это алгоритм, проверяющий отношение выводимости $\Gamma \vdash A$. В общем случае алгоритм автоматического доказательства теорем не существует, но для формальных теорий с несложной структурой (таких как исчисление высказываний, исчисление предикатов с одним одноместным предикатом) подобные алгоритмы известны.

Вообще говоря, в построенном в главе 3 исчислении высказываний (благодаря полноте исчисления) проверка выводимости формулы состоит в проверке того, является ли формула тавтологией или нет. Это можно легко установить по таблицам истинности. Но этот метод не обеспечивает построения вывода формулы.

Метод резолюций – классический алгоритм автоматического доказательства теорем. Для простоты изложения рассмотрим его для исчисления высказываний. Для любого множества формул Γ и любой формулы A метод дает утвердительный ответ, если $\Gamma \vdash A$, и дает отрицательный ответ, если неверно, что $\Gamma \vdash A$.

Теорема о доказательстве от противного. Если $\Gamma, \neg A \vdash F$, где F – тождественно ложная формула, то $\Gamma \vdash A$.

Доказательство.

Доказательство проведем для частного случая, когда Γ представляет собой одну формулу. По теореме дедукции, $\Gamma, \neg A \vdash F \Leftrightarrow \Gamma \to (\neg A \to F)$ – тавтология.

Преобразуем правую часть равносильности, учитывая, что формула F тождественно ложна.

$\Gamma \to (\neg A \to F) = \neg\Gamma \vee (\neg\neg A \vee F) = \neg\Gamma \vee A \vee F = \neg\Gamma \vee A = = \Gamma \to A$ – тавтология $\Leftrightarrow$ $\Gamma \vdash A$, что и требовалось доказать.

Как правило, в качестве формулы F используют пустую формулу □, которая не имеет никакого значения ни в какой интерпретации, и, по определению, является противоречием.

Метод резолюций использует специальную форму формул, которая называется предложением.

Определение. Предложением называется дизъюнкция формул вида A или $\neg A$, где A – атом (буква).

Любая формула исчисления высказываний может быть преобразована в предложение следующей последовательностью действий:

1. Замена импликации по формуле: $A \to B = \neg A \vee B$ (проверьте самостоятельно). В результате в формуле остаются связки: $\neg$, $\vee$, $\wedge$.
2. Преобразование выражений с инверсиями по закону двойного отрицания: $\neg\neg A = A$, законам де Моргана: $\neg(A \vee B) = \neg A \wedge \neg B$, $\neg(A \wedge B) = \neg A \vee \neg B$. В результате инверсии остаются только перед буквами.
3. Приведение формулы к конъюнктивной нормальной форме с помощью дистрибутивных законов:
   $$A \wedge (B \vee C) = (A \wedge B) \vee (A \wedge C),$$
   $$A \vee (B \wedge C) = (A \vee B) \wedge (A \vee C).$$
4. Преобразование конъюнктивной нормальной формы во множество предложений: $AB \Rightarrow A, B$.

Напомним, что связки $\vee$, $\wedge$ используются здесь для удобства записи.

Определение. Множество формул называется невыполнимым, если оно не имеет модели, то есть интерпретации, в которой все формулы истинны.

Без доказательства приведем следующую теорему.

Теорема. Если из формулы A получено множество Δ предложений, то формула A тождественно ложна тогда и только тогда, когда множество Δ невыполнимо.

До сих пор мы пользовались только одним правилом вывода – Modus ponens. В других исчислениях высказываний имеют место и другие правила вывода.

Правило резолюций. Даны предложения: $C_1 = P \vee C_1'$, $C_2 = \neg P \vee C_2'$, где P – пропозициональная буква, C_1' и C_2' – предложения (в частности, пустые или содержащие только одну букву или ее отрицание). Правило резолюций формулируется так: $C_1,\ C_2 \vdash C_1' \vee C_2'$.

$C_1,\ C_2$ называются *резольвируемыми предложениями*, а $C_1' \vee C_2'$ – *резольвентой*. Правило резолюций будем обозначать R.

Теорема. Резольвента логически следует из резольвируемых предложений.

Доказательство. В вышеприведенных обозначениях, нам нужно доказать, что $C_1 \to \left(C_2 \to \left(C_1' \vee C_2'\right)\right)$ – тавтология (по теореме дедукции).

Предположим, что $\left|C_1 \to \left(C_2 \to \left(C_1' \vee C_2'\right)\right)\right| = 0 \Leftrightarrow$

$$\Leftrightarrow \begin{cases} |C_1| = 1, \\ \left|C_2 \to \left(C_1' \vee C_2'\right)\right| = 0, \end{cases} \Leftrightarrow \begin{cases} |C_1| = 1, \\ |C_2| = 1, \\ \left|C_1' \vee C_2'\right| = 0, \end{cases} \Leftrightarrow \begin{cases} |C_1| = 1, \\ |C_2| = 1, \\ \left|C_1'\right| = 0, \\ \left|C_2'\right| = 0, \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} \left|C_1' \vee P\right| = 1, \\ \left|C_2' \vee \neg P\right| = 1, \\ \left|C_1'\right| = 0, \\ \left|C_2'\right| = 0, \end{cases} \Leftrightarrow \begin{cases} |P| = 1, \\ |\neg P| = 1, \\ \left|C_1'\right| = 0, \\ \left|C_2'\right| = 0, \end{cases} \Leftrightarrow \begin{cases} |P| = 1, \\ |P| = 0, \\ \left|C_1'\right| = 0, \\ \left|C_2'\right| = 0. \end{cases}$$

Полученное противоречие доказывает утверждение теоремы.

Правило резолюций применяется в опровержении методом резолюций – алгоритме, устанавливающем выводимость $\Gamma \vdash A$.

Запишем $\neg A$. Каждая формула из множества Γ и формула $\neg A$ независимо преобразуются во множество предложений. В этом множестве нужно найти резольвируемые предложения и применить к ним правило резолюций. Резольвенты добавляются во множество предложений до тех пор, пока не будет получено пустое предложение. Возможны два случая:

Среди множества предложений нет резольвируемых. Вывод: теорема опровергнута, и формула A не выводима из множества формул Γ.

- Получено пустое предложение. Теорема доказана. Имеет место выводимость $\Gamma \vdash A$.

Примеры.

1. Методом резолюций доказать теорему $\vdash \neg A \to (A \to B)$.

Доказательство. Запишем инверсию исходной формулы:
$\neg\left(\neg A \to \left(A \to B\right)\right)$.

Заменим все импликации по соответствующей формуле:
$\neg\left(\neg A \to \left(A \to B\right)\right) = \neg\left(\neg\neg A \vee \left(\neg A \vee B\right)\right)$.

Применим закон двойного отрицания и закон де Моргана:

$\neg(\neg A \to (A \to B)) = \neg(A \vee (\neg A \vee B)) = \neg A \wedge \neg(\neg A \vee B) =$
$= \neg A \wedge \neg\neg A \wedge \neg B = \neg A \wedge A \wedge \neg B.$

Получаем предложения: $\neg A,\ A,\ \neg B$. Резольвируем их:

1. $\neg A$ – предложение.
2. A – предложение.
3. $\neg B$ – предложение.
4. □. R 1, 2.

2. Методом резолюций доказать теорему
$\vdash A \to (B \to A \wedge B).$

Доказательство. Запишем инверсию исходной формулы:
$\neg(A \to (B \to A \wedge B)).$

Заменим все импликации по соответствующей формуле:
$\neg(A \to (B \to A \wedge B)) = \neg(\neg A \vee (\neg B \vee A \wedge B)).$

Применим закон двойного отрицания и закон де Моргана:
$\neg(A \to (B \to A \wedge B)) = \neg\neg A \wedge \neg(\neg B \vee (A \wedge B)) =$
$= A \wedge B \wedge \neg(A \wedge B) = A \wedge B \wedge (\neg A \vee \neg B).$

Получаем предложения: $A,\ B,\ \neg A \vee \neg B$.

1. A – предложение.
2. B – предложение.
3. $\neg A \vee \neg B$ – предложение.
4. $\neg B$. R 1, 3.
5. □. R 2, 4.