Лекция 6

Множества и логика

6.1 Логические переменные, логические связки

В этом разделе мы обсудим связь теоретико-множественных операций и логики.

Начнём с примера. Как уже показано выше, значение каждой формулы с множествами задаётся таблицей, в которой для каждого набора вариантов вхождений элемента в множества, к которым применяются операции, указано, принадлежит ли данный элемент множеству-результату выполнения всех этих операций.

Мы записывали в таблицу значения 1 и 0. При этом подразумевалось, что 1 означает истинность утверждения вида «элемент x принадлежит множеству A», а 0 означает ложность такого утверждения.

Это соответствие между логическими значениями «истина», «ложь» и цифрами 1, 0 является стандартным и далее оно всюду подразумевается, если не оговорено что-то иное.

Посмотрим на таблицу, задающую пересечение множеств:

$x \in A$	$x \in B$	$x \in A \cap B$
0	0	0
0	1	0
1	0	0
1	1	1

В первых двух столбцах таблицы указаны возможные логические значения утверждений «элемент x принадлежит множеству A», «элемент x принадлежит множеству B». В третьей указаны логические значения для составного утверждения

«элемент x принадлежит множеству A» И «элемент x принадлежит множеству B».

Это утверждение состоит из двух частей, его истинность полностью определяется истинностью этих частей. Как именно, указано связующим словом «И».

Такие составные высказывания возникают очень часто. Они получаются применением *логических связок*. В примере мы использовали связку, которая называется *конъюнкция*. Мы видели, что конъюнкция соответствует пересечению множеств,

Есть и другие связки, они также соответствуют операциям и высказываниям о множествах.

Ниже в таблице приведены значения самых употребительных связок: конъюнкции $\wedge$, дизъюнкции $\vee$, суммы по модулю 2, она же XOR, она же «исключающее ИЛИ» (обозначение $\oplus$), равносильности $\equiv$ и импликации (логическое следование: «если A, то B», «из A следует B», обозначение $\to$).

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

Контрольный вопрос 6.1. Напишите таблицу значений для связки $y \to x$.

На примере мы убедились, что конъюнкция соответствует пересечению множеств. Аналогично дизъюнкция соответствует объединению, а XOR — симметрической разности.

Что соответствует импликации на языке множеств? Посмотрев на таблицу значений, видим, что импликация ложна тогда и только тогда, когда есть элемент, входящий в первое множество и не входящий во второе. По определению это означает, что первое множество не является подмножеством второго. Поэтому импликация на языке множеств означает утверждение о включении множеств $A \subseteq B$. Аналогично проверяется, что равносильность означает равенство множеств $A = B$.

А какая связка отвечает разности множеств? В таблице такой связки нет. Чтобы выразить разность множеств, нам нужна ещё одна связка: отрицание (мы её будем обозначать $\neg$). Она применяется к одному утверждению и означает высказывание о ложности этого утверждения.

Таблица отрицания очень простая: $\neg 0 = 1$, $\neg 1 = 0$.

Задача 6.1. Проверьте, составив таблицы значений, что теоретико-множественной операции разности $A \setminus B$ отвечает связка, которая имеет вид $x \wedge \neg y$.

Для связок выполняется довольно много тождеств, которые легко проверить по таблицам истинности (выполните эту проверку!).

Коммутативность конъюнкции, дизъюнкции и XOR:

$$x \wedge y = y \wedge x, \quad x \vee y = y \wedge x, \quad x \oplus y = y \oplus x. \tag{6.1}$$

Ассоциативность тех же связок:

$$(x \wedge y) \wedge z = x \wedge (y \wedge z), \quad (x \vee y) \vee z = x \vee (y \vee z), \quad (x \oplus y) \oplus z = x \oplus (y \oplus z). \tag{6.2}$$

Тождества дистрибутивности (пару из них вы уже видели в виде теоретико-множественных тождеств:

$$(x\wedge y)\vee z=(x\vee z)\wedge(y\vee z),\quad (x\vee y)\wedge z=(x\wedge z)\vee(y\wedge z),\quad (x\oplus y)\wedge z=(x\wedge z)\oplus(x\wedge z). \tag{6.3}$$

Формулы упрощения получаются подстановкой констант вместо одной из переменных

$$\begin{aligned} &0\wedge y=0, \quad 1\wedge y=y, \quad 0\vee y=y, \quad 1\vee y=1,\\ &0\to y=1, \quad 1\to y=y, \quad x\to 0=\neg x, \quad x\to 1=1,\\ &0\oplus y=y, \quad 1\oplus y=\neg y. \end{aligned} \tag{6.4}$$

Логические тождества выражают законы логики. Если истинно утверждение, выражающееся левой частью тождества, то истинно и утверждение, выражающееся правой частью тождества. И наоборот.

Тут уже уместно небольшое отступление о расстановке скобок. В логических тождествах возникают уже довольно сложные формулы, использующие разные логические связки. В таких формулах нам приходится расставлять скобки, чтобы было ясно, какая из связок применяется первой, какая второй, и так далее. Аналогично арифметическим операциям, чтобы сократить число скобок, можно договориться о том, какие связки применяются раньше, а какие позже. Принято считать, что связка отрицание $\neg$ имеет самый высокий приоритет и всегда применяется первой. Следующая по важности связка — это конъюнкция $\wedge$, она применяется второй. Следующей применяются связки дизъюнкция $\vee$ и XOR. Наконец, самый низкий приоритет у связки импликации $\to$. Между связками $\vee$ и XOR нет устоявшегося правила приоритетности. Обычно используют правило, что связки одного приоритета применяются, начиная с самой левой. Такая ситуация может возникнуть не только из-за применения $\vee$ и XOR, но и при применении нескольких импликаций подряд. Для надёжности в таких сомнительных случаях можно поставить лишнюю пару скобок. Впрочем, эти правила нам почти не понадобятся.

Приведём несколько примеров логических тождеств, которые уже встречались в рассуждениях и будут встречаться в дальнейшем.

Логический закон двойного отрицания (отрицание отрицания утверждения равносильно самому утверждению) записывается тождеством

$$\neg\neg x=x, \tag{6.5}$$

которое совершенно очевидно из таблицы истинности отрицания.

Тождество

$$x\to y=\neg y\to\neg x \tag{6.6}$$

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». Проверка тождества (6.6) легко производится по таблице.

Законы де Моргана задают правило взятия отрицания от конъюнкции и дизъюнкции

$$\neg(x \vee y) = \neg x \wedge \neg y; \quad \neg(x \wedge y) = \neg x \vee \neg y. \tag{6.7}$$

Доказать эти тождества легко, разобрав случаи возможных значений переменных.

Равенства (6.7) обобщаются на случай нескольких переменных:

$$\neg(x_1 \vee x_2 \vee \cdots \vee x_n) = \neg x_1 \wedge \neg x_2 \wedge \cdots \wedge \neg x_n; \quad \neg(x_1 \wedge x_2 \wedge \cdots \wedge x_n) = \neg x_1 \vee \neg x_2 \vee \cdots \vee \neg x_n. \tag{6.8}$$

Справедливость этих тождеств проверяется индукцией по числу переменных (база — тождества (6.7)).

Задача 6.2. Докажите аккуратно тождества (6.8).

На языке множеств законы де Моргана формулируются так: (I) элемент x не принадлежит объединению семейства множеств тогда и только тогда, когда он не принадлежит ни одному из этих множеств; (II) элемент x не принадлежит пересечению семейства множеств тогда и только тогда, когда он не принадлежит хотя бы одному из этих множеств. В таком виде законы де Моргана применимы и к бесконечным семействам множеств.

В конце раздела вернёмся к теоретико-множественных тождествам и покажем пример использования логических тождеств для доказательства теоретико-множественных.

Пример 6.3. Докажем, что

$$(A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_n) \setminus (B_1 \cup B_2 \cup \cdots \cup B_n) = (A_1 \setminus B_1) \cap (A_2 \setminus B_2) \cap \cdots \cap (A_n \setminus B_n). \tag{6.9}$$

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

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

Но это и есть логическая формула, отвечающая правой части (6.9).

6.2 Наблюдения

В этом разделе собрано несколько замечаний о логических связках и том, как они возникают в математике.

Во-первых, можно заметить, что постоянно используемые нами в рассуждениях *кванторы* «для любого» и «существует» можно рассматривать как конъюнкцию и дизъюнкцию, возможно с бесконечным числом переменных. Действительно, конструкция вида «для любого x выполняется свойство $A(x)$» соответствует конъюнкции

$$A(x_1) \wedge A(x_2) \wedge \dots$$

по всем возможным значениям x и эта конъюнкция бесконечна, если x принимает бесконечное количество значений. А конструкция «существует x, для которого выполняется свойство $A(x)$» соответствует дизъюнкции

$$A(x_1) \vee A(x_2) \vee \dots,$$

которая также иногда оказывается бесконечной. Квантор «для любого» обычно называют *квантором всеобщности* и обозначают знаком $\forall$, а квантор «существует » называют *квантором существования* и обозначают знаком $\exists$.

Если теперь перевести на этот язык законы де Моргана, то получится, что при перестановке квантора и отрицания квантор меняется на противоположный.

Пример 6.4. Рассмотрим утверждение: «у любого целого числа n есть простой делитель k». Это утверждение построено с помощью квантора всеобщности по n и квантора существования по k. По законам де Моргана отрицание этого утверждения равносильно утверждению «существует целое число n, которое не делится ни на одно простое число k» (теперь вначале квантор существования, а потом — квантор всеобщности).

Поскольку число 1 не делится ни на одно простое число, второе утверждение истинно, а первое, соответственно, ложно.

Связь между логическими тождествами и законами логики помогает понять и другие свойства связок и правил логики, используемых в математических рассуждениях.

Во-первых, правила логики объясняют важность отсутствия противоречий в математических рассуждениях. Противоречие означает, что мы получили, что одновременно выполнено некоторое утверждение x и его отрицание $\neg x$, а такого не может быть. Логически этому соответствует тому, что выражение

$$x \wedge \neg x$$

ложно независимо от того, чему равно x, а значит $x \wedge \neg x = 0$. Далее можно заметить, что в выражение $0 \to y$ истинно независимо от того, чему равен y. Подставляя получаем, что $x \wedge \neg x \to y$. Таким образом из того, что доказано x и $\neg x$ сразу следует любое утверждение y. И если в математическое рассуждение закралось противоречие, то из него мгновенно можно вывести любое, даже самое нелепое, утверждение. Так что наличие любого противоречия позволяет доказать что угодно и математика как наука теряет всякий смысл.

Возможно, стоит пояснить, почему в определении импликации мы считаем, что $0 \to 0 = 1$, $0 \to 1 = 1$, то есть, из лжи следует ложь и из лжи следует истина. На самом деле, это вполне согласуется с бытовым применением конструкции «если ..., то ...». Представим себе, что кто-то делает следующее заявление: "Если я завтра заболею, то не приду на занятия". Если на следующий день этот человек не заболел и пришел на занятия, следует ли считать, что он соврал? А если он не заболел и не пришел? И то, и другое было бы странно, ведь человек и вовсе ничего не говорил про этот случай. Нечто содержательное было сказано только для той ситуации, когда он заболел. Так что, если посылка утверждения ложна, то и в обычной жизни утверждение считают истинным.

Пример на эту тему можно привести и в математике. Рассмотрим утверждение «если число n делится на 4, то n четно». Это утверждение верно (почему?). И оно не перестанет быть верным, если вместо произвольного числа подставить какое-нибудь конкретное, например 9. Посылка утверждения становится ложной, 9 не делится на 4, но само утверждение остается истинным.

Из правил логики можно также объяснить вырожденные случаи, которые встречаются, например, в теории графов.

Пример 6.5. Оказывается, что граф, состоящий из одной вершины, является одновременно и кликой, и независимым множеством. Развернув определения, видим, что про данный граф утверждается истинность двух высказываний: «любая пара вершин в этом графе связана ребром», «любая пара вершин в этом графе не связана ребром».

В графе на одной вершине вообще нет ни одной пары вершин, как нет и рёбер. Как применить квантор всеобщности, когда множество значений пусто (не содержит ни одного элемента)?

Это так сразу не ясно, зато ясно, как это делать в случае квантора существования. Ясно, что подобное высказывание будет ложно: оно утверждает существование элемента с некоторыми свойствами, выбранного из совокупности, в которой нет ни одного элемента. Если мы уже знаем, что эльфов не бывает, то утверждение «существует гладко выбритый эльф» следует признать ложным.

Таким образом, мы можем взять отрицания наших утверждений всеобщности. По законам де Моргана мы получаем утверждения «существует пара вершин в графе, которая не связана ребром» и «существует пара вершин в графе, которая связана ребром» соответственно. Как мы уже обсудили выше, это ложные утверждения. Значит, их отрицания истинны.

Тот же результат можно получить и другим способом. Утверждение «любая пара вершин в этом графе связана ребром» можно переформулировать в виде «если $\{x, y\}$ – пара вершин графа, то x и y соединена ребром». Если в графе только одна вершина, то для всех x и y посылка этой импликации ложна. А значит, как мы обсуждали выше, утверждение истинно.

Неформально можно заметить, что разобранный пример объясняет, почему конъюнкция пустого множества членов истинна, а дизъюнкция пустого множества членов ложна. Примеров такого рода есть очень много.

Задача 6.6. Проверьте, что граф на одной вершине связный и эйлеров.

Задача 6.7. Верно ли, что минимальное натуральное число, которое делится на все простые числа, больше 2015?

6.3 Какие связки необходимы?

В этой главе мы ввели разные логические связки, соответствующие разным конструкциям в русском языке. Но достаточно ли их чтобы выразить любое, сколь угодно сложное высказывание, основанное на данных простых? Все ли рассмотренные связки необходимы или без каких-то можно обойтись? Сейчас мы обсудим эти вопросы, но сначала уточним их.

Элементарные высказывания будем обозначать переменными $x_1, x_2, \ldots, x_n, \ldots$. Произвольное высказывание, зависящее от элементарных высказываний $x_1, \ldots, x_n$, мы будем обозначать через $f(x_1, \ldots, x_n)$. Все, что мы формально требуем от такого высказывания, — это чтобы его значение определялось значениями переменных $x_1, \ldots, x_n$. То есть при произвольных значениях переменных $x_1 = \alpha_1, \ldots, x_n = \alpha_n$ высказывание $f(\alpha_1, \ldots, \alpha_n)$ должно принимать однозначно определенное значение, либо истина, либо ложь. Другими словами, мы хотим, чтобы f была *функцией* от переменных $x_1, \ldots, x_n$. Подробнее функции мы обсудим в следующей главе.

Составные высказывания можно задавать таблицей – для всех значений переменных указывать значение высказывания. Такие таблицы мы рисовали в начале главы, когда определяли высказывание $f(x, y) = x \wedge y$ и другие. Также сложные высказывания можно задавать формулами с помощью связок. Например, можно определить $f(x_1, x_2, x_3) = (x_1 \wedge x_2) \vee \neg x_3$.

Более экзотический пример получается если определить $f(x_1, x_2, x_3) = x_1$ или даже $f(x_1, x_2, x_3) = 1$. В первом случае мы говорим, что наше высказывание, зависящее от трех элементарных высказываний, есть просто первое из этих трех высказываний, а во втором, что оно просто всегда истинно. При этом в первом случае x_2 и x_3 никак не используются, а во втором и вовсе не используется ни одно из элементарных высказываний. Ничего страшного в этом нет, определением это не запрещается.

Заметим, что одно и то же высказывание можно задать разными формулами.

Пример 6.8. Рассмотрим высказывания (1) «из утверждений A_1, A_2, A_3 истинны более половины»; (2) «среди утверждений A_1, A_2, A_3 есть истинные и ложные»; (3) «не все утверждения A_1, A_2, A_3 истинны и не все утверждения A_1, A_2, A_3 ложны».

Высказывания (1) и (2) существенно различны: например, они различаются на наборе логических переменных $x_1 = 1$; $x_2 = 0$; $x_3 = 0$ (то есть A_1 истинно, а два других утверждения ложны).

Высказывания (2) и (3) по существу одинаковы. Понять это можно, например, из таблицы значений (приведём в ней и значения первого высказывания):

x_1	x_2	x_3	(1)	(2)	(3)
0	0	0	0	0	0
0	0	1	0	1	1
0	1	0	0	1	1
0	1	1	1	1	1
1	0	0	0	1	1
1	0	1	1	1	1
1	1	0	1	1	1
1	1	1	1	0	0

Какие связки можно использовать при построении таких формул? Здесь возможны разные варианты. Можно выбрать какие-то из связок, которые мы уже определили, можно добавить каких-то еще. Скажем, может оказаться полезным использовать связку «из утверждений A_1, A_2, A_3 истинны более половины».

Если некоторого набора связок достаточно, чтобы выразить любое составное высказывание, такой набор называется *полным*.

Теперь мы можем точнее сформулировать вопросы из начала этого раздела. Можно ли с помощью формул из уже введенных связок выразить любое высказывание? Можно ли обойтись меньшим набором связок?

Оказывается, верна такая теорема, которую мы постепенно докажем в этом разделе.

Теорема 6.1. *Отрицание и конъюнкция образуют полный набор.*

Остановимся на еще одном тонком моменте. Что все-таки разрешается использовать в формулах? Ясно, что можно использовать переменные, более того, разрешается даже использовать лишние переменные, которые в составном высказывании не участвуют (подумайте, зачем это может понадобиться). Ясно также, что разрешается использовать связки из заданного набора. Можно ли что-то еще? Например, можно ли использовать 0 и 1? В принципе, на последний вопрос можно было бы ответить и да, и нет — в обоих вариантах основные вопросы этого раздела остались бы осмысленными. Чтобы сохранить возможность ставить вопрос для всех вариантов, мы запрещаем использовать 0 и 1 по умолчанию, но разрешаем добавлять их в систему связок. Можно считать, что 0 и 1 – это связки с нулевым числом переменных.

Прежде чем переходить к доказательству полноты разных систем связок, полезно получше разобраться в объекте, который мы изучаем. Мы начнём с того, что определим, сколько вообще есть высказываний $f(x_1, \ldots, x_n)$ от n переменных $x_1, \ldots, x_n$.

Рассмотрим таблицу, задающую высказывание f. В таблице будет 2^n строк — это количество способов присвоить каждой из n переменных одно из двух логических значений.

Высказывание определяется последним столбцом, в котором также стоят 0 и 1. Для разных высказываний столбцы должны различаться.

Итак, осталось подсчитать количество столбцов из 2^n ячеек, каждая из которых содержит 0 или 1. Таких столбцов 2^{2^n} штук (то же самое рассуждение).

6.3.1 Полнота дизъюнкции, конъюнкции и отрицания

Таблицы значений помогают также понять, почему любое высказывание выражается через дизъюнкции, конъюнкции и отрицания. Пусть есть два составных высказывания f_1 и f_2. Как выглядит таблица для дизъюнкции $f_1 \vee f_2$, т.е. высказывания «f_1 или f_2»? В тех строках таблицы, в которых есть 1 для f_1 или для f_2, будет стоять 1 (см. таблицу дизъюнкции). В тех строках, где у f_1 и f_2 стоят нули, будет стоять 0.

Это рассуждение показывает, что любое высказывание может быть выражено как дизъюнкция таких высказываний, у которых ровно в одной строке стоит 1, а в остальных стоят нули. Действительно, выберем все строки таблицы высказывания, в которых стоят единицы; для каждой такой строки образуем высказывание, которое истинно только в данной строке, а в остальных ложно; дизъюнкция всех этих высказываний и будет выражать искомое высказывание.

Осталось научиться выражать через дизъюнкции, конъюнкции и отрицания высказывания того специального вида, который мы использовали в предыдущей конструкции. Одно высказывание такого вида построить легко, это конъюнкция всех переменных $x_1 \wedge \ldots \wedge x_n$. В её таблице значений есть ровно одна строка, в которой конъюнкция равна 1, в остальных она равна 0.

Чтобы получить высказывание, которое истинно ровно для одного (но произвольного) набора логических значений элементарных высказываний, нужно конъюнкцию подправить. Для этого используем наряду с элементарными высказываниями x_i их отрицания $\neg x_i$.

Обозначим значения элементарных высказываний $\alpha_1, \alpha_2, \ldots, \alpha_n$. Если $\alpha_i = 1$, то включаем в конъюнкцию переменную x_i. Если $\alpha_i = 0$, то включаем в конъюнкцию отрицание переменной $\neg x_i$.

Построенная конъюнкция принимает значение 1 лишь тогда, когда все её члены равны 1. Из правила построения следует, что это происходит ровно на одном наборе значений элементарных высказываний $\alpha_1, \ldots, \alpha_n$. Действительно, проверим, что на любом другом наборе $\beta_1, \ldots, \beta_n$ она ложна. Раз наборы отличаются, значит $\alpha_i \neq \beta_i$ для некоторого i. Есть две возможности. Первая: $\alpha_i = 1$, $\beta_i = 0$, и в конъюнкцию входит переменная x_i, которая обнуляется на втором наборе. Вторая возможность: $\alpha_i = 0$, $\beta_i = 1$, и в конъюнкцию входит $\neg x_i$, который обнуляется на втором наборе.

Пример 6.9. Выразим указанным способом XOR через дизъюнкцию, конъюнкцию и отрицание:

$$x \oplus y = (x \wedge \neg y) \vee (\neg x \wedge y).$$

Первый член дизъюнкции отвечает строке $1, 0$ в таблице XOR, второй член — строке $0, 1$.

Мы выразили произвольное составное высказывание в виде дизъюнкции конъюнкций переменных или их отрицаний. Такое выражение называется дизъюнктивная нормальная форма (ДНФ).

Обратите внимание, что представление в виде ДНФ не единственно. Например, дизъюнкция переменных $x_1 \vee x_2 \vee \cdots \vee x_n$ является ДНФ. Но если применить описанную выше конструкцию, получится другая ДНФ для того же высказывания (как она выглядит?). Эта ДНФ намного длиннее. ДНФ, которые получаются из строк таблицы описанным выше способом, называют совершенными.

Задача нахождения самой короткой ДНФ, представляющей данное высказывание, в общем случае очень трудна.

Задача 6.10. КНФ (конъюнктивная нормальная форма) — это конъюнкция дизъюнкций переменных или их отрицаний. Докажите, что любое высказывание выражается в виде КНФ.

6.3.2 Полнота конъюнкции и отрицания

Теперь уже нетрудно доказать теорему – для этого осталось избавиться от дизъюнкции.

С помощью законов 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 $\neg\neg x = x$).

Возьмём высказывание, выраженное через дизъюнкции, конъюнкции и отрицания. Каждую дизъюнкцию заменим по закону де Моргана на выражение, содержащее лишь конъюнкции и отрицания. Выполнив все такие замены, получим высказывание, выраженное лишь через конъюнкции и отрицания.

Пример 6.11. Выразим указанным способом XOR через конъюнкцию и отрицание:

$$x \oplus y = \neg(\neg(x \wedge \neg y) \wedge \neg(\neg x \wedge y)).$$

6.3.3 Алгебраическое доказательство теоремы 6.1

Мы приведем еще одно доказательство теоремы. Для этого мы докажем полноту системы связок $\wedge, \oplus, 1$.

Почему из этого будет следовать теорема? Мы уже выразили $\oplus$ через конъюнкцию и отрицание, см. пример 6.11. Кроме того, через конъюнкцию и отрицание можно выразить и тождественно истинное утверждение:

$$1 = \neg(x \wedge \neg x).$$

Поэтому достаточно выразить любое высказывание через $\wedge, \oplus, 1$ и применить тот же приём, что в предыдущем разделе: последовательно убрать из выражения $\oplus$ и 1.

Чем хороши выражения, использующие только $\wedge, \oplus, 1$? Для связок $\wedge, \oplus, 1$ выполняются обычные свойства арифметических операций. Трюк состоит в том, чтобы

посмотреть на 0 и 1 как на вычеты по модулю 2. Тогда $\wedge$ соответствует произведению вычетов, а $\oplus$ – сумме вычетов.

Поэтому неудивительно, что эти связки можно использовать для представления составных высказываний в виде многочленов. Многочлен по определению — сумма произведений. В данном случае сумма это XOR, а произведение — конъюнкция. Такие многочлены называются *многочленами Жегалкина*. Свободный член у этих многочленов равен 0 или 1.

Докажем индукцией по n, что произвольное высказывание $f(x_1, \ldots, x_n)$ можно выразить формулой со связками $\wedge, \oplus, 1$. База индукции — 0 высказываний. Высказываний f от нуля переменных всего два – 0 и 1. Константа 1 уже есть, осталось выразить константу 0: $0 = 1 \oplus 1$.

Пусть утверждение доказано для всех составных высказываний от n элементарных высказываний. Докажем выразимость для составных высказываний от $n+1$ элементарного высказывания. Для этого по высказыванию $f(x_1, \ldots, x_{n+1})$ определим два высказывания от n элементарных высказываний, а именно, $f_0(x_1, \ldots, x_n) = f(x_1, \ldots, x_n, 0)$ и $f_1(x_1, \ldots, x_n) = f(x_1, \ldots, x_n, 1)$.

По предположению индукции и f_0, и f_1 выражаются через связки $\wedge, \oplus, 1$. Выразим теперь f:

$$f = ((1 \oplus x_{n+1}) \wedge f_0) \oplus (x_{n+1} \wedge f_1)\,.$$

Действительно, при $x_{n+1} = 0$ обращается в 0 второе слагаемое, при $x_{n+1} = 1$ — первое. В любом случае получаем совпадение левой и правой частей равенства.

6.4 Формула включений-исключений

Теперь вернемся к перечислительной комбинаторике и приведем еще два доказательства формулы включений-исключений. Напомним, что формула включений-исключений обобщает правило суммы и даёт выражение для объединения нескольких, возможно пересекающихся, множеств. Для двух и трех множеств мы получили такие выражения

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

При доказательстве второй из этих формул уже использовались круги Венна: мы проверяли, что каждый элемент объединения посчитан ровно один раз, по отдельности для каждой части, на которые круги Венна разбивают объединение.

Формулы для двух и трёх множеств подсказывают общий вид формулы включений-исключений. Нужно взять сумму мощностей всех множеств. Некоторые элементы при этом посчитаны более одного раза. Поэтому нужно вычесть мощности попарных пересечений множеств, после чего некоторые элементы объединения вообще не будут посчитаны. Далее нужно последовательно прибавлять и вычитать мощности тройных, четверных и т.д. пересечений, включая их в итоговую сумму с чередующимися знаками.

Способ построения итоговой формулы из этого описания понятен. Но удобно представить итоговую формулу в более компактном виде. Для этого введём обозначения. Множества, для которых ищем объединение, обозначим A_1, A_2, …, A_n. Через S будем обозначать подмножество множества $\{1,\ldots,n\}$, каждое такое подмножество выделяет некоторое семейство подмножеств $\{A_i : i \in S\}$ Через A_S обозначим пересечение всех множеств, входящих в семейство S, т.е.

$$A_S = \bigcap_{i\in S} A_i.$$

В таких обозначениях формула включений-исключений записывается достаточно компактно:

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{S\neq\varnothing} (-1)^{|S|+1}|A_S|. \tag{6.10}$$

Здесь в сумме исключено пустое семейство множеств, чтобы не создавать лишних вопросов. Однако, если вспомнить наши обсуждения выше, легко сообразить, что пересечение пустого семейства должно быть пусто. Поэтому такое исключение делать не обязательно.

Знаки в сумме (6.10) определяются количеством множеств в семействе. Из примеров для $n = 2$ и $n = 3$ мы видим, что сами множества (т.е. пересечения по семействам множеств, содержащих одно множество) должны входить со знаком «+». Для остальных семейств знак определяется из правила чередования знаков.

Приведем два доказательства этой формулы.

6.4.1 Первое доказательство

Индукция по числу множеств. База индукции — одно множество, формула очевидна: $|A| = (-1)^{1+1}|A|$.

Индуктивный переход использует формулу для количества элементов в объединении двух множеств:

$$\begin{aligned}|(A_1 \cup \cdots \cup A_{n-1}) \cup A_n| &= |A_1 \cup \cdots \cup A_{n-1}| + |A_n| - |A_n \cap (A_1 \cup \cdots \cup A_n)| = \\ &= |A_1 \cup \cdots \cup A_{n-1}| + |A_n| - |(A_n \cap A_1) \cup \cdots \cup (A_n \cap A_{n-1})|.\end{aligned}$$

Для первого и третьего слагаемых по предположению индукции справедлива формула (6.10) для $n-1$ множества. Поэтому первое слагаемое дает вклад в сумму (6.10) для n множеств вида

$$\sum_{\substack{S\neq\varnothing\\ S\subseteq\{1,\ldots,n-1\}}} (-1)^{|S|+1}|A_S|.$$

Второе слагаемое — это в точности $(-1)^{1+1}A_{\{n\}}$.

Рассмотрим теперь последнее слагаемое. По индуктивному предположению оно равно

$$\sum_{\substack{S\neq\varnothing\\ S\subseteq\{1,\ldots,n-1\}}} (-1)^{|S|+1}|B_S|,$$

где вместо множеств A_i в формулу включений-исключений для $n-1$ множества подставлены множества $B_i = A_n \cap A_i$.

Для любого $S \subseteq \{1, \ldots, n-1\}$ выполняется равенство

$$B_S = \bigcap_{i \in S} (A_n \cap A_i) = A_n \cap A_S = A_{S \cup \{n\}}.$$

Получается, что мощность объединения $|(A_1 \cup \cdots \cup A_{n-1}) \cup A_n|$ представлена в виде суммы таких же слагаемых, что и в сумме (6.10): первое слагаемое отвечает семействам, не содержащим A_n, второе и третье — семействам, содержащим A_n. Нужно ещё проверить, что эти слагаемые входят с правильными знаками. Для первых двух слагаемых это ясно из самих формул. Для третьего заметим, что мощность S отличается от мощности $S \cup \{n\}$ на 1, так как $S \subseteq \{1, \ldots, n-1\}$. Это даёт лишний знак «$-$». Но в формулу для объединения двух множеств это слагаемое также входит со знаком «$-$». Поэтому окончательный знак будет правильным:

$$-(-1)^{|S|+1} = (-1)^{|S \cup \{i\}|+1}.$$

6.4.2 Второе доказательство

Формула (6.10) очень похожа на обычное алгебраическое тождество

$$1 - (1-x_1)(1-x_2)\ldots(1-x_n) = x_1 + x_2 + \cdots + x_n - x_1x_2 - \cdots + x_1x_2x_3 + \ldots \quad (6.11)$$

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 $x \notin A$.

Будем считать, что все рассматриваемые множества лежат в каком-то объемлющем множестве (*универсуме*), например, в объединении всех множеств, для которых доказывается формула. Мощность множества легко выражается как сумма индикатора по всему универсуму:

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

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 индикаторная функция для объединения $A = \cup_i A_i$ выражается как

$$\chi_A = 1 - (1 - \chi_{A_1})(1 - \chi_{A_2})\ldots(1 - \chi_{A_n}) \quad (6.12)$$

(используем закон де Моргана и выражаем дополнение к объединению как пересечение дополнений). Теперь заменим правую часть (6.12) на правую часть (6.11), произведения индикаторных функций — на индикаторные функции пересечений и просуммируем по универсуму.

6.4.3 Формула для симметрической разности

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

$$|A_1 \triangle A_2 \triangle \cdots \triangle A_n| = \sum_i |A_i| - 2\sum_{i<j} |A_i \cap A_j| + 4 \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \ldots \quad (6.13)$$

Эту формулу легко получить, несколько изменив рассуждение с индикаторными функциями. Пусть $A = A_1 \triangle A_2 \triangle \cdots \triangle A_n$. Тогда

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

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.