Лекция 3: множества и логика

Дискретная математика, ВШЭ, факультет компьютерных наук

(Осень 2014 – весна 2015)

Мы уже использовали понятие множества и в дальнейшем будем его использовать постоянно. Сейчас мы обсудим это понятие и связанные с ним более систематически.

Неформально, множество — это совокупность каких-то элементов и полностью определяется своими элементами. Мы будем говорить, что элемент x принадлежит множеству A, если он является его элементом. Обозначать это будем так: $x \in A$ (таким образом, эта запись означает утверждение и принимает логические значения «истина», «ложь»).

Равенство множеств $A = B$ это утверждение, которое означает, что множества состоят из одних и тех же элементов. Более подробно: любой элемент множества A принадлежит множеству B и любой элемент множества B принадлежит множеству A.

Эти два условия естественно разделить. Получим отношение включения между множествами. Если любой элемент множества A принадлежит множеству B, то множество A называется подмножеством множества B, обозначение $A \subseteq B$.

Равенство множеств и включение напоминают равенство чисел и сравнение чисел по величине и обладают похожими свойствами.

Есть уникальное множество — пустое, — которое не содержит никаких элементов. Обозначение $\varnothing$.

Если элементов в множестве мало, его можно задать, указав все эти элементы. При этом принято заключать список элементов в фигурные скобки. Хотя на письме мы вынуждены записывать множества в каком-то порядке, этот порядок не играет роли. Поэтому

$$\{0, 2, 4, 6, 8\} = \{4, 2, 0, 8, 6\}$$

и это просто разные обозначения множества четных цифр.

Количество элементов в множестве A, если оно конечно, будем обозначать $|A|$ и называть мощностью множества. Мощность возможно определить и для бесконечных множеств, но это более тонкий вопрос и сейчас мы его обсуждать не будем.

На множествах определено большое количество операций, самые важные из которых мы сейчас перечислим.

Объединение множеств. Обозначение $A \cup B$. Это множество, состоящее в точности из всех элементов множеств A и B.

Пересечение множеств. Обозначение $A \cap B$. Это множество, состоящее в точности из тех элементов, которые принадлежат обоим множествам A и B.

Разность множеств. Обозначение $A \setminus B$. Это множество, состоящее в точности из тех элементов, которые принадлежат множеству A, но не принадлежат множеству B.

Симметрическая разность множеств. Обозначение $A \triangle B$. Это множество, состоящее в точности из тех элементов, которые принадлежат ровно одному из множеств: либо A, либо B.

Есть графический способ иллюстрировать операции с множествами: круги Венна. На паре кругов легко нарисовать объединение, пересечение, разность и симметрическую разность множеств.

Элементами множества могут быть другие множества. По любому множеству A определено множество его подмножеств, которое обозначается 2^A. Есть способ определить возведение в степень A^B для любых множеств, но мы пока его не будем обсуждать.

Декартово произведение множеств. Обозначение $A \times B$. Это множество, состоящее из всех последовательностей длины 2 вида (a, b), где $a \in A$, $b \in B$.

Формулу произведения можно выразить через декартово произведение так:

$$|A \times B| = |A| \cdot |B|.$$

Декартова степень множества. Обозначение A^n. Это множество, состоящее из всех последовательностей длины n, каждый член которых принадлежит множеству A.

1 Теоретико-множественные тождества

Может так оказаться, что две разные формулы с теоретико-множественными операциями задают одно и то же множество при любых значениях входящих в них переменных множеств. Такая пара фомул образует теоретико-множественное тождество и запиывается через знак равенства.

Простейшие примеры тождеств

$$A \cup B = B \cup A;\ A \cap B = B \cap A;\ (A \cup B) \cup C = A \cup (B \cup C);\ (A \cap B) \cap C = A \cap (B \cap C).$$

Они очевидны из определения.

Вот менее очевидный пример тождества:

$$(A \cap B) \setminus C = (A \setminus C) \cap B.$$

Нарисуем левую и правую часть на картинке кругов Венна. Видим, что множество получается одно и то же в обоих случаях.

Почему рассуждение с картинкой корректно? Оно на самом деле скрывает под собой разбор возможных случаев. Каждый элемент может принадлежать или не принадлежать одному из трех множеств. Поэтому всего есть 8 вариантов, которые отмечены на рисунке. Для каждого варианта можно проверить, что элемент входит в множество, задавамое левой частью, тогда и только тогда, когда он входит в множество, задаваемое правой частью.

Аналогично можно доказывать и другие тождества. Например, тождества дистрибутивности для объединения и пересечения

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C); \quad (A \cup B) \cap C = (A \cap C) \cup (B \cap C).$$

Ассоциативность симметрической разности

$$(A \triangle B) \triangle C = A \triangle (B \triangle C)$$

также можно увидеть на картинке.

2 Логические переменные, логические связки

Но при большом количестве переменных-множеств круги Венна становятся не слишком удобными.

Заметим, что значение каждой формулы с множествами задается фактически таблицей, в которой для каждого набора вариантов вхождений элемента в множество указано, принадлежит ли данный элемент множеству-результату.

Вхождения элементов принимают логические значения «истина» 1 и «ложь» 0. Таблица, о которой шла речь, задает функцию из наборов логичеких значений в логические значения. Такие функции называются булевыми (или логическими). Функции от логических аргументов, отвечающие основным операциям, назовем логическими связками. Обычно используются такие связки как отрицание конъюнкция (соответствует пересечению), дизъюнкция (соответствует объединению), сумма по модулю 2, она же XOR, она же «исключающее ИЛИ»

(соответствует симметрической разности), равносильность $\equiv$ и импликация (или логическое следование) $\to$. Вот таблицы для этих связок

x	y	$x \wedge y$	$x \vee y$	$x \to y$	$x \oplus y$
0	0	0	0	1	0
0	1	0	1	1	1
1	0	0	1	0	1
1	1	1	1	1	0

Есть еще связка, применяемая к одной переменной: отрицание $\neg 0 = 1$, $\neg 1 = 0$.

Теоретико-множественной операции разности $A \setminus B$ не соответствует связка в стандартном наборе. задаваемую ею функцию можно выразить через имеющиеся связки. Это функция $x \wedge \neg y$.

Получаем более упорядоченный способ доказательства теоретико-множественных формул: составить соответствующие логические формулы Φ_1 и Φ_2, после чего проверить, что Φ_1 и Φ_2 задают одну и ту же логическую функцию. Разумеется, в общем случае мы ничего не выигрываем. Всё равно нужно разбирать таблицы истинности. Но в некоторых случаях так рассуждать проще.

Дело в том, что одни связки выражаются через другие, что облегчает доказательство равенства функций. Например,

$$x \oplus y = x \wedge \neg y \vee \neg x \wedge y. \tag{1}$$

Обратите внимание, что в правой части пропущены скобки. Восстанавливаются они, если указать старшинство связок. Порядок убывания старшинства отрицание, конъюнкция, дизъюнкция, импликация, XOR.

В виде логических тождеств выражаются законы логики. Приведем два примера. Законы де Моргана

$$\neg(x \vee y) = \neg x \wedge \neg y; \quad \neg(x \wedge y) = \neg x \vee \neg y$$

определяют как брать отрицание от дизъюнкции или конъюнкции. Тождество

$$x \to y = \neg y \to \neg x$$

выражает принцип контрапозиции (теорема равносильна обратной к противоположной). Этот принцип часто используется в математических доказательствах: вместо доказательства утверждения «если А, то Б» зачастую удобнее изменить посылку и доказывать равносильное утверждение «если не Б, то не А».

Приведем пример использования логических формул при доказательстве теоретико-множественных тождеств. Докажем, что

$$(A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n) \setminus (B_1 \cup B_2 \cup \cdots \cup B_n) = (A_1 \setminus B_1) \cap (A_2 \setminus B_2) \cap \cdots \cap (A_n \setminus B_n). \tag{2}$$

Запишем логическую формулу для левой части

$$(a_1 \wedge a_2 \wedge \cdots \wedge a_n) \wedge \neg(b_1 \vee b_2 \vee \cdots \vee b_n).$$

Применяя закон де Моргана, получим

$$a_1 \wedge a_2 \wedge \cdots \wedge a_n \wedge \neg b_1 \wedge \neg b_2 \wedge \cdots \wedge \neg b_n.$$

Конъюнкция коммутативна, поэтому та же самая функция предствляется формулой

$$(a_1 \wedge \neg b_1) \wedge (a_2 \neg b_2) \wedge \cdots \wedge (a_n \wedge \neg b_n).$$

Но это и есть логическая формула, отвечающая правой части (2).

3 Полнота систем связок

Система связок называется полной, если формулами, использующими эти связки, можно выразить любую булеву функцию. Введенных связок уже достаточно для полноты. Более того, справедлива следующая теорема.

Теорема 1. *Система* $\{\neg, \wedge\}$ *полна.*

Прежде доказательства теоремы сделаем такое наблюдение. Если выразить какую-то связку через заданную систему связок, то для доказательства полноты достаточно искать формулы, включающие эту дополнительную связку. Действительно, дополнительную связку всегда можно исключить, подставляя ее выражение через исходную систему связок (размер формулы при этом может сильно увеличиться).

3.1 Первое доказательство полноты

С помощью де Моргана дизъюнкция выражается через конъюнкцию и отрицание (и наоборот):

$$x \vee y = \neg(\neg x \wedge \neg y); \qquad x \wedge y = \neg(\neg x \vee \neg y)$$

(мы также использовали очевидное тождество $\neg\neg x = x$).

Поэтому достаточно доказать полноту системы связок $\{\neg, \wedge, \vee\}$.

Для начала выразим функцию f_α, которая принимает значение 1 только на одном наборе значений переменных α_1, α_2, …, α_n. Эта функция выражается как конъюнкция литералов (литерал — переменная или ее отрицание). Если $\alpha_i = 1$, то включаем в конъюнкцию переменную x_i. Если $\alpha_i = 0$, то включаем в конъюнкцию отрицание переменной $\neg x_i$.

Конъюнкция принимает значение 1 лишь тогда, когда все ее аргументы принимают значение 1. Поэтому лишь для набора $(\alpha_1, \ldots, \alpha_n)$ эта конъюнкция принимает значение 1.

Чтобы выразить произвольную функцию f, возьмем дизъюнкцию f_α по всем таким α, что $f(\alpha) = 1$. Такая дизъюнкция равна 1 в любой точке α. Если же $f(\beta) = 0$, то все члены дизъюнкции обращаются в 0 и вся дизъюнкция обращается в 0. Получили искомое выражение.

Формула, которую мы получили, имеет специальный вид. Он называется дизъюнктивная нормальная форма (ДНФ). По определению, это дизъюнкция конъюнкций литералов. Примером ДНФ является дизъюнкция переменных $x_1 \vee x_2 \vee \cdots \vee x_n$. Заметим, что если мы будем для такой функции выписывать ДНФ тем способом, который изложен в доказательстве, получится куда более длинная ДНФ (в ней будет $2^n - 1$ конъюнктов). ДНФ, которые возникли в доказательстве, называют (из уважения к их длине) совершенными. Задача нахождения самой короткой ДНФ, предсатвляющей данную функцию, в общем случае очень трудна.

3.2 Второе доказательство

Мы уже выразили $\oplus$ через конъюнкцию, дизъюнкцию и отрицание, см. (1). Значит, достаточно выразить любую функцию через $\{\wedge, \oplus, \neg\}$. Более того, нам потребуется разве что одно отрицание.

Будем строить выражение функции в системе $\{\wedge, \oplus, 1\}$ (разрешаем использовать константу 1). Для этих связок выполняются обычные свойства арифметических операций (они реализуются как умножение и сложение чисел с точностью до четности). Поэтому любую формулу с этими связками возможно преобразовать в тождественно равную ей формулу в виде многочлена (сумма произведений). Такие многочлены называются многочлена Жегалкина. У свободный член у этих многочленов равен 0 или 1.

Докажем полноту $\{\wedge, \oplus, 1\}$ индукцией по числу переменных. База индукции — 0 переменных. Константа 1 уже есть, осталось выразить константу 0: $0 = 1 \oplus 1$.

Пусть утверждение о полноте доказано для всех булевых функций от n переменных. Докажем его для булевых функций от $n + 1$ переменной. По функции $f(x_0, x_1, \ldots, x_n)$ определим две функции от n переменных:

$$f_0(x_1, \ldots, x_n) = f(0, x_1, \ldots, x_n); \quad f_1(x_1, \ldots, x_n) = f(1, x_1, \ldots, x_n).$$

По предположению индукции они выражаются в системе $\{\wedge, \oplus, 1\}$. Тогда равенство

$$f(x_0, x_1, \ldots, x_n) = (1 \oplus x_0) \wedge f_0(x_1, \ldots, x_n) \oplus x_0 \wedge f(1, x_1, \ldots, x_n)$$

выполняется для всех значений переменных (при $x_0 = 0$ обращается в 0 второе слагаемое, при $x_0 = 1$ — первое). Подставляя в правую часть формулы для f_0 и f_1, получаем представление для f.

Чтбы доказать полноту системы $\{\wedge, \oplus, \neg\}$, осталось избавиться от 1. Это просто: $1 \oplus x = \neg x$.

3.3 О полноте теоретико-множественных операций

Можно ли выразить любую функцию связками, отвечающими теоретико-множественным операциям? Ответ: нет. Причина очень проста. Эти связки, как говорят, сохраняют 0, т.е. задают булевые функции, которые на наборе из одних 0 принимают значение 0. Но тогда и любая формула из таких связок будет сохранять 0 (подставляем только 0 всюду).

Значит, отрицание выразить через такие фуннкции не удастся. И это вполне понятно: «отрицание» множества A невозможно определить корректно. В него должны входить все элементы, которые не принадлежат A. То есть, в отрицание множества $\{1\}$ обязаны входить и все равнобедренные треугольники, и функция $\sin x$. Это вполне бессмысленно. (Замечание: часто используемая операция дополнения к множеству всегда применяется в тех случаях, когда множество является подмножеством некоторого большого фиксированного множества (универсума), скажем, множества натуральных чисел. В этом случае дополнение есть просто разность универсума и нашего множества.

Однако любую функцию, которая сохраняет 0, выразить через теоретико-множественные связки, возможно. Проверить это легко, используя представления функций в виде ДНФ. Если функция сохраняет 0, ее ДНФ должна в каждом конъюнкте содержать хотя бы одну переменную. Но такой дизъюнкт выражается через теоретико-множественную разность:

$$x_1 \wedge x_2 \wedge \cdots \wedge x_k \wedge \neg y_1 \wedge \cdots \wedge \neg y_n = (x_1 \wedge x_2 \wedge \cdots \wedge x_k) \setminus (y_1 \vee y_2 \vee \cdots \vee y_n).$$

3.4 Формула включений - исключений

Теперь вернемся к переслительной комбианторике. Наша цель — обобщить формулу суммы. В теоретико-множественных обозначениях эта формула утверждает

$$|A \cup B| = |A| + |B|, \quad \text{если } A \cap B = \varnothing.$$

Если пересечение множеств непусто (варианты не взаимно исключающие), формула суммы неверна.

Определим, насколько ошибается формула суммы. Посмотрев на круги Венная, видим, что элементы пересечения посчитаны дважды (один раз как элементы A, другой — как элементы B). То есть ошибка в точности равна $|A \cap B|$ и правильная формула имеет вид

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Посмотрим, что будет в случае трех множеств. Элементы, которые входят в два множества, посчитаны дважды, а элементы, входящие во все множества, посчитаны трижды. Правильная формула будет иметь вид

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap B| - |B \cap C| + |A \cap B \cap C|.$$

Действительно, для каждой области диаграммы Венна посчитаем ее вклад в такую сумму и убедимся, что вклад всех областей, кроме внешней, равен 1.

Теперь уже можно предложить хороший вариант для общей формулы:

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \cdots = \sum_{\varnothing \neq I \subset \{1,2,\ldots,n\}} (-1)^{|I|+1} \left| \bigcap_{i \in I} A_i \right|. \qquad (3)$$

Это правильная формула.

3.5 Первое доказательство

Индукция по числу множеств. База индукции — одно множество, формула очевидна.

Индуктивный переход использует формулу для объединения двух множеств.с

$$|(A_1 \cup \dots \cup A_{n-1}) \cup A_n| = |A_1 \cup \dots \cup A_{n-1}| + |A_n| - |(A_n \cap A_1) \cup \dots \cup (A_n \cup |A_{n-1})|.$$

Для первого и третьего слагаемых по предположению индукции справедлива формула (3) для $n-1$. Поэтому первое слагаемое дает вклад в (3) для n для всех множеств I, которые не содержат n. Второе отвечает множеству $I = \{n\}$. Последнее отвечает множествам I, содержащим n (перемена знака связана с переменой мощности множества).

3.6 Второе доказательство

Формула (3) очень похожа на обычное алгебраическое тождество

$$1 - (1 - x_1)(1 - x_2) \dots (1 - x_n) = x_1 + x_2 + \dots + x_n - x_1x_2 - \dots + x_1x_2x_3 + \dots \tag{4}$$

И это неслучайно. Введем индикаторную (или характеристическую) функцию множества. Для множества A по определению $\chi_A(x) = 1$, если $x \in A$, и $\chi_A(x) = 0$, если $x \notin A$.

Мощность множества легко выражается как сумма индиктора по всему универсуму (мы считаем, что все множества лежат в одном универсуме):

$$|A| = \sum_u \chi_A(u).$$

Теперь заметим, что индикаторная функция для дополнения множества (т.е. разности универсума и множества) равна $1 - \chi_A$, для пересечения множеств это просто произведение индикаторных функций этих множеств. А индикторная функция для объединения $A = \cup_i A_i$ выражается как

$$\chi_A = 1 - (1 - \chi_{A_1})(1 - \chi_{A_2}) \dots (1 - \chi_{A_n}) \tag{5}$$

(используем закон де Моргана и выражаем дополнение к объединению как пересечение дополнений). Теперь заменим правую часть (5) на правую часть (4), произведения индикаторных функций — на индикаторные функции пересечений и просуммируем по универсуму.

3.7 Формула для симметрической разности

В симметрическую разность $A_1 \triangle A_2 \triangle \dots \triangle A_n$ входят те элементы, которые принадлежат нечетному числу множеств из семейства A_i. Для мощности симметрической разности также есть формула через пересечения:

$$|A_1 \triangle A_2 \triangle \dots \triangle A_n| = \sum_i |A_i| - 2\sum_{i<j} |A_i \cap A_j| + 4 \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \dots \tag{6}$$

Эту формулу также легко получить с помощью индикаторов. Пусть $A = A_1 \triangle A_2 \triangle \dots \triangle A_n$. Тогда

$$2\chi_A = 1 - (1 - 2\chi_{A_1})(1 - 2\chi_{A_2} \dots (1 - 2\chi_{A_n}).$$

Действительно, $1 - 2\chi_A$ принимает значения ± 1, причем -1 означает вхождение элемента в множество. Если элемент входит в четное число множеств, на таком элементе произведение будет равно $+1$ (вклад в правую часть равен 0), а если в нечетное — то -1 (вклад в правую часть равен 2). Теперь осталось раскрыть скобки и заменить произведения индикаторов на индикаторы пересечений.