Лекции по Дискретной математике

Соколов П.П.

2024

Оглавление

Глава 1

Алгебра логики

1.1 Высказывания

Перед тем, как доказывать всевозможные полезные в повседневной жизни программиста факты и утверждения, необходимо договориться о некотором общем языке, в рамках которого производится математика. В нашем случае, это язык булевой логики, в которой основным объектом является *высказывание*.

Определение 1.1. *Высказывание* — предложение, о котором можно однозначно сказать, истинно оно или ложно.

Пример 1.1. “В первые 4 миллиарда лет своего существования Земля вращалась вокруг Солнца” — истинное высказывание.

Пример 1.2. “Сейчас на улице солнечно, и завтра у нас нет пар” является высказыванием, хоть его истинность и зависит от текущего положения дел.

Пример 1.3. “Либо работай, либо готовься к экзамену” высказыванием не является, поскольку вопрос об истинности этого предложения не имеет смысла.

Но каким образом мы можем рассуждать об истинности или ложности высказываний? Заметим, что на самом деле высказывания бывают как минимум двух разных видов:

Определение 1.2. *Составное высказывание* — высказывание, составленное из других, более простых, высказываний.

Определение 1.3. *Атомарное высказывание* — самое короткое, «неделимое» высказывание; то, которое нельзя разделить на более простые.

Истинность атомарных высказываний математически установить не так просто; знание о них дано нам заранее, в виде явного указания, истинны они или нет. Для краткости записи, в алгебре логики каждое атомарное высказывание обозначают отдельной латинской буквой — p, q, r, A, B, C,...

В свою очередь, истинность составного высказывания уже можно определить, если известна истинность его частей. Например, в примере 1.2, если сейчас на улице действительно солнечно и действительно завтра нет пар, то всё высказывание целиком также истинно. Заметим, что мы смогли сделать этот вывод благодаря интуитивному пониманию значения слова “и”; в формальной логике, ему соответствует *логическая связка* “И” (также обозначается как $\wedge$).

Определение 1.4. *Логическая связка* — конструкция, позволяющая получать новые составные высказывания из других (возможно, тоже составных) высказываний.

Пример 1.4. “ИЛИ” (также обозначается как $\vee$) является логической связкой, создающей новое высказывание из двух других.

Пример 1.5. “НЕ” (также обозначается как $\neg$) является логической связкой, создающей по высказыванию новое, являющееся противоположным по смыслу исходному.

При желании, можно придумать свои, совершенно другие логические связки; что важно, так это то, что же они всё-таки обозначают — то есть, как истинность получающегося при использовании связки утверждения зависит от истинностей составных частей. Это можно задать с помощью *таблицы истинности*.

Определение 1.5. *Таблица истинности* для связки n высказываний — таблица из $n+1$ столбца и 2^n строчек, где для каждого возможного случая (набора из n фактов об истинности либо ложности каждой части составного высказывания) найдётся ровно одна строчка, где в первых n клетках будет выписан этот случай, а в последней клетке указано, истинно ли соответствующее составное высказывание в этом случае.

Пример 1.6. Таблицы истинности для всех упомянутых логических связок (для краткости совмещены в одну таблицу):

p	q	$p \wedge q$	$p \vee q$	$\neg p$
0	0	0	0	1
0	1	0	1	1
1	0	0	1	0
1	1	1	1	0

Кроме этого, есть ещё одна очень важная связка — импликация ($\to$).

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

По смыслу, она соответствует утверждению формата “если p, то q”. На первый взгляд, её таблица истинности может показаться немного странной; однако же рассмотрим следующие случаи:

- Если p ложно, то, каким бы ни было q, само по себе утверждение $p \to q$ истинно: из лжи может следовать что угодно.
- Если q истинно, то $p \to q$ само по себе истинно уже хотя бы потому, что истинно q: в "доказательстве" для $p \to q$ мы можем воспользоваться "доказательством" для q, само по себе p никак не затронув.
- Если p истинно, а q ложно, то $p \to q$ истинным быть не может по определению: из истинных утверждений не могут следовать ложные.

Кроме следствия одних утверждений из других, естественно задуматься о равносильности утверждений: $(p \equiv q) := (p \to q) \wedge (q \to p)$ (здесь $:=$ обозначает "равно по определению").

Как уже говорилось ранее, в конечном итоге истинность абсолютного большинства высказываний зависит от истинности атомарных высказываний, в них входящих; тем не менее, есть некоторые особые случаи, которые мы рассмотрим далее.

1.2 Эквивалентные высказывания, тавтологии

Определение 1.6. *Эквивалентные высказывания* — те высказывания, которые истинны одновременно (либо ложны одновременно) во всех возможных случаях.

Пример 1.7. Произвольное высказывание A эквивалентно само себе: $A \Leftrightarrow A$.

Проведём небольшое наблюдение: если $A \Leftrightarrow B$, то $A \equiv B$ истинно всегда.

Определение 1.7. Утверждения, истинные во всех возможных случаях (истинностях/ложностях входящих в них атомарных высказываний), называются *тавтологиями*.

Определение 1.8. Утверждения, ложные во всех возможных случаях, называются *противоречием*.

Как доказывать эквивалентности и то, что утверждения являются тавтологиями? Например, таблицами истинности.

Пример 1.8. Следующие утверждения являются тавтологиями:

a) $p \wedge p \equiv p$;
b) $p \vee p \equiv p$;
c) $\neg(p \vee q) \equiv \neg p \wedge \neg q$;
d) $\neg(p \wedge q) \equiv \neg p \vee \neg q$;
e) $p \wedge q \equiv q \wedge p$;
f) $p \vee q \equiv q \vee p$;
g) $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$;
h) $p \vee (q \vee r) \equiv (p \vee q) \vee r$;
i) $p \wedge (q \vee r) \equiv p \wedge q \vee p \wedge r$;
j) $p \vee q \wedge r \equiv (p \vee q) \wedge (p \vee r)$;
k) $\neg q \to \neg p \equiv p \to q$;
l) $\neg(\neg p) \equiv p$;

(У $\neg$ самый высокий приоритет; $\wedge$ приоритет более высокий, чем у $\wedge$; у $\to$ — ниже всех, кроме $\equiv$, имеющего самый низкий приоритет.)

Кроме этого, существуют другие, более удобные способы доказательств тавтологичности: с помощью разбора случаев; с помощью замены частей высказывания на эквивалентные им; наконец, от противного.

1.3 Кванторы существования и всеобщности

На самом деле, в основаниях математики используется ещё чуть более сложный язык, чем состоящий из атомарных высказываний и логических связок. В абсолютном большинстве случаев перед математиком — да и любым исследователем, использующим математику как инструмент, в том числе и грамотным программистом — стоит задача не просто установления истинности либо ложности некоторых утверждений, но исследования свойств некоторого математического объекта. Для этого необходимы выразительные средства, позволяющие рассуждать о совокупностях объектов.

Зачастую объекты, находящиеся на рассмотрении математика, обозначаются латинскими буквами: x, y, z, G, V, E,.... Далее мы можем формулировать утверждения формата "x делится на 15 без остатка" и т.д. Но откуда берутся все эти иксы и игреки, о которых мы говорим? Существует два основных способа рассуждать об объектах: 1) как о некотором достоверно существующем объекте, который мы просто обозначаем буквой; 2) как о произвольном по своей сути объекте — в качестве обозначаемого должен подойти любой из них. Для каждого из них есть своё средство в языке, называемое *квантором*.

Квантор существования $\exists x.\varphi(x)$ позволяет формулировать высказывания вида "существует x такой, что выполнено $\varphi(x)$", где $\varphi(x)$ — произвольное высказывание про x.

Квантор всеобщности $\forall x.\varphi(x)$ позволяет формулировать высказывания вида "для любого x выполнено $\varphi(x)$", где $\varphi(x)$ — произвольное высказывание про x.

Пример 1.9. Высказывание "единорогов не существует" можно записать как "$\neg\exists x.x$ — единорог" (на всякий случай замечу, что истинности этого высказывания я не утверждал).

Пример 1.10. Высказывание "не существует максимального простого числа" можно записать как "$\neg\exists x.(x$ — простое$) \wedge \forall y.(y$ — простое$) \to y \leqslant x$".

При попытке определить истинность высказываний с, например, квантором всеобщности $\forall x$ возникает вопрос: из какой совокупности берётся x? Это произвольный математический объект? Объект реального мира? Формула? Число?

В действительности, при использовании формул с кванторами всегда заранее фиксируется, из какого набора подбираются объекты. Этот набор называется *носителем*, либо *предметной областью*; в абсолютном большинстве случаев, носитель является множеством. А что это значит, мы рассмотрим в следующей главе.

Глава 2

Теория множеств

2.1 О наивной теории множеств

У любого человека есть некоторое интуитивное представление о том, что такое множество: это некоторая коллекция объектов, называемых *элементами* множества.

Определение 2.1. $x \in X$ означает "x является элементом множества X".

Определение 2.2. $\{x_1, \ldots, x_n\}$ — обозначение множества, в точности состоящего из элементов $x_1, \ldots, x_n$.

(Заметим, что ничего не мешает множествам самим быть элементами некоторых других множеств: $0 \in \mathbb{N} \in \{\mathbb{N}\} \in \ldots$)

Также естественно считать, что множества полностью определяются тем, какие элементы в них содержатся; также это можно понимать как "в множествах нет дополнительной структуры"; это называется

Аксиома 2.1 (Аксиома экстенсиональности)**.** *Множества равны тогда и только тогда, когда в них содержатся одни и те же элементы.*

$$A = B \iff \forall x.(x \in A) \equiv (x \in B).$$

Однако недаром теория множеств, которую мы здесь вводим, называется "наивной" — оказывается, интуитивное представление о множествах может завести нас в ловушку, в которую попались логики начала XX века, пытаясь показать непротиворечивость математики. Проблемы начинаются, когда мы начинаем отождествлять множество X и предикат принадлежности к нему $\in X$, т.е. когда мы вводим следующую аксиому:

Аксиома (Аксиома неограниченного выделения)**.** *Для любого условия $\varphi(x)$ на объектах существует множество объектов, удовлетворяющих этому условию. Оно обозначается $\{x \mid \varphi(x)\}$.*

(Обратите внимание, что мы её не нумеруем — для того, чтобы отделить её от остальных аксиом и теорем, которыми мы в действительности пользуемся.)

Пользуясь введёнными на данный момент определениями и аксиомами, мы уже можем вывести противоречие. Такие противоречия, которые выводятся из на первый взгляд невинных предположений, называются *парадоксами*; их особая ценность заключается в том, что они обнажают несовершенство рассуждений: либо ошибочность предположений, либо некорректность самого хода рассуждений.

Итак, *парадокс Рассела*. Формально его можно оформить как теорему:

Теорема 2.1 (Парадокс Рассела)**.**
Наивная теория множеств противоречива.

Доказательство. По шагам.

1. Рассмотрим следующие объекты x: $x \in x$. Такие иксы называются "самосодержащими".

2. В свою очередь, если $x \notin x$, то x называется "несамосодержащим".

3. По аксиоме неограниченного выделения, совокупность

$$R = \{x \mid x \notin x\}$$

   является множеством. Другими словами, существует множество несамосодержащих множеств, называющееся R.

4. По закону исключённого третьего из алгебры логики, должно быть верно ровно одно из $R \in R$ либо $R \notin R$. Однако рассмотрим оба случая:

   - Пусть $R \in R$, то есть R является несамосодержащим. Но тогда по определению несамосодержащих выполнено $R \notin R$.
   - Пусть $R \notin R$, то есть R не является несамосодержащим. Но тогда он самосодержащий, то есть $R \in R$.

5. Рассмотрев оба случая, пришли к противоречию. Значит, исходные предположения также противоречивы.

□

Примечание. Точно такие же парадоксы содержатся и в естественном языке: рассмотрим понятие "несамоописывающий". Является ли оно самоописывающим?

Примечание. Пересказанный в виде логической задачи, парадокс Расселя также называется парадоксом брадобрея: «Добрый брадобрей бреет тех и только тех жителей города, кто не бреется сам. Кто бреет брадобрея?»

Найденная в самых основаниях математики зияющая дыра парадокса породила отдельную область логических исследований, занимающаяся вопросами корректности доказательств и, в целом, логическими основаниями математики. В качестве решения проблемы было предложено сразу несколько решений; новые появляются до сих пор. Однако мы не будем изучать их все, а остановимся на том, которое победило в конечном счёте и на данный момент доминирует. О нём — далее.

2.2 Теория множеств Цермело-Френкеля

Ключевая идея теории ZF (краткое название теории множеств Цермело-Френкеля) — просто нужно быть осторожнее в рассуждениях о том, является ли что-то множеством или нет. В частности, не бывает "слишком больших" множеств (содержащих вообще всё) и самосодержащих.

Как и в наивной теории множеств, в ZF конечные наборы $\{x_1, \ldots, x_n\}$ являются множествами, а равные множества — в точности те, которые содержат одинаковые элементы. Кроме этого, в ZF есть:

Аксиома 2.2 (Аксиома (ограниченного) выделения)**.** *Для любого множества A и условия $\varphi(x)$ на его объектах существует множество объектов из A, удовлетворяющих этому условию. Оно обозначается $\{x \in A \mid \varphi(x)\}$.*

Заметим, что, хоть это и является ограничением исходной проблематичной аксиомы, мы всё ещё можем восстановить парадокс Рассела, если в качестве A мы возьмём некоторое "множество всех множеств" U. К счастью, в ZF такого U не существует: это гарантируется *аксиомой регулярности*, которую мы здесь не приводим, а вместо этого приводим два полезных следствия из неё:

Следствие 2.1. *Множество не может содержать само себя: $\forall x. x \notin x$. В частности, не существует множества всех множеств U, поскольку для него было бы выполнено $U \in U$.*

Следствие 2.2. *Не бывает бесконечно убывающей цепочки множеств $\ldots \in x_3 \in x_2 \in x_1 \in x_0$.*

(Заметьте, что возрастающие цепочки разрешены: $0 \in \mathbb{N} \in \{\mathbb{N}\} \in \ldots$)

Из аксиомы выделения также следует существование множества, являющегося пересечением двух других множеств:

Определение 2.3. *Пересечением* множеств A и B называется множество $A \cap B := \{x \in A \mid x \in B\}$.

Следствие 2.3. *В пересечении A и B содержатся в точности те элементы, которые содержатся и в A, и в B.*

$$x \in A \cap B \iff x \in A \wedge x \in B.$$

Также можно встретить такую запись: $A \cap B = \{x \mid x \in A \wedge x \in B\}$. Как мы уже знаем, формально она некорректна, но поскольку ясно, как построить такое множество с помощью аксиомы *ограниченного* выделения, такой записью пользоваться можно.

Из *аксиомы объединения* (опять же, здесь мы её не приводим) следует существование множества, являющегося объединением двух и более множеств (опять же, впереди не вполне корректная, но более простая и наглядная запись):

Определение 2.4 (Объединение множеств)**.** $A \cup B := \{x \mid x \in A \vee x \in B\}$.

Определение 2.5 (Объединение семейства множеств)**.** Пусть дана последовательность множеств $A_1, \ldots, A_n, \ldots$. Существует множество, являющееся их объединением:

$$\bigcup_{i=1}^{\infty} A_i = \{x \mid \exists i.\ x \in A_i\}$$

Из *аксиомы бесконечности* следует, что совокупность натуральных чисел $\mathbb{N}$ является множеством; из *аксиомы степени* — что совокупность подмножеств множества A тоже является множеством:

Определение 2.6. Множество S *является подмножеством* множества A, если все элементы S также являются элементами A:

$$S \subseteq A \ :\Longleftrightarrow\ \forall x.\ x \in S \to x \in A.$$

Аксиома 2.3 (Аксиома степени aka аксиома булеана)**.** *Для любого множества X существует множество всех его подмножеств 2^X, также обозначаемое $\mathcal{P}(X)$:*

$$2^X := \mathcal{P}(X) := \{S \mid S \subseteq X\}.$$

Кроме этого, из аксиом ZF выводится существование следующих разновидностей множеств:

Определение 2.7 (Декартово произведение)**.** Для любых двух множеств A и B существует множество $A \times B$ упорядоченных пар, где первая компонента пары — из множества A, а вторая — из множества B:

$$A \times B \ :=\ \{(a, b) \mid a \in A \wedge b \in B\}.$$

Определение 2.8. Для любых двух множеств A и B существует множество B^A всюду определённых функций из A в B (про функции мы поговорим подробнее позднее):

$$B^A \ :=\ \{f \mid f : A \to B\}.$$

2.2.1 Разность, дополнение и универсум

Ещё одно определение уже знакомого вам из школы множества:

Определение 2.9 (Разность множеств)**.** $A \setminus B := \{x \in A \mid x \notin B\}$.

Кроме этого, часто также рассматривают следующую операцию

Определение 2.10 (Дополнение множества)**.** $\overline{A} := U \setminus A$.

Где U — некоторый загадочный "универсум", содержащий кроме A вообще "всё". Как мы знаем, множества всех множеств не существует; что же такое U?

На самом деле, конкретное определение U зависит от задачи. В какой-нибудь конкретной области математики (математический анализ, линейная алгебра, комбинаторика...) за U можно взять предметную область:

- В математическом анализе — множество действительных чисел $\mathbb{R}$, объединённое со всеми, получаемыми из него с помощью операций, описанных в предыдущей секции;
- В линейной алгебре — аналогично, но для произвольного поля $\mathbb{F}$, над которым производятся вычисления;
- В комбинаторике — аналогично, но для конечных подмножеств натуральных чисел.

В случае, если конкретная предметная область не определена — например, если исследуется истинность высказываний про произвольные множества — универсумом следует взять множество, содержащее все элементы, которые могут рассматриваться в доказательстве.

2.3 Аксиома выбора

Кроме исходных аксиом ZF, в математике часто приходится прибегать к так называемой *аксиоме выбора.*

Определение 2.11. *Семейством* множеств $F_1, \ldots, F_n, \ldots$ называется множество F, их содержащее как элементы: $F_1 \in F, \ldots, F_n \in F, \ldots$

(В семействе может быть множеств гораздо больше, чем натуральных чисел; более того, множества в семействе могут быть вообще никак не пронумерованы.)

Аксиома 2.4 (Аксиома выбора aka AoC)**.** *Для всякого семейства F непустых множеств существует функция* $\texttt{choice}(F)$*, каждому множеству X из семейства сопоставляющая элемент этого множества. Другими словами,*

$$\texttt{choice}(F) : F \to \bigcup_{X \in F} X$$

$$\texttt{choice}(F)(X) \in X$$

В наивном понимании вещей (если, например, представлять множества как просто коллекции объектов) AoC, конечно, выполняется — и, действительно, для достаточно маленьких семейств F функцию $\texttt{choice}(F)$ можно построить благодаря другим аксиомам, не прибегая к AoC. Но в применении к более крупным семействам она позволяет получать какие-то уж совсем странные следствия: удваивать сферы, упорядочивать произвольные множества,.... Может показаться, что такая странная аксиома должна приводить к противоречиям, однако таковые до сих пор не были найдены.

Учитывая полезность AoC для доказательства фундаментальных результатов в теории порядков и в коммутативной алгебре, её всё-таки используют; система аксиом ZF вместе с AoC называется ZF+C либо просто ZFC.

2.3.1 Непротиворечивость ZF(C), теорема о неполноте

Всё же возникает вопрос: мы узнали, что наивная теория множеств противоречива. Можем ли мы доказать, что ZF непротиворечива?

К сожалению, нет: из *первой Теоремы Гёделя о неполноте* следует, что в любой теории, позволяющей формулировать и доказывать некоторые достаточно простые факты о натуральных числах, нельзя доказать собственную непротиворечивость; в нашем случае это значит, что, пользуясь стандартным аппаратом теории множеств, непротиворечивость самого аппарата по себе доказать нельзя, для этого необходимы некоторые более сильные предположения.

Но об этом переживать не стоит: во-первых, есть риск из программиста превратиться в логика или философа; во-вторых, учитывая долгую историю математики, в ходе которой противоречия так и не были найдены либо устранялись без серьёзных потерь, вероятность того, что Ваше доказательство вдруг окажется некорректным, очень и очень мала.

Однако если и извлечь урок из всей этой истории, то следующий: чем на меньшее количество дополнительных предположений опирается доказательство, тем лучше (тем меньше шанс, что какие-то предположения окажутся неверны); чем проще доказательство, тем оно лучше (поскольку его будет проще поправить, если какие-то предположения окажутся неверны).