

МГТУ ФН-12 МГТУ ФН-12 МГТУ ФН-12

Московский государственный технический университет
имени Н.Э. Баумана

Факультет «Фундаментальные науки»
Кафедра «Математическое моделирование»

А.Н. Канатников

МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ

Конспект лекций

Для студентов кафедры ИУ9

Москва
2009

МГТУ ФН-12 МГТУ ФН-12 МГТУ ФН-12

1. АЛГЕБРА ВЫСКАЗЫВАНИЙ

1.1. Введение

Феномен математического доказательства. Теоремы и аксиомы. Аксиоматический метод и его развитие. Понятие исчисления. Цели формализации в математике.

Математическая логика — математическая дисциплина о законах правильного мышления. Можно выделить два первоисточника этой дисциплины. Первый — аристотелевская логика, представляющая собой науку о правильном построении суждений, о структуре суждений и о построении умозаключений, т.е. последовательности суждений, в которой одни суждения необходимо вытекают из других. Вторым первоисточником — феномен математического доказательства. Математика отличается от других естественнонаучных дисциплин тем, что все ее факты требуют доказательств в виде некоторых умозаключений. Ссылки на опыт и наблюдения в математике, как правило в расчет не берутся. Можно, конечно, не согласиться с тем, что доказательство в виде цепи умозаключений — прерогатива только математики. И можно задаваться вопросом, почему математика так устроена. Но это уже отдельные вопросы.

Математическое доказательство строится как цепь некоторых умозаключений, в которой одни суждения выводятся из других. Разумеется, в каждой такой цепи должны быть первичные суждения, обосновывать которые не требуется. В результате принцип математического доказательства привел к тому, что мы называем аксиоматическим методом. Впервые аксиоматический метод как научный принцип мы наблюдаем в „Началах“ Евклида, в которой все положения сформулированы как теоремы, доказываемые с помощью некоторого набора первичных утверждений — аксиом.

Первоначально считалось, что аксиомами могут быть такие утверждения, истинность которых очевидна. Однако уже Евклиду пришлось столкнуться с тем, что для достижения требуемого результата (обоснования всех имеющихся к тому времени в геометрии фактов) одних очевидных истин недостаточно. Споры вызвал знаменитый пятый постулат Евклида, который в современной формулировке гласит, что через точку вне прямой можно провести, и притом только одну, прямую, не пересекающую данную. Неочевидный характер этого постулата связан с непосредственным использованием понятия бесконечного. Если постулат о том, что через две точки можно провести прямую, в определенном смысле можно проверить на практике, то пятый постулат нет, так как невозможно обеспечить неограниченное продолжение прямой.

Именно исследования пятого постулата (а точнее, борьба с пятым постулатом) привели к созданию неевклидовой геометрии, с одной стороны, и к новому взгляду на понятие аксиомы, с другой. Новый взгляд на понятие аксиомы можно выразить следующим образом: очевидность аксиомы не обязательна, но важно, чтобы из набора выбранных аксиом не вытекало каких-либо противоречий. Неевклидова геометрия как раз и была создана как набор логических выводов из системы аксиом, в которых вместо пятого постулата было взято его отрицание. Пытаясь прийти к противоречию, Лобачевский старался вывести пятый постулат из других аксиом, а взамен получил развитую логически непротиворечивую теорию.

Создание неевклидовой геометрии — это первый поворотный момент в развитии аксиоматического метода (в литературе иногда именно это событие считают моментом создания аксиоматического метода). Следующий поворотный момент на рубеже 19–20 вв. вызван открытием противоречий (их называют антиномиями) в теории множеств. Опять ситуация возникла из-за произвольного использования понятия бесконечности. Интуитивно ясно, что противоречия возникают, когда о том или ином понятии судят, еще не определив его толком. Парадокс Рассела состоит в рассмотрении множества всех множеств, не принадлежащих самому себе. Но

на бытовом уровне должно быть ясно, что для того, чтобы говорить о принадлежности какого-либо объекта множеству, этот объект должен быть однозначно определен. Значит, говорить о принадлежности множества самому себе неправомерно. Но тогда что такое множество, как дать формально строгое определение этого понятия, исключающее подобные парадоксы?

Беда однако не приходит одна. Найденные парадоксы касаются не только множеств, но и некоторых определений. Парадокс Рассела можно квалифицировать как „плохое определение“, при котором объект определяется рекурсивно, через себя самого. Это говорит о том, что и приемы конструирования логических суждений, без которых математика невозможна, также должны быть подвергнуты точному математическому исследованию. Основой для такого исследования явилась символика, подобная алгебраической, в которой математические суждения и связи между ними записываются в виде математических формул. Эти формулы подчиняются определенным правилам преобразований и соединений, а логика может быть превращена в некую алгебру, подобную алгебре арифметических выражений или уравнений.

Эти соображения привели к дальнейшему уточнению понятия „аксиоматический метод“. Аксиоматический метод — это формальное описание математических теорий, при котором все теоремы теории являются логическим следствием аксиом, при этом содержательный смысл аксиом не является существенным: лишь такие следствия не были взаимоисключающими. Поскольку насчет правил логического вывода возникли разногласия, сами эти правила тоже должны быть формализованы. С введением символики в логику изложение математической теории превращается в некоторый набор исходных формул, т.е. неких буквенных конструкций, сконструированных по определенным правилам, которых можно преобразовать с помощью фиксированного набора правил преобразования. Содержательный смысл исходных формул, их преобразования и получаемых при этом новых формул игнорируется.

Подобная конструкция называется формальным исчислением. Характерные ее черты:

- фиксированный набор используемых символов, называемый *алфавитом теории*;
- определенный набор правил составления формул из алфавита (совокупность всех правильно составленных формул называется *языком теории*);
- выделенный набор правильно составленных формул, объявляемых истинными (это *система аксиом теории*);
- строго определенный набор правил преобразования формул, с помощью которых из уже имеющихся истинных формул получают новые истинные формулы — теоремы теории.

Построение исчислений не является высшей целью развития математики. На это указывает положение дел в таких классических областях математики, как дифференциальное и интегральное исчисления, геометрия. Эти разделы, несмотря на их многолетнюю историю, по-прежнему излагаются на содержательном, а не формальном, уровне. Парадоксы теории множеств — до сих пор нерешенная проблема. Однако это не мешает с успехом использовать теорию множеств в самых различных математических дисциплинах.

Дело в том, что формализация математической теории — это метод математического исследования этой теории, который позволяет провести анализ исходных положений теории, выявить скрытые допущения, используемые при построении теории и т.п. Собственно, для любого формального исчисления ставятся три вопроса: непротиворечивость, полнота и разрешимость. Под непротиворечивостью понимается, что в этой теории нет взаимно противоположных теорем A и $\neg A$. Под полнотой понимается то, что любое утверждение A , которое может быть сформулировано на языке теории может быть либо доказано, либо опровергнуто (т.е. доказано противоположное утверждение $\neg A$). Наконец, под разрешимостью понимается существование алгоритма (т.е. некоторого конечного набора процедур), позволяющего для любого утверждения теории проверить, верно оно или нет.

При содержательном анализе формальной теории приходится выходить за ее рамки. Поэтому вокруг формальной теории возникает другая теория: „учение о формальной теории“, которую называют *метатеорией*. Метатеория формирует свой язык, расширяющий язык формальной теории, который называется *метаязыком*.

Непротиворечивость конкретной теории можно установить, построив модель этой теории в рамках другой теории. В результате мы приходим к заключению: если та, другая теория непротиворечива, то и наша теория непротиворечива. В этом случае говорят об относительной непротиворечивости. Абсолютная непротиворечивость означает, что данная теория непротиворечива независимо от того, являются непротиворечивыми другие теории или нет.

В 20 в. практически все математические теории получили свои модели в рамках арифметики. Так, все числовые системы были построены на базе множества натуральных чисел. Все геометрические теории имеют естественную интерпретацию на базе множества действительных чисел. Связь алгебры и геометрии общеизвестна. Однако выяснилось, что непротиворечивость формальной арифметики нельзя доказать средствами самой арифметики и что формальная арифметика не обладает ни свойством полноты, ни свойством разрешимости. Выходит, в математике, как и в других науках абсолютной истины нет.

1.2. Алгебра логики

Высказывания и их истинностные значения. Понятие логической операции. Логические операции $\vee$, $\wedge$, $\rightarrow$, $\sim$, $\neg$. Пропозициональные формулы: пропозициональные переменные и шаг индукции ($X \vee Y$, $X \wedge Y$, $X \rightarrow Y$, $\neg X$). Истинностные функции и пропозициональные формулы.

Напомню, что под высказыванием понимается любое предложение, относительно которого можно сказать истинно оно или нет, т.е. утвердительное предложение. Строго говоря, сказанное не следует рассматривать как настоящее математическое определение — лишь как указание на те реальные объекты, которые могут служить иллюстрацией к точной математической теории.

Формирование предложений в естественном языке указывает на то, что высказывания могут объединяться с помощью связывающих союзов. С математической точки зрения эти союзы реализуют операции над высказываниями. В математической логике рассматривают только такие операции над высказываниями, для которых истинность результирующего высказывания можно определить исходя из истинности исходных независимо от смысла этих высказываний, т.е. независимо от того, что именно утверждают эти высказывания.

Вообще говоря, под операцией на множестве A понимают любое отображение $\varphi: A^n \rightarrow A$, которое любому упорядоченному набору из n элементов множества A (кортежу) ставит в соответствие элемент того же множества. Натуральный показатель n называют **арностью** этой операции. Ясно, что множество всех операций на заданном множестве бесконечно, даже если само множество конечно. Однако на практике ограничиваются операциями небольшой арности: **унарными** ($n = 1$), **бинарными** ($n = 2$), **тернарными** ($n = 3$). Кроме того, практические важные операции обладают определенными свойствами (например, свойство коммутативности для бинарных операций).

Ассоциация „операция — функция“ наталкивает на мысль о введении нульарных операций (функций без аргументов). С точки зрения математики нульарная операция — это постоянная функция или, иными словами, некоторый фиксированный элемент множества A . В качестве таких элементов выступают, например, число 0 или 1, т.е. элементы, чем-то выделяющиеся с точки зрения других операций.

Выделим пять операций над высказываниями:

- 1) дизъюнкция (соответствует союзу „или“);
- 2) конъюнкция (соответствует союзу „и“);
- 3) импликация (соответствует фразе типа „если ..., то ...“);
- 4) эквиваленция (соответствует фразе типа „... тогда и только тогда, когда ...“);
- 5) отрицание (соответствует союзу „не“).

Первые четыре из этих операций бинарные, последняя унарная. Относительно указанных операций можно сказать лишь, что они формируют новое высказывание. При этом, зная, истинны или ложны исходные высказывания, можно сказать, является ли истинным вновь

образованное высказывание. Введенные пять операций мы будем называть **логическими** или **пропозициональными**.

Для символической записи высказываний и операций над ними необходимо ввести некоторый набор символов и сформулировать правила записи с помощью этих символов. Набор символов (алфавит) в сочетании с набором правил записи представляет собой некоторый язык — язык алгебры высказываний. Вообще говоря, алфавит позволяет из заданного набора символов составлять цепочки символов (слова, фразы). Множество всех цепочек символов разделяется на две группы: правильные и неправильные. Правильные цепочки можно назвать словами, их множество и называется языком.

На практике язык можно определить как множество цепочек, удовлетворяющих некоторым требованиям, которые в конечном счете сводятся к тому, является ли данная цепочка интерпретируемой с точки зрения выполнения операций или нет. Но часто язык определяют, указывая правила, по которым из уже построенных слов можно строить новые. Набор таких правил называется **грамматикой**. Хотя любой математический язык проще любого естественного, многие закономерности у них схожи. Так слова русского языка собираются из отдельных частей с помощью некоторых правил. Описание языка с помощью грамматики в математике приводит к особому типу определения, так называемому индуктивному определению. При таком определении сначала задаются первичные, элементарные слова (это база индукции), а затем указываются правила, по которым из уже построенных слов формируются новые (шаг индукции).

Алфавит языка алгебры высказываний составляют множество **пропозициональных переменных**, множество **функциональных символов** (символов операций, или **логических связей**) $\vee$, $\wedge$, $\rightarrow$, $\sim$, $\neg$ и множество служебных символов (две круглые скобки). Формулы языка вводятся индуктивно.

База индукции: пропозициональные переменные представляют собой формулы.

Шаг индукции: если X и Y — формулы, то формулами являются $(X \vee Y)$, $(X \wedge Y)$, $(X \rightarrow Y)$, $(X \sim Y)$, $\neg X$.

Договоримся о следующих обозначениях. Будем обозначать: пропозициональные переменные — строчными латинскими буквами конца алфавита (x , y , z и т.д.); какие-либо формулы — прописными латинскими буквами конца алфавита (X , Y , Z и т.д.). Для сокращения количества скобок в формулах с целью улучшить их читаемость договоримся о дополнительных правилах. Это правило приоритета операций. Вместо, например $((X \Delta Y) \Delta Z)$, как положено по определению, будем писать $X \Delta Y \Delta Z$, имея в виду, что операции выполняются слева направо, причем сначала отрицание, затем дизъюнкция и конъюнкция, а потом импликация и эквиваленция. Соглашение не относится к самому языку и служит лишь для удобства: в любой момент сокращенную запись формулы однозначным образом можно преобразовать в полную запись со всеми нужными скобками. В математический язык эти правила вводить нет смысла, поскольку они ничего не добавляют к математической сути вопроса.

В наших рассуждениях будут встречаться формулы, которые относятся к введенному языку, но, кроме того, придется использовать и дополнительные обозначения и символику, чтобы рассуждать не в рамках языка, а о самом языке и его формулах. Так, обозначения переменных — это элемент языка алгебры высказываний, а обозначения формул или соглашение о приоритете уже выходят за рамки языка. В этом случае говорят о расширении рассматриваемого языка или о **метаязыке**. На практике язык и метаязык тесно переплетаются и трудно делимы.

Рассмотрим какую-либо формулу, например $(x \rightarrow y) \rightarrow z$. Об истинности этой формулы можно судить, если известно, истинны ли элементарные высказывания x , y , z . Например, если x и z ложны, а y истинна, то $x \rightarrow y$ является истинной, а $(x \rightarrow y) \rightarrow z$ ложной. Приписав истинной формуле значение 1, а ложной — 0, мы получаем функцию, которая по значениям истинности пропозициональных переменных (элементарных высказываний) определяет значение истинности всей формулы. Эта функция есть отображение вида $h: \{0, 1\}^n \rightarrow \{0, 1\}$ (и аргументы, и функция принимают значения 0 и 1). Она называется **истинностной функцией** данной

формулы. Позже мы увидим, что любая двузначная (булева) функция от n аргументов есть истинностная функция некоторой пропозициональной формулы с n переменными.

Замечание. Отметим различия понятий „формула“ и „функция“. Первое понятие связано с языком, на котором описываются свойства математических объектов. Формула имеет некоторый набор переменных, если заданы значения этих переменных, то формула также имеет некоторое значение. В этом смысле формулу можно рассматривать как запись некоего правила, которое заданным значениям переменных ставит в соответствие новое значение. Это похоже на понятие функции, но функция (отображение) есть реальный математический объект, а не запись о нем в некотором языке. Кроме того, исходные значения, по которым отображение формирует значение, должны быть упорядочены. Одна и та же формула задает разные функции. Так, формула $x - t$ определяет и функцию $f(x, t)$, и функцию $f(t, x)$, а также, например, функцию $f(x, y, t)$. Чтобы с формулой связать некоторую функцию n аргументов, необходимо установить связь между аргументами функции и переменными формулы. Это в языках программирования реализуется формальными переменными: $f(x, t) = x - t$.

Понятие истинностной функции позволяет и введенные логические операции рассматривать совершенно формально — как формульную запись некоторых истинностных функций (табл. 1.1). В дальнейшем через $|X|$ мы будем обозначать истинностную функцию формулы X .

Таблица 1.1

x	y	$\neg x$	$x \vee y$	$x \wedge y$	$x \rightarrow y$	$x \sim y$
0	0	1	0	0	1	1
0	1		1	0	1	0
1	0	0	1	0	0	0
1	1		1	1	1	1

1.3. Тавтологии и эквивалентность формул

Тавтологии. Формулы выполнимые и опровержимые. Теорема о правиле *modus ponens*: если X и $X \rightarrow Y$ — тавтологии, то и Y — тавтология. Подстановка. Эквивалентность формул алгебры высказываний. Теорема о заменах. Следствие 1: если X — тавтология, то и $S(z_1, z_2, \dots, z_n | Y_1, Y_2, \dots, Y_n | X)$ — тавтология. Следствие 2: инвариантность эквивалентности относительно логических операций. Способы получения эквивалентных формул: на основе свойств логических операций; на основе взаимосвязей операций; на основе двойственности.

Среди формул алгебры высказываний выделяют:

- **тождественно истинные**, или **тавтологии**, истинные при любой истинности переменных;
- **выполнимые**, имеющие значение 1 хотя бы для одного набора значений пропозициональных переменных;
- **опровержимые**, имеющие значение 0 хотя бы для одного набора значений пропозициональных переменных.
- **тождественно ложные**, или **противоречия**, ложные при любой истинности переменных.

Эти четыре понятия связаны между собой. Формула, не являющаяся опровержимой, есть тавтология. Такие формулы описывают универсальные логические законы. Именно с использованием тавтологий проводится любое математическое доказательство. Формула, не являющаяся выполнимой, тождественно ложна, т.е. представляет собой противоречие.

Для тавтологий (противоречий) истинностная функция есть константа 1 (0). Для выполнимых формул истинностная функция не равна постоянной 0, а для опровержимых — постоянной 0.

Пример 1.1. Формула $(x \vee (\neg y)) \rightarrow z$ является одновременно выполнимой и опровержимой: она истинна, если переменная z обозначает истинное высказывание, и ложна, если, например, переменные y и z обозначают ложные высказывания. Это можно увидеть, составив истинностную функцию, которая в данном случае описывается вектором 01110101. Формула $(x \vee (\neg x))$ является тавтологией, а формула $(x \wedge (\neg x))$ — противоречием. #

Следующее утверждение отражает часто используемое на практике умозаключение, называемое *modus ponens* (модус поненс).

Теорема 1.1. Если формулы X и $X \rightarrow Y$ являются тавтологиями, то и формула Y есть тавтология.

◀ Пусть формулы X и Y построены из переменных $z_1, \dots, z_n$. Выберем для этих переменных какие-либо значения. Тогда об истинности формулы $X \rightarrow Y$ можно судить на основании истинности формул X и Y . Анализируя истинностную функцию для импликации, видим, что при истинности X и ложности Y формула $X \rightarrow Y$ является ложной. Но по условию теоремы эта формула тождественно истинная, как и формула X . Следовательно, формула Y не может быть ложной при выбранных значениях переменных. Поскольку значения переменных выбирались произвольно, заключаем, что формула Y тождественно истинна, т.е. тавтология. ▶

Как и в булевой алгебре, введем понятие *эквивалентных формул* алгебры высказываний — формул, имеющих равные истинностные значения при любых значениях входящих в формулы переменных. Альтернативное определение: формулы X и Y называются эквивалентными, если формула $X \sim Y$ является тавтологией. Нетрудно показать, рассуждая как в последней теореме, что формула $X \sim Y$ является тавтологией тогда и только тогда, когда при любых значениях переменных формулы X и Y одновременно или истинны, или ложны, т.е. истинностные функции этих формул совпадают. Для эквивалентных формул введем обозначение $X \equiv Y$. Итак, $X \equiv Y \Leftrightarrow X \sim Y$ — тавтология. Обратите внимание на три символа эквивалентности в последней фразе. Первый обозначает отношение эквивалентности формул, введенное на множестве формул алгебры высказываний, третий — операцию эквиваленции, а второй — по сути та же эквиваленция, но в утверждении, в котором формулируется свойство самой алгебры высказываний, и ее следует отнести к сфере метаязыка.

Имеются некоторые стандартные приемы, приводящие к эквивалентным формулам. Один из них — подстановка. Если мы в формуле заменим одну из подформул другой, то получим новую цепочку символов. Нетрудно доказать индукцией по построению, что это цепочка будет формулой. Заменяемая подформула может встречаться несколько раз. В этом случае говорят о *вхождении подформулы*. Замена может выполняться для одного какого-либо вхождения данной подформулы или для всех.

Под подстановкой будем понимать замену всех вхождений в формулу одной или нескольких переменных некоторыми формулами. Результат подстановки в формулу X вместо переменных $z_1, \dots, z_n$ формул $Y_1, \dots, Y_n$ обозначают примерно так: $S(z_1, \dots, z_n | Y_1, \dots, Y_n | X)$. Мы также будем использовать обозначение $X_{Y_1, \dots, Y_n}^{z_1, \dots, z_n}$.

Отметим, что замена в формуле X одного или нескольких вхождений подформулы Y формулой Z можно рассматривать как получение самой формулы X и результата замены $\hat{X}$ подстановкой в третью формулу $\hat{X}$ вместо некоторой переменной u формул Y (для получения X) и Z (для получения $\hat{X}$). Какие именно вхождения Y меняются, определяется конструкцией формулы $\hat{X}$. Например, в формуле $X = (x \rightarrow y) \vee (x \wedge (x \vee y))$ два вхождения формулы $Y = x \rightarrow y$. Взяв $\hat{Z} = u \vee (x \wedge (x \vee y))$, в результате подстановки $\hat{Z}_Y^u$ получим X , а в результате подстановки $\hat{Z}_{x \sim y}^u$ получим формулу $\hat{X} = (x \sim y) \vee (x \wedge (x \vee y))$ — результат замены в X первого вхождения Y на формулу $Z = x \sim y$.

Введем также обозначение $X[x_1, x_2, \dots, x_n]$, имея в виду, что список $x_1, x_2, \dots, x_n$ содержит все переменные, входящие в формулу X .

Теорема 1.2. Если $X \equiv Y$, то при замене всех вхождений какой-либо переменной u и в формуле X , и в формуле Y какой-либо формулой Z получим эквивалентные формулы, т.е.

$$X \equiv Y \Rightarrow X_Z^u \equiv Y_Z^u.$$

Если в формуле X заменить одно из вхождений подформулы Y эквивалентной формулой Z , то получим формулу, эквивалентную X , т.е.

$$Y \equiv Z \Rightarrow X \equiv X_Z^Y.$$

◀ Объединим списки переменных у формул X, Y, Z в общий упорядоченный список $z_1, z_2, \dots, z_k, u$. Тогда условие эквивалентности $X \equiv Y$ можно записать как равенство истинностных функций:

$$f_X(z_1, \dots, z_k, u) = f_Y(z_1, \dots, z_k, u). \quad (1.1)$$

Замена всех вхождений переменной u формулой Z приводит к композиции истинностных функций: если $\tilde{X} = X_Z^u, \tilde{Y} = Y_Z^u$, то

$$f_{\tilde{X}}(z_1, \dots, z_k, u) = f_X(z_1, \dots, z_k, f_Z(z_1, \dots, z_k, u)) \quad (1.2)$$

и

$$f_{\tilde{Y}}(z_1, \dots, z_k, u) = f_Y(z_1, \dots, z_k, f_Z(z_1, \dots, z_k, u)) \quad (1.3)$$

Из равенств (1.1)–(1.3) вытекает, что

$$f_{\tilde{X}}(z_1, \dots, z_k, u) = f_{\tilde{Y}}(z_1, \dots, z_k, u),$$

а это равносильно эквивалентности формул $\tilde{X}$ и $\tilde{Y}$.

Пусть дана формула $X[x_1, \dots, x_n]$, в которую входит подформула $Y[x_1, \dots, x_n]$ (мы можем считать, что подформула включает все переменные исходной формулы, рассматривая недостающие как фиктивные). Заменяем подформулу Y новой переменной z , которая не входит в список $x_1, \dots, x_n$. Получим новую формулу $\Gamma[x_1, \dots, x_n, z]$, связь которой с исходной формулой можно записать в виде $X = \Gamma|_Y^z$. Замена подформулы $Y[x_1, \dots, x_n]$ эквивалентной формулой $Z[x_1, \dots, x_n]$ приведет к новой формуле $\tilde{X} = \Gamma|_Z^z$.

Задав упорядоченный список переменных $x_1, x_2, \dots, x_n, z$, можем для формул рассмотреть их истинностные функции. По условию $f_Y(x_1, x_2, \dots, x_n) = f_Z(x_1, x_2, \dots, x_n)$ (так как $Y \equiv Z$). Подстановки вместо z формул Y и Z можно записать как композицию функций:

$$\begin{aligned} f_X(x_1, x_2, \dots, x_n) &= f_\Gamma(x_1, x_2, \dots, x_n, f_Y(x_1, x_2, \dots, x_n)), \\ f_{\tilde{X}}(x_1, x_2, \dots, x_n) &= f_\Gamma(x_1, x_2, \dots, x_n, f_Z(x_1, x_2, \dots, x_n)). \end{aligned}$$

Из равенства $f_Y(x_1, x_2, \dots, x_n) = f_Z(x_1, x_2, \dots, x_n)$ вытекает равенство $f_X(x_1, x_2, \dots, x_n) = f_{\tilde{X}}(x_1, x_2, \dots, x_n)$, что равносильно эквивалентности $X \equiv \tilde{X}$. ▶

Следствие 1.1. Если X — тавтология, то и $\mathbf{S}(z_1, \dots, z_n | Y_1, \dots, Y_n | X)$ — тавтология.

◀ Можно рассуждать так. Тавтологии — это формулы, эквивалентные, например, формуле $W = x \vee \neg x$. В качестве переменной x можно выбрать ту, которая не входит в формулу X . В силу теоремы, заменив в формулах X и W все вхождения переменных $z_1, \dots, z_n$ формулами $Y_1, \dots, Y_n$, мы получим эквивалентные формулы. Но формула W при этом не изменится. Поэтому вновь построенная формула $\mathbf{S}(z_1, \dots, z_n | Y_1, \dots, Y_n | X)$ будет эквивалентна формуле W , т.е. будет являться тавтологией. ▶

Следствие 1.2. Пусть $X \equiv Z$ и $Y \equiv W$. Тогда $(X \vee Y) \equiv (Z \vee W)$, $(X \wedge Y) \equiv (Z \wedge W)$, $(X \rightarrow Y) \equiv (Z \rightarrow W)$, $(X \sim Y) \equiv (Z \sim W)$, $(\neg X) \equiv (\neg Z)$.

◀ Формулу $(Z \circ W)$, где $\circ$ — одна из логических связок, можно рассматривать как результат замены в формуле $(X \circ Y)$ сперва подформулы X эквивалентной формулой Z , а затем подформулы Y эквивалентной формулой W . Согласно доказанной теореме такая замена приводит к эквивалентной формуле. Аналогичны рассуждения и для отрицания. ▶

С помощью подстановки можно получать эквивалентные формулы, отталкиваясь от известных свойств логических операций.

Теорема 1.3. Для любых пропозициональных формул X , Y и Z верны следующие эквивалентности: 1) $X \wedge X \equiv X$; 2) $X \wedge Y \equiv Y \wedge X$; 3) $(X \wedge Y) \wedge Z \equiv (X \wedge (Y \wedge Z))$; 4) $X \vee X \equiv X$; 5) $X \vee Y \equiv Y \vee X$; 6) $(X \vee Y) \vee Z \equiv (X \vee (Y \vee Z))$; 7) $X \wedge (Y \vee Z) \equiv (X \wedge Y) \vee (X \wedge Z)$; 8) $X \vee (Y \wedge Z) \equiv (X \vee Y) \wedge (X \vee Z)$; 9) $X \wedge (Y \vee X) \equiv X$; 10) $X \vee (Y \wedge X) \equiv X$.

◀ Непосредственно из таблицы для истинностной функции вытекает, что $x \wedge x \equiv x$. Подставив вместо всех вхождений переменной x формулу X , получим эквивалентность $X \wedge X \equiv X$. Остальные эквивалентности доказываются аналогично. ▶

Еще один способ получения эквивалентностей — замена одних операций другими по соответствующим формулам. Из теории булевых функций вытекает, что верны следующие эквивалентности:

$$(\neg(\neg x)) \equiv x, \quad (\neg(x \vee y)) \equiv (\neg x) \wedge (\neg y), \quad (x \rightarrow y) \equiv ((\neg x) \vee y).$$

Отталкиваясь от этих эквивалентностей можно доказать следующее.

Теорема 1.4. Для любых пропозициональных формул X , Y и Z верны следующие эквивалентности:

- 1) $(\neg(\neg X)) \equiv X$ (закон двойного отрицания);
- 2) $(\neg(X \vee Y)) \equiv (\neg X) \wedge (\neg Y)$ (перенос отрицания через конъюнкцию);
- 3) $(\neg(X \wedge Y)) \equiv (\neg X) \vee (\neg Y)$ (перенос отрицания через дизъюнкцию);
- 4) $(\neg(X \rightarrow Y)) \equiv (X \wedge (\neg Y))$ (перенос отрицания через импликацию);
- 5) $(X \rightarrow Y) \equiv ((\neg X) \vee Y)$ (представление импликации через дизъюнкцию);
- 6) $(X \rightarrow (\neg X)) \equiv (\neg X)$ (закон упрощения);
- 7) $(X \rightarrow Y) \equiv ((\neg Y) \rightarrow (\neg X))$ (закон контрапозиции).

◀ Доказывается теорема так же, как и предыдущая. Например, на основании простой эквивалентности $(\neg(\neg x)) \equiv x$, устанавливаемой непосредственно, путем подстановки вместо переменной x формулы X получаем эквивалентность $(\neg(\neg X)) \equiv X$. ▶

Для формул, содержащих только три операции $\neg$, $\vee$, $\wedge$, имеет место принцип двойственности. Для каждой такой формулы X в результате взаимной замены операций $\vee$ и $\wedge$ получим новую формулу X^* , которую назовем двойственной для X . Отметим, что если X^* двойственна X , то X двойственна X^* , так что отношение двойственности симметрично. Это можно выразить формулой $X^{**} = X$ (знак равенства отражает совпадение формул, а не их эквивалентность). Учитывая эквивалентности

$$\neg(x \vee y) \equiv \neg x \wedge \neg y, \quad \neg(x \wedge y) \equiv \neg x \vee \neg y, \quad (1.4)$$

Приходим к эквивалентности

$$X^* \equiv \neg X_{\neg t_1, \dots, \neg t_n}^{t_1, \dots, t_n}, \quad (1.5)$$

где $t_1, t_2, \dots, t_n$ — полный список переменных, входящих в X . Доказательство проводится индукцией по построению формулы. Действительно, для переменных утверждение очевидно. Пусть $X = Y \vee Z$. Тогда, согласно первой эквивалентности (1.4) $\neg X = \neg(Y \vee Z) \equiv \neg Y \wedge \neg Z$. Предполагая в соответствии с индуктивным предположением, что

$$\neg Y_{\neg t_1, \dots, \neg t_n}^{t_1, \dots, t_n} \equiv Y^*, \quad \neg Z_{\neg t_1, \dots, \neg t_n}^{t_1, \dots, t_n} \equiv Z^*,$$

закключаем, что

$$X^* = Y^* \wedge Z^* \equiv \neg Y_{\neg t_1, \dots, \neg t_n}^{t_1, \dots, t_n} \wedge \neg Z_{\neg t_1, \dots, \neg t_n}^{t_1, \dots, t_n} = (\neg Y \wedge \neg Z) \Big|_{\neg t_1, \dots, \neg t_n}^{t_1, \dots, t_n} \equiv \neg X_{\neg t_1, \dots, \neg t_n}^{t_1, \dots, t_n}.$$

Аналогично доказательство в случае второй операции.

Теорема 1.5. Если формулы X и Y эквивалентны, то и формулы X^* , Y^* эквивалентны.

◀ Действительно, из эквивалентности $X \equiv Y$ получаем $\neg X \equiv \neg Y$ и $\neg X_{\neg t_1, \dots, \neg t_n}^{t_1, \dots, t_n} \equiv \neg Y_{\neg t_1, \dots, \neg t_n}^{t_1, \dots, t_n}$. Согласно (1.5) делаем вывод $X^* \equiv Y^*$. ▶

Принцип двойственности приводит к еще одному способу получения эквивалентных формул.

1.4. Функции алгебры логики

Понятие булевой функции. Множества $\mathcal{P}_{2,n}$ и $\mathcal{P}_2$. Композиция функций. Множество функций и его замыкание. Замкнутые и полные множества функций. Теорема: если F полно и все функции в F выражаются через функции множества G , то G полно. Понятие базиса. Стандартный базис. Базис Жегалкина. Понятие ДНФ и КНФ. Примеры построения ДНФ и КНФ. Совершенные ДНФ и КНФ. Теорема о существовании СДНФ и СКНФ. Утверждение: каждая истинностная функция соответствует некоторой пропозициональной формуле. Штрих Шеффера и стрелка Пирса.

Под **функцией алгебры логики**, или **булевой функцией** понимают любое отображение $f: \{0, 1\}^n \rightarrow \{0, 1\}$. Это значит, что каждый аргумент булевой функции, как и сама функция, принимает два значения 0 и 1. Частными случаями булевых функций являются логические операции, которые формально оперируют высказываниями, но по сути своей есть функции, в которых и аргументы, и значение могут принимать лишь два значения: ИСТИНА и ЛОЖЬ. Так, отрицание есть булева функция одного переменного, а дизъюнкция, конъюнкция, импликация, эквиваленция — функции двух переменных.

Булеву функцию можно рассматривать как некое логическое условие, которые по входам — значениям аргументов вырабатывает логическое значение 0 (ложь) или 1 (истина).

Для булевых функций можно ввести операцию **суперпозиции**. Это вариант обычной композиции отображений, использующий понятие формулы. Пусть заданы функции $f(x_1, \dots, x_n)$, $g_1(u_{11}, \dots, u_{1,m_1}), \dots, g_n(u_{n1}, \dots, u_{n,m_n})$. Тогда можно образовать функцию

$$F(u_{11}, \dots, u_{1,m_1}, \dots, u_{n1}, \dots, u_{n,m_n}) = f(g_1(u_{11}, \dots, u_{1,m_1}), \dots, g_n(u_{n1}, \dots, u_{n,m_n})),$$

которую и назовем суперпозицией функций $f, g_1, \dots, g_n$. В действительности при суперпозиции некоторые из переменных u_{ij} могут совпадать. В частном случае все функции g_i могут иметь один и тот же набор переменных, и тогда суперпозиция — это обычная композиция отображений. Здесь нетрудно увидеть, что суперпозиция — это построение некоторой формулы из исходных функций и выбор функции, определяемой этой формулой. Порядок переменных определяется порядком функций и порядком их аргументов.

Мы не будем здесь проводить строгие построения, но поставим следующий вопрос: каково множество булевых функций, которое может быть получено из данного множества функций F с использованием суперпозиции? Ясно, что ответ зависит от множества F . В первую очередь нас будут интересовать условия на множество F , при выполнении которых можно утверждать, что каждая булева функция может быть построена таким способом.

Множество всех булевых функций, которые могут быть получены из данного множества X функций с использованием суперпозиции, назовем **замыканием** X и обозначим $[X]$. Множество X булевых функций назовем **полным**, если его замыкание совпадает с множеством $\mathcal{P}_2$ всех булевых функций. Конечное полное множество называют **базисом** в множестве булевых функций.

Операция замыкания сродни, например, замыканию множества элементов группы по операции группы или замыканию множества точек на плоскости, состоящему в присоединении к множеству всех его предельных точек. Замыкание можно рассматривать как унарную операцию на подмножествах множества $\mathcal{P}_2$. Свойства операции замыкания:

- 1) $[\emptyset] = \emptyset$;
- 2) $[[X]] = [X]$;
- 3) $F \subset [X]$;
- 4) $[X] \cup [Y] \subset [X \cup Y]$.

Первое свойство носит формальный характер. Второе вытекает из конечности процедуры построения любой формулы: достаточно, следуя по дереву синтаксического анализа, последовательно заменять функции из $[X]$ их формулами над X . Третье и четвертое свойства очевидны.

Из четвертого свойства вытекает, что если $X \subset Y$, то $[X] \subset [Y]$. Действительно, включение $X \subset Y$ равносильно равенству $X \cup Y = Y$. Если $X \subset Y$, то в силу свойства 4 заключаем, что $[X] \cup [Y] \subset [X \cup Y] = [Y]$. Следовательно, $[X] \subset [Y]$.

Из указанных свойств замыкания вытекает следующее утверждение.

Теорема 1.6. Если F — полное множество булевых функций, каждая из которых представлена формулой над множеством G , то и G — полное множество.

◀ Так как каждая функция из F есть формула над G , то $F \subset [G]$. Из свойств замыкания вытекает, что

$$[F] \subset [[G]] = [G].$$

Но поскольку $[F]$ совпадает с множеством всех булевых функций, то и $[G]$ совпадает с множеством всех булевых функций, т.е. G — полный базис. ►

Доказанная теорема позволяет строить базисы исходя из уже известных базисов. Один из таких базисов (это станет ясно из дальнейшего) составляют дизъюнкция, конъюнкция и отрицание. Этот базис назовем **стандартным**. Через эти операции можно выразить другие логические операции:

$$X \rightarrow Y \equiv \neg X \vee Y, \quad X \sim Y \equiv (X \wedge Y) \vee (\neg X \wedge \neg Y).$$

Имея в виду эти формулы можно было бы ограничиться только тремя операциями $\neg$, $\vee$, $\wedge$. Более того, можно ограничиться двумя операциями, заменив $\vee$ или $\wedge$.

Среди формул, содержащих дизъюнкцию, конъюнкцию и отрицание можно выделить в некотором роде канонические формулы.

Назовем элементарной конъюнкцией формулу $X_1 \wedge X_2 \wedge \dots \wedge X_n$, в которой каждая подформула X_i либо элементарная, либо отрицание элементарной. Удобно ввести обозначение $x_i^{\sigma_i}$ с $\sigma_i \in \{0, 1\}$, считая, что $x_i^1 = x_i$ и $x_i^0 = \neg x_i$. Тогда элементарную конъюнкцию можно записать в виде $x_1^{\sigma_1} \wedge x_2^{\sigma_2} \wedge \dots \wedge x_n^{\sigma_n}$.

Элементарная конъюнкция или дизъюнкция нескольких элементарных конъюнкций называется **дизъюнктивной нормальной формой**, или **ДНФ**. Пример: $(x_1 \wedge x_2) \vee (\neg x_1 \wedge x_3)$.

Двойственным к ДНФ понятием является **конъюнктивная нормальная форма**, или **КНФ**. Это элементарная дизъюнкция или конъюнкция нескольких элементарных дизъюнкций.

Количество переменных в элементарной конъюнкции называется ее длиной. Если в ДНФ все элементарные конъюнкции имеют одинаковый состав переменных и отличаются только распределением между переменными знаков отрицания, то ДНФ называется **совершенной** (сокращенно **СДНФ**). Аналогично вводится понятие **совершенной КНФ** (СКНФ).

Теорема 1.7. Каждая формула алгебры высказываний, не являющаяся противоречием, имеет эквивалентную ей совершенную ДНФ. Каждая формула алгебры высказываний, не являющаяся тавтологией, имеет эквивалентную ей совершенную КНФ. #

◀ Структура самой формулы не имеет значения. Пусть $x_1, x_2, \dots, x_n$ — список всех переменных, входящих в формулу, и $f(\xi_1, \xi_2, \dots, \xi_n)$ истинностная функция этой формулы (ξ_i — истинностное значение переменной x_i).

Отметим, что элементарная конъюнкция $x_1^{\sigma_1} \wedge x_2^{\sigma_2} \wedge \dots \wedge x_n^{\sigma_n}$ истинна при $\xi_1 = \sigma_1, x_2 = \sigma_2, \dots, \xi_n = \sigma_n$ и ложна при любом другом варианте истинностных значений переменных. Поэтому в СДНФ при заданном наборе истинностных значений переменных максимум одна элементарная конъюнкция имеет истинностное значение 1.

Для каждого набора $\sigma_1, \sigma_2, \dots, \sigma_n$, для которого $f(\sigma_1, \sigma_2, \dots, \sigma_n) = 1$ составляем элементарную конъюнкцию $x_1^{\sigma_1} \wedge x_2^{\sigma_2} \wedge \dots \wedge x_n^{\sigma_n}$, а затем из них составляем СДНФ. Получим формулу, для которой $f(\xi_1, \xi_2, \dots, \xi_n)$ является истинностной функцией. Значит, эта СДНФ эквивалентна исходной формуле. Для построения СДНФ требуется лишь, чтобы истинностная функция хотя бы при одном наборе истинностных значений переменных принимала значение 1, т.е. исходная формула не должна быть противоречием.

Утверждение о КНФ является двойственным утверждением о ДНФ и может быть получено взаимной заменой в рассуждениях дизъюнкции и конъюнкции. ▶

Следствие 1.3. Каждая булева функция является истинностной функцией какой-либо позициональной формулы.

◀ Действительно, доказательство теоремы построено так, что характер формулы не является существенным. Если $f(\xi_1, \xi_2, \dots, \xi_n)$ не равна тождественно 0, мы можем для нее построить СДНФ. Если $f(\xi_1, \xi_2, \dots, \xi_n)$ не равна тождественно 1, мы можем построить СКНФ. Таким образом, любая функция имеет либо СДНФ, либо СКНФ, либо и то, и другое. ▶

Исходя из стандартного базиса можно строить и другие базисы. Один из них — **базис Жегалкина**, состоящий из сложения по модулю 2 „ $\oplus$ “, умножения (она же конъюнкция) „ $\cdot$ “, и нулевой операции (постоянной функции) 1. Отметим, что алгебраическая система $(\{0, 1\}, \{\oplus, \cdot\})$ есть поле $\mathbb{Z}_2$ вычетов по модулю 2, а формулы, построенные на операциях „ $\oplus$ “ и „ $\cdot$ “ представляют собой многочлены в $\mathbb{Z}_2$ (их называют **многочленами Жегалкина**).

Нетрудно прямой проверкой убедиться в том, что

$$x \oplus y \equiv \bar{x}y + x\bar{y} \equiv (\neg x \wedge y) \vee (x \wedge \neg y), \quad 1 \equiv x + \bar{x} \equiv x \vee \neg x,$$

где первое представление дано в альтернативной символике операций: дизъюнкция как сложение $x + y$, конъюнкция как умножение xy , отрицание как **дополнение** $\bar{x}$. Согласно теореме 1.6, базис Жегалкина — полное множество.

Представление булевой функции через базис Жегалкина — это представление ее в виде многочлена в поле $\mathbb{Z}_2$, при этом все переменные в многочлене имеют степень 1, поскольку в $\mathbb{Z}_2$ имеем $x^k = x$ для любого элемента x . Учитывая это, заключаем, что для функции $f(x_1, \dots, x_n)$ от n аргументов соответствующий многочлен имеет не более 2^n слагаемых (одно слагаемое нулевой степени, n слагаемых 1-й степени, C_n^2 слагаемых 2-й степени и т.д.). Например, для функции трех переменных многочлен Жегалкина имеет вид:

$$f(x_1, x_2, x_3) = a_0 \oplus a_{11}x_1 \oplus a_{12}x_2 \oplus a_{13}x_3 \oplus a_{21}x_1x_2 \oplus a_{22}x_1x_3 \oplus a_{23}x_2x_3 \oplus a_3x_1x_2x_3.$$

Итак, в многочлене Жегалкина 2^n слагаемых и, значит, 2^n коэффициентов. Записывая 2^n значений функции, мы получим систему уравнений, из которой можем найти все коэффициенты многочлена. Этот подход носит название **метода неопределенных коэффициентов**. В принципе можно показать, что такая система имеет и притом единственное решение (это следует из того, что любая булева функция представима многочленом Жегалкина, причем такой многочлен единственный).

Кроме базиса Жегалкина существуют и другие базисы. Основным способом проверки множества функций на полноту является сведение к стандартному базису. Оказывается, такую проверку можно свести к простой проверке некоторых свойств функций заданного множества.

Введем пять так называемых **классов Поста**. Класс T_0 содержит все функции, удовлетворяющие условию $f(0, 0, \dots, 0) = 0$, т.е. функции, принимающие нулевое значение при нулевых значениях всех аргументов. Аналогично T_1 — это класс функций, удовлетворяющих условию $f(1, 1, \dots, 1) = 1$. Класс S — это класс **самодвойственных функций**, т.е. функций, удовлетворяющих условию $f(x_1, \dots, x_n) = f(\bar{x}_1, \dots, \bar{x}_n)$, где $\bar{x} = 1 - x$ — отрицание. Вектор значений самодвойственной функции удовлетворяет условию $b_1 b_2 \dots b_n = b_n b_{n-1} \dots b_1$.

Для двух булевых векторов $a = a_1 a_2 \dots a_n$ и $b = b_1 b_2 \dots b_n$ полагаем $a \leq b$, если $a_i \leq b_i$, $i = \overline{1, n}$. Булеву функцию $f(x) = f(x_1, x_2, \dots, x_n)$ назовем **монотонной**, если $f(x) \leq f(y)$ при $x \leq y$. Множество всех монотонных функций составляют класс M .

Наконец, класс L **линейных функций** составляют функции, у которых полином Жегалки-на имеет степень не выше первой.

Каждый из классов Поста является замкнутым множеством. Доказательство можно провести методом индукции по построению формулы. При этом ни один из классов не совпадает с множеством $\mathcal{P}_2$ всех булевых функций. Отсюда вытекает, что если заданное множество F булевых функций включено в один из классов Поста, то оно не является полным, поскольку его замыкание также будет включено в этот класс Поста. Мы получили необходимое условие полноты множества булевых функций. Оказывается, что это условие является и достаточным.

Теорема 1.8 (критерий Поста). Множество F булевых функций полно тогда и только тогда, когда оно не является подмножеством ни одного из классов Поста.

◀ Необходимость сформулированного критерия установлена выше. Поэтому сосредоточим внимание на доказательстве достаточности критерия. Это доказательство сводится к построению на основе множества F функций стандартного базиса, причем можно ограничиться только отрицанием и умножением, поскольку сложение (дизъюнкция) выражается через отрицание и умножение:

$$x + y = \overline{\bar{x} \bar{y}}.$$

Пусть F не является подмножеством ни одного из классов Поста. Для каждой функции $f \in F$ рассмотрим формулу $g(x) = f(x, x, \dots, x)$. Поскольку F не содержится в T_0 и в T_1 , в F , во-первых, есть непостоянные функции, а во-вторых есть хотя бы одна функция f_1 , для которой $g_1(0) = 1$, и есть хотя бы одна функция f_2 , для которой $g_2(1) = 0$. Это возможно, если одна из функций $g_1(x)$ и $g_2(x)$ есть отрицание, либо обе функции постоянны и представляют константы 0 и 1. Рассмотрим оба случая.

Пусть функции $g_1(x)$ и $g_2(x)$ являются константы 0 и 1. Тогда для любой функции $f \in F$ формула $f(\alpha_1, \alpha_2, \dots, \alpha_{i-1}, x, \alpha_{i+1}, \dots, \alpha_n)$, в которой α_j — константы, есть формула над F . Выберем функцию f , не являющуюся монотонной. Тогда существуют два булевых вектора p и q , удовлетворяющие условиям $p < q$ и $f(p) = 1$, $f(q) = 0$. Векторы p и q можно соединить цепочкой $p = p_0, p_1, \dots, p_k = q$ непосредственно предшествующих друг другу векторов (соседних). В этой цепочке найдется два соседних вектора p_{j-1} и p_j , которые отличаются только одной компонентой с некоторым номером i и на которых $f(p_{j-1}) = 1$, $f(p_j) = 0$. Пусть α_j , $j \neq i$, одинаковые компоненты этих векторов. Тогда формула $f(\alpha_1, \alpha_2, \dots, \alpha_{i-1}, x, \alpha_{i+1}, \dots, \alpha_n)$ представляет собой операцию отрицания.

Предположим, например, что функция $g_1(x)$ является отрицанием. Тогда мы можем составлять формулы вида $f(x \oplus \sigma^1, \dots, x \oplus \sigma_n)$, где $x \oplus \sigma$ есть переменная x при $\sigma = 0$ и ее отрицание при $\sigma = 1$. Выберем функцию $f \in F$, не являющуюся самодвойственной. Тогда можно указать такой булев вектор $p \in \mathbb{B}^n$, что $f(\bar{p}) \neq f(p)$, откуда $f(\bar{p}) = f(p)$. Пусть $\sigma_1, \dots, \sigma_n$ — компоненты вектора p . Рассмотрим функцию $g(x) = f(x \oplus \sigma^1, \dots, x \oplus \sigma_n)$, определяемую выбранной несамодвойственной функцией f и вектором p . Так как $0 \oplus \sigma_i = \sigma_i$, $1 \oplus \sigma_i = \bar{\sigma}_i$, то $g(0) = f(p) = f(\bar{p}) = f(\sigma_1 \oplus 1, \dots, \sigma_n \oplus 1) = g(1)$. Следовательно, функция $g(x)$ является константой. Пусть, например, $g(x) = 1$. Тогда $\bar{g}(x) = 0$ — другая константа.

Итак, мы показали, что множество F , не являющееся подмножеством классов T_0 , T_1 , S , M , позволяет получить в виде формул отрицание и обе константы. Для построения формулы для

произведения выберем функцию $f \in F$, не являющуюся линейной. Составляя формулы вида $f(X_1, X_2, \dots, X_n)$, где X_i — это либо переменная x , либо переменная y , мы получим функции двух аргументов. Покажем, что среди таких функций есть нелинейные. В полиноме Жегалкина, представляющем функцию f , выберем нелинейное (степени два или выше) слагаемое наименьшей степени. Пусть это слагаемое имеет вид $x_{i_1}x_{i_2} \dots x_{i_k}$. В формуле $f(X_1, X_2, \dots, X_n)$ положим $X_{i_1} = x$, $X_{i_j} = y$, $j = 2, \dots, k$, а для остальных переменных, не вошедших в выбранное слагаемое выберем значение 0. Тогда выбранное слагаемое преобразуется в xy , остальные нелинейные слагаемые обнулятся, и мы получим функцию вида $g(x, y) = xy \oplus \alpha x \oplus \beta y \oplus \gamma$.

Так как

$$g(x, y) = xy \oplus \alpha x \oplus \beta y \oplus \gamma = (x \oplus \beta)(y \oplus \alpha) \oplus \alpha\beta \oplus \gamma = (x \oplus \beta)(y \oplus \alpha) \oplus \gamma',$$

закключаем, что $g(x \oplus \beta, y \oplus \alpha) \oplus \gamma' = xy$. Но $x \oplus \sigma$ — это переменная x при $\sigma = 0$ и ее отрицание $\bar{x}$ при $\sigma = 1$. Поэтому, если $g(x, y)$ принадлежит замыканию F , то и функция $g(x \oplus \beta, y \oplus \alpha) \oplus \gamma' = xy$, т.е. конъюнкция, принадлежит замыканию F .

Итак, мы показали, что если множество F не является подмножеством никакого класса Поста, то формулами над F можно представить отрицание и конъюнкцию, а значит, и дизъюнкцию. В этом случае, согласно теореме 1.6, множество F полное. ►

Пример 1.2. Полное множество составляет единственная функция $x \mid y = \neg(x \wedge y)$, называемая *штрихом Шеффера*. Проверка критерия Поста здесь элементарна, и мы на этом не будем останавливаться. Нетрудно также с помощью этой функции представить функции стандартного базиса:

$$\bar{x} = \overline{xx} = x \mid x, \quad xy = \overline{x \mid y} = (x \mid y) \mid (x \mid y), \quad x + y = \overline{\bar{x} \bar{y}} = \bar{x} \mid \bar{y}$$

Аналогична стрелка Пирса. Она тоже составляет базис.

Пример 1.3. В математической логике ключевой операцией является импликация. Совместно с отрицанием она составляет базис: отрицание не попадает в классы T_0 , T_1 , M , а импликация оказывается за бортом классов S и L . Впрочем, как и в случае других базисов, можно через импликацию и отрицание представить дизъюнкцию и конъюнкцию, а затем сослаться на теорему 1.6.

ОГЛАВЛЕНИЕ

1. Алгебра высказываний	1
1.1. Введение	1
1.2. Алгебра логики	3
1.3. Тавтологии и эквивалентность формул	5
1.4. Функции алгебры логики	9
2. Исчисление высказываний	14
2.1. Основные положения теории N	14
2.2. Правила естественного вывода	16
2.3. Глобальные свойства теории N	21
3. Алгебра предикатов	26
3.1. Предикаты и кванторы	26
3.2. Логико-математические языки	27
3.3. Переименования и подстановки	30
3.4. Семантика логико-математического языка	33
3.5. Логические законы	35
3.6. Замены	38
3.7. Упрощение формул	40
4. Исчисление предикатов	42
4.1. Построение теории P	42
4.2. Правила естественного вывода	43
4.3. Глобальные свойства теории P	45
5. Генценовские формальные системы	52
5.1. Исчисление GV	52
5.2. Исчисление GP	56
6. Примеры формальных теорий	59
6.1. Теория групп	59
6.2. Формальная арифметика	61
7. Метод резолюций	66
7.1. Скулемовские функции	66
7.2. Метод резолюций для исчисления высказываний	68
7.3. Метод резолюций для исчисления предикатов	71