ВВЕДЕНИЕ. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Все математические дисциплины можно условно разделить на *дискретные* и *непрерывные*. Дискретная математика – это та часть математики, главной особенностью которой является изучение отдельных объектов, без привлечения понятия непрерывности, т.е. дискретность – это антипод непрерывности. В дискретной математике отсутствует понятие предельного перехода, присущее классической, «непрерывной» математике. Она занимается изучением дискретных структур, которые возникают как внутри математики, так и в ее приложениях. Однако она зародилась в глубокой древности, раньше, чем непрерывная математика, хотя особую значимость приобрела только в последние десятилетия, в связи с повсеместным внедрением в практику информационных технологий.

Таким образом, в широком смысле дискретная математика включает в себя все разделы математики, в которых не используются топологические методы, в частности понятие непрерывности. Это – все разделы алгебры, математическая логика, почти вся теория чисел (в том числе всевозможные компьютерные арифметики), многие разделы экономико-математических методов, комбинаторика и многие другие дисциплины. В более узком смысле дискретная математика – это те разделы математической логики, алгебры, теории чисел и математической кибернетики, которые непосредственно составляют теоретический фундамент информатики. В этом узком смысле дискретная математика включает в себя теорию булевых функций и их минимизацию, теорию графов и многие разделы теоретической кибернетики, теорию автоматов и формальных грамматик, комбинаторику, теорию алгоритмов (в том числе теорию сложности вычислений), криптографию и теорию кодирования.

Некоторые из вышеперечисленных разделов имеют не только многочисленные «внутренние» (с точки зрения специалиста по информационным системам или вычислительной техники) приложения, используемые, к примеру, при построении различных дискретных устройств, в программировании и т.д., но их результаты и методы применяются также при решении многих нужных для практики задач. Например, при рассмотрении транспортных задач, для нахождения оптимальных решений в управлении, для выделения «узких мест» при планировании и разработке проектов, при составлении оптимальных расписаний, а также при моделировании сложных технологий и процессов различной природы.

Целью изучения дисциплины является ознакомление студентов с системой понятий и некоторыми наиболее важными в приложениях методами теории множеств, математической логики, теории булевых функций и теории графов. Знания и навыки, полученные при ее изучении, используются в дисциплинах: «Информатика», «Программирование», «Структуры и алгоритмы обработки данных в ЭВМ», «Базы данных», «Экспертные и интеллектуальные системы» и т.д. Но в особенности знания по дискретной математике пригодятся при изучении дисциплин, связанных с функциональным и логическим программированием, кодированием и защитой информации.

Основная задача состоит в том, чтобы будущие специалисты чётко освоили основные понятия и приёмы работы с булевыми функциями и графами: построение таблиц значений; поиск и исключение фиктивных переменных; приведение булевых функций к стандартной форме (д.н.ф., к.н.ф., многочлен Жегалкина); основные методы минимизации булевых функций; построение диаграммы (рисунка) графа по его матрицам смежности и инцидентности и обратная задача; установление изоморфизма (одинаковости) графов; определение основных характеристик и свойств графов (векторы степеней, планарность, эйлеровость, гамильтоновость и т.п.); изучение важного частного случая графов – деревьев и их свойств.

За недостатком места о приложениях говорится относительно мало. Однако такие примеры содержатся в литературе.

Данное пособие предназначено в основном для изучения основ именно дискретной математики в узком понимании слова, хотя при этом затронуты основополагающие разделы математической логики – исчисление высказываний и исчисление предикатов. Однако математическую логику настоятельно рекомендуется изучать по более фундаментальным источникам, например, [1, 11,15,16,19,23,29]. В то же время, многие разделы дискретной математики в узком смысле слова в данном пособии никак не отражены, в частности, теория кодирования и криптография, теория алгоритмов и теория сложности вычислений. Это связано, в первую очередь, с ограниченностью отводимого времени для изучения дисциплины в учебных планах у студентов, обучающихся информационным технологиям и использованию вычислительной техники. Курс лекций будет также полезен будущим специалистам по прикладной математике, в частности по математическому и компьютерному моделированию.

Пособие – это существенно поработанный и дополненный вариант пособий [20,21].

ЧАСТЬ ПЕРВАЯ. ЭЛЕМЕНТЫ ТЕОРИИ МНОЖЕСТВ И МАТЕМАТИЧЕСКОЙ ЛОГИКИ

Как уже отмечалось выше во «Введении» это пособие не предназначено для глубокого изучения основ математики, в частности математической логики и теории множеств. Тем не менее, изложенного здесь материала по этим разделам математики вполне достаточно для будущих инженеров почти по всем техническим специальностям, в том числе по математическому и компьютерному моделированию.

1 МНОЖЕСТВА. ОПЕРАЦИИ НАД НИМИ. СВОЙСТВА МНОЖЕСТВ

2 БИНАРНЫЕ ОТНОШЕНИЯ. ВАЖНЕЙШИЕ ТИПЫ БИНАРНЫХ ОТНОШЕНИЙ

3 БУЛЕВЫ АЛГЕБРЫ. ВЫСКАЗЫВАНИЯ И ОПЕРАЦИИ НАД НИМИ. СЛОЖНЫЕ ВЫСКАЗЫВАНИЯ КАК БУЛЕВЫ ФУНКЦИИ

4 ИСЧИСЛЕНИЕ ВЫСКАЗЫВАНИЙ. МЕТОДЫ ДОКАЗАТЕЛЬСТВ В ЛОГИКЕ ВЫСКАЗЫВАНИЙ. ТЕОРЕМА О ПОЛНОТЕ ИСЧИСЛЕНИЯ ВЫСКАЗЫВАНИЙ

См. лекции 1-4

5 ПРЕДИКАТЫ И КВАНТОРЫ. НЕКОТОРЫЕ ПРАВИЛА ДЕЙСТВИЙ С КВАНТОРАМИ. ПРИМЕНЕНИЯ ЯЗЫКА ФОРМУЛ ДЛЯ ЗАПИСИ СЛОЖНЫХ УТВЕРЖДЕНИЙ

5.1 Предикаты и кванторы

Развитием алгебры высказываний является логика предикатов. Это тоже логическая система или определенный язык описания знаний. В логике предикатов наряду с высказываниями рассматриваются более сложные утверждения, называемые *предикатами*.

5.1.1 Рассмотрим вначале некоторые

Примеры 5.1 а) «x – простое число». Это выражение не является высказыванием, пока мы не заменим переменную x на какое-либо определенное число. При x=1 и x =6 получим ложное высказывание, при x=3 или x=7 – истинное. Таким образом, выражение «x – простое число» есть некоторая функция $P(x)$, зависящая от переменной x. Область определения $P(x)$ – множество целых чисел, область значений $P(x)$ – высказывания.

б) «x больше y». Это выражение можно рассматривать как функцию $Q(x,y)$, зависящую от переменных x и y. Она становится высказыванием после того, как x и y заменим их значениями.

В общем случае под *предикатом от n переменных* (или *n-арным предикатом*) понимается утверждение $P(x_1,x_2,..,x_n)$, которое становится высказыванием (т.е. истинным или ложным) после подстановки вместо переменных $x_1,x_2,..,x_n$ их конкретных значений из множеств $M_1,M_2,...,M_n$, соответственно. Элементы этих множеств называются иногда *предметами*, а переменные $x_1,x_2,..,x_n$ – *предметными переменными*. Множества $M_1,M_2,...,M_n$ называют *сортами* переменных. Множество $M_1\times M_2\times...\times M_n$ (декартово произведение, см. подраздел 1.4) упорядоченных наборов длины n называется в этом случае *областью определения* (или *полем*) предиката $P(x_1,x_2,..,x_n)$. Если число предметных переменных равно нулю, то предикат есть высказывание.

Замечание. Термин «поле» в указанном выше смысле – название устаревшее. В современной алгебре и математической логике за термином «поле» закреплён другой смысл.

Будем обозначать:

$x,y,z,..,x_1,x_2,x_3,...$ (малые буквы конца латинского алфавита, возможно с индексами) – предметные переменные;

$a,b,c,..,a_1,a_2,a_3,...$ (малые буквы начала латинского алфавита, возможно с индексами) – предметы из множеств $M_1,M_2,..,M_n$;

$A(x)$, B, $F(x,y)$, $P(x_1,x_2,..,x_n)$,... – предикаты. Символы 0,1, как и прежде, обозначают ложь и истину, соответственно.

5.1.2 К предикатам можно применять операции алгебры высказываний (конъюнкцию, дизъюнкцию, импликацию, эквивалентность, отрицание) и получать новые предикаты. Это действительно так: заменяя предметные переменные в предикатах их значениями из некоторого множества предметов, мы получим высказывания истинные или ложные, а применяя к ним операции логики высказываний, получим новые высказывания.

Например, «$x = y \vee x < y$» – – новый предикат, полученный применением операции дизъюнкции из предикатов «$x = y$» и «$x < y$».

5.1.3 Помимо операций алгебры высказываний в логике предикатов есть две специфические операции, связанные с природой предикатов. Эти операции вначале определим для одноместных предикатов.

5.1.3.1 Пусть дан предикат $P(x)$, зависящий от одной переменной и определенный на множестве M.

Выражение $\forall xP(x)$ (читается: «для всякого x, верно $P(x)$») означает высказывание, истинное только в том случае, когда предикат $P(x)$ истинен *для всех элементов* множества M. Здесь символ $\forall$ – знак *квантора всеобщности*.

Выражение $\exists xP(x)$ (читается: «существует x такой, что $P(x)$ верно») означает высказывание, истинное только в том случае, когда предикат $P(x)$ истинен *хотя бы для одного элемента* из M; символ $\exists$ – знак *квантора существования*.

Примеры 5.2 Применение кванторов. Пусть даны предикаты над множеством натуральных чисел:

а) $x^2 = xx$, тогда $\forall x(x^2 = xx)$ – истинное высказывание;

б) $x+2 = 7$, тогда $\forall x(x+2=7)$ – ложное, а $\exists x(x+2=7)$ – истинное высказывание;

в) $x+2 = x$, тогда $\exists x(x+2 = x)$ и $\forall x(x+2 = x)$ – ложные высказывания.

5.1.3.2 Случай, когда предикат зависит от n переменных. Пусть $G(x_1,x_2,...,x_n)$ – предикат от переменных $x_1,x_2,...,x_n$ над «полем» $M= M_1\times M_2\times...\times M_n$. Подставим вместо переменных $x_1,...,x_{i-1},x_{i+1},...,x_n$ элементы $a_1,...,a_{i-1}, a_{i+1},...,a_n$ из множеств $M_1,...,M_{i-1},M_{i+1},...,M_n$, соответственно. Получим предикат $G(a_1,...,a_{i-1},x_i,a_{i+1},...,a_n)$, зависящий только от одной переменной x_i. Следовательно, выражение $\forall x_iG(a_1,...,a_{i-1},x_i,a_{i+1},...,a_n)$ есть высказывание. Поэтому выражение $\forall x_iG(x_1,..,x_{i-1}, x_i,x_{i+1},..,x_n)$ есть предикат от $n-1$ переменной. Он не зависит от x_i. Значение его для данного набора $(a_1,...,a_{i-1}, a_{i+1},...,a_n)$ равно истине, если предикат $G(a_1,...,a_{i-1},x_i,a_{i+1},...,a_n)$ истинен для всякого элемента (предмета) x_i из M_i.

Аналогичные рассуждения можно провести для квантора вида $\exists x$. С помощью операций конъюнкции, дизъюнкции, импликации, эквивалентности, отрицания, а также операций «навешивания» кванторов можно получать более сложные предикаты. При этом вхождения предметных переменных, по отношению к которым применялись операции «навешивания» кванторов, называются *связанными*, а остальные вхождения – *свободными*.

П р и м е р 5.3 В формуле $\forall x A(\underline{x},y) \vee \exists z \forall y(B(\underline{z},\underline{y},t) \to A(\underline{z},\underline{y}))$ первое вхождение переменной x, оба вхождения z, второе и третье y – связанные (они подчёркнуты), а первое вхождение y и единственное вхождение переменной t – свободные. Обратите внимание, $\forall x$, $\exists z$ и $\forall y$ – кванторы, а не вхождения переменных.

5.2 Равносильные и общезначимые формулы логики предикатов

5.2.1 Рассматривая формулы логики предикатов над системой M, можно говорить о формулах, *р а в н о с и л ь н ы х н а д* данной (*а л г е б р а и ч е с к о й*) *с и с т е м о й* или *с т р у к т у р о й* («полем»), то есть о таких формулах, которые принимают одно и то же значение при замене всех свободных предметных переменных их значениями из *о с н о в н о г о м н о ж е с т в а с и с т е м ы* (или из её *н о с и т е л я*) (предметами) и всех символов предикатов – конкретными предикатами.

П р и м е р 5.4 Рассмотрим формулы $\forall x W(x)$ и $\exists x W(x)$ над системами («полями»): 1) M_1, состоящей из множества $\{a\}$ и предикатов $A(x)$ и $B(x)$, $A(a)$ истинно, $B(a)$ ложно; 2) M_2, состоящей из множества $\{a,b\}$ и предиката $A(x)$: $A(a)$ истинно, $A(b)$ ложно. Тогда формулы $\forall x W(x)$ и $\exists x W(x)$ равносильны на системе M_1, но не над структурой M_2.

Формулы логики предикатов называются *р а в н о с и л ь н ы м и*, если они равносильны над любой алгебраической системой (полем).

Т е о р е м а 5.1 *Следующие формулы равносильны*:

1. $\forall x W(x)$ и $\forall y W(y)$; 2. $\exists x W(x)$ и $\exists y W(y)$ – *правила переименования связанных переменных*.

3. $\neg\forall x W(x)$ и $\exists x \neg W(x)$; 4. $\neg\exists x W(x)$ и $\forall x \neg W(x)$ – *правила внесения отрицания*.

5. $\forall x \forall y V(x,y)$ и $\forall y \forall x V(x,y)$. 6. $\exists x \exists y V(x,y)$ и $\exists y \exists x V(x,y)$ – *правила перестановки однородных кванторов*.

7. $\forall x(W(x) \wedge U(x))$ и $\forall x W(x) \wedge \forall x U(x)$. 8. $\exists x(W(x) \vee U(x))$ и $\exists x W(x) \vee \exists x U(x)$ – *правила внесения кванторов внутрь (конъюнкции и дизъюнкции)*.

9. $\forall x W(x) \wedge U$ и $\forall x(W(x) \wedge U)$. 10. $\exists x W(x) \wedge U$ и $\exists x(W(x) \wedge U)$ – *правила вынесения кванторов из конъюнктивного члена*.

11. $\forall x W(x) \vee U$ и $\forall x(W(x) \vee U)$. 12. $\exists x W(x) \vee U$ и $\exists x(W(x) \vee U)$ – *правила вынесения кванторов из дизъюнктивного члена*.

13. $U \to \forall x W(x)$ и $\forall x(U \to W(x))$. 14. $U \to \exists x W(x)$ и $\exists x(U \to W(x))$ – *правила вынесения кванторов из заключения импликации*.

15. $\forall x W(x) \to U$ и $\exists x(W(x) \to U)$. 16. $\exists x W(x) \to U$ и $\forall x(W(x) \to U)$ – *правила вынесения кванторов из посылки импликации*.

Причём, в пп. 9-16 формула U не содержит x свободно.

5.2.2 Среди всех формул логики предикатов можно выделить формулы, истинные над любым полем (на любой системе), их называют *общезначимыми*. Равносильность формул и общезначимость можно рассматривать как логические законы. В общем случае выяснить вопросы, является ли данная формула общезначимой или равносильны ли данные формулы, сложно, так как приходится использовать понятие бесконечности. Более того, доказано, что нет единого алгоритма, решающего эту задачу в общем случае [11,16,19,23].

Тем не менее, имеется достаточно много общезначимых формул, для которых это их свойство можно довольно просто обосновать. Говорят, что формула логика предикатов есть *частный случай тавтологии*, если она получена из тождественно истинной формулы исчисления высказываний (см. п. 3.2.3) заменой пропозициональных переменных предикатами (или более общо, формулами исчисления предикатов). Несложно понять, что верна следующая

Теорема 5.2 *Все частные случаи тавтологий суть общезначимые формулы.*

Пример 5.5 Формула $\forall yP(x,y) \rightarrow (\forall x\exists z(W(x,z)\wedge\forall zU(z)) \rightarrow \forall yP(x,y))$ – общезначимая, поскольку она является частным случаем тавтологии $A\rightarrow(B\rightarrow A)$. А равносильная с ней формула $\forall yP(x,y) \rightarrow \forall y(\forall x\exists z(W(x,z)\wedge\forall zU(z)) \rightarrow P(x,y))$ (объясните, почему эти формулы равносильны) частным случаем тавтологии не является, хотя понятно, что тоже общезначимая.

Одними частными случаями список общезначимых формул не исчерпывается. Примеры таких формул даёт

Теорема 5.3 *Следующие формулы общезначимы*:

1. $\forall xW(x) \rightarrow \exists xW(x)$ – *не формальный смысл: квантор всеобщности сильнее квантора существования.*

2. $\exists x\, \forall zV(x,z) \rightarrow \forall z\, \exists xV(x,z)$ – *не формальный смысл: «если есть один x для всех z, то и у каждого z есть свой x».*

Упражнение 5.1 *Приведите конкретные примеры, показывающие, что обратные импликации в теореме 5.3 в общем случае неверны.*

Сформулированные в теоремах 5.1-3 общезначимые формулы и эквивалентности очень часто употребляются в реальных рассуждениях, как в теоретических построениях, так и в обосновании различных прикладных исследований, в виде *законов логики* (см. также примеры из разделов 3,4 и 6). По этой именно причине равносильность формул в теореме 5.1 названа правилами. Настоятельно рекомендуется запомнить их вместе с утверждениями о высказываниях и особенно таблицу 3.1 и по возможности их применять, особенно в тех ситуациях, когда вы анализируете сложные утверждения.

5.3 Исчисление предикатов

Точно также как алгебра высказываний является содержательным (семантическим) изложением логики без кванторов, так и *теория моде-*

л е й, очень краткое и элементарное введение в которую было изложено в двух предыдущих подразделах, есть содержательная (семантическая) часть логики предикатов. А более формальными (синтаксическими) изложениями этих теорий являются исчисление высказываний, несколько вариантов которого было описано в разделе 4, и *и с ч и с л е н и е   п р е д и к а т о в*, о котором мы сейчас дадим начальные сведения, более подробно с этим можно ознакомиться по книгам [11,16,19,23].

5.3.1 Обычно формализацию логики предикатов начинают с описания *с и г н а т у р ы*, т.е. списка *с и м в о л о в* предикатов, *ф у н к ц и й* и выделенных элементов (*к о н с т а н т н ы х* символов), которые разрешается использовать. Перед тем, как определить формулы, определяют *т е р м ы*, которые являются почти точным аналогом понятия арифметического выражения в программировании. Соответственно этому, меняется определение формулы [11,16,19,23].

Ограничимся системами A, Клини и L из пп. 4.2.1, 4.3.2 и 4.3.3, при наличии специального выделенного предиката «=», означающего равенство. Во всех этих трёх системах расширяется список схем аксиом (сначала указан номер аксиомы в расширенной системе Клини, а в скобках – в системе A и L):

$K_{14}(A_{12},L_4)$ $\forall x\, \varphi \to (\varphi)^x_t$

– неформально: «вместо универсальной переменной x (т.е. той, что находится под действием квантора всеобщности) можно подставлять её любое допустимое значение t»;

$K_{15}(A_{13},L_5)$ $(\varphi)^x_t \to \exists x\varphi$

– неформально: «если при каком-то конкретном допустимом значении t переменной x формула верна, то истинна та же формула с квантором существования»;

$K_{16}(A_{14},L_6)$ $x = x$

– неформально: «объект сам себе равен»;

$K_{17}(A_{15},L_7)$ $x = y \to ((\varphi)^z_x \to (\varphi)^z_y$

– неформально: «равные объекты имеют одинаковые свойства».

К правилу вывода *modus ponens* добавляются два новых. При условии, что x не входит свободно в φ, имеет место правило *о б о б щ е н и я*:

$$\frac{\varphi \to \psi}{\varphi \to \forall x\psi};$$

и правило *в в е д е н и я   с у щ е с т в о в а н и я* в посылку (при том же условии на переменную x и формулу φ, что и выше):

$$\frac{\psi \to \varphi}{\exists x\psi \to \varphi}.$$

5.3.2 Несмотря на внешнюю схожесть с исчислением высказываний, ситуация здесь на много порядков сложнее. Ввиду этого, часть теорем из п. 4.2.3 для исчисления предикатов просто не верны, в частности, исчисление предикатов не разрешимо, а часть теорем приобретает более сложный вид – см., например, теорему о существовании моделей в [11,19].

Но эта сложность исчисления предикатов проистекает вовсе не от того, что мы его неудачно формализовали. Эта сложность является просто отражением в формальной теории сложности устройства того мира, что нас окружает. Наиболее ярко исчисление предикатов проявляет себя в первую очередь в теоретических исследованиях. На практике оно применяется в основном при создании разнообразных языков функционального и особенно логического программирования.