Лекции по дисциплине «Дискретная математика»

Введение

 В курс лекций входит теория множеств, комбинаторика, математическая логика, основы общей алгебры, теория графов, конечные автоматы, теория алгоритмов и элементы теории игр. Изложение материала имеет ознакомительный характер, поэтому в данном курсе практически нет доказательств теорем и утверждений. Лекции ориентированы на повышение математической культуры и эрудиции будущих программистов, а также на прикладное использование материала в практике программирования и математического моделирования.

 Планируется, что лекции будут расширены путем добавления в них примеров программ на Python для реализации основных конструкций.

 Определение множества

 Понятие множества относится к фундаментальным понятиям не только математики, но и любого абстрактного мышления. Строгих определений понятий «множество», «элемент множества», «принадлежность к множеству» и т.д. не существует. Однако они и не нужны, поскольку каждый это понимает априорно. В тоже время интуитивное понимание множества и способов его задания приводит к известным парадоксам и логическим проблемам типа «множество всех множеств». Для разрешения этих проблем используют конструкции, основанные на введении аксиомы выбора или эквивалентных ей утверждений. В курсе дискретной математики мы, как правило, будем иметь дело с конечными или счетными множествами, для которых этих проблем нет. Мы будем говорить о множестве, как об определенной совокупности объектов, которые будем называть элементами множества.

 Сразу же нужно ввести понятие пустого множества. Множество, которое не содержит ни одного элемента называется пустым множеством, которое обозначается через ∅. Традиционно множества будем обозначать заглавными буквами: A, B, C, . . . , а элементы маленькими буквами: a, b, c, . . . . Если элемент множества a принадлежит множеству A, то будем писать a ∈ A.

 В противном случае пишем a /∈ A. Мы будем говорить, что два множества A и B равны и писать A = B, если оба множества состоят из одинаковых элементов. В этом определении есть один (и не один) нюанс. Равны ли множества A = {1, 2, 3, 4, 5} и B = {5, 4, 3, 2, 1, }? Да, равны, поскольку множества предполагаются неупорядоченными. А равны ли множества F1 = {Apple, P ear, Orange} и F1 = {Apple, Apple, P ear, Orange}? Если в качестве элементов мы рассматриваем одни и те же яблоки, то да — эти множества равны1 . Мы будем говорить, что множество A есть подмножество множества B, если каждый элемент множества A является элементом множества B. Будем использовать для этого стандартное обозначение A ⊂ B. Отношение подмножества является нестрогим, поэтому если A = B, то A ⊂ B (и, соответственно, B ⊂ A).

 Если нужно рассматривать именно строгое отношение подмножества, которое называется собственным подмножеством, то это будем каждый раз оговаривать специальною. Будем рассматривать следующие основные операции над множествами. Во-первых, множества можно объединять. Пусть A и B два множества, тогда их объединением, обозначаемым 1Выходит два яблока равны одному яблоку.

 Теория множеств 10 A∪B называется множество, состоящее из всех элементов множества A и множества B. Заметим, что, например, {1, 2, 3, 4} ∪ {2, 3, 4, 5} = {1, 2, 3, 4, 5}. Иногда вместо объединения множеств говорят о сумме множеств. Во-вторых, операция пересечения множеств. Пусть A и B два множества, тогда их пересечением, обозначаемым A∩B называется множество, состоящее из элементов, являющихся одновременно элементами множества A и множества B. Эта операция легко может приводить к пустым множествам. Будем говорить, что множества A и B не пересекаются, если A ∩ B = ∅. Очевидно, что обе эти операции являются симметричными A ∩ B = B ∩ A, A ∪ B = B ∪ A. В-третьих, рассматривается операция (уже не симметричная) разности двух множеств, обозначаемой A \ B. При этом разность множества A и B определяется, как множество, содержащее те и только те элементы множества A, которые не содержатся в B. Разумеется, A \ A = ∅. Симметричную разность двух множеств A и B определим следующей формулой A△B = (A \ B) ∪ (B \ A). Симметричная разность множеств состоит из тех элементов, которые не являются одновременно элементами обоих множеств. Чтобы определить операцию дополнения множеств, нужно ввести понятие универсального множества. Пусть в фиксированной ситуации мы рассматриваем только множества, являющиеся подмножеством одного множества U, которое называется универсальным множеством. Тогда для множества A, (A ⊂ U) дополнением является множество A, которое определяется по формуле A = U \ A. Иногда используют обозначение CA, для дополнения, но мы так делать не будем. Еще раз подчеркнем, что дополнение имеет смысл только при фиксации универсального множества.

 2. Мощность множеств

 Давайте зафиксируем обозначения для некоторых множеств, с которыми мы будем постоянно иметь дело. Во-первых, это множество натуральных чисел N = {0, 1, 2, . . . }. Мы будем считать, что ноль является натуральным числом. В этом вопросе много споров и каждый по своему прав. Я выбрал этот вариант только для того, что если потребуется ряд из положительных целых чисел, то эстетичнее исключить ноль, чем его добавлять в противном случае. Во-вторых, множество целых чисел Z = {. . . , −2, −1, 0, 1, 2, . . . }. В-третьих, множество рациональных чисел, обозначаемое Q, заметим, что для определения этого множества мы воспользовались схемой свертки. В-четвертых, самое главное множество — это множество действительных чисел R. И, наконец, множество комплексных чисел — C.

 В следующей главе мы будем встречаться с большим количеством пространств, которые являются множествами, и имеют устоявшиеся обозначения, но о них мы пока говорить не будем. Рассмотренные выше множества являются множествами чисел. А что такое число? По идее число выражает некоторую количественную характеристику, необходимую для счета. В этом смысле только комплексные числа выбиваются из ряда. Их появление обусловлено операцией извлечения квадратного корня. Есть и дальнейшие обобщения чисел — кватернионы и др. Однако для нас важным будет определение чисел как алгебраическое поле. В общей алгебре полем называется множество M, которая является коммутативной группой относительно операции сложения + с нулевым элементом 0, а также коммутативную группу с операцией умножения ∗ над ненулевыми элементами множества M. При этом эти операции должны удовлетворять свойствам дистрибутивности умножения относительно сложения.

 Множества Q, R и C являются полями с обычными операциями сложения и умножения. Часто употребляются устойчивые выражения «поле комплексных числе», «над полем действительных чисел». Теперь мы рассмотрим принципиальное понятие в теории множеств — понятие мощности множества. В быту, встречаясь с множествами — множество гостей, множество подчиненных, множество комнат в квартире, множество конфет в вазе и т.д., нас прежде всего интересует количество элементов в данном множестве. Если для одних множеств мы можем мыслить (помнить и различать) все элементы как, например, множество комнат в своей квартире или множество своих детей, то для других множеств, наоборот, важно лишь количество, например, количество баранов в стаде, множество патронов в магазине и т.д. Для конечных множеств понятие мощности совпадает с количеством элементов. С конечными множествами более менее все понятно, обратимся к бесконечным множествам. Можно несколькими способами дать определение бесконечного множества. Определение «множество, содержащее бесконечное множество элементов» не годится, потому что тогда нужно давать определение «бесконечности», что, как раз, определяется через бесконечные множества. Определение — бесконечное множество это множество не являющееся конечным, корректно, но неконструктивно и, не раскрывает сути. Мы сделаем следующим образом.

 По определению множество натуральных чисел N является бесконечным. Тогда множество A называется бесконечным, если существует такое подмножество B ⊂ A, что между элементами множества N и B существует взаимно однозначное соответствие. Можно дать еще одно эквивалентное определение. Множество называется бесконечным, если у него существует собственное подмножество (то есть не совпадающее с самим множеством) для элементов которых можно установить взаимно однозначное соответствие. Проверим, что множество N в этом определении является бесконечным. Действительно, рассмотрим собственное подмножество N1 = N \ {0}, тогда для любому элементу a ∈ N1 соответствует единственный элемент b = a − 1, который принадлежит множеству N. И так, мощность конечного множества есть количество элементов этого множества. Множества, которые допускают взаимно однозначное соответствие имеют одинаковую мощность. Мощность множества N обозначается ℵ0

 2. Множества имеющие мощность ℵ0 называются счетными. Используют различные обозначения для мощности множества: |A|, #A и др. Мощность множества не является числом, однако для этих величин можно ввести порядок, то есть для любых двух мощностей a и b верно одно из трех a < b, a = b, a > b. Не являясь числами, мощности множеств являются трансфинитами или кардинальными числами. Мощность ℵ0 является наименьшей мощностью бесконечных множеств. Хорошо известно, что |N| = |Z| = |Q|. Бесконечным множеством, имеющим большую мощность, является множество R. Мощность этого множества называется мощностью континуума и обозначается c. Хорошо известно, что ℵ0 < c. Возникает вопрос о существовании множества, имеющего мощность a такую, что ℵ0 < a < c. Континуум-гипотеза, сформулированная Г. Кантором в 1877 году, утверждает, что таких множеств не существует. В 1940 году К. Гедель доказал, что отрицание континуум-гипотезы является недоказуемым при аксиоме выбора.

 3. Отображения множеств Еще одно понятие, которое понимается интуитивно, относится к отображением множеств. Пусть задано два множества X и Y . Мы будем говорить, что A есть отображение из X в Y , если задано правило, которое каждому элементу x ∈ X ставит в однозначное соответствие элемент y ∈ Y. При этом пишут A : X → Y. Мы будем говорить всегда об однозначных отображениях. В случаях, когда необходимо рассматривать многозначные отображения, мы будем говорить об однозначных отображениях в подмножества. 2Произносится «алеф-ноль».

 Вместо термина «отображение» будем также использовать и другие синонимы, например, функция. Если множества X и Y представляют собой пространства, то часто будем говорить об операторе, если множество Y представляет собой множество чисел (действительных или комплексных), то будем говорить и функционале. Иногда отображение будет определено не на всем X, а лишь на некотором подмножестве X1 ⊂ X, это подмножество называется областью определения отображения A и обозначается D(A). С другой стороны подмножество Y1 ⊂ Y состоящее из y ∈ Y , таких, что существует x ∈ D(A), y = A[x], называется областью значения отображения Y . Для любого x ∈ D(A) элемент y = A[x] называется образом x. А для фиксированного y ∈ Y множество таких x ∈ D(A), что A[x] = y называется прообразом y.

 Понятия образа и прообраза легко обобщаются на понятия образа и прообраза для множеств. Если область значения отображения есть все Y , то такое отображение называется сюръективным. Если для двух различных x1, x2 ∈ X их образы различны, то такое отображение называется инъективным. Отображение одновременно сюръективное и инъективное называется биективным. Биективное отображение, или биекция — это взаимнооднозначное отображение. Введем понятие прямого произведения двух множеств X и B. Прямым произведением, обозначаемым X × Y называется множество, состоящее из всех упорядоченных пар (x, y), где x ∈ X, а y ∈ Y . Например, прямое произведение R × R есть множество точек, обозначаемое R 2.

 Аналогично, можно ввести понятие и прямого произведения n множеств. Рассмотрим некоторое непустое множество X. Для некоторых упорядоченных пар из этого множества мы введем понятия отношения. Будем говорит, что x1 находится в отношении ϕ с x2 и писать x1ϕx2. Отношения могут иметь различные свойства:

 1. Отношение называется рефлексивным, если xϕx для всех x ∈ X.

 2. Отношение называется симметричным, если из x1ϕx2 следует, что x2ϕx1

 3. Транзитивным отношение называется, если из x1ϕx2 и x2ϕx3 следует, что x1ϕx3. Отношение, обладающее всеми тремя свойствами — рефлексивностью, симметричностью и транзитивностью, называется отношением эквивалентности. Если на множестве X задано отношение эквивалентности, то это множество можно разбить на классы эквивалентности. Будем говорить, что подмножество K ⊂ X есть класс эквивалентности для отношения эквивалентности ϕ если для всех x1, x2 ∈ K имеет место x1ϕx2 и в X \ K не существует элементов, состоящих в отношении с элементами из K. Для любого элемента x ∈ X класс эквивалентности определяется следующим образом Kx = {x ′ ∈ X : x1ϕx′ }. Для любых x и y, которые не состоят в отношении эквивалентности, соответствующие классы эквивалентности не пересекаются. Поэтому все множество X можно разбить на классы эквивалентности X = [ α Kα. При этом можно каждый класс эквивалентности отождествить с некоторым новым элементом и рассматривать исходное множество, как множество классов эквивалентности.

 Глава II Комбинаторика и вероятность

 1. Основные комбинаторные понятия Комбинаторика или комбинаторный анализ посвящен изучению подмножеств конечных множеств. Комбинаторные задачи играют выдающуюся роль в прикладной математики. Дело в том, что комбинаторные методы часто позволяют находить решения для множеств, содержащих огромное число элементов. Рассмотрим конечное1 множество A, содержащее N элементов, т.е. |A| = N. Через 2 A мы обозначим множество всех подмножеств множества A. Какова мощность этого множества? Само обозначение уже подсказывает, что мощность этого множества равна 2 |A| = 2N . Покажем, что это, действительно, так. Заметим, что в множество 2 A включается и пустое множество, которое тоже считается. Итак, занумеруем произвольным образом все элементы множества A A = {a1, a2, . . . , aN }. Далее для любого множества θ ∈ 2 A можно построить двоичную строку из N нулей и единиц θN = (α1, α2, . . . , αN ), где αn = 1, an ∈ θ, 0, an ∈/ θ. 1В этой главе все множества будут предполагаться конечными. 16 Глава II. Комбинаторика и вероятность 17 Ясно, что количество этих двоичных строк равно 2 N.

 Вот пример множества всех подмножеств. Пусть A = {a, b, c}. Тогда множество всех подмножеств будет состоять из 8 элементов 2 A = {∅, {a}, {b}, {c}, {a, b}, {a, c}, {b, c}, {a, b, c}}. Кроме вычисления (перечисления) всех подмножеств множества A в дискретной математике рассматривают такие важные понятия, как размещение, перестановки и сочетания. Размещением элементов из A по k называется упорядоченное подмножество множество из k элементов множества A. Размещения по 2 для множества A = {a, b, c} следующие (a, b),(b, a),(a, c),(c, a),(b, c),(c, b). Число размещений множества из N элементов по k обозначается (N)k. Не сложно вычислить это число, которое завит от двух параметров — N и k. По определению считаем (N)k = 0, k > N, (0)0 = (N)0 = 1. Далее для случая, когда 0 < k < N имеем, что при построении размещения на первое место можно выбрать один из N вариантов, на второе — из (N − 1), последний — из (N − k + 1). В итоге мы получаем (N)k = N(N − 1). . .(N − k + 1). Эту формулу можно записать компактнее с помощью факториала (N)k = N! (N − k)!. Напомним, что факториал определяется для натуральных чисел следующим образом n! = n(n − 1). . . 2 · 1, для n > 0, по определению 0! = 1.

 Мы рассмотрели размещения без повторений, когда не допускается повторяющихся элементов. Если разрешить повторы, то мы получим размещения с повторами.

 Размещения с повторами имеют смысл слов определенной длины, составленных из фиксированного алфавита — множества A. Например, пусть A = {0, 1} есть двоичный алфавит, тогда множество, размещений из A по 8 с повторениями будет множество двоичных чисел, состоящих из 8 бит, что соответствует множеству байтов. Количество байтов равно 256 = 28 . Несложно понять, что для множества A, состоящего из N элементов количество размещений по k с повторами равно Nk . Действительно, на первое место можно выбрать одним из N вариантов, на второе — тоже N и т.д. k раз. В частном случае размещения без повторов, когда N = k, такое размещение называется перестановкой. Для нашего множества A = {a, b, c} перестановки суть следующие множества (a, b, c),(a, c, b),(b, a, c),(b, c, a),(c, a, b),(c, b, a). Количество перестановок равно (N)N = N!. Еще очень важным комбинаторным понятием является понятие сочетания элементов из множества A по k. Сочетанием называется неупорядоченное подмножество из k элементов, принадлежащих множеству A.

 Например, для A = {a, b, c} сочетанием по 2 будут подмножества {a, b}, {a, c}, {b, c}. Количество сочетаний множества из N элементов по k обозначается C k N . Сочетания отличаются от размещений тем, что они неупорядоченные. Соответственно, каждому сочетанию соответствуют k! размещений, поэтому для числа сочетаний имеем следующая формула C k N = (N)k k! = N! k!(N − k)!, в которой предполагается, что 0 ≤ k ≤ N. По определению полагаем C k N = 0 Глава II. Комбинаторика и вероятность 19 при k > N. Сочетания возникают, например, в биноме Ньютона (a + b) n = C 0 N a n + C 1 na n−1 b + · · · + C n−1 n abn−1 + C n n b n = = Xn k=0 C k na n−k b k . Рассмотрим пример применения сочетаний для оценки шансов в игре «Спортлото». В этой игре нужно угадать 5 чисел из 36, либо 6 из 49. Какая из этих игр лучше (для игрока)? Число комбинаций «5 из 36» равняется сочетанию C 5 36 = 36! 5!31! = 376992. А для игры «6 из 49» число комбинаций C 6 49 = 49! 6!43! = 13983816. Таким образом, выиграть в лотерею «5 из 36» примерно в 37 раз легче. Еще простой пример применения сочетаний. Сколько возможно раскладов 6 карт из колоды в 36 карт? Ответ C 6 36 = 36! 6!30! = 1947792. Поэтому можно утверждать, что с огромной вероятностью Вам ни разу не выпадал одинаковый набор в карты при игре в «Дурака» (при условии, если колода была хорошо перетасованна).

 2. Принцип включения-исключения Как мы видим, комбинаторика позволяет с единых позиций находить точные ответы на нетривиальные вопросы. Очень эффективным средством является принцип включенияисключения. Пусть для конечного множества A задана некоторая система подмножеств A1, A2, . . . , An. Не предполагается, что эти подмножества исчерпывают исходное множество или являются непересекающимися — это могут быть любые подмножества. Если мы знаем (можем легко сосчитать) мощности любых пересечений этих множеств, то можно найти мощность исходного множества A, если объединение всех Ai совпадает с Aб либо наоборот найти мощность подмножества множества A, которое состоит из элементов, не входящих ни в одно из Ai . Действительно имеет место следующая формула, называемая принципом включения-исключения |A \ (A1 ∪ · · · ∪ An)| = |A| −Xn i=1 |Ai |+ + X 1≤i1<···< p < 1, а неудача, соответственно, с вероятностью q = 1 − p. Будем считать, что проводится n отдельных опытов. В результате реализации схемы Бернулли мы получаем серию из n нулей и единиц. Найдем вероятность того, что будет ровно m успехов при реализации схемы Бернулли. Будем рассуждать комбинаторно. Вероятность реализации любой конкретной последовательности, содержащей ровно m единиц (успехов) и n − m нулей (неудач), например 11 . . . 100 . . . 0 равна Pmn = pp . . . pqq . . . q = p mq n−m. Но нас интересует вероятность любой последовательности, содержащей m единиц и n − m нулей.

 Поскольку вероятности любых таких последовательностей равны Pmn, то для этого необходимо подсчитать количество всех возможных таких последовательностей и умножить на на вероятность Pmn. Количество таких последовательностей равняется числу сочетаний n элементов по m, поэтому число этих последовательностей в точности равно C m n . Таким образом, искомая вероятность может быть найдена по формуле Pn(m) = C m n p mq n−m. Кстати, можно заметить, что сумма получившихся вероятностей равна единице, что согласуется с вероятностными соображениями Xn m=0 Pn(m) = Xn m=0 C m n p mq n−m = (p + q) n = 1.

 Глава III Математическая логика

 1. Логика высказываний Математическая логика играет важнейшую роль в дискретной математики и ее приложениях. Как отдельная математическая дисциплина математическая логика включает в себя формальные системы, доказуемость математических утверждении, теорию алгоритмов, вычислимость и многие другие аспекты оснований математики. Мы рассмотрим вопросы исчисления высказываний и предикатов, а также приложение математической логики к формализации знаний в компьютерных программах. Высказыванием называется утверждение, которое может быть либо истинным, либо ложным.

 Сразу же сделаем замечание, что мы будем рассматривать двоичную логику, где для высказываний возможны только «истина» или «ложь». Варианты типа «не знаю» или «не определено» не допустимы. Также мы не будем рассматривать варианты «истинно с вероятностью p» и т.д. Вообще существуют теории многозначной логики и нечеткой логики, но мы будем рассматривать только двоичную логику. Итак, высказывания это утверждения типа «Волга впадает в Каспийское море», «2 × 2 = 5», «Любое четное число больше 2 может быть разложено в сумму двух простых чисел». Здесь первое высказывание является истинным, второе — ложным, а третье — в настоящий момент нерешенная математическая проблема (проблема Гольдбаха). Сразу договоримся, что математическая логика не занимается вопросам какое высказывание ложно, а какое нет.

 Поскольку высказывания являются субъективными, например «Плутон — девятая планета Солнечной системы» раньше было истинным, а сейчас считается ложным, не говоря уже об оценочных высказываниях типа «черешня вкуснее вишни» или спорных высказываниях «Бога есть» / «Бога нет». В математической логике высказывания — это символы, часто обозначаемые буквами A, B, C и т.д., которые могут иметь одно из двух значений, которые мы будем обозначать 0 и 1, причем 0 означает ложное высказывание, а 1 — истинное, как это принято в языках программирования C/C++. Будем писать A = 0, B = 1. Имея определенный запас высказываний, мы можем создавать новые высказывания с помощью логических операций. Для таких высказываний мы уже сможем методами математической логики выяснить ложность или истинность.

 Первая логическая операция — это операция отрицания A Высказывание A истинно тогда, когда ложно A и ложно, когда истинно A. Читается «не A». Вторая операция называется конъюнкцией, которая применяется к паре высказываний A&B, читается «A и B». Высказывание A&B истинно тогда и только тогда, когда A = 1 и B = 1. Третьей операций является операция дизъюнкция также применяемая к паре высказываний A ∨ B, читается «A или B». Соответственно, высказывание A ∨ B истинно тогда, когда истинно хотя бы одно из высказываний A или B. Четвертая логическая операция — это операция импликация или логическое следование. Также применяется для пары высказываний A → B, читается «из A следует B». Высказывание A → B ложно тогда и только тогда, когда A истинно, а B ложно. Во всех остальных случаях это высказывание истинно. Если операции логического отрицания, конъюнкции и дизъюнкции интуитивно поняты любому разумному человеку, то с операцией импликации иногда возникают сложности. Дело в том, что если A = 0, то результатом операции будет 1 вне зависимости от B.

 Как говорил, Д. Гильберт «Разрешите мне принять, что дважды два — пять, и я докажу, что из печной трубы вылетает ведьма!» – из ложного предположения следует что угодно. Пятая операция — это операция эквивалентности двух высказываний A ∼ B, читается «A эквивалентно B». Высказывание A ∼ B истинно тогда, когда либо A = 1 и B = 1, либо A = 0 и B = 0. С помощью введенных операций и с использованием скобок, для обозначения приоритета можно конструировать произвольно сложные высказывания, например, W = (A ∨ B) → ((B&C) ∨ (D ∼ E)). Знак равенства означает, что мы получаем новое высказывание W по приведенной формуле. Заметим, что используемые нами операции не являются независимыми и могут быть выражены друг через друга. Вот примеры A&B = A ∨ B, A ∼ B = (A → B)&(B → A), A → B = (A ∨ B). Вообще говоря, все логические операции можно выразить через две операции ∨ и или операции & и . Далее, существует большое количество формул, устанавливающих равносильность сложных высказываний.

 Приведем только некоторые из них A = A, A&B = B&A, A ∨ B = B ∨ A, (A ∨ B) ∨ C = A ∨ (B ∨ C), (A&B)&C = A ∨ (B&C), A&(B ∨ C) = (A&B) ∨ (A&C), A ∨ (A&B) = A, A&(A ∨ B) = A. Рассмотрим подробнее первую формулу, которая имеет название «отрицание отрицания».

 Согласно этой формуле высказывание будет истинным, если ложным будет отрицание этого высказывания. С точки зрения логики высказываний эта формула не вызывает сомнения. Но с точки зрения конструктивной логики здесь есть вопросы. Дело в том, что опровергнуть отрицание может быть значительно сложнее, чем доказать исходное высказывание. Например, вместо доказательства вины обвиняемого можно предложить самому обвиняемому опровергнуть обвинение. Ясно, что это неэквивалентные ситуации. Поэтому принцип презумпции невиновности в России гарантируется статьей 49 Конституции РФ и является базовым в большинстве стран. Этот принцип звучит так: «Человек не виновен, пока не доказано обратное». Формула называется тождественно истинной или тавтологией, если она принимает истинное значение при всех значениях входящих в нее высказываний. Например такая формула A ∨ A = 1, которая называется исключение третьего «A или не A». Формула называется невыполнимой, если она принимает ложное значение при всех значениях переменных. Например A&A. Если формула не является невыполнимой, то она называется выполнимой. Для того, чтобы выяснить будет ли истинной заданная формула при определенных значениях входящих в нее переменных необходимо построить таблицу истинности для этой формулы. В этой таблице перечисляются все возможные комбинации входящих переменных и значение формулы. Рассмотрим пример для формулы A ∨ (B&C). A B C A ∨ (B&C) 1 1 1 1 1 1 0 1 1 0 1 1 1 0 0 1 0 1 1 1 0 1 0 0 0 0 1 0 0 0 0 0 Из комбинаторных формул мы знаем, что количество строк у таблицы истинности равно 2 N , где N равно количеству переменных.

 Ясно, что для формул имеющих большое количество переменных таблицы истинности будут очень громоздкими. Существуют различные методы эквивалентного преобразования логических формул, которые облегчают проверку истинности или ложности при заданных значениях переменных. В частности, можно доказать, что любую формулу можно привести к эквивалентной формуле, которая является дизъюнкцией элементарных конъюнкций. Такая форма формулы называется дизъюнктивной нормальной формой. Аналогично конъюнктивной нормальной формой называется вид формулы, когда она представляет собой конъюнкцию элементарных дизъюнкций.

 Например, формула (A&B&C) ∨ A ∨ (A&B) находится в дизъюнктивной нормальной форме, а формула (A ∨ B)&(B ∨ C)&A находится в конъюнктивной нормальной форме. Использование нормальных форм позволяет в ряде случаев сразу сделать вывод о значении формулы. Например, сразу видно, что последняя формула имеет ложное значение, если ложным является переменная A.

 2. Правила вывода и рассуждения Математическая логика дает формальные приемы для проведения правильных рассуждений, при заданных посылках. Рассуждением Глава III. Математическая логика 31 называется процесс установления истинности высказывания, которое называется логическим выводом при конъюнкции набора высказываний, которые называются посылками. Дадим определение правильного рассуждения. Рассуждение называется правильным, если из конъюнкции посылок следует заключение, т.е. всякий раз, когда все посылки истинны, заключение тоже истинно. Пусть X1, X2, . . . , Xn — набор высказываний, называемых посылками, а D — высказывание, являющееся заключением рассуждения. Тогда это рассуждение записывается следующим образом X1, X2, . . . , Xn D . Наиболее часто используемое рассуждение можно записать следующим образом A → B, A B . Это рассуждение по правилу modus ponens. Легко видеть, что это правильное рассуждение. В качестве примера такого рассуждения можно привести следующее рассуждение «Если космической аппарат стал искусственным спутником Земли, то он движется с первой космической скоростью. Наш космический аппарат вышел на орбиту спутника Земли. Следовательно, наш аппарат движется со второй космической скоростью». Другой распространенный способ правильного рассуждения записывается в виде A → B, B A . Пример такого рассуждения. «Если продукты ГМО вредны, то они опасны для человека. Продукты ГМО не опасны для человека1. Следовательно, продукты ГМО не вредны.» Рассмотрим теперь неправильные рассуждения. Например рассуждение по формуле A → B, B A . Примером такого рассуждения является рассуждение «Если функция f(x) дифференцируема, то она непрерывна. 1European Commission Directorate-General for Research and Innovation; Directorate E — Biotechnologies, Agriculture, Food; Unit E2 — Biotechnologies (2010)

 Функция f(x) непрерывна. Следовательно функция f(x) дифференцируема». Заметим, что неправильные рассуждения могут приводить к правильным выводам. Правила вывода и автоматические рассуждения используются в экспертных системах, которые могут получать заключения по заданным посылкам. Экспертные системы последовательно задают пользователям вопросы, после чего система, используя правила вывода, приходит к заключению. Рассмотрим простейшую схему для экспертной системы, основанной на логических правилах. Во-первых, рассматриваем набор высказываний X1, X2, . . . , Xn. Эти высказывания называются фактами в экспертной системе. Экспертная система «узнает» факты с помощью опроса пользователя. Во-вторых, в системе считается истинным набор высказываний вида Xi → Yj , Yk → Ym. Здесь Yk — это выводы экспертной системы. В-третьих, в системе используются истинные высказывания вида (Yi1&Yi2& . . . &Yik ) → Di , где D1, D2, . . . , Dm суть решения экспертной системы. Схема работы экспертной системы состоит в трех этапах. 1. Получение фактов, т.е. присвоение переменным Xi логических значений. 2. Получение выводов Yj с использованием логических правил вывода. 3. Вывод решений экспертной системы. Второй этап в этой системе может быть опущен, если правила вывода сразу могут дать решение экспертной системы по полученным фактам.

 Рассмотрим простой пример экспертной системы для классификации животных. Фактами в данной системе будет следующий набор высказываний: X1 = животное имеет крылья. X2 = животное умеет плавать. X3 = животное умеет летать. X4 = животное имеет бинокулярное зрение. X5 = животное имеет усы. С помощью опроса пользователя система присваивает каждому высказыванию значение 0 или 1. В качестве выводов в экспертной системе будем использовать следующие высказывания. Y1 = животное — птица. Y2 = животное — рыба. Y3 = животное — млекопитающее.

 Наконец, в нашей экспертной системе мы используем следующие решения. D1 = животное — курица. D2 = животное — сокол. D3 = животное — сом. D4 = животное — щука. D5 = животное — тигр. D5 = животное — баран. Для нахождения значений высказываний Yi и Dj необходимо использовать правила вывода. Мы будем считать верными следующие формулы X1 → Y1, X2 → Y2, (X1&X2) → Y3, которые дают возможность прийти к некоторым промежуточным выводам. Далее рассмотрим правила вывода для нахождения решений экспертной системы. (Y1&X3) → D1, (Y1&X3) → D2, (Y2&X5) → D3, (Y2&X5) → D4, (Y3&X4) → D5, (Y3&X4) → D6. Таким образом, мы получаем, что если в результате опроса пользователя будут установлены следующие факты X1 = 0, X2 = 0, X3 = 0, X4 = 1, X5 = 1, то наша система придет к выводу, что «животное — млекопитающее» и заключению, что мы имеем дело с тигром. 3. Логика предикатов Рассмотренные выше высказывания по сути были только логические переменные, значение которых было фиксированным. Для проведения настоящих рассуждений необходимо использовать логику предикатов. Предикаты — это высказывания с параметрами, которые могут быть истинными или ложными в зависимости от параметров. Дадим точное определение. Рассмотрим произвольное множество M, которое будем называть множеством предметов или объектов. На этом множестве определим однозначную функцию P : M → {0, 1}, которая каждому объекту (предмету) x ∈ M ставит в соответствие ложь или истину (0 или 1). Следовательно, для каждого x ∗ ∈ M конструкция P(x ∗ ) есть высказывание. Приведем примеры простых предикатов. Пусть M = N — множество целых чисел. Построим предикат P(n) = {n является простым числом}. Имеем различные высказывания P(2) = 1, P(3) = 1, но P(4) = 0 и т.д. Можно рассматривать предикаты, зависящие от нескольких переменных. В этом случае множество M можно считать прямым произведением, например, M = P eoples×N, где P eoples — множество людей в фиксированный момент времени. Рассмотрим предикат P(x, n) = {Человек x имеет возраст n лет}.

 Математическая логика не рассматривает вопрос о том, как именно вычислять предикат, поскольку это вопросы предметной области. Будем считать, что предикат определен на всем множестве объектов. Вообще говоря, для каждого предиката нужно задавать свою область определения — множество предметов. Из предикатов и высказываний можно строить новые предикаты с помощью логических операций. Например, пусть предметное множество состоит из множества автомобилей и суммы денег, введем предикаты P1(m, x) = {машина m стоит x рублей}, P2(x) = {я имею x рублей}. Тогда можно определить новый предикат P3(m, x) = P1(m, x)&P2(x). Этот предикат может иметь смысл — «я могу купить машину m». Однако с помощью предикатов можно создавать новые высказывания и с использованием кванторов. Пусть мы имеем множество предметов M и предикат P(x), тогда построим высказывание ∀xP(x), которое является истинным, если P(x) истинно для всех x ∈ M, и ложным, если существует хотя бы один x ′ ∈ M, для которого P(x ′ ) = 0. Этот квантор читается «для всех x P(x) истинно». Квантор ∀ называется квантором всеобщности. Говорят, что квантор всеобщности связывает переменную. Если предикат зависит от нескольких переменных, а квантор всеобщности применяется по одной, то мы получаем предикат от одного переменного. Например, пусть у нас есть предикат, зависящий от двух натуральных чисел, и заданный по формуле P(n, m) = {n ≤ m}. Образуем новый предикат Q(n) = ∀m(P(n, m)). Имеем Q(0) = 1; Q(n) = 0, n > 0.

 Следующий квантор — это квантор существования. Который обозначается следующим образом ∃xP(x). Этот квантор из предиката делает высказывание, которое истинно, если существует хотя бы один элемент x ′ ∈ M такой, что P(x ′ ) = 1, если такого элемента не существует, то это высказывание будет ложным. Читается «сущесвтует такой x, что P(x) истинно». Например, для предиката P(x) = {|sin x| > 1}, определенного на множестве действительных чисел, высказывание ∃xP(x) ложное. Впрочем, если мы рассмотрим этот предикат, определенный на множестве комплексных чисел, то полученное высказывание будет уже истинным. Квантор существования также связывает переменную. Можно комбинировать кванторы. Например, для предиката P(n, m) = {n ≤ m} построим высказывание A = ∃n(∀m(P(n, m))).

 Это высказывание будет истинным. А высказывание B = ∀n(∃m(P(n, m))). будет ложным, поскольку существует такое m, что не для любого n будет выполнено n ≤ m. Кванторы всеобщности и существования являются двойственными друг к другу в том смысле, что имеют место следующие соотношения ∀x(P(X)) = ∃x(P(x)) и ∃x(P(X)) = ∀x(P(x)).

 С помощью предикатов можно определять множества, как подмножества множества предметов. Пример, множество предметов — действительные числа R, предикат P(x) = {sin x = 0}, построим множество корней для функции sin x с помощью этого предиката Q = {x ∈ R : P(x) = 1}. Таким образом, любой предикат задает два подмножества в множестве предметов — подмножество, для которого этот предикат истинный, и подмножество, для которого этот предикат ложный. Рассмотрим на одном общем множестве предметов M два предиката P(x) и Q(x). Как мы видели выше эти предикаты определяют два подмножества множества MP = {x ∈ M : P(x) = 1} и MQ = {x ∈ M : Q(x) = 1}. Определим теперь новый предикат на этом же множестве предметов R(x) = P(x) ∨ Q(x) и для этого предиката свое множество MR = {x ∈ M : R(x) = 1}. Легко заметить, что имеет место следующее соотношение MR = MP ∪ MQ. Аналогично, если мы определим предикат S(x) = P(x)&Q(x) и, соответственно, множество MS = {x ∈ M : S(x) = 1}, Глава III. Математическая логика 38 то получим соотношение MS = MP ∩ MQ. Рассмотрим еще предикат, построенный по формуле T(x) = P(x). Тогда для множества MT = {x ∈ M : T(x) = 1}, имеем MT = MP , то есть дополнение к множеству. По сути предикат в данном случае используется в качестве индикаторной функции для задания множеств.