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

Пример 1. “В первые 4 миллиарда лет своего существования Земля вращалась вокруг Солнца” — истинное высказывание.

Пример 2. “Сейчас на улице солнечно, и завтра у нас нет пар” является высказыванием, хоть его истинность и зависит от текущего положения дел.

Пример 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 2. *Составное высказывание* — высказывание, составленное из других, более простых, высказываний.

Определение 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 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 4. *Логическая связка* — конструкция, позволяющая получать новые составные высказывания из других (возможно, тоже составных) высказываний.

Пример 4. “ИЛИ” (также обозначается как $\vee$) является логической связкой, создающей новое высказывание из двух других.

Пример 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 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 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 и тавтологии

Определение 6. *Эквивалентные высказывания* — те высказывания, которые истинны одновременно (либо ложны одновременно) во всех возможных случаях.

Пример 7. Произвольное высказывание A эквивалентно само себе: $A \Leftrightarrow A$.

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

Определение 7. Утверждения, истинные во всех возможных случаях (истинностях/ложностях входящих в них атомарных высказываний), называются *тавтологиями.*

Определение 8. Утверждения, ложные во всех возможных случаях, называются *противоречием.*

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

Пример 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 $\rightarrow$ — 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;
- 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:

- как о некотором достоверно существующем объекте, который мы просто обозначаем буквой;
- 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.

Пример 9. Высказывание "единорогов не существует" можно записать как "$\neg\exists x.x$ — единорог" (на всякий случай замечу, что истинности этого высказывания я не утверждал).

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

Пример 10. Высказывание "не существует максимального простого числа" можно записать как "$\neg\exists x.(x$ — простое$) \wedge \forall y.(y$ — простое$) \rightarrow y \leqslant x$".

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*; строго говоря, носитель должен являться множеством. А что это значит, мы рассмотрим в следующей главе.