ЛЕКЦИОННЫЙ КУРС
ПО МАТЕМАТИЧЕСКОЙ ЛОГИКЕ И ТЕОРИИ АЛГОРИТМОВ

(автор – разработчик курса: к.ф.-м.н., доцент кафедры «вычислительной техники и электроники» Иордан В.И.)

ЛЕКЦИЯ 1

ВВЕДЕНИЕ

Логика – это наука о законах и формах «познающего мышления». Логика изучает мышление, мыслительные процессы, направленные на обнаружение и обоснование истины, на поиск путей преодоления трудностей в решении задач в различных сферах деятельности человека, в т.ч. в решении задач с помощью «искусственного интеллекта».

Логику интересует лишь форма и законы мышления, но не содержание (точнее говоря, содержание в меньшей степени), т.е. логика сходна с грамматикой языковых выражений и проверяет их на истинность. При изучении логики вводят различные *формальные языки*, структура которых всегда проще, чем структура естественных языков общения. Например, алгоритмические языки программирования к ним также относятся: к *функциональным языкам* относятся ЛИСП, Clean и др., а в качестве языка *логического программирования* можно упомянуть язык ПРОЛОГ.

Математическая логика (МЛ) – это логика, развиваемая с помощью математических методов, т.е. логика, используемая в математике. МЛ занимается построением *формальных теорий и формальных языков*, предназначенных для представления таких фундаментальных понятий, как «отношение», «функция», «аксиома», доказательство (теорема) и изучением основанных на этих понятиях «логических и логико-математических исчислений». МЛ позволила определить понятия «алгоритма», «вычислимой функции», развила семантику формальных языков и теорий, построила систему «логического вывода», которую пытаются реализовать в области IT в виде системы «искусственного интеллекта (искусственного разума)».

Формальные теории в своей основе состоят из четырех компонентов: а) алфавит языка; б) формулы языка исчисления, которые с использованием алфавита образуют *формальный язык*; в) аксиомы; г) правила «вывода» - правила построения «новых» формул по уже имеющимся формулам.

ЧАСТЬ I. МАТЕМАТИЧЕСКАЯ ЛОГИКА

ГЛАВА 1. АЛГЕБРА ВЫСКАЗЫВАНИЙ. ИСЧИСЛЕНИЕ ВЫСКАЗЫВАНИЙ

1.1. Высказывания и логические «связки» (логические операции)

Логика (алгебра) высказываний изучает связи между высказываниями, т.е. одни высказывания строятся по определенным правилам синтаксиса из других, в т.ч. из *элементарных* высказываний (ЭВ).

Определение 1. *Высказывание* – это утверждение, иначе говоря, языковое предложение (не обязательно сформулированное человеком, например, выражение на алгоритмическом языке), которое в результате логического анализа может быть признано либо «*истинным* (true)», либо «*ложным* (false)».

Определение 2. *Высказывание*, построенное с помощью логических операций (связок) из элементарных высказываний (ЭВ), называется «*составным*» высказыванием (СВ).

Обозначения логических связок:

а) отрицание (инверсия): $\neg$;

б) конъюнкция (логическое умножение, операция «И»): $\wedge$ или &;

в) дизъюнкция (логическое сложение, операция «ИЛИ»): $\vee$ или +;

г) импликация: $\rightarrow$.

Элементарные высказывания обозначаются пропозициональными переменными: A, B, C, либо переменными с индексами: A1, A2…..

Определение 3. *Отрицанием (инверсией)* высказывания А, обозначаемым C= ┐A= или $C = \overline{A}$, называется высказывание, которое *истинно* тогда и только тогда, когда высказывание А *ложно*.

Читается как «**не А**», «**неверно что А**».

Определение 4. *Конъюнкцией* (*логическим умножением*) высказываний А и В, обозначаемой C=A∧B=A&B, называется высказывание С, которое *истинно* тогда и только тогда, когда оба высказывания А и В одновременно *истинны*.

Читается как «**А вместе с В**», «**как А, так и В**».

Определение 5. *Дизъюнкцией* (*логическим сложением, неразделительной дизъюнкцией*) высказываний А и В, обозначаемой C=A∨B=A+B, называется высказывание, которое *ложно* тогда и только тогда, когда оба высказывания А и В одновременно *ложны*.

Читается как «**А или В**». Иногда дизъюнкцию поясняют грамматической конструкцией «**и/или**», т.е. акцентируется *истинность дизъюнкции* в случае *истинности* обоих высказываний А и В. «*Разделительная дизъюнкция*» («*исключающее* ИЛИ», «*арифметическая сумма по модулю* 2»), обозначаемая $C = A \vee \vee B = A \oplus B$, оказывается *ложной* в отличие от *неразделительной дизъюнкции* C=A∨B при одновременной *истинности* высказываний А и В.

Определение 6. *Импликацией* высказываний А и В, обозначаемой C=A→B, называется высказывание, которое *ложно* тогда и только тогда, когда высказывание А *истинно*, а высказывание В *ложно*.

Читается как: «**из А следует В**», «**если А, то В**», «**для А необходимо В**», «**для В достаточно А**». Высказывание А называется «***условием***» или «***посылкой***», а высказывание В называется «***заключением*** (***следствием***)».

Определение 7. *Эквиваленцией* высказываний А и В, обозначаемой $C = A \Leftrightarrow B = (A \equiv B)$, называется высказывание, которое *истинно* тогда и только тогда, когда оба высказывания одновременно либо *истинны*, либо *ложны*.

Осмысление **Определений 1-7** позволяет записать сводную «таблицу истинности» приведенных выше логических связок (операций).

A	B	┐A=$\overline{A}$	┐B=$\overline{B}$	A∧B=A&B	A∨B	$A \vee\vee B = A \oplus B$	A→B	$A \Leftrightarrow B$
0	0	1	1	0	0	0	1	1
0	1	1	0	0	1	1	1	0
1	0	0	1	0	1	1	0	0
1	1	0	0	1	1	0	1	1

ЛЕКЦИЯ 2

1.2. Формулы «Исчисления высказываний (ИВ)». Интерпретация формул

Определение 1. *Формулой* (*пропозициональной формулой*) называется составное (в том числе и элементарное) высказывание, которое, используя алфавит пропозициональных переменных, строится согласно следующим правилам синтаксиса:

1. Любая пропозициональная переменная – это формула.
2. Если А и В – формулы, то формулами будут и следующие структуры: ┐A=$\overline{A}$, ┐B=$\overline{B}$, A→B.
3. Формулами будут являться только лишь те высказывания, которые построены по правилам 1 и 2.

Замечание: «забегая вперед», в «исчислении высказываний (ИВ)» оперируют лишь двумя логическими операциями (достаточно лишь двух операций): отрицанием и импликацией. В «алгебре высказываний» (в более широкой теории, чем ИВ) дополнительными конструкциями (структурами) формул будут: A∧B=A&B, A∨B, $A \vee\vee B = A \oplus B$, $A \Leftrightarrow B$. Иногда говорят, что формулы в ИВ исчисляются «*по индукции*» или «*по структуре*».

Определение 2. *Подформулой* В формулы А называется любое высказывание, входящее в составное высказывание А и являющееся формулой.

Примеры: а) A&B→&C∨D – это не формула, так как записаны две подряд операции (импликация и конъюнкция); б) (A&B)→(C∨D).

Определение 3. *Интерпретацией* формулы А (обозначение I(A)) называется *определение значений истинности* (*ложности*) формулы А при подстановке конкретных *истинностных* значений вместо входящих в формулу А пропозициональных переменных.

Определение 4. Формула А называется *выполнимой*, если она *истинна* в некоторой интерпретации, т.е. принимает значение 1 (“логической единицы”), и называется *опровержимой*, если она ложна в некоторой интерпретации (принимает значение 0 – «логического нуля»).

Определение 5. Формула А называется *общезначимой* или *тождественно-истинной* или *тавтологией*, если она *истинна* во всевозможных интерпретациях.

Определение 6. Формула А называется *невыполнимой* или *противоречивой* или *противоречием*, если она *ложна* во всевозможных интерпретациях.

Примеры: а) $A \vee \overline{A}$ – это тавтология (в обоих возможных случаях интерпретации равна 1). На «латыни» читается как «tertium non datur” («третьего не дано» или «закон исключенного третьего»); б) $A \wedge \overline{A}$ – это противоречие (в обоих возможных случаях интерпретации равно 0); в) формула A→B будет *выполнимой* в трех случаях интерпретации (см. выше таблицу истинности) и в одном случае (A=1 и B=0) формула оказывается *опровержимой*.

Групповая теорема 1. Пусть А некоторая формула. Тогда:
1) если А – тавтология, тогда $\overline{A}$ – противоречие, и наоборот;
2) если А – противоречие, то $\overline{A}$ – тавтология, и наоборот;
3) если А – тавтология, то неверно, что А – противоречие, но не наоборот;
4) если А – противоречие, то неверно, что А – тавтология, но не наоборот.

Доказательство следует из определений – достаточно просто проверяется таблицей истинности.

Теорема 2. Если формулы А и (А→В) – *тавтологии*, тогда формула В также является *тавтологией* (частный случай правила вывода «Modus Ponens» в ИВ).

Доказательство осуществим методом «*от противного*»:
Пусть I(B) = 0. По условию теоремы I(A) = 1. Тогда интерпретация формулы I(A→B) равна 0, что противоречит условию о том, что (А→В) – *тавтология*. Следовательно, предположение I(B) = 0 не верно, а верно условие I(B) = 1. Поэтому формула В во всех интерпретациях *истинна* и является *тавтологией* – теорема доказана.

Наиболее важные тавтологии

1. $A \vee \overline{A}$ – закон исключенного третьего или «третьего не дано» (лат., “tertium non datur”).
2. А→А
3. А→(В→А) – аксиома «упрощения» в системе аксиом ИВ.
4. (А→В) →((В→С) →(А→С)) – «цепное рассуждение».
5. А→(В→С))→((А→В)→(А→С) – аксиома «самодистрибутивности» в системе аксиом ИВ.
6. (А&В)→А; (А&В)→В
7. А→(АvВ); В→(АvВ)
8. А→(В→(А&В))
9. $A \to (A \vee B) = A \to (\overline{\overline{A}} \vee B) = A \to (\overline{A} \to B)$
10. $(\overline{B} \to \overline{A}) \to ((\overline{B} \to A) \to B)$
11. ((А→В)→А)→А – закон Пирса.

Замечание: многие формулировки теорем можно представить в виде логических схем (формул высказываний):

1. для так называемой *прямой теоремы* верна формула A→B;
2. теорема, представленная в *обратной* формулировке (*обратная теорема*), соответствует формуле B→A;
3. *противоположная* по отношению к *прямой* формулировке теоремы соответствует формуле $\overline{A} \to \overline{B}$;
4. *противоположная обратной* формулировке теоремы соответствует формуле $\overline{B} \to \overline{A}$, которая эквивалентна формулировке *прямой теоремы*, т.е. $\overline{B} \to \overline{A} = A \to B$. Другими словами, *противоположная обратной* формулировке *прямой* теоремы представляет собой так называемый метод доказательства «*от противного (обратного)*».

ЛЕКЦИЯ 3

1.3. Логическое следование (следствие). Логическая эквивалентность – равносильность формул. Основные равносильности (правила равносильных преобразований). Правило подстановки. Теоремы «о равносильностях»

Определение 1. Формула B называется *логическим следованием* формулы A, если формула B *истинна* во всех тех случаях интерпретации, в которых *истинна* формула A. Обозначение: A=>B

Определение 2. Формулы A и B *логически эквивалентны*, если они являются логическим следствием друг друга, иначе говоря, если совпадают их значения *истинности* во всех интерпретациях. Обозначается A⇔B.

Основные эквивалентности:

1. A∧B=B∧A, A∨B=B∨A – коммутативность;
2. (A∧B) ∧C=A∧(B∧C), (A∨B)∨C=A∨(B∨C) – ассоциативность;

3. A∧(B∨C)=(A∧B)∨(A∧V), A∨(B∧C)=(A∨B)∧(A∨C) – дистрибутивность;

4. A∧(A∨B)=A, A∨(A∧B)=A – поглощение;

5. $\overline{A \wedge B} = \overline{A} \vee \overline{B}$, $\overline{A \vee B} = \overline{A} \wedge \overline{B}$ – правила де Моргана;

6. A∧A=A, A∨A=A – идемпотентность;

7. A∨0=A, A∧0=0 – свойства «нуля»;

8. A∨1=1, A∧1=A – свойства «единицы»;

9. (A∧B)∨($A \wedge \overline{B}$)=A∧(B∨$\overline{B}$)=A∧1=A – «склеивание» (преобразования в прямом направлении) и «расщепление» (преобразования в обратном направлении);

   (A∨B)∧($A \vee \overline{B}$)=A∨(B∧$\overline{B}$)=A∧0=A – «склеивание» (преобразования в прямом направлении) и «расщепление» (преобразования в обратном направлении);

10. $\overline{\overline{A}} = A$ – инволютивность, (A→B)= $A \to B = \overline{A} \vee B$.

Теорема 1. Формула Q является *логическим следованием* формулы $P_1 \wedge P_2 \wedge .... \wedge P_n$ тогда и только тогда, когда формула $P_1 \wedge P_2 \wedge .... \wedge P_n \to Q$ является тавтологией.

1. *Доказательство прямой теоремы (необходимость).* Дано: верна формула логического следования $P_1 \wedge P_2 \wedge .... \wedge P_n \Rightarrow Q$. Доказать, что формула $P_1 \wedge P_2 \wedge .... \wedge P_n \to Q$ является тавтологией. Возможны два случая:

а) для логического следования: $I(P_1 \wedge P_2 \wedge .... \wedge P_n)$=1 и $I(Q)$=1. Тогда $I(P_1 \wedge P_2 \wedge .... \wedge P_n \to Q)$=1.

б) $I(P_1 \wedge P_2 \wedge .... \wedge P_n)$=0. Тогда $I(P_1 \wedge P_2 \wedge .... \wedge P_n \to Q)$=1 при любом значении формулы Q. Т.о., формула $P_1 \wedge P_2 \wedge .... \wedge P_n \to Q$ является тавтологией.

2. *Доказательство обратной теоремы (достаточность).* Дано: формула $P_1 \wedge P_2 \wedge .... \wedge P_n \to Q$ является тавтологией. Доказать, что верна формула логического следования $P_1 \wedge P_2 \wedge .... \wedge P_n \Rightarrow Q$.

Пусть $I(P_1 \wedge P_2 \wedge .... \wedge P_n)$=1. Тогда $I(Q)$=1, иначе бы формула $P_1 \wedge P_2 \wedge .... \wedge P_n \to Q$ не была бы тавтологией. Т.о., согласно определению *логического следования* формула $P_1 \wedge P_2 \wedge .... \wedge P_n \Rightarrow Q$ выполнима (верна).

Теорема 2. Формула Q является *логическим следованием* формулы $P_1 \wedge P_2 \wedge .... \wedge P_n$ тогда и только тогда, когда формула $P_1 \wedge P_2 \wedge .... \wedge P_n \wedge \overline{Q}$ является *противоречием*.

Доказательство. На основании предыдущей теоремы выполнимость формулы *логического следования* $P_1 \wedge P_2 \wedge .... \wedge P_n \Rightarrow Q$ эквивалентна тому, что формула $P_1 \wedge P_2 \wedge .... \wedge P_n \to Q$ является *тавтологией*. Тогда ее отрицание должно быть противоречием, т.е. формула $\overline{P_1 \wedge P_2 \wedge .... \wedge P_n \to Q}$ – противоречие. В последней формуле заменим по равносильности импликацию: $\overline{P_1 \wedge P_2 \wedge .... \wedge P_n \to Q} = \overline{\overline{P_1 \wedge P_2 \wedge .... \wedge P_n} \vee Q}$ – противоречие. Далее, используя правила Моргана, получим $\overline{\overline{P_1 \wedge P_2 \wedge .... \wedge P_n} \vee Q} = \overline{\overline{P_1 \wedge P_2 \wedge .... \wedge P_n}} \wedge \overline{Q}$ и, используя свойство инволютивности, получим $P_1 \wedge P_2 \wedge .... \wedge P_n \wedge \overline{Q}$ – противоречие. Теорема доказана.

Сохранение свойства «тавтологии» при подстановке формул вместо аргументов

Рассмотрим два случая подстановки каких-либо формул вместо аргумента x исходной формулы $A(……., x, ……)$.

Обозначение подстановки $A(……., x, ……)\{B/x\}$ подразумевает подстановку формулы В вместо некоторых вхождений аргумента x в формулу $A(……., x, ……)$, т.е. не обязательно вместо всех вхождений.

Обозначение подстановки $A(……., x, ……)\{B//x\}$ подразумевает подстановку формулы B вместо всех вхождений аргумента x в формулу $A(……., x, ……)$ без исключения.

Теорема 3. Если формула $A(\ldots\ldots., x, \ldots\ldots)$ – тавтология, то для любой формулы В результат ее подстановки в исходную формулу (тавтологию) является также тавтологией, т.е. $C{=}A(\ldots\ldots., x, \ldots\ldots)\{B//x\}$ – тавтология.

Доказательство. Возможны два значения (0 или 1) переменной x, вместо которой в исходной формуле-тавтологии $A(\ldots\ldots., x, \ldots\ldots)$ производится подстановка формулы B, которая также может принимать только два таких же значения (0 или 1). Поэтому формула $C{=}A(\ldots\ldots., x, \ldots\ldots)\{B//x\}$ также будет принимать только значение 1 аналогично исходной формуле-тавтологии $A(\ldots\ldots., x, \ldots\ldots)$. Теорема доказана.

Вывод: операция подстановки сохраняет свойство «*тавтологичности*» для результата подстановки в случае, когда исходная формула является тавтологией.

Следствие из теоремы 3. Пусть $C{=}A(\ldots\ldots., x, \ldots\ldots)\{B//x\}$, т.е. $C{=}A(\ldots\ldots., B, \ldots\ldots)$. Кроме того, имеется формула D, логически эквивалентная формуле B, т.е. $D{\equiv}B$. Тогда результат подстановки $A(\ldots\ldots., B, \ldots\ldots)\{D/B\}$ логически эквивалентен формуле $C{=}A(\ldots\ldots., B, \ldots\ldots)$.