Министерство образования и науки Российской Федерации

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

В. М. Зюзьков

МАТЕМАТИЧЕСКАЯ ЛОГИКА И ТЕОРИЯ АЛГОРИТМОВ

Учебное пособие

Томск
«Эль Контент»
2015

УДК [510.6 + 510.5](075.8)
ББК 22.12я73
З-981

Рецензенты:
Крылов П. А., докт. физ.-мат. наук, профессор, зав. кафедрой алгебры Томского государственного университета;
Карпов А. Г., канд. техн. наук, доцент кафедры компьютерных систем в управлении и проектировании ТУСУРа.

Зюзьков В. М.
З-981 Математическая логика и теория алгоритмов : учебное пособие / В. М. Зюзьков. — Томск : Эль Контент, 2015. — 236 с.

ISBN 978-5-4332-0197-2

Учебное пособие содержит теоретический материал, изучение которого предусмотрено программой курса «Математическая логика и теория алгоритмов» направлений подготовки бакалавров «Информатика и вычислительная техника» и «Управление в технических системах».

УДК [510.6 + 510.5](075.8)
ББК 22.12я73

ISBN 978-5-4332-0197-2

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Знания достигаются не быстрым бегом,
а медленной ходьбой.

Томас Бабингтон Маколей (1800–1859 гг.)

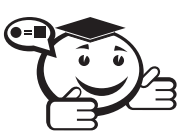
Учебное пособие содержит традиционные разделы математической логики: теорию множеств, пропозициональную логику и логику предикатов, а также введение в аксиоматические формальные системы, основные формализации алгоритмов и вычислимости и введение в классификации алгоритмов и задач по сложности.

Предмет математической логики и теории алгоритмов наряду со специальными знаниями описывает взаимосвязи между научным подходом в познании реального мира, логикой и математикой. Содержание математической логики последних 100 лет включает в себя не только традиционную логическую и математическую проблематику, но некоторые вопросы философии, психологии и искусственного интеллекта. О таких вопросах говорится в главах о миссии математической логики, истории логики и математических доказательствах. Материал этих глав должен возбудить интерес у студентов с самым различным уровнем подготовки. Чтение дополнительной литературы (классической и современной, учебной и научной), указанной в библиографических ссылках после каждой главы, полезно пытливому студенту.

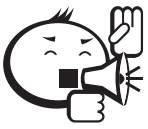
Для контроля понимания изученного материала предлагается ответить на вопросы после каждой главы.

Соглашения, принятые в книге

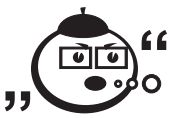
Для улучшения восприятия материала в данной книге используются пиктограммы и специальное выделение важной информации.



Эта пиктограмма означает определение или новое понятие.



Эта пиктограмма означает внимание. Здесь выделена важная информация, требующая акцента на ней. Автор здесь может поделиться с читателем опытом, чтобы помочь избежать некоторых ошибок.



Эта пиктограмма означает цитату.

Эта пиктограмма означает теорему.

Эта пиктограмма означает лемму.

Пример

Эта пиктограмма означает пример. В данном блоке автор может привести практический пример для пояснения и разбора основных моментов, отраженных в теоретическом материале.

Выводы

Эта пиктограмма означает выводы. Здесь автор подводит итоги, обобщает изложенный материал или проводит анализ.

Контрольные вопросы по главе

Рекомендуемая литература к главе

Глава 1

МИССИЯ МАТЕМАТИЧЕСКОЙ ЛОГИКИ

> …Это непросто. Мы встаем в три часа утра, а ложимся в одиннадцать. Много занимаемся медитацией, работаем в саду, здесь есть свои трудности, а вам к тому же будет нелегко из-за непривычной обстановки. Все будет чужим: язык, то, как мы сидим, еда. Вы не получите никакой выгоды из того, чему здесь научитесь. Но это не страшно: вы научитесь чему-то новому для себя, а это никогда не помешает.
>
> *Яавилем ван де Ватеринг. Пустое зеркало*

Математическая логика возникла, когда в логических исследованиях стали применять математические методы. Поэтому глава начинается с определения науки логики.

Следующий параграф посвящен математике. Для чего нужно изучать математику? Чем занимаются математики? Какая практическая польза от математики?

Логические и математические рассуждения нередко сопровождаются ошибками. В третьем параграфе описываются классические софизмы и парадоксы.

Глава завершается определением математической логики. Рассказывается о ее целях и задачах, об отношении к реальному миру.

1.1 Логика

Что такое математическая логика? Прежде чем выяснить это, необходимо ответить на вопрос — что есть логика? Перечислим несколько различных определений, серьезных и не очень.

Джон Локк (John Locke; 1632–1704 гг., английский философ): «*Логика есть анатомия мышления*».

Джон Стюарт Милль (John Stuart Mill; 1806–1873 гг., английский философ): «*Логика не тождественна знанию, хотя область ее и совпадает с областью знания. Логика есть общий ценитель и судья всех частных исследований. Она не задается целью находить очевидность; она только определяет, найдена очевидность или нет. Логика не наблюдает, не изобретает, не открывает — она судит.*

<...> Итак, логика есть наука об отправлениях разума, служащих для оценки очевидности; она есть учение как о самом процессе перехода от известных истин к неизвестным, так и о всех других умственных действиях, поскольку они помогают этому процессу».

Льюис Кэрролл (Lewis Carroll, настоящее имя Charles Lutwidge Dodgson; 1832–1898 гг., английский писатель, математик, логик, философ): «*Траляля: «Если бы это было так, это бы еще ничего, а если бы ничего, оно бы так и было, но так как это не так, так оно и не этак! Такова логика вещей!*».

Из книги «Алиса в Зазеркалье», перевод Н. Демуровой.

Джеймс Тёрбер (James Thurber; 1894–1961 гг., американский художник газетных сатирических комиксов, писатель и юморист): «*If you can touch the clocks and never start them, then you can start the clocks and never touch them*[1]*. That's logic, as I know and use it*» [2].

Амброз Бирс (Ambrose Bierce; 1842–1913 гг., американский писатель, журналист, автор юмористических и «страшных» рассказов) [3]: «*Логика (сущ.). Искусство размышлять и излагать мысли в неукоснительном соответствии с людской ограниченностью и неспособностью к пониманию. Основа логики — силлогизм, состоящий из большой и меньшей посылок и вывода. Например*:

Большая посылка: *Шестьдесят людей способны сделать определенную работу в шестьдесят раз быстрее, чем один человек*.

Меньшая посылка: *Один человек может выкопать яму под столб за 60 секунд*.

Вывод: *Шестьдесят людей могут выкопать яму под столб за 1 секунду*.

Это можно назвать арифметическим силлогизмом, где логика соединена с математикой, что дает нам двойную уверенность в правильности вывода».

Бертран Рассел (Bertrand Russell; 1872–1970 гг., британский философ, общественный деятель и математик) [4]: «*Логика. Деятельность может обеспечить только одну половину мудрости; другая половина зависит от воспринимающей бездеятельности. В конечном счете, спор между теми, кто основывает логику на «истине», и теми, кто основывает ее на «исследовании», происходит из различия в ценностях и на определенном этапе становится бессмысленным*.

В логике будет пустой тратой времени рассматривать выводы относительно частных случаев; мы имеем дело всегда с совершенно общими и чисто формальными импликациями, оставляя для других наук исследование того, в каких случаях предположения подтверждаются, а в каких нет.

Хотя мы больше не можем довольствоваться определением логических высказываний как вытекающих из закона противоречия, мы можем и должны все же признать, что они образуют класс высказываний, полностью отличный от тех, к знанию которых мы приходим эмпирически. Все они обладают свойством, которое <...> мы договорились называть «тавтологией». Это, в сочетании с тем фактом, что они могут быть выражены исключительно в терминах переменных и логических констант (где логическая константа — это то, что остается постоянным в высказывании, даже когда все его составляющие изменяются), даст определение логики или чистой математики».

[1] Если вы можете трогать часы и никогда не завести их, то вы можете завести часы, их не трогая (перевод мой — В. З.).

Непейвода Н. Н. (Непейвода Николай Николаевич; род. 1949 г., советский и российский математик, учёный в области теоретической информатики и математической логики) [5]: «*Логика — наука, изучающая с формальной точки зрения понятия, методы их определения и преобразования, суждения о них и структуры доказательных рассуждений*».

Высказанные определения дают предварительную картину логики. В дальнейшем мы обстоятельно и более точно познакомимся с логикой, используемой в математике.

В отличие от ремесла и искусства наука невозможна без доказательств и логики. Вольно говоря, доказательства — это кирпичи, из которых строятся научные теории; логика — цемент, скрепляющий эти кирпичи. Хорошая идея ничего не стоит, если ее невозможно доказать, — она должна быть рационально обоснована, а этого не добиться без прочного и надежного логического фундамента.

Доказательство *— это рациональный логический переход от принятой точки зрения (**предпосылки**) к тому рубежу, где ее необходимо обосновать или подтвердить (**вывод**). Предпосылки — это некоторые основные положения, принятые (хотя бы временно), для того чтобы можно было осуществить доказательство. Предпосылки могут быть установлены различными способами: логически, эмпирически (на основе наблюдений и опыта) или могут быть следствием уже доказанных положений. Переход от предпосылок к выводам осуществляется с помощью рассуждений. Надежность доказательства в целом определяется точностью предпосылок.*

Логика *— наука об анализе доказательств, аргументов и установлении принципов, на основании которых могут быть сделаны надежные рассуждения.*

Логику интересует лишь форма наших мыслей, но не их содержание. Разнообразие содержания укладывается в сравнительно небольшое число форм. Грубо говоря, логику интересуют сосуды — бутылки, ведра, бочки, — а не то, что в них налито.

В этом отношении логика сходна с грамматикой, которую мы изучали в школе. Грамматика тоже исследует и описывает формы языковых выражений, отвлекаясь от их содержания. Известное стихотворение «Бармаглот» из «Алисы в Зазеркалье» Льюиса Кэрролла начинается со следующих строк:

Варкалось. Хливкие шорьки
Пырялись по наве.
И хрюкотали зелюки,
Как мюмзики в мове...

Знание грамматики позволяет нам обнаружить, что в этих строчках является подлежащим, сказуемым и т. д. Мы можем говорить о роде, числе, падеже наших существительных, не имея ни малейшего представления о том, что обозначают

соответствующие слова. Более того, как говорит Алиса об этих строках: они «наводят на всякие мысли, хоть и неясно — на какие». Аналогичное знание о формах мысли дает нам логика.

При изучении логики мы вводим различные формальные языки. Дело в том, что формальные языки всегда проще, чем структура естественных языков. Иногда естественный язык может быть очень сложен.

Вот как, например, ***Марк Твен*** обыгрывает особенности словообразования в немецком языке [6, с. 59]: «*В одной немецкой газете, — уверяет он, — я сам читал такую весьма занятную историю*:

Готтентоты (по-немецки: ***хоттентотен****), как известно, ловят в пустынях кенгуру (по-немецки:* ***бейтельрате*** *— сумчатая крыса). Они обычно сажают их в клетки (****коттэр****), снабженные решетчатыми крышками (****латтенгиттер****) для защиты от непогоды (****веттер****).*

Благодаря замечательным правилам немецкой грамматики все это вместе — кенгуру и клетки — получают довольно удобное название ***латтенгиттерветтеркоттэрбейтельратте****.*

Однажды в тех местах, в городе Шраттертроттэле, был схвачен негодяй, убивший готтентотку, мать двоих детей.

Такая женщина по-немецки должна быть названа ***хоттентотенмуттер****, а ее убийца сейчас же получил в устах граждан имя* ***шраттертроттэльхоттентотенмуттэраттэнтэтэр****, ибо убийца — по-немецки* ***аттэнтэтэр****.*

Преступника поймали и за неимением других помещений посадили в одну из клеток для кенгуру, о которых выше было сказано. Он бежал, но снова был изловлен. Счастливый своей удачей, негр-охотник быстро явился к старшине племени.

— Я поймал этого... Бейтельратте? Кенгуру? — в волнении вскричал он.

— Кенгуру? Какого? — сердито спросил потревоженный начальник.

— Как какого? Этого самого! Латтенгиттерветтеркоттэрбейтельратте.

— Яснее! Таких у нас много... Непонятно, чему ты так радуешься?

— Ах ты, несчастье какое! — возмутился негр, положил на землю лук и стрелы, набрал в грудь воздуха и выпалил:

— Я поймал шраттертроттэльхоттентотенмуттэраттэнтэтэрлаттенгиттерветтеркоттэрбейтельратте! Вот кого!

Тут начальник подскочил, точно подброшенный пружиной:

— Так что же ты мне сразу не сказал этого так коротко и ясно, как сейчас?!».

Примерами доказательных рассуждений являются приведенные выше цитаты из произведений Амброза Бирса и Джеймса Тёрбера. Эти же цитаты есть примеры ***дедукции***. При дедуктивном доказательстве заключение выводится из предпосылки, и доказательство считается «обоснованным». «Надежное» доказательство, проводимое по логическим законам, гарантирует верный вывод, если предпосылки верны. Но логически законы действуют и в случае, когда предпосылки ложны. Следующее рассуждение является логически корректным, несмотря на ложность предпосылок.

Все марсиане имеют деревянные ноги.

Геракл — марсианин.

Следовательно, у Геракла — деревянные ноги.

Вывод дедуктивного доказательства скрыт в его предпосылках; иными словами, вывод «не выходит за пределы» предпосылки и не добавляет к ней ничего нового. Невозможно, таким образом, принять предпосылки и отвергать вывод, не вступая во внутреннее противоречие.

Другой основной метод доказательства — ***индукция***. В типичном индуктивном рассуждении основной закон или принцип следует из определенных наблюдений за внешним миром. Например, множество наблюдений показывает, что млекопитающие рожают детенышей, и индуктивно можно заключить, что так размножаются все млекопитающие. Подобное доказательство не может быть строго обоснованным (в отличие от дедуктивного), его заключение не обязательно следует из предпосылки. Так, существование яйцекладущих млекопитающих — ехидны и утконоса — опровергает казавшееся таким правдивым заключение. Индуктивное доказательство всегда выходит за рамки предпосылки, которая не влечет за собой обязательную истинность заключения, но предполагают его возможность. Индуктивные доказательства — это обобщения и всевозможные экстраполяции от частного к общему; от наблюдаемого к ненаблюдаемому; от прошлого и настоящего — к будущему.

Ошибки при индуктивном доказательстве могут приводить к серьезным последствиям. Г. Попов[1] считает, что индуктивное доказательство о классовом расколе крестьян в России, проделанное В. И. Лениным в книге «Развитие капитализма в России» на базе статистических отчетов и обследований, является ошибочным[2] [7].

В человеческих отношениях логика не является обязательной, но часто приносит пользу. Но и алогичные рассуждения иногда тоже оказываются полезными. Приведем две шутки.

Дровосек и математик. «*Дровосек пришел к математику и просит у него рубль взаймы. При этом он обещает через месяц вернуть два рубля, а в залог оставляет свой топор. Математик дает дровосеку рубль, а когда тот собирается уходить, говорит*:

— Постой, я кое-что придумал. Тебе ведь будет трудно возвращать через месяц сразу два рубля. Так может, ты лучше вернешь половину долга сейчас?

После долгих раздумий дровосек соглашается, отдает рубль математику и идет домой.

— Странно! — думает он по дороге. — Денег у меня по-прежнему нет, топора тоже, да еще один рубль я остался должен. И что самое главное, всё правильно!».

Ирландец и пиво. «*Ирландец заходит в дублинский бар и заказывает три пинты «Гиннесса». Получив заказ, он делает глоток сначала из первой кружки, потом из второй, затем из третьей, — и продолжает пить тем же манером, пока кружки не пустеют. После этого он повторяет свой заказ.*

— Может, лучше заказывать по одной? Тогда пена не успеет осесть, — предупредительно замечает бармен.

---

[1] Гавриил Харитонович Попов — советский экономист и российский политик. Один из видных лидеров демократического движения в СССР и России в конце 1980-х — начале 1990-х годов.

[2] Г. Попов сообщает о характерной детали личности В. И. Ленина: он отлично владел дедукцией, но был слабым в индукции — единственная оценка «хорошо» в гимназическом аттестате Ленина была как раз по логике.

— Я знаю, — отзывается посетитель. — Но, видите ли, в чем дело: у меня есть два брата, один из них сейчас в Австралии, а другой — в Америке. Когда мы расставались, то поклялись друг другу, что будем пить именно так — в память о тех днях, когда мы выпивали вместе. Так что две пинты я беру для братьев, а третью — для себя.

— Какая прекрасная традиция! — восклицает растроганный бармен.

Ирландец стал в этом баре постоянным посетителем, всякий раз делая один и тот же заказ. Однако как-то раз, в очередной свой визит, он заказал всего две пинты. Это заметили другие завсегдатаи, и над баром повисла тишина. Когда ирландец подошел к стойке за следующей порцией, бармен произнес:

— Примите мои соболезнования!

— Не волнуйтесь, все в порядке! — отозвался ирландец. — Просто я стал мормоном, и мне пришлось бросить пить».

1.2 Математика

> Математик это сделает лучше. Универсальный принцип.
>
> *Гуго Штейнгауза*[1]

> Математик так же, как художник или поэт, создаёт узоры. И если его узоры более устойчивы, то лишь потому, что они составлены из идей... Узоры математика так же, как узоры художника или поэта, должны быть прекрасны; идеи так же, как цвета или слова, должны гармонически соответствовать друг другу. Красота есть первое требование: в мире нет места для некрасивой математики.
>
> *Годфри Харди*[2]

Возникновение логики как науки о дедуктивных рассуждениях связано с именем Аристотеля (384–322 гг. до н. э.)[3]. Но развитие логики по-настоящему пошло лишь в XX веке, когда математика, как писал Н. Н. Непейвода, «доросла до того, чтобы применять свои методы для анализа своей собственной структуры, и таким образом, первой из наук перешла со стадии экстенсивного роста на стадию рефлексии»[4].

Появилась новая наука — ***математическая логика*** — унаследовавшая задачи формальной логики, но использовавшая для их решения математический аппарат.

Рассмотрим науку математику, ее особенности, ее проблемы, с точки зрения логики и частично психологии.

---

[1] Гуго Дионисий Штейнгауз (1887–1972 гг.) — польский математик. Смысл его принципа, конечно, не в том, что медиков и юристов надо вербовать только среди математиков, но с назиданием, что представитель каждой специальности, владеющий стилем и методом мышления, почерпнутым при творческом изучении математики, будет и в своей области работать лучше.

[2] Годфри Харолд Харди (1877–1947 гг.) — знаменитый английский математик.

[3] См. следующую главу, посвященную истории логики.

[4] Рефлексия — самоанализ, в науке — применение методов данной науки к ней самой.

Первое, что мы должны выяснить — это зачем изучать математику? Математику изучают на протяжении всего многолетнего школьного образования. Какая цель? Ведь не секрет, что многие математические школьные знания никогда не используются большинством взрослых.

На наш взгляд здесь надо полностью согласиться с мнением В. А. Успенского[1]. Перескажем извлечения из его работы [8].

Математика составляет неотъемлемую часть человеческой культуры, но образование состоит не только в расширении круга знаний. В неменьшей степени оно предполагает и расширение навыков мышления. Главная цель обучения математике — психологическая.

Эта цель состоит не столько в сообщении знаний и даже не в столько обучении методу, сколько в *расширении* психологии обучающегося, в привитии ему строгой дисциплины мышления (слово «дисциплина» обозначает здесь приверженность к порядку и способность следовать этому порядку).

Есть три важнейших умения, выработке которых должны способствовать математические занятия. Называем их в порядке возрастания важности:

1) во-первых, умение отличать истинное от ложного (или доказанное от недоказанного);
2) во-вторых, умение отличать имеющее смысл от бессмыслицы;
3) в-третьих, умение отличать понятное от непонятного.

Даже в научной печати встречаются бессмысленные тексты. Коллектив научно-популярной газеты «Троицкий вариант» во главе с М. С. Гельфандом (доктором биологических наук) провел общественную акцию. Была написана статья — перевод на русский язык англоязычной статьи, сгенерированной компьютерной программой. Статья содержала правдоподобно выглядящий, но слабосвязанный и бессмысленный текст. Под названием «*Корчеватель: Алгоритм типичной унификации точек доступа и избыточности*» и от имени несуществующего аспиранта Михаила Жукова из несуществующего Института информационных проблем РАН эта статья была отправлена для публикации в журнал «Журнал научных публикаций аспирантов и докторантов» (г. Курск). Данный журнал входил в список научных журналов ВАК Минобрнауки России. После оплаты услуги публикации в размере 4500 рублей статья была принята к печати, получив положительный отзыв рецензента о том, что «статья принята с небольшими замечаниями» [9].

Чтобы квалифицировать высказывание как ложное, бессмысленное или непонятное, надо сделать некоторое усилие — иногда это требует интеллектуальных усилий, а иногда ваша точка зрения противоречит мнению авторитетного лица. Не все и не всегда готовы на такое усилие.

Способность к такому усилию, о котором только что говорилось, тренируется (во всяком случае, должна тренироваться) на уроках математики и при общении с математиками. Дело в том, что математика — наука по природе своей демократическая.

В начальных математических знаниях нуждается каждый человек. Но практическая польза математики весьма нетривиальная.

[1] Владимир Андреевич Успенский (род. 1930 г., Москва) — российский математик.

Математика обладает свойством опережать экспериментальные знания и позволяет нам силой мысли проникать в те уголки Вселенной, куда мы физически проникнуть не можем. Классический пример такого рода — это знаменитое открытие Нептуна на кончике пера. Вскоре после открытия Урана в конце XVIII века в движении этой планеты стали выявляться непонятные аномалии — она то «отставала» от расчётного положения, то опережала его. Было высказано предположение о том, что имеющиеся нарушения в траектории Урана можно объяснить, если предположить, что есть еще одна планета, доселе неизвестная. Из видимых с помощью телескопа нарушений движений Урана, с помощью сложных математических расчетов длиной в несколько лет удалось узнать, где могло бы двигаться новое небесное тело. Вычисления массы и орбиты новой планеты проводил французский математик Урбен Леверье. В 1846 году астрономы обнаружили новую планету в указанной Леверье точке небесной сферы.

Математика помогает узнать недостающие куски реальности. Это ярко выразилось в истории с электричеством и радиосвязью. К моменту открытия никто не знал слова «радиосвязь». К середине XIX века имелись некоторые физические законы, полученные экспериментально. Был математически выраженный закон Кулона, который говорил о том, как электрические заряды притягиваются, был закон Ампера — закон о магнитных и электрических полях — о том, какие магнитные поля создаются токами, потом появился закон Фарадея. Это были математические утверждения, которые существовали изолировано и более или менее сами по себе. Джеймс Максвелл[1] задался целью найти, нет ли единого математического формализма, в котором все эти законы записывались бы однотипно и в некотором смысле равномерно.

Максвелл сформулировал систему уравнений в дифференциальной форме, описывающих электромагнитное поле и его связь с электрическими зарядами и токами в вакууме и сплошных средах. Эти уравнения сыграли ключевую роль в развитии представлений теоретической физики и оказали сильное, зачастую решающее влияние не только на все области физики, непосредственно связанные с электромагнетизмом, но и на многие возникшие впоследствии фундаментальные теории, предмет которых не сводился к электромагнетизму (одним из ярчайших примеров здесь может служить специальная теория относительности).

В современном взгляде на Вселенную можно выделить два ключевых момента:

1) гипотеза об объективном существовании мира вне человека предполагает, что полное описание физической реальности не зависит от субъективного мнения человека;

2) любой вариант объективного описания реальности представляет собой некую математическую структуру. Современная физическая картина мира является по сути дела математической.

Приведенные примеры могут создать впечатление, что математика в основном занимается решением задач, которые имеют прикладное значение.

Это не так. ***Станислав Лем***[2] весьма образно описывает, чем занимается математик. Приведем отрывок из его книги «Сумма технологий» [10]: «*Давайте пред-*

[1] Джеймс Клерк Максвелл (1831–1879 гг.) — британский физик и математик.

[2] Станислав Лем (1921–2006 гг.) — польский писатель, философ, фантаст и футуролог.

ставим себе портного-безумца, который шьет всевозможные одежды. Он ничего не знает ни о людях, ни о птицах, ни о растениях. Его не интересует мир, он не изучает его. Он шьет одежды. Не знает, для кого. Не думает об этом. Некоторые одежды имеют форму шара без всяких отверстий, в другие портной вшивает трубы, которые называет «рукавами» или «штанинами». Число их произвольно. Одежды состоят из разного количества частей.

Портной заботится лишь об одном: он хочет быть последовательным. Одежды, которые он шьет, симметричны или асимметричны, они большого или малого размера, деформируемы или раз и навсегда фиксированы. Когда портной берется за шитье новой одежды, он принимает определенные предпосылки. Они не всегда одинаковы, но он поступает точно в соответствии с принятыми предпосылками и хочет, чтобы из них не возникало противоречие. Если он пришьет штанины, то потом уж их не отрезает, не распарывает того, что уже сшито, ведь это должны быть все же костюмы, а не кучи сшитых вслепую тряпок.

Готовую одежду портной относит на огромный склад. Если бы мы могли туда войти, то убедились бы, что одни костюмы подходят осьминогу, другие — деревьям или бабочкам, некоторые — людям. Мы нашли бы там одежды для кентавра и единорога, а также для созданий, которых пока никто не придумал. Огромное большинство одежд не нашло бы никакого применения. Любой признает, что сизифов труд этого портного — чистое безумие.

Точно так же, как этот портной, действует математика. Она создает структуры, но неизвестно чьи. Математик строит модели, совершенные сами по себе (то есть совершенные по своей точности), но он не знает, модели ЧЕГО он создает. Это его не интересует. Он делает то, что делает, так как такая деятельность оказалась возможной. Конечно, математик употребляет, особенно при установлении первоначальных положений, слова, которые нам известны из обыденного языка. Он говорит, например, о шарах, или о прямых линиях, или о точках. Но под этими терминами он не подразумевает знакомых нам понятий. Оболочка его шара не имеет толщины, а точка — размеров. Построенное им пространство не является нашим пространством, так как оно может иметь произвольное число измерений...».

Опыт развития математики убеждает, что самые, казалось бы, оторванные от практики ее разделы рано или поздно находят важные применения. Приведем несколько примеров.

1. Теория чисел, одна из древнейших в математике, долгое время считалась чем-то вроде «игры в бисер»[1]. Оказалось, что без этой теории немыслима современная криптография, равно как и другие важные направления, объединенные названием «защита информации».
2. Специалисты по теоретической физике интересуются новейшими разработками алгебраической геометрии и даже такой абстрактной области, как теория категорий.
3. Теория категорий используется в функциональном программировании — язык Haskell (реализация монад) [12].

[1] Г. Харди, известный своими работами в теории чисел и математическом анализе, писал: «Я никогда не делал чего-нибудь «полезного». Ни одно мое открытие не принесло или могло бы принести, явно или не явно, к добру или к злу, малейшего изменения в благоустройстве мира» [11].

Г. Штейнгауз предложил следующую оригинальную классификацию «математик» [13, с. 49–50]. Одной из целей математики является открытие и доказательство новых утверждений. Математику, которая занимается именно этим, назовем логической математикой или математикой «α». Математику, которая занимается решением задач типа школьных, задач с ясной постановкой и очевидно существующим решением, назовем математикой «β». На основе того факта, что утверждения чистой математики можно применять и к другим наукам, возникла математика «γ», которую называют прикладной. При этом мы должны научиться выполнять ряд вычислений. Как проще и лучше осуществлять стандартные вычислительные операции — этому учит практическая математика, которую можно назвать математикой «δ».

Неполный, односторонний взгляд на сущность математики заключается в том, что огромное большинство людей никогда не имеют дела с математикой, иной нежели «δ». Большинство образованных людей не встречаются с математикой, отличной от «β» и «δ».

Поэтому зададим себе вопрос: какое значение в жизни имеет математика «α» и «γ»? Ответ на этот вопрос вы найдете в параграфе 1.4.

Математика — это не просто наука, а вдобавок система традиций, ценностей, восприятия и даже мировоззрения целого научного сообщества.

Особенности научной этики математика описывает ***Н. Н. Непейвода***: «*Математику неприлично заниматься тем, что не допускает точной формулировки, и самому формулировать утверждения, которые могут быть поняты двояко*.

Ему неприлично выдавать правдоподобное утверждение за доказанное, он имеет право утверждать лишь то, для чего он имеет полное доказательство.

Ему нельзя утаивать открытое им доказательство, он обязан предоставить его на максимально широкое обсуждение, для проверки всеми заинтересованными лицами.

Если кто-то нашел ошибку в доказательстве, математик не имеет право настаивать на своем, а обязан поблагодарить за помощь и публично объявить о своей ошибке и пересмотреть доказательство или формулировку теоремы.

Если кто-то нашел опровергающий пример для доказанного им утверждения, автор доказательства даже не имеет права требовать, чтобы нашли еще ошибку и в его доказательстве; текст, объявленный доказательством, уже никого не интересует.

Эти достаточно точные и строгие критерии показывают, почему именно в среде математиков устойчивей всего сохраняется понятие научной этики и чести ученого».

1.3 Софизмы и парадоксы

История логики и математики полна неожиданных и интересных софизмов и парадоксов. И зачастую именно их разрешение служило толчком к новым открытиям, из которых, в свою очередь, вырастали новые софизмы и парадоксы. Необходимо различать между собой парадоксы и софизмы.

Парадокс *— рассуждение либо высказывание, в котором пользуясь средствами, не выходящими (по видимости) за рамки логики, приходят к заведомо неприемлемому результату, обычно к противоречию.*

Софизм *(от греч. sophisma — уловка, выдумка, головоломка) — мнимое доказательство, в котором обоснованность заключения, кажущаяся, порождается чисто субъективным впечатлением, вызванным недостаточностью логического или семантического анализа.*

Задача от Блондинки — пример логической ошибки в рассуждениях.

Классическая блондинка из анекдотов — красивая, но интеллектуально элементарная девушка, интересующаяся поддержанием своей привлекательности, покупкой нарядов, любовниками и деньгами, источниками которых являются богатые, но непривлекательные мужчины. Юмористический образ блондинки присущ многим европейским культурам.

Условие. Я взяла у друга в долг 100 рублей, которые благополучно потеряла. Тогда я пошла к подруге и взяла в долг еще 50 рублей. Купила две шоколадки по 10 рублей. Оставшиеся 30 рублей вернула другу. Осталась должна 70 рублей другу и 50 рублей подруге, всего 120 рублей. Плюс купленные шоколадки. Итого 140 рублей.

Вопрос. Куда подевались 10 рублей?

В отличие от логической ошибки, возникающей непроизвольно и являющейся следствием невысокой логической культуры, софизм является преднамеренным нарушением логических правил. Обычно он тщательно маскируется под истинное суждение.

Софистами называли группу древнегреческих философов IV–V века до н. э., достигших большого искусства в логике. В период падения нравов древнегреческого общества появляются так называемые учителя красноречия, которые целью своей деятельности считали и называли приобретение и распространение мудрости, вследствие чего они именовали себя софистами. Их задачей обычно было научить убедительно защитить любую точку зрения, какая только могла понадобиться ученику, при этом вполне допускались логические передержки, применение противоречивых норм, бытовавших у разных народов, неправомерные переходы от общего правила к частному случаю, который этим правилом, по существу, не предусмотрен.

Существует множество софизмов, созданных еще в древности и сохранившихся до сегодняшнего дня. Заключение большей части из них носит курьезный характер. Например, софизм «вор» выглядит так: «Вор не желает приобрести ничего дурного; приобретение хорошего есть дело хорошее; следовательно, вор желает хорошего». Странно звучит и следующее утверждение: «Лекарство, принимаемое больным, есть добро; чем больше делать добра, тем лучше; значит, лекарство нужно принимать в больших дозах». Существуют и другие известные софизмы, например: «Сидящий встал; кто встал, тот стоит; следовательно, сидящий стоит» или софизм «рогатый»: «То, что ты не потерял, ты имеешь; ты не потерял рога, следовательно, ты их имеешь».

Более интересен софизм «Эватл и Протагор».

Эватл брал уроки софистики у софиста Протагора под тем условием, что гонорар он уплатит только в том случае, если выиграет первый процесс. Ученик после обучения не взял на себя ведения какого-либо процесса и потому считал себя вправе не платить гонорара. Учитель грозил подать жалобу в суд, говоря ему следующее: «Судьи или присудят тебя к уплате гонорара или не присудят. В обоих случаях ты должен будешь уплатить. В первом случае в силу приговора судьи, во втором случае в силу нашего договора». На это Эватл отвечал: «Ни в том, ни в другом случае я не заплачу. Если меня присудят к уплате, то я, проиграв первый процесс, не заплачу в силу нашего договора, если же меня не присудят к уплате гонорара, то я не заплачу в силу приговора суда».

А вот современный софизм, обосновывающий, что с возрастом «годы жизни» не только кажутся, но и на самом деле короче: «Каждый год вашей жизни — это её $1/n$ часть, где n — число прожитых вами лет. Но $n+1 > n$. Следовательно, $1/(n+1) < 1/n$».

Еще один софизм, связанный с физикой: «Вечный двигатель первого рода невозможен, поскольку его запрещает первое начало термодинамики; вечный двигатель второго и третьего рода запрещают соответственно второе и третье начала термодинамики; поскольку четвертого начала термодинамики нет, то вечный двигатель четвертого рода возможен».

Рассмотрим математические софизмы. Объяснять, в чем состоит ошибочность рассуждения в каждом софизме, мы не будем, чтобы не лишать читателя удовольствия самостоятельно найти ее.

1. *Тождественные преобразования, использующие операции со степенями и мнимой единицей*:

$$1 = 1^{1/2} = (i^4)^{1/2} = i^2 = -1;$$

$$1 = 1^{1/2} = \big((-1)\cdot(-1)\big)^{1/2} = (-1)^{1/2}\cdot(-1)^{1/2} = i^2 = -1.$$

Каждое из этих двух преобразований «доказывает», что $1 = -1$.

2. *Квадратное уравнение имеет три корня*.

Как известно, квадратное уравнение может иметь либо два корня, либо один, либо вообще не иметь корней. Но так ли это на самом деле? Посмотрите на вот это уравнение:

$$\frac{(-a+x)(-b+x)}{(-a+c)(-b+c)} + \frac{(-a+x)(-c+x)}{(-a+b)(b-c)} + \frac{(-b+x)(-c+x)}{(a-b)(a-c)} = 1.$$

Здесь a, b, c — любые различные числа. Поскольку в числителе каждой дроби перемножаются две скобки, содержащие x, то это уравнение, несомненно, является квадратным. Однако подставим в него $x = a$: первое слагаемое станет равным 1, а второе и третье содержат множитель $(x - a)$, поэтому обратятся в 0. Таким образом, при $x = a$ получаем равенство $1 = 1$, т. е. $x = a$ — корень этого уравнения. Совершенно аналогично проверяется, что $x = b$ и $x = c$ тоже являются корнями. Значит, это уравнение имеет три различных корня.

3. *Числа Фибоначчи*.

Последовательность чисел Фибоначчи $f(n)$ определяется по правилам: $f(1) = f(2) = 1$ и $f(n) = f(n-1) + f(n-2)$ при $n > 2$. Первые 10 чисел суть 1, 1, 2, 3, 5,

8, 13, 21, 34, 55. Возьмем квадрат со стороной $f(7) = 13$. Разрежем его на 4 части и составим из них прямоугольник (рис. 1.1). Стороны прямоугольника $f(8) = 21$ и $f(6) = 8$. Площадь квадрата равна 169, а площадь прямоугольника равна 168. Площади равносоставленных четырехугольников оказались неравными.

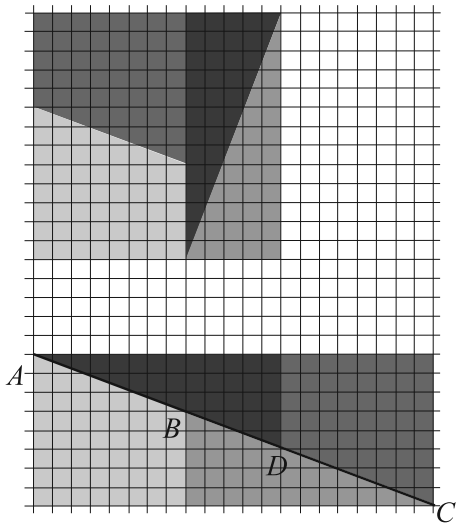


Рис. 1.1 – $f(7)^2$ и $f(6) \times f(8)$

Теперь возьмем квадрат со стороной $f(8) = 21$. Разрежем его на 4 части и составим из них прямоугольник (рис. 1.2). Стороны прямоугольника $f(7) = 13$ и $f(9) = 34$. Площадь квадрата равна 441, а площадь прямоугольника равна 442. Площади равносоставленных четырехугольников снова оказались неравными.

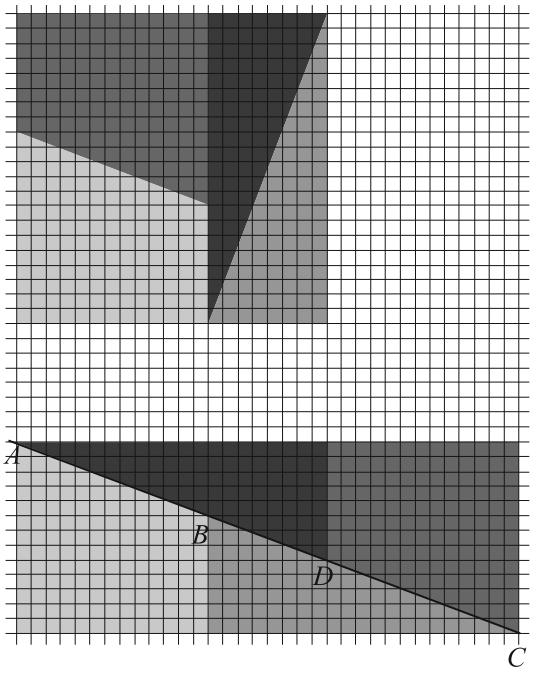


Рис. 1.2 – $f(8)^2$ и $f(7) \times f(9)$

Аналогичное построение можно провести для любых трех последовательных чисел Фибоначчи.

4. *Карта России*.

На карте России масштаба 1:15 000 000 все размеры уменьшены в 15 миллионов раз. Если население в 150 миллионов уменьшить во столько же раз — останется 10 человек. Казалось бы, им должно хватить места. Но на карте и одному тесно (рис. 1.3).

Рис. 1.3 – Карта России

В параграфе 7.2 главы 7 мы познакомимся еще с одним софизмом.

Перейдем к парадоксам. Парадоксы сопровождают развитие логики с древних времен. Их появление всегда с беспокойством воспринималось мыслителями. И если раньше их рассматривали как некий курьез мысли, которого можно избежать при должной осторожности в рассуждениях, то в современной логике отношение к парадоксам гораздо серьезнее. С ними действительно связаны реальные проблемы. Анализ парадоксов часто приводит к пересмотру основ логических теорий, к уточнению понятий и допущений и даже к появлению новых направлений в логике. Далеко не все парадоксы оказываются на деле легко разрешимыми.

1. **Парадокс «Лжец»**. Его открытие приписывают древнегреческому философу Евбулиду (IV в. до н. э.). Вся проблема заключается в интерпретации простой фразы: «Я лгу». Является это высказывание истинным или ложным? Из истинности этого утверждения следует его ложность, и наоборот.

Другую форму парадокса лжеца предложил французский логик Иоанн Буридан (XIII век).

Обозначим через P высказывание, содержащееся в рамке:

P ложно

Является это высказывание истинным или ложным?

Логики продолжают обсуждать парадокс лжеца и по сей день. Предлагалось немало вариантов решения, однако ни одно из решений не является общепризнанным.

2. **Апория Зенона: Ахиллес и черепаха**. Древнегреческий философ Зенон[1] доказывал, что Ахиллес, один из самых сильных и храбрых героев, осаждавших древнюю Трою, никогда не догонит черепаху, которая, как вы, конечно, знаете, отличается крайне медленной скоростью передвижения.

Вот примерная схема его рассуждений. Предположим, что Ахиллес и черепаха начинают свое движение одновременно и Ахиллес стремится догнать черепаху. Примем для определенности, что Ахиллес движется в 10 раз быстрее черепахи и что их отделяют друг от друга 100 м. Когда Ахиллес пробежит расстояние в 100 м, отделяющее его от того места, откуда начала свое движение черепаха, то в этом месте Ахиллес ее уже не застанет, так как она пройдет вперед расстояние в 10 м. Когда Ахиллес минует и эти 10 м, то и там черепахи уже не будет, поскольку она успеет перейти на 1 м в новое место. Достигнув и этого нового места, Ахиллес опять не найдет там черепахи, потому что она успеет пройти расстояние, равное 10 см, и снова окажется несколько впереди его. Это рассуждение можно продолжать до бесконечности, и придется признать, что быстроногий Ахиллес никогда не догонит медленно ползущую черепаху.

Апории Зенона, из которых до нас дошло только девять, имеют глубокий смысл и направлены на вскрытие понятия бесконечности, и до сих пор привлекают внимание математиков и философов, которые продолжают давать им самые различные объяснения. Рассматриваемая здесь апория Зенона даже на сегодняшний день далека от своего окончательного разрешения.

3. **Парадокс крокодила**. У одной египтянки крокодил похитил ребенка. Египтянка просила вернуть ребенка, и крокодил обещал ей это, если она правильно укажет, как поступит крокодил.

Мать ребенка сказала: «Ты не возвратишь мне моего ребенка».

На это крокодил ответил: «Если ты, действительно, права, то ты, как сама говоришь, не получишь назад ребенка; если же твое высказывание неверно, то, согласно нашему уговору, ты не получишь ребенка. В любом случае ребенок должен остаться у меня».

«Наоборот — возразила женщина, — если мое высказывание верно, то я получу ребенка назад в силу нашего условия; если же я ошиблась, то это означает, что ты сам вернешь мне ребенка. В каждом из случаев я получу ребенка назад».

Кто прав: мать или крокодил? К чему обязывает крокодила данное им обещание? К тому, чтобы отдать ребенка или, напротив, чтобы не отдать его? И к тому и к другому одновременно. Это обещание внутренне противоречиво, и, таким образом, оно невыполнимо в силу законов логики.

4. **Парадокс Берри**. Впервые парадокс опубликован Бертраном Расселлом, приписав его авторство Дж. Дж. Берри (1867–1928 гг.), библиотекарю библиотеки в Оксфорде.

Рассмотрим выражение:

«*Наименьшее натуральное число, которое нельзя описать менее чем одиннадцатью словами*».

---

[1] Зенон (около 490–430 гг. до н. э.) — представитель элейской философской школы, которого Аристотель считал основателем диалектики как искусства познания истины с помощью спора или истолкования противоположных мнений. «Апория» в переводе с греческого означает «трудность».

Поскольку слов конечное число, существует конечное множество фраз из менее чем одиннадцати слов и, следовательно, конечное подмножество натуральных чисел, определяемых фразой из одиннадцати слов. Однако множество натуральных чисел бесконечно, следовательно, существуют числа, которые нельзя определить фразой из менее чем одиннадцати слов. Среди них, очевидно, существует наименьшее натуральное число (наименьшее число можно выбрать из любого подмножества натуральных чисел), не описываемое менее чем одиннадцатью словами. Но именно это число определяется приведённой выше фразой и в ней менее одиннадцати слов, а значит, не может являться искомым наименьшим числом и не может описываться данной фразой. Возникает парадокс: должно существовать число, описываемое данной фразой, но поскольку выражение само себе противоречит, не может существовать числа, им описываемого.

5. **Парадокс Греллинга** назван в честь открывшего его немецкого математика Курта Греллинга.

Разделим все прилагательные на два множества: *самодескриптивные*, обладающие тем свойством, которое они выражают, и *несамодескриптивные*. Такие прилагательные, как «многосложное», «русское» и «трудновыговариваемое» принадлежат к числу самодескриптивных. А такие как «немецкое», «однокоренное» и «невидимое» — к числу несамодескриптивных. К какому из двух множеств принадлежит прилагательное «несамодескриптивное»? Если оно несамодескриптивное, оно обладает обозначаемым им свойством и должно быть самодескриптивным. Если же оно самодескриптивное, оно не имеет обозначаемого им свойства и должно быть несамодескриптивным.

6. **Парадокс брадобрея**. Единственному деревенскому брадобрею приказали: «Брить всякого, кто сам не бреется, и не брить того, кто сам бреется». Кто побреет брадобрея?

Математическая форма этого парадокса называется **парадоксом Бертрана Рассела** и рассматривается в теории множеств — глава 3.

7. **Парадокс неожиданной казни**. Впервые сформулирован и опубликован в 1948 года философом Д. Дж. О′Коннором.

Однажды в воскресенье начальник тюрьмы вызвал преступника, приговорённого к казни, и сообщил ему:

«Вас казнят на следующей неделе в полдень» и

«День казни станет для вас сюрпризом, вы узнаете о нём, только когда палач в полдень войдёт к вам в камеру».

Начальник тюрьмы был честнейшим человеком и никогда не врал. Заключённый подумал над его словами и улыбнулся: «В воскресенье меня казнить не могут! Ведь тогда уже в субботу вечером я буду знать об этом. А, по словам начальника, я не буду знать день своей казни. Следовательно, последний возможный день моей казни — суббота. Но если меня не казнят в пятницу, то я буду заранее знать, что меня казнят в субботу, значит, и её можно исключить». Последовательно исключив пятницу, четверг, среду, вторник и понедельник, преступник пришёл к выводу, что начальник не сможет его казнить, выполнив все свои слова.

На следующей неделе палач постучал в его дверь в полдень в среду — это было для него полной неожиданностью. Всё, что начальник тюрьмы сказал, осуществилось. Где недостаток в рассуждении заключённого?

В дальнейшем мы познакомимся еще с несколькими парадоксами: парадокс Карри (глава 4), принцип пьяницы (глава 5), парадокс Банаха—Тарского (глава 6), парадоксы Гемпеля и изобретателя из главы 7.

Парадоксы лжеца, крокодила, Берри, Греллинга и брадобрея относятся к парадоксам автореференции. ***Автореференция (самоссылочность)*** — явление, которое возникает в системах высказываний в тех случаях, когда некое понятие ссылается само на себя. Иначе говоря, если какое-либо выражение является одновременно самой функцией и аргументом этой функции. Автореференция часто сопряжена с парадоксом.

Ввиду того, что парадоксы обнажают скрытые концептуальные противоречия и переводят их в прямые и открытые, они, согласно законам творческого мышления, помогают при развитии новых идей и концепций.

1.4 Математическая логика

Развитие математики на протяжении XIX в. характеризовалось стремлением к систематизации, к установлению единства в многообразии математических фактов и методов, на первый взгляд весьма далеких друг от друга. Ценным было также критическое уяснение и строгое обоснование фундаментальных понятий. Был создан богатый логический аппарат, с помощью которого создавался формальный язык математики, повышалась строгость доказательств.

Необходимость математической строгости привела к математической логике. Математическая логика выросла из философских вопросов относительно оснований математики, но в настоящее время переросла свои философские корни и стала неотъемлемой частью математики в целом.

Математическая логика — логика по предмету, математика по методу.

Логика отличается от других наук фундаментальностью рассматриваемых проблем, а математическая логика — сочетанием весьма сложного аппарата с сохранением философской глубины и с полностью неординарным взглядом на математический мир.

Задачи, решаемые математической логикой.

1. Создание формальных языков и методов в логике, более точных и эффективных, чем использовавшихся до этого.
2. Удовлетворение естественного философского интереса к основаниям математики и расширение нашего понимания математики, ее возможностей и ограничений как науки.
3. Исследование в области компьютерных наук (computer science).

Решение этих задач во многом обеспечивается реализацией следующей идеи: записывать математические утверждения в виде последовательностей символов и оперировать с ними по формальным правилам. При этом правильность рассуждений можно проверять только по синтаксическим правилам, не рассматривая семантику (смысл) утверждений.

Принято считать, что всякое точно сформулированное математическое утверждение можно записать формулой теории множеств (одной из наиболее общих формальных теорий), а всякое строгое математическое доказательство преобра-

зовать в формальный вывод в этой теории (последовательность формул теории множеств, подчиняющуюся некоторым простым правилам).

Если говорить о решении конкретных математических задач, то математическая логика больше мешает, чем помогает, — ибо задумывалась как метаматематическая дисциплина, призванная наблюдать математику извне. Не способствовать доказательству теорем, а извне оценивать сам процесс обоснования.

Рэймонд Смаллиан[1] (рис. 1.4) писал: «Многие люди спрашивают меня, что такое математическая логика и какова ее цель. К сожалению, ни одно простое определение не может дать даже самое отдаленное понимание математической логики. Только после погружения в этот предмет его сущность становится очевидной. Что касается *цели*, то существует множество целей, но, снова, можно понять их только после некоторого изучения предмета. Тем не менее есть одна цель, и ее я могу сказать вам прямо сейчас: сделать точным понятие *доказательства*».

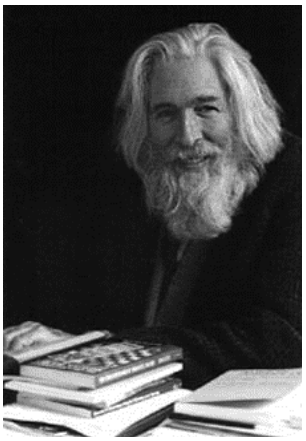


Рис. 1.4 – Рэймонд Смаллиан

Очень важна роль математической логики в основаниях математики. Основания математики — особая сфера исследований оформилась в начале XX в. в связи с проблемой устранения парадоксов, обнаружившихся в теории множеств. Первая задача этих исследований состоит в обосновании строгости признанных доказательств и освобождении существующих математических теорий от парадоксов известных типов. Вторая — в выявлении условий полной надежности математической теории в смысле строгости доказательств и отсутствия противоречий. Первую задачу в настоящее время следует считать в целом решенной, поскольку имеются достаточные основания полагать формализованные доказательства абсолютно строгими (свободными от контрпримеров) и поскольку указаны приемлемые ограничения формулировки аксиом теории множеств, гарантирующие отсутствие в ней парадоксов всех известных типов. Что касается второй задачи, то преобладающее мнение сегодня состоит в том, что она не может быть полностью решена, по крайней мере, в рамках чисто логических подходов.

Что касается компьютерных наук, то теория алгоритмов — является разделом математической логики и содержит множество важных красивых результатов.

Для лучшего понимания предмета математической логики — как соотносятся логика и реальный мир — рассмотрим задачу, предложенную Р. Смаллианом [14].

Молодая девушка Порция обладала умом, которой не уступал ее красоте. Она решила выбрать спутника жизни при помощи логической задачи. Порция заказала две шкатулки, серебряную и золотую, и в одну из них положила свой портрет. На крышках шкатулок красовались надписи.

[1] Рэймонд Меррилл Смаллиан (англ. *Raymond Merrill Smullyan*; род. 1919 г.) — американский математик, логик, пианист, даосский философ, астроном-любитель и фокусник-престидижитатор. Автор многочисленных научно-популярных книг по логике и математике: о логических загадках и парадоксах, передовых концепциях логики, например о теореме Гёделя о неполноте. Кроме того, написал несколько книг о даосской философии, в которых предпринята попытка разрешения большинства философских проблем и интеграции математики, логики и философии.

На золотой	На серебряной
Портрет не в этой шкатулке	*Ровно одно из двух высказываний, выгравированных на крышках, истинно*

Претенденту на руку Порции предлагалось выбрать шкатулку, и если он был достаточно удачлив (или достаточно умен), чтобы выбрать шкатулку с портретом, то получал право назвать Порцию своей невестой. Какую шкатулку выбрать?

Претендент рассуждал следующим образом. Если высказывание, выгравированное на крышке серебряной шкатулке, истинно, то это означает, что истинно ровно одно из двух высказываний. Тогда высказывание, выгравированное на крышке золотой шкатулки, должно быть ложным.

С другой стороны, предположим, что высказывание, помещенное на крышке серебряной шкатулки, ложно. В этом случае утверждение о том, что ровно одно из двух высказываний истинно, было бы неверным. Это означает, что либо оба высказывания истинны, либо оба ложны. Оба высказывания не могут быть истинными, так как по предположению второе высказывание ложно. Следовательно, оба высказывания ложны. Таким образом, высказывание, выгравированное на крышке золотой шкатулки, и в этом случае оказывается ложным.

Итак, независимо от того, истинно или ложно высказывание на крышке серебряной шкатулки, высказывание, выгравированное на крышке золотой шкатулки, должно быть ложным. Следовательно, портрет Порции должен находиться в золотой шкатулке.

Придя к такому выводу, кандидат в женихи открывает золотую шкатулку. К его неописуемому ужасу шкатулка была пуста. Порция открывает серебряную шкатулку — портрет лежит в ней. В чем ошибка претендента?

Приведем объяснение Р. Смаллиана. Претенденту на руку Порции следовало бы понять, что без информации об истинности или ложности любого высказывания или об отношении принимаемых высказываниями значений истинности высказывания не позволяют прийти к какому-либо выводу и портрет может находиться где угодно.

Что мешает вам взять любое число шкатулок, положить в одну из них какой-нибудь предмет и сделать на крышках любые надписи, какие только вам заблагорассудится? Эти надписи не будут нести в себе никакой информации о предмете, спрятанном в одной из шкатулок.

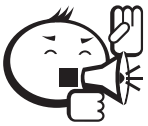
Ошибка претендента заключается также в том, что каждое из высказываний, выгравированных на крышках шкатулок, он считал либо истинным, либо ложным. На крышке золотой шкатулки было выгравировано: «Портрет не в этой шкатулке». Это высказывание заведомо либо истинно, либо ложно, так как портрет либо находится в золотой шкатулке, либо его там нет. В действительности, оно оказалось истинным, так как Порция положила портрет в серебряную шкатулку.

Теперь предположим, что нам известно, что Порция положила портрет в серебряную шкатулку. Что можно сказать о высказывании, выгравированном на крышке этой шкатулки? Истинно оно или ложно? Оказывается, оно не может быть ни истинным, ни ложным, так как в любом случае мы приходим к противоречию (проведите рассуждение самостоятельно). На этом Р. Смаллиан заканчивает обсуждение своей задачи.

Об отношении математической логики к реальному миру говорит следующая цитата из книги ***Ю. И. Манина***[1] [15]: «*Предметом логики не является внешний мир, но лишь системы его осмыслевания. Логика одной из таких систем — математики — в силу своей нормализованности представляет подобие жесткого трафарета, который можно накладывать на любую другую систему. Соответствие или расхождение этого трафарета с системой, однако, не служит критерием ее пригодности либо мерилом ценности. Физик не обязан быть ни последовательным, ни непротиворечивым — он должен эффективно описывать природу на определенных уровнях. Тем менее логичны естественные языки и непосредственная работа сознания. Вообще логичность как условие эффективности появляется лишь в узкоспециализированных сферах человеческой деятельности*».

Иногда создается впечатление, что новые математические теоремы получаются путем сочетания других, уже известных. Заслуга их авторов в том, что они обладали достаточными способностями, чтобы правильно объединить нужные теоремы и применить правила логики. Однако сама по себе логика ничего не производит: нужно что-то, что заставило бы ее работать, и это «что-то» — результат интуиции, аналогий, проб и ошибок. Именно в том, чтобы заставить логику работать, и заключается математическое творчество.

Вспомним классификацию Г. Штейнгауза из параграфа 1.2. Какой математикой занимается математическая логика? Математикой «α» и «γ» — когда открываются и доказываются новые утверждения или когда математику применяют в других науках. Если мы решаем типичные задачи, используя определенный шаблон, или вычисляем по заданным правилам, т. е. осуществляем математику «β» и «δ», то математическая логика не нужна. Достаточно просто быть последовательным.



Если кратко сказать о соотношении математики и логики к реальному миру, то справедлив следующий тезис: *Математика и логика изучают все воображаемые миры, а естественные науки — только реальный мир*.

Контрольные вопросы по главе 1

1. Как дополнить посылки в силлогизме, приведенном Амбросом Бирсом (см. параграф 1.1), чтобы вывод не вызывал сомнения в правильности?
2. Шерлок Холмс в своих расследованиях преступлений действовал следующим образом. Для начала он тщательно изучал конкретную ситуацию, а лишь потом делал общий вывод, опираясь на свой предыдущий опыт, используя аналогии и рассматривая возможные варианты. В истории лите-

[1] Юрий Иванович Манин (родился в 1937 году) — российский математик, один из основоположников некоммутативной алгебраической геометрии и квантовой информатики.

ратуры не было персонажа, более прославившегося своими дедуктивными способностями. Заслуженно ли? Может быть, на самом деле он применял индуктивную логику?

3. Найдите ошибку в софизме «карта России».
4. В чем различия между логической ошибкой, софизмом и парадоксом?
5. Какую математику («α», «β», «γ», «δ» — по классификации Г. Штейнгауза) будет применять выпускник ТУСУРа в своей инженерной деятельности?
6. Что изучает логика?

Рекомендуемая литература к главе 1

[1] Милль Дж. Ст. Система логики силлогистической и индуктивной: Изложение принципов доказательства в связи с методами научного исследования : пер. с англ. / Дж. Ст. Милль. — 5-е изд., испр. и доп. — М., 2011. — 832 с.

[2] Thurber James. The Thirteen Clocks / James Thurber. — Simon & Schuster, 1950. — 124 p.

[3] Бирс Амброз. Словарь Сатаны / Амброз Бирс. — М. : Центрполиграф, 2003.

[4] Рассел Б. Философский словарь разума, материи и морали / Б. Рассел. — Киев : Изд-во Port-Royal, 1996.

[5] Непейвода Н. Н. Прикладная логика : учеб. пособие / Н. Н. Непейвода. — 2-е изд., испр. и доп. — Новосибирск : Изд-во Новосиб. ун-та, 2000. — 521 с.

[6] Никифоров А. Книга о логике / А. Никифоров. — М. : Гнозис, 1996.

[7] Попов Г. Ошибка в проекте. Ленинский тупик / Г. Попов. — М. : Издательский дом Международного университета в Москве, 2008. — 512 с.

[8] Успенский В. А. Апология математики / В. А. Успенский. — СПб. ; Амфора, 2009. — 554 с.

[9] Александр Емельяненков. С учёным видом. Как за 4,5 тысячи рублей в журнале опубликовали заведомую галиматью // Российская газета. — 2008. — N 4782. — URL : http://www.rg.ru/2008/10/29/journal-nauka.html (дата обращения 08.05.2015).

[10] Лем С. Сумма технологии / С. Лем. — М. : АСТ ; СПб. : TerraFantastica, 2002. — 668 с.

[11] Харди Г. Г. Апология математика / Г. Г. Харди. — Ижевск : НИЦ «Регулярная и хаотическая динамика», 2000. — 104 с.

[12] Зюзьков В. М. Ленивое функциональное программирование : учеб. пособие / В. М. Зюзьков. — 2-е изд., перераб. и доп. — 2007. — 294 с.

[13] Штейнгауз Г. Математика — посредник между духом и материей : пер. с польск. / Г. Штейнгауз. — М. : БИНОМ. Лаборатория знаний, 2005. — 351 с.

[14] Смаллиан Р. Как же называется эта книга? / Р. Смаллиан. — М. : Мир, 1981. — 238 с.

[15] Манин Ю. И. Доказуемое и недоказуемое / Ю. И. Манин. — М. : Мир ; Советское радио, 1979. — 168 с.

Глава 2

КРАТКАЯ ИСТОРИЯ ЛОГИКИ

Но внезапно я услышал голос властный и певучий.
Повторялся Вечный Шепот днем и ночью: «Впереди
что-то ждет тебя. Не бойся. Поищи за дальней кручей.
Отправляйся и отыщешь. Что-то ждет тебя. Иди!».

Р. Киплинг. Первооткрыватель

2.1 Становление логики

Многие науки зародились в античной Греции, и логика не была исключением. Например, Фалес (ок. 625–547 гг. до н. э., рис. 2.1) и Пифагор (570–490 гг. до н. э., рис. 2.2) использовали логические рассуждения в математике.

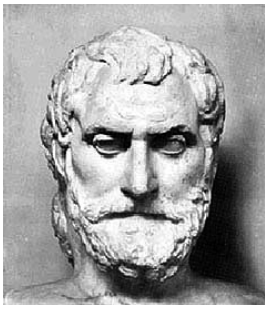


Рис. 2.1 – Фалес

Фалес традиционно считается основоположником греческой науки, и его именем названа геометрическая теорема: *если параллельные прямые, пересекающие стороны угла, отсекают равные отрезки на одной его стороне, то они отсекают равные отрезки и на другой его стороне*.

Пифагор создал религиозно-философскую школу пифагорейцев. В основе вещей лежит число, учил Пифагор, познать мир — значит, познать управляющие им числа. Изучая числа, пифагорейцы разработали числовые отношения и нашли их во всех областях человеческой деятельности. Античные авторы отдают Пифагору авторство известной теоремы: квадрат гипотенузы прямоугольного треугольника равняется сумме квадратов катетов. В рядах его школы была доказана теорема, утверждающая, что длина диагонали единичного квадрата не представима в виде отношения целых чисел. При этом использовался метод доказательства от противного (см. главу 7). Утверждение этой теоремы поколебало взгля-

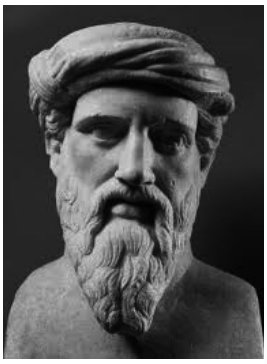


Рис. 2.2 – Пифагор

ды пифагорейцев на число, поскольку они не знали других чисел, кроме целых или отношений целых чисел (рациональных).

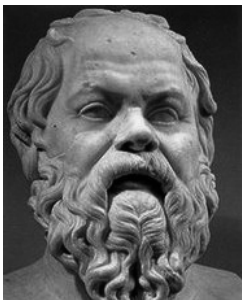


Рис. 2.3 – Сократ

Сократ (ок. 469–399 гг. до н. э., рис. 2.3) и Платон (ок. 427–347 гг. до н. э., рис. 2.4) применяли рассуждения математического типа в философских вопросах.

Многие высказывания, традиционно относимые к историческому Сократу, характеризуются как «парадоксальные», потому что они, с логической точки зрения, вроде бы противоречат здравому смыслу. К числу так называемых сократовских парадоксов относятся фразы:

Никто не желает зла.

Никто не делает зла по своей воле.

Добродетель — это знание.

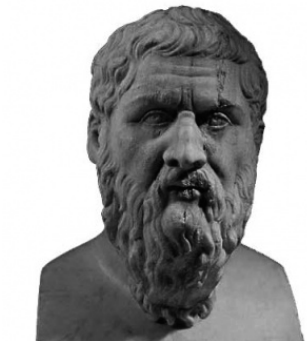


Рис. 2.4 – Платон

«Сократовыми парадоксами» также могут называться самоссылающиеся парадоксы, образцом которых является фраза в отношении знания, также приписываемая Сократу: «Я знаю только то, что ничего не знаю, но другие не знают и этого».

Свои приёмы исследования Сократ сравнивал с «искусством повивальной бабки»; его метод вопросов, предполагающих критическое отношение к догматическим утверждениям, получил название «*сократовской иронии*». Сократ своих учеников приводил к истинному суждению через *сократовский диалог*, где задавал общий вопрос, получив ответ, задавал следующий уточняющий вопрос и так далее до окончательного ответа.

От Платона идет ***реализм*** (другими словами, математический платонизм) — философское направление в математике, последователи которого считают, что математические объекты (сущности) существуют независимо от математиков. Большинство современных математиков, поддерживают эту позицию.

Рис. 2.5 – Аристотель

Но настоящим основателем классической логики был Аристотель (384–322 гг. до н. э., рис. 2.5).

Аристотель впервые сформулировал законы логики — ***законы правильного мышления***. Он рассматривал логику как (научный) инструмент для познания мира. Используя геометрию как модель, он обнаружил, что научные знания состоят из ***доказательств***, доказательства из ***силлогизмов***, силлогизмы из ***утверждений***, утверждения из ***термов***.

Открытые им силлогизмы являются схемами (законами) рассуждений. Они содержат исходные утверждения (***посылки)*** и утверждение — ***заключение***. Силлогизм устроен таким образом, что если мы принимаем посылки (считаем их истинами), то мы должны принять заключение (должны считать его истинным).

Пример

Вот классический пример наиболее известного силлогизма: *Все люди смертны, Сократ — человек, следовательно, Сократ смертен*.

Другой пример этого же силлогизма был приведен в первой главе — утверждение, в котором заключение — «*у Геракла — деревянные ноги*».

Знаменитый математик древности Евклид (III в. до н. э., рис. 2.6), строго говоря, не был логиком, но его вклад в логику неоспорим.

Рис. 2.6 – Евклид

Главная работа Евклида «Начала» (в латинизированной форме — «Элементы») содержит изложение планиметрии, стереометрии и ряда вопросов теории чисел; в ней он подвёл итог предшествующему развитию греческой математики и создал фундамент дальнейшего развития математики. До сих пор классическая геометрия называется в его честь евклидовой. Его величайшим достижением была логическая организация геометрических утверждений в совокупность аксиом и теорем.

Евклид начал изложение геометрии с ***аксиом*** (некоторые из них с наиболее сложной формулировкой и связанные с геометрическими построениями назывались им ***постулатами***) — истинных утверждений, которые, по его мнению, просты и самоочевидны. Используя аксиомы, он доказывал ***теоремы*** — истинные утверждения, более сложные и не очевидные.

Возможно, создание никакого другого учебника не имело столь радикальных последствий для развития всей человеческой мысли на протяжении последующих двух тысяч лет. «Начала» Евклида стали предтечей современных формальных (аксиоматических) систем.

Греческие гении Пифагор, Платон и Евклид решительно отклонили попытки экспериментального поиска геометрической истины, которую они считали в высшей степени объективной, в противоположность всему, что говорят о мире наши ощущения, подвластные иллюзиям и ежеминутно показывающие каждому все новый образ этого мира.

В то время когда последователи Аристотеля продолжали его труд, связанный с логикой силлогизмов, другая греческая школа философов, стоики, исследовали другой подход. Они изучали так называемые ***условные утверждения***, имеющие форму *если..., то...* Например,

Если облака собираются на западе, то будет дождь.

С помощью условных утверждений проводились логические рассуждения.

Пример

Посылки:

Если облака собираются на западе, то будет дождь.
Облака собираются на западе.

Заключение:

Будет дождь.

Используемый в данном примере логический закон рассуждения стал называться ***modus ponens*** (модус поненс).

Определенно, имеется связь между подходами в логических рассуждениях у Аристотеля и стоиков, поэтому после столетия независимого развития эти подходы слились вместе в рамках одной дисциплины.

Независимо возникла буддистская логика, но дальнейшее развитие логики в Европе имеет своим исходным пунктом изучение Аристотеля.

Рис. 2.7 – Фрэнсис Бэкон

Средневековая логика в Европе развивалась главным образом в направлении схоластической интерпретации сочинений Аристотеля, а сама логика часто использовалась для утверждения и обоснования догматов веры. В эпоху возрождения Фрэнсис Бэкон (1561–1626 гг., рис. 2.7) — английский философ — задался амбициозной целью построить логику открытия в опытных науках с помощью разработанных им методов индуктивного исследования: сходства, различия, остатков и сопутствующих изменений. Силлогистика, по мнению Бэкона, является бесполезной для открытия новых истин; в лучшем случае она может служить лишь для оправдания и обоснования их.

После возникновения в математике анализа бесконечно малых возродился интерес к дедуктивной логике.

Математическая логика с внешней стороны отличается от «обычной» тем, что она широко пользуется языком математических и логических знаков, исходя из того, что в принципе они могут совсем заменить слова обычного языка и принятые в обычных живых языках способы объединения слов в предложения.

Довольно рано возникла идея о том, что, записав все исходные допущения на языке специальных знаков, похожих на математические, можно заменять рассуждение вычислением. Точно же сформулированные правила таких логических вычислений можно перевести на язык вычислительной машины, которая тогда будет способна автоматически выдавать интересующие нас следствия из введенных в нее исходных допущений.

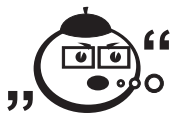
Своего рода «логическую машину» сконструировал еще в средние века Раймунд Луллий (1235–1315 гг.), дав ей, впрочем, лишь совершенно фантастические применения.

Рис. 2.8 – Готфрид Вильгельм Лейбниц

Более определенный и близкий к реально осуществленному впоследствии замысел универсального логического исчисления развивал Готфрид Вильгельм Лейбниц (1646–1716 гг., рис. 2.8) — немецкий философ, логик, математик. Лейбниц надеялся даже, что в будущем философы вместо того, чтобы бесплодно спорить, будут брать бумагу и вычислять, кто из них прав.

Готфрид Лейбниц считал, подобно Аристотелю, что логика может стать независимым орудием для научного познания мира. Он был первым, кто продвинул логику вперед после Аристотеля. Он пытался записывать логические утверждения в символическом виде, надеясь свести рассуждения к манипулированию символами, к вычислениям. Это была первая попытка создать символическую логику.

Лейбниц надеялся, что символическая логика преобразует философию, политику и даже религию в чистые исчисления, обеспечивая заслуживающий доверия метод для получения объективных ответов на все жизненные задачи.



В самой известной цитате из работы «Искусство открытия» (1685 г.) Лейбниц говорит: «Это единственный способ исправить наши рассуждения, чтобы сделать их также ясными как у математиков, так что мы могли бы найти ошибку с первого взгляда, а когда возникают споры, мы могли бы просто сказать: «Давайте вычислим и увидим, кто прав».

В 1686 году было издано философское эссе Готфрида Лейбница «Рассуждения о метафизике» (Discours de metaphysique), в котором поставлен вопрос: как отличить факты, которые можно описать неким законом, от фактов, никаким законам не подчиняющихся? В четвертом разделе своего эссе Лейбниц высказал очень простую и глубокую мысль: теория должна быть проще данных, которые она объясняет, иначе она не объясняет ничего. Концепция научного закона становится бессмысленной, если допускает неограниченный уровень математической сложности, потому что в таком случае всегда можно сформулировать закон независимо от того, насколько случайны и беспорядочны факты. И наоборот, если единственный закон, объясняющий какие-то данные, оказывается слишком сложным, то рассматриваемые данные на самом деле не подчиняются никакому закону.

Но его идеи были далеко впереди его времени, поэтому они не были восприняты современниками. Только через двести лет логики переоткрыли их и стали использовать.

2.2 Начало математической логики

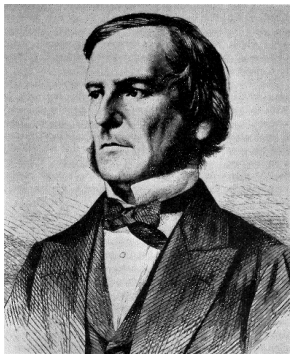


Рис. 2.9 – Джордж Буль

После своего зарождения большей частью логика изучалась неформально, т. е. без использования символов вместо слов. Но в конце XIX столетия математики развили ***символическую логику***, в которой вычисляемые символы заменили слова и утверждения. Три ключевых вклада в символическую логику сделали Джордж Буль (1815–1864 гг., рис. 2.9) — английский математик и логик, Георг Кантор (1845–1918 гг., рис. 2.10) — немецкий математик и Готлоб Фреге (1848–1825 гг., рис. 2.11) — немецкий логик, математик и философ.

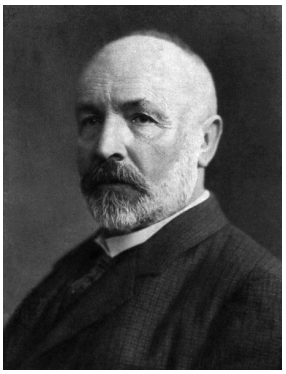


Рис. 2.10 – Георг Кантор

Рис. 2.11 – Готлоб Фреге

Названная так по имени ее открывателя, ***булева алгебра*** была первой разработанной системой, которая рассматривала логику как исчисление. Поэтому булеву алгебру можно считать предшественником математической логики. Булева алгебра подобна стандартной арифметике — два значения: 0 и 1 (ложь и истина) и две операции: умножение и сложение (конъюнкция и дизъюнкция). Буль не считал логику разделом математики, но находил глубокую аналогию между символическим методом алгебры и символическим методом представления логических форм и силлогизмов.

Пример

Пусть имеется два утверждения: A и B соответственно:

A: «*Волга впадает в Каспийское море*»;

B: «*Ангара впадает в озеро Байкал*».

Так как первое утверждение истинное, а второе ложное, мы можем сказать: $A = 1$ и $B = 0$.

В булевой алгебре сложение интерпретируется как «*или*», так что утверждение

«*Волга впадает в Каспийское море или Ангара впадает в озеро Байкал*»

вычисляется как $A + B = 1 + 0 = 1$.

Так как булевское выражение имеет значение 1, то это утверждение — истина.

Георг Кантор — первооткрыватель теории множеств, влияние которой на логику и математику трудно переоценить.

Неформально говоря, любое ***множество*** есть просто совокупность (собрание) некоторых объектов (элементов), которые могут иметь что-то общее между собой, или между элементами может не быть ничего общего.

Пример

Пять примеров множеств:

- $\{2, 3, 5, 7, 11, 13, 17, 19, \ldots\}$ — бесконечное множество, содержащее все простые числа;
- {пешка, конь, слон, ладья, ферзь, король};
- $\big\{\{1, 2\},\ \{3, 4\},\ \{1, 2, 3\}\big\}$ — множество из трех элементов, которые сами являются множествами;
- {Африка, Байкал, ноябрь, дыхание, Млечный путь, красота};
- множество людей, погибших во Второй мировой войне.

Простая конструкция множеств является чрезвычайно эффективной для описания важных и фундаментальных идей логики. Например, рассмотрим утверждение:

«*Названия всех штатов США, содержащие букву z, начинаются с буквы A*».

Это утверждение можно проверить, определив два множества:

- множество всех штатов, названия которых содержат букву *z*;
- множество штатов, названия которых начинается с буквы *A*.

Множество 1: {Arizona}

Множество 2: {Alabama, Alaska, Arizona, Arkansas}

Как вы видите, каждый элемент первого множества является элементом второго множества. Поэтому первое множество является ***подмножеством*** второго множества, так что исходное утверждение истинно.

Несмотря на очевидную простоту — или, скорее, благодаря этой простоте — теория множеств вскоре стала основанием логики и, более того, основанием современной математики. Но нельзя сказать, что теорию множеств математики — современники Кантора — все восприняли с воодушевлением. После публикации идей Кантора об актуальной бесконечности, теоретико-множественный подход встретил острое неприятие многими крупными математиками того времени. Основными оппонентами в то время были немецкие математики Герман Шварц (1843–1921 гг.) и, в наибольшей степени, Леопольд Кронекер (1823–1891 гг.), полагавший, что математическими объектами могут считаться лишь натуральные числа и то, что к ним

непосредственно сводится (известна его фраза о том, что «Бог создал натуральные числа, а всё прочее — дело рук человеческих»).

Тем не менее к концу XIX века теория множеств стала общепризнанной после успешного использования теории множеств в анализе, а также особенно после широкого применения Давидом Гильбертом теоретико-множественного инструментария.

Теория множеств детально излагается в главе 3.

Готлоб Фреге ввел первые реальные системы формальной логики: логику высказываний и объемлющую её логику предикатов.

Логика высказываний, называемая также ***пропозициональной логикой*** (см. главу 4), использует буквы для обозначения простых утверждений (высказываний), которые соединяются вместе в сложное высказывание с помощью логических операций (связок).

Пять операций логики высказываний в русском языке можно передать словами: «не», «и», «или», «если…, то», «тогда и только тогда».

Пример

Пусть имеются
высказывание A: «Лена едет в трамвае»,
высказывание B: «Петя находится дома».
Тогда мы можем определить сложные высказывания:
«Лена едет в трамвае *и* Петя находится дома»;
«*Если* Лена *не* едет в трамвае, *то* Петя находится дома».
Полученные высказывания символически обозначаются формулами:

$$A\&B, \quad \neg A \to B.$$

В первой формуле символ & обозначает «и», во втором высказывании символ $\neg$ заменяет «не», а символ $\to$ обозначает «если…, то».

Более сложная система, ***логика предикатов***, расширяет логику высказываний. Используются буквы (слова) для именования объектов (предметов) из некоторой предметной области и имена для предикатов. Предикаты обозначают свойства объектов или отношения между объектами.

Пример

Пусть предикат $M(x)$ обозначает свойство людей «x едет в трамвае», а предикат $H(x)$ обозначает свойство людей «x находится дома». При этих обозначениях высказывания, записанные в виде формул пропозициональной логики $A\&B$ и $\neg A \to B$, в логике предикатов записываются теперь как

$$M(\text{Лена}) \ \& \ H(\text{Петя}),$$
$$\neg M(\text{Лена}) \to H(\text{Петя}).$$

Кроме пропозициональных операций логика предикатов содержит две операции, называемыми ***кванторами***, которые служат для обозначения дополнительных конструкций, позволяющих создавать более сложные формулы. Кванторы в формулах заменяют выражения вида «для всех» и «некоторый». Например, они позволяют представить утверждения:

«*Все люди едут в трамвае*»,
«*Некоторые люди находятся дома*»

в виде формул $\forall x M(x)$ и $\exists x H(x)$ соответственно.

Логика предикатов — наиболее общий язык для классической математической логики (есть и неклассические логики) — описан в главе 5.

В конце XIX века, следуя примеру Евклида, математики стремились свести все в математике к множеству теорем, логически выводимых из небольшого числа аксиом. Фреге обнаружил возможность того, что сама математика может быть выведена из логики и теории множеств. Начиная с нескольких аксиом о множествах, он показал, что числа и, в конечном счете, вся математика следуют логически из этих аксиом.

Теория Фреге удовлетворительно работала до тех пор, пока Бертран Рассел (1872–1970 гг., рис. 2.12) — не обнаружил парадокс, названный впоследствии его именем (см. главу 3). Фреге не нашел как освободиться от этого противоречия.

Но Рассел сумел избавиться от подобных парадоксов в теории множеств. В 1910–1913 годы Бертран Рассел и Альфред Уайтхед (1861–1947 гг., рис. 2.13) написали фундаментальный труд «Principia Mathematica», в котором, используя идеи Фреге, обосновали математику на аксиомах теории множеств и логики.

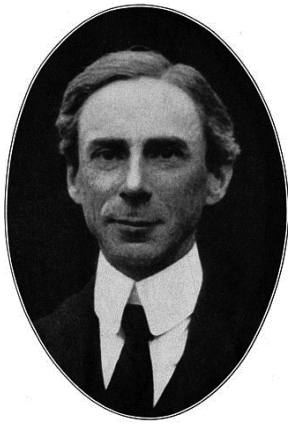


Рис. 2.12 – Бертран Рассел — философ, математик

Рис. 2.13 – Альфред Уайтхед — философ, математик, логик

2.3 Математическая логика в своем блеске и великолепии

Геттингенская программа

Рис. 2.14 – Давид Гильберт

В двадцатых годах XX века с программой обоснования математики на базе математической логики выступил знаменитый немецкий математик Гильберт (1862–1943 гг., рис. 2.14) — немецкий математик-универсал.

Гильберт, вокруг которого сложилась к тому времени школа блестящих последователей, в целой серии работ наметил план исследований в области оснований математики, получивший впоследствии название «Геттингенской программы».

В максимально упрощенном виде ее можно изложить следующим образом: математику можно представить в виде набора следствий, выводимых из некоторой системы аксиом, и доказать, что:

1. Математика является ***полной***, т. е. любое математическое утверждение можно доказать или опровергнуть, основываясь на правилах самой дисциплины.
2. Математика является ***непротиворечивой***, т. е. нельзя доказать и одновременно опровергнуть какое-либо утверждение, не нарушая принятых правил рассуждения.
3. Математика является ***разрешимой***, т. е., пользуясь правилами, можно выяснить относительно любого математического утверждения, доказуемо оно или опровержимо.

Фактически программа Гильберта стремилась выработать некую общую процедуру для ответа на все математические вопросы или хотя бы доказать существование таковой.

Сам ученый был уверен в утвердительном ответе на все три сформулированных им вопроса: по его мнению, математика действительно была полной, непротиворечивой и разрешимой. Оставалось только это доказать.

С этого времени и начинается современный этап развития математической логики, характеризующийся применением точных математических методов при изучении формальных аксиоматических теорий.

Заметим, что роль логического исчисления как средства открытия новых истин даже в области математики долго оставалась более чем скромной. Зато символический язык математической логики оказался на границе девятнадцатого и двадцатого веков очень важным подспорьем в изучении логических основ математики, поскольку он позволял избегать всякой неточности мысли, которая легко проскальзывает при использовании слов обычного языка, смысл которых дается не точным определением, а созданием привычки к принятому словоупотреблению.

Теоремы Гёделя

«Principia Mathematica», труд Рассела и Уайтхеда, строго обосновал математику на основе логики, но сюрпризы были обнаружены в самой логике.

Для любой математической теории, определенной с помощью множества аксиом, возникают два вопроса: является ли теория непротиворечивой и полной. Непротиворечивость теории означает, что, делая логические следствия из аксиом, мы получаем только истинные утверждения. Полнота означает, что все истинные утверждения теории можно вывести из ее аксиом.

В 1931 году Курт Гёдель (1996–1978 гг., рис. 2.15) — австрийский логик и математик — доказал, что бесконечное множество математических утверждений являются истинными, но не могут быть доказаны, исходя из аксиом «Principia Mathematica». Он также установил, что попытка свести математику к непротиворечивой системе аксиом дает тот же самый результат: существует бесконечное множество математических истин, называемых ***неразрешимыми*** утверждениями, которые недоказуемы с помощью этой системы.

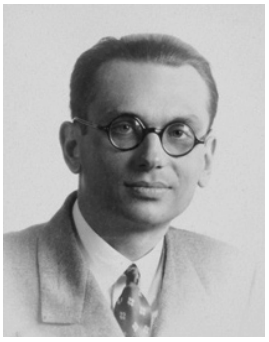


Рис. 2.15 – Курт Гёдель

Этот результат, называемый ***теоремой о неполноте***, сразу выдвинул Гёделя в число великих математиков XX века.

Второй результат — ***теорема о непротиворечивости*** — утверждает, что непротиворечивость любой аксиоматической теории не может быть доказана средствами самой теории.

В сущности, теорема Гёделя о неполноте похоронила надежды Лейбница о существовании логического метода, который мог бы вычислить ответ на все научные вопросы. Логика, по крайней мере в настоящем виде, недостаточна, чтобы доказать каждую математическую истину, тем более любую истину в нашем мире.

Теоремы Гёделя показали, что Геттингенская программа Гильберта нереализуема.

Неклассическая логика

Сведение математики и логики к небольшому списку аксиом естественно вызвало вопрос: что произойдет, если исходные аксиомы будут другими?

Например, позволить утверждениям иметь не только два истинностных значения «истина» и «ложь», но и третье значение, выражаемое словами «возможно» («вероятно», «нейтрально»). Другими словами, отказаться от аксиомы «Закон исключенного третьего» (см. главу 6). Древние греки считали невыполнение этого закона немыслимым нарушением логических рассуждений, но описание логики просто как аксиоматической системы (теории) сделало это допустимым.

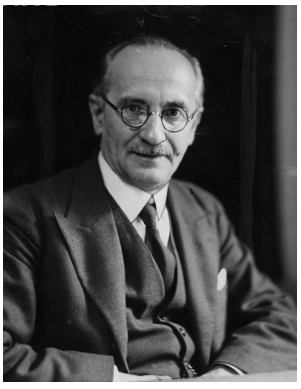


Рис. 2.16 – Ян Лукасевич

В 1917 году Ян Лукасевич (1878–1956 гг., рис. 2.16) — польский логик, был первым, кто стал рассматривать *многозначные логики*, введя третье истинностное значение «возможно». В такой логике возможно определять истинностные значения утверждений, подобных следующему:

В 2030 году человечество колонизирует Марс.

Добавление значения «возможно» к «истина» и «ложь» стало первым радикальным отступлением от ***классической логики*** — всей той логики, которая была до этого. Возникла новая ветвь логики — ***неклассическая логика*** (см. [1]).

Эра компьютеров

Появление компьютеров связано с развитием такого раздела математической логики, как теория алгоритмов. Развитие мышления в области математических наук всегда было в наибольшей степени алгоритмичным по сравнению с прочими науками, тем не менее всеобщая компьютеризация еще более отчетливо выявила эту сторону математического мышления.

Не менее тесная связь методов математической логики и современных компьютеров прослеживается по следующим двум направлениям. Во-первых, математическая логика используется при физическом конструировании и создании компьютеров (алгебра высказываний и булевы функции — математический аппарат для конструирования переключательных и функциональных схем, составляющих элементную базу компьютеров).

Во-вторых, программное обеспечение современных компьютеров широко использует математическую логику. В основе многочисленных языков программирования лежат теория алгоритмов, теория формальных систем, логика предикатов. Такие парадигмы программирования, как логическое (язык Prolog) и функциональное программирование (язык Haskell), основаны на применении логических теорий: автоматического доказательства теорем и лямбда-исчисления соответственно. Кроме того, синтез логики и компьютеров привел к возникновению баз знаний и экспертных систем, что явилось важнейшим этапом на пути к созданию искусственного интеллекта — машинной модели человеческого разума.

Основной вклад в теорию алгоритмов сделали Чёрч и Тьюринг. Алонзо Чёрч (1903–1995 гг., рис. 2.17) американский математик и логик — прославился разработкой теории лямбда-исчисления, последовавшей за его знаменитой статьёй 1936 года, в которой он показал существование алгоритмически неразрешимых задач. Эта статья предшествовала знаменитому исследованию Алана Тьюринга на тему проблемы остановки, в котором также было продемонстрировано существование задач, неразрешимых механическими способами. Впоследствии Чёрч и Тьюринг показали, что лямбда-исчисления и машина Тьюринга имели одинаковые свойства, таким образом доказывая, что различные «алгоритмические процессы вычислений» могли иметь одинаковые возможности. Эта работа была оформлена как тезис Чёрча.

Алан Тьюринг (1912–1954 гг., рис. 2.18) — английский математик и логик — доказал, что проблема остановки для машины Тьюринга неразрешима: в общем случае невозможно алгоритмически определить, остановится ли когда-нибудь данная машина Тьюринга. Хотя доказательство Тьюринга было обнародовано в скором времени после эквивалентного доказательства Алонзо Чёрча, в котором использовалось лямбда-исчисление, сам Тьюринг был с ним не знаком. Подход Алана Тьюринга принято считать более доступным и интуитивным. Идея «Универсальной Машины», способной выполнять функции любой другой машины или, другими словами, вычислить всё, что можно в принципе вычислить, была крайне оригинальной.

В главе 8 мы более подробно познакомимся с работами Чёрча и Тьюринга.

Рис. 2.17 – Алонзо Чёрч

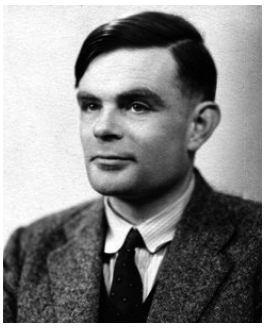


Рис. 2.18 – Алан Тьюринг

Бурбаки

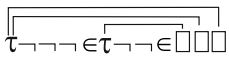
Николя Бурбаки (фр. *Nicolas Bourbaki*) — собирательный псевдоним, под которым группа математиков разных стран, преимущественно французских, выступила с проектом дать систематическое изложение современной математики на основе аксиоматического метода. Образовалась группа в 1935 году из бывших питомцев Высшей нормальной школы. Численность и точный состав группы не разглашался, но известно, что лидерами ее стали известные математики Андре Вейль, Жан Дельсарт, Жан Дьёдонне, Анри Картан и Клод Шевалле. В многотомном трактате «***Начала математики***» (Eléments de Mathématique), выходящем с 1939 года, развивается формальная аксиоматическая система, которая, по замыслу авторов, должна охватить главнейшие разделы математики. Основные принципы изложений: единство и полная формализация математики на основе теории множеств; систематичность; догматизм и самодостаточность; изложение, всегда идущее от общего к частному; ключевая роль понятия «структуры». Изложение носит сугубо абстрактный характер. Структуры определяются посредством аксиом, например: структуры порядка, группы, топологические структуры. Способ рассуждения — от общего к частному. Классификация математики, производимая по типам структур, значительно отличается от традиционной.

В книгах Бурбаки были впервые введены символ для пустого множества $\varnothing$; символы **N**, **Z**, **Q**, **R**, **C** для множеств натуральных, целых, рациональных, действительных и комплексных чисел; термины «*инъекция*», «*сюръекция*» и «*биекция*» (см. главу 3); знак «опасный поворот» на полях книги, показывающий, что данное место в доказательстве может быть неправильно понято.

В трактате все математические теории описываются на основании аксиоматической теории множеств в духе крайней абстракции. Например, определение обыкновенного натурального числа 1 в «Теории множеств» даётся следующим образом:

$$\tau_z\Big((\exists u)(\exists U)\Big(u = (U, \{\varnothing\}, Z) \text{ и } U \subset \{\varnothing\} \times Z$$
$$\text{и } (\forall x)\Big(\big(x \in \{\varnothing\}\big) \Rightarrow (\exists y)\big((x, y) \in U\big)\Big)$$
$$\text{и } (\forall x)(\forall y)(\forall y')\Big(\big((x, y) \in U \text{ и } (x, y') \in U\big) \Rightarrow (y = y')\Big)$$
$$\text{и } (\forall y)\Big((y \in Z) \Rightarrow (\exists x)\big((x, y) \in U\big)\Big)$$
$$\text{и } (\forall x)(\forall x')(\forall y)\Big(\big((x, y) \in U \text{ и } (x', y) \in U\big) \Rightarrow (x = x')\Big)\Big)\Big).$$

Причём, учитывая, что в этой записи уже сделаны сокращения, например пустое множество ∅ определяется в языке теории множеств Бурбаки как

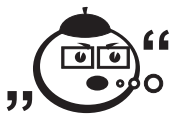


мы получаем, что полная запись обыкновенной единицы состоит из 4 523 659 424 929 символов [2]!

Деятельность этого коллектива принесла существенные плоды в таких областях математики, как топология, топологическая алгебра, алгебра, теория алгебраических чисел, функциональный анализ и др. Во Франции написано более 40 книг этого трактата. В 1959–1987 годах были переведены на русский язык более 20 томов. В 1968 году Бурбаки объявил о прекращении своей деятельности. Задуманный трактат остался незаконченным.

Математика XX века восприняла влияние формалистких взглядов Н. Бурбаки: «…стиль практически всех научных работ по математике в период от пятидесятых по семидесятые годы постепенно изменился в сторону формализации, стал в той или иной степени походить на формально-бурбакистскую манеру, притом, как правило, этот процесс происходил неосознанно» [3].

Строгость изложения в книгах Бурбаки в какой-то мере сформировала современный стандарт строгости математических текстов.



Г. Штейнгауз [4]*: «Но невозможно обучение математике по работам Николя Бурбаки, потому что ученики лишены способности познания той математики, которая представляет собой «нечто вроде экспериментальной физики», и поэтому преподаватели обязаны указывать одной рукой в уже пройденное прошлое, а другой — в еще неизвестное будущее…».*

Контрольные вопросы по главе 2

1. Существуют ли математические объекты независимо от математиков?
2. Для чего применяется алгоритм Евклида?
3. Какие идеи Лейбница были восприняты только через 200 лет после его смерти?
4. Кто является основателем булевой логики?
5. Как в информатике используется математическая логика?

Рекомендуемая литература к главе 2

[1] Непейвода Н. Н. Прикладная логика : учеб. пособие / Н. Н. Непейвода. — 2-е изд., испр. и доп. — Новосибирск : Изд-во Новосиб. ун-та, 2000. — 521 с.

[2] Mathias A. R. D. A Term of Length 4529659424929 / A. R. D. Mathias. — Synthese. — 2002. — N 133. — P. 75–86.

[3] Сосинский А. Б. Умер ли Бурбаки? // Математическое просвещение. — 1998. — Вып. 2.

[4] Штейнгауз Г. Математика — посредник между духом и материей : пер. с польск. / Г. Штейнгауз. — М. : БИНОМ. Лаборатория знаний, 2005. — 351 с.

Глава 3

ОСНОВЫ ТЕОРИИ МНОЖЕСТВ

Никто не изгонит нас из рая, который основал Кантор.

Давид Гильберт о теории множеств

3.1 Интуитивная теория множеств

Понятие множества является основным, неопределяемым понятием, поэтому мы можем его только пояснить, например с помощью следующего *псевдоопределения*. Под ***множеством*** S будем понимать любое собрание определенных и различимых между собою объектов, мыслимое как единое целое. Эти объекты называются ***элементами множества*** S.

В этом интуитивном определении, принадлежащем немецкому математику Георгу Кантору, существенным является то обстоятельство, что собрание предметов само рассматривается как один предмет, мыслится как единое целое. Что касается самих предметов, которые могут входить во множество, то относительно них существует значительная свобода. Это может быть множество студентов в аудитории, множество целых чисел, множество точек плоскости. Заметим, что канторовская формулировка позволяет рассматривать множества, элементы которых по той или иной причине нельзя точно указать (например, множество простых чисел, множество белых носорогов и т. п.). Не следует думать, что множество обязательно должно содержать в каком-то смысле однородные объекты. Можно объединить в одно множество и королей, и капусту.

Символом $\in$ обозначается ***отношение принадлежности***. Это понятие также не определяется формально. Запись $x \in S$ означает, что элемент x принадлежит множеству S. Если элемент x не принадлежит множеству S, то пишут $x \notin S$.

Г. Кантором сформулировано несколько интуитивных принципов, которые естественно считать выполняющимися для произвольных множеств.

Множество всех объектов x, обладающих свойством $A(x)$, обозначается $\{x \mid A(x)\}$. Если $Y = \{x \mid A(x)\}$, то $A(x)$ называется ***характеристическим свойством*** множества Y.

Интуитивный принцип абстракции. *Любое характеристическое свойство $A(x)$ определяет некоторое множество X, а именно множество тех и только тех предметов x, для которых выполнено свойство $A(x)$.*

Интуитивный принцип объемности. *Множества A и B считаются равными, если они состоят из одних и тех же элементов. (Часто это выражают словами: «Множества равны, если их характеристические свойства эквивалентны»).*

Записывают $A = B$, если A и B равны, и $A \neq B$ — в противном случае.

Пример 3.1

Проиллюстрируем принцип объемности. Множество A всех положительных четных чисел равно множеству B положительных целых чисел, представимых в виде суммы двух положительных нечетных чисел. Действительно, если $x \in A$, то для некоторого целого положительного числа m имеем $x = 2m$; тогда $x = (2m - 1) + 1$, т. е. $x \in B$. Если $x \in B$, то для некоторых целых положительных p и q имеем $x = (2p - 1) + (2q - 1) = 2(p + q - 1)$, т. е. $x \in A$.

Множество, элементами которого являются объекты $a_1, a_2, \ldots, a_n$ и только они, обозначают $\{a_1, a_2, \ldots, a_n\}$. Его определение через характеристическое свойство:

$$\{a_1, a_2, \ldots, a_n\} = \{x \mid x = a_1 \text{ или } x = a_2 \text{ или } \ldots \text{ или } x = a_n\},$$

где «или» является ***неразделительным***[1]. Исходя из этого тождества можно видеть, в частности, что

$$\{a, b\} = \{b, a\},\ \{a, a\} = \{a\}.$$

В общем случае порядок, в котором элементы расположены при описании множества, не имеет значения; не имеет значения также возможность неоднократного повторения одних и тех же элементов при описании множества.

Стоит отметить еще одну тонкость. Нужно строго различать x и $\{x\}$. Первое выражение обозначает сам элемент, а второе — множество, содержащее этот один элемент. Разница между ними примерно такая же, как между шимпанзе и шимпанзе, посаженным в клетку в зоопарке: $\{x\}$ скорее похоже на такую клетку, чем на ее обитателя.

[1] В русском языке «разделительное или» употребляется при соотнесении однородных членов предложения или целых предложений (по значению взаимоисключающих или заменяющих друг друга), указывая на необходимость выбора между ними. Пример: Сходи в магазин и купи там яблоки или апельсины.

«Неразделительное или» употребляется, чтобы передать смысл «то или другое или оба вместе». Иногда письменно передается конструкцией «или/и». Пример: Целое число n делится на 2 или/и на 3.

*Множество A есть **подмножество** множества B (обозначается $A \subseteq B$), если каждый элемент A есть элемент B; т. е. если $x \in A$, то $x \in B$. В частности, каждое множество есть подмножество самого себя. Если A не является подмножеством B, то, значит, существует элемент A, не принадлежащий B. Отношение $\subseteq$ между множествами называется отношением **включения**.*

Следовательно, $\{1, 2, 3\} \subseteq \{1, 2, 3, 4\}$, но $\{1, 2, 5\}$ не является подмножеством множества $\{1, 2, 3, 4\}$. Если $A = \{x \mid x$ — футболист факультета$\}$, $B = \{x \mid x$ — спортсмен факультета$\}$, а $C = \{x \mid x$ — самый сильный математик факультета$\}$, то $A \subseteq B$, а C не является подмножеством B в общем случае.

Заметим, что имеют место утверждения для произвольных множеств:

а) $X \subseteq X$;

б) если $X \subseteq Y$, $Y \subseteq Z$, то $X \subseteq Z$;

в) если $X \subseteq Y$ и $Y \subseteq X$, то $X = Y$.

Теперь мы можем утверждать, что доказательство равенства множеств A и B состоит из двух этапов:

1. Доказать, что A есть подмножество B.
2. Доказать, что B есть подмножество A.

*Множество A есть **собственное подмножество** множества B (обозначается $A \subset B$), если $A \subseteq B$ и $A \neq B$. Если A не является собственным подмножеством B, то это означает, что либо $A = B$, либо существует элемент A, не принадлежащий B. Отношение $\subset$ между множествами называется отношением **строгого включения**.*

Пример 3.2

В математике широко используются следующие множества чисел (с соответствующими обозначениями):

- множество натуральных чисел — $\mathbf{N}$ (считаем, что $0 \in \mathbf{N}$);
- множество целых чисел — $\mathbf{Z}$;
- множество рациональных чисел — $\mathbf{Q}$;
- множество вещественных чисел — $\mathbf{R}$;
- множество комплексных чисел — $\mathbf{C}$.

Для этих множеств выполнены строгие включения: $\mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$. Очевидно, для произвольных множеств, если $X \subset Y$, $Y \subset Z$, то $X \subset Z$.

Не надо смешивать отношения принадлежности и включения. Например, имеем $\{1\} \in \{\{1\}\}$ и $\{1\}$ не является подмножеством $\{\{1\}\}$. С другой стороны, $1 \notin \notin \{\{1\}\}$, так как единственным элементом множества $\{\{1\}\}$ является элемент $\{1\}$.

Множество, не содержащее элементов, называется ***пустым*** *и обозначается* $\varnothing$.

Пустое множество есть подмножество любого множества. Очевидно, что пустое множество задается тождественно ложным характеристическим свойством, и соответственно все пустые множества равны. Поэтому считается, что множество квадратных кругов равно множеству белых ворон.

Множество всех подмножеств A называется ***множеством-степенью*** *и обозначается* $\boldsymbol{P}(A)$.

Пример 3.3

Если $A = \{1, 2, 3\}$, то $\boldsymbol{P}(A) = \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$.

В дальнейшем неоднократно будем пользоваться утверждением, что если множество A состоит из n элементов, то множество $\boldsymbol{P}(A)$ состоит из 2^n элементов.

Расплывчатость, недостаточность канторового определения понятия множества стала понятной, когда в 1879 году итальянский логик Бурали-Форти, а немного позже выдающийся философ и логик Бертран Рассел открыли парадоксы, связанные с понятием множества.

В математике рассматривается одна теория — теория множеств, которая длительное время претендовала на выразимость в ней всех математических понятий. В ней пытаются базироваться на одних лишь множествах, и тогда ее универсум (собрание, совокупность) должен быть множеством всех множеств. Но выяснилось, что принятие существования множества всех множеств приводит к парадоксам.

Так, например, одна из аксиом «наивной» теории множеств: если X — множество, то для любого условия A имеем $\{x \mid x \in X \text{ и } A(x)\}$ — также множество. Выберем теперь свойство A следующим образом: $A(x)$ — «x не содержит себя в качестве элементов». Примером множества, обладающего свойством A, служит, например, любое конечное множество. Если обозначить через $\boldsymbol{U}$ универсум — множество всех множеств, то тогда можно определить множество

$Y = \{x \mid x \in \boldsymbol{U} \text{ и } A(x)\} = \{x \mid x \in \boldsymbol{U} \text{ и } x \notin x\}$. Спрашивается, выполняется ли $Y \in Y$ или $Y \notin Y$? Любое из этих двух предположений влечет противоположное утверждение.

. . . . . .

Этот парадокс впервые обнаружил Бертран Рассел. Другая, более популярная форма этого парадокса известна как парадокс брадобрея (см. параграф 1.3 главы 1).

Парадокс Рассела и другие трудности, связанные с неограниченным использованием абстрактных понятий в математике, свидетельствовали о кризисе математики на рубеже XIX и XX веков. В частности, о том, что широко используемая теория множеств в ее интуитивном, «наивном» изложении является противоречивой. Например, для устранения таких противоречий и парадоксов для теории множеств были предложены аксиоматические теории (см. главу 6).

3.2 Операции над множествами. Диаграммы Эйлера—Венна

Рассмотрим методы получения новых множеств из уже существующих.

. . . . . .

Объединением *множеств A и B называется множество $A \cup B$, все элементы которого являются элементами множества A или/и B:*

$$A \cup B = \{x \mid x \in A \text{ или/и } x \in B\}.$$

Пересечением *множеств A и B называется множество $A \cap B$, элементы которого являются элементами обоих множеств A и B:*

$$A \cap B = \{x \mid x \in A \text{ и } x \in B\}.$$

. . . . . .

Очевидно, что выполняются включения $A \cap B \subseteq A \subseteq A \cup B$ и $A \cap B \subseteq B \subseteq A \cup B$. Говорят, что два множества ***не пересекаются***, если их пересечение — пустое множество.

. . . . . .

Относительным дополнением *множества A до множества X называется множество $X \setminus A$ всех тех элементов множества X, которые не принадлежат множеству A:*

$$X \setminus A = \{x \mid x \in X \text{ и } x \notin A\}.$$

Симметрическая разность $A \Delta B$ *состоит из элементов, которые принадлежат ровно одному из множеств A и B:*

$$A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B).$$

Множество $X \setminus A$ называют также ***разностью множеств*** *X и A.*

. . . . . .

Операцию абсолютного дополнения, как правило, вводят лишь тогда, когда фиксирован универсум $\boldsymbol{U}$ (в данном случае под универсумом понимается некоторое множество, для которого все рассматриваемые в определенном контексте множества являются подмножествами).

Абсолютным дополнением *множества A называется множество $\overline{A}$ всех тех элементов x, которые не принадлежат множеству A:*

$$\overline{A} = \{x \mid x \in \boldsymbol{U} \text{ и } x \notin A\}.$$

Заметим, что $\overline{A} = \boldsymbol{U} \backslash A$. Часто вместо $\overline{A}$ будем писать $\neg A$ (символ $\neg$ используется также для обозначения отрицания в логике высказываний (см. главу 4).

Первым стал использовать теперь общепринятые обозначения операций над множествами Пеано[1] (1888 г.).

При решении целого ряда задач Эйлер[2] (рис. 3.1) использовал идею изображения множеств с помощью кругов. В этом случае множества обозначают кругами или просто овальными областями на плоскости и внутри этих областей условно располагают элементы множества. Часто все множества на диаграмме размещают внутри квадрата, который представляет собой универсум $\boldsymbol{U}$. Если элемент принадлежит более чем одному множеству, то на диаграмме области, отвечающие таким множествам, должны перекрываться, чтобы общий элемент мог одновременно находиться в соответствующих областях (рис. 3.2).

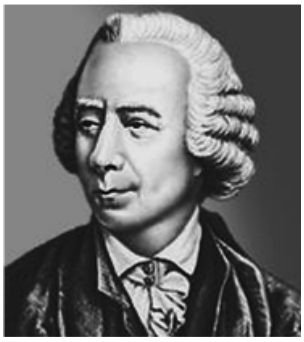


Рис. 3.1 – Леонардо Эйлер

Здесь не имеет значения относительный размер кругов либо других замкнутых областей, но лишь их взаимное расположение. Безусловно, такие диаграммы могут играть в математике лишь ту роль, что чертежи в геометрии: они иллюстрируют, помогают представить и доказать.

Объединение, пересечение и дополнение обычно называются ***булевыми операциями***, составленные из множеств с их помощью выражения — ***булевыми выражениями***, значение такого выражения — ***булевой комбинацией*** входящих в него множеств, а равенство двух булевых выражений — ***булевыми тождествами***.

[1] Джузеппе Пеано (1858–1932 гг.) — итальянский математик. Внёс вклад в математическую логику, аксиоматику, философию математики.

[2] Леонард Эйлер (1707 г., Швейцария — 1783 г., Санкт-Петербург, Российская империя) — швейцарский, немецкий и российский математик и механик, внёсший фундаментальный вклад в развитие этих наук. Почти полжизни провёл в России.

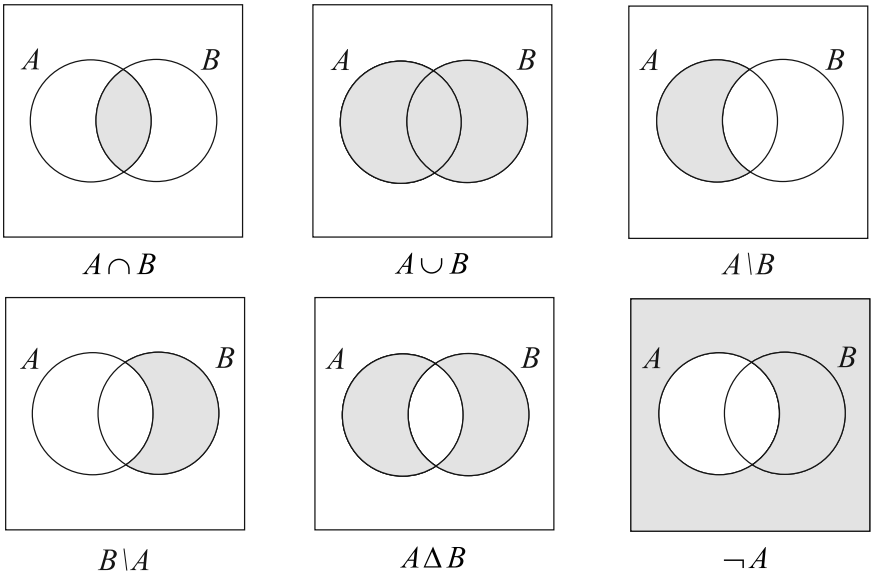


Рис. 3.2 – Операции над множествами

Теорема 1. Для любых подмножеств A, B и C универсума $\boldsymbol{U}$ выполняются следующие основные булевы тождества:

1. $A \cup B = B \cup A$ (коммутативность $\cup$).

1′. $A \cap B = B \cap A$ (коммутативность $\cap$).

2. $A \cup (B \cup C) = (A \cup B) \cup C$ (ассоциативность $\cup$).

2′. $A \cap (B \cap C) = (A \cap B) \cap C$ (ассоциативность $\cap$).

3. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (дистрибутивность $\cup$ относительно $\cap$).

3′. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (дистрибутивность $\cap$ относительно $\cup$).

4. $A \cup \varnothing = A$.

4′. $A \cap \boldsymbol{U} = A$.

5. $A \cup \neg A = \boldsymbol{U}$.

5′. $A \cap \neg A = \varnothing$.

6. $A \cup A = A$ (идемпотентность $\cup$).

6′. $A \cap A = A$ (идемпотентность $\cap$).

7. $A \cap \boldsymbol{U} = \boldsymbol{U}$.

7′. $A \cap \varnothing = \varnothing$.

8. $\neg(A \cup B) = \neg A \cap \neg B$.

8′. $\neg(A \cap B) = \neg A \cup \neg B$.

9. $A \cup (A \cap B) = A$.

9′. $A \cap (A \cup B) = A$.

Тождества 8 и 8′ называются законами де Моргана[1], а тождества 9 и 9′ — законами поглощения.

. . . . . .

Доказательство. Докажем тождество 3. Сначала покажем, что $A \cup (B \cap C)$ есть подмножество $(A \cup B) \cap (A \cup C)$. Действительно, если $x \in A \cup (B \cap C)$, то $x \in A$ или $x \in B \cap C$. Если $x \in A$, то $x \in A \cup B$ и $x \in A \cup C$. Следовательно, x принадлежит $(A \cup B) \cap (A \cup C)$. Если $x \in B \cap C$, то $x \in B$ и $x \in C$. Отсюда $x \in A \cup B$ и $x \in A \cup C$, а значит, $x \in (A \cup B) \cap (A \cup C)$. Теперь покажем, что выполнено $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. Если $x \in (A \cup B) \cap (A \cup C)$, то $x \in A \cup B$ и $x \in A \cup C$. Следовательно, $x \in A$ или $x \in B$ и $x \in C$, т. е. $x \in B \cap C$. Отсюда $x \in A \cup (B \cap C)$.

Докажем тождество 8. Пусть $x \in \neg(A \cup B)$. Тогда $x \in \boldsymbol{U}$ и $x \notin A \cup B$. Следовательно, $x \notin A$ и $x \notin B$. Отсюда $x \in \neg A$ и $x \in \neg B$, а значит, x принадлежит $\neg A \cap \neg B$. Итак, $\neg(A \cup B) \subseteq \neg A \cap \neg B$. Пусть теперь $x \in \neg A \cap \neg B$. Тогда $x \in \neg A$ и $x \in \neg B$. Следовательно, $x \in \boldsymbol{U}$ и $x \notin A$ и $x \notin B$. Значит, x не принадлежит $A \cup B$, т. е. $x \in \neg(A \cup B)$. Итак, $\neg A \cap \neg B \subseteq \neg(A \cup B)$.

Остальные тождества доказываются аналогично. Рекомендуется сделать это самостоятельно. Если какое-то тождество не выполняется для произвольных непустых множеств, то всегда можно построить контрпример, используя круги Эйлера. Но оказывается с помощью диаграмм можно и доказывать.

Для этого используются частный случай кругов Эйлера — диаграммы Венна[2]. При n, равном 2 и 3, диаграммы Венна обычно изображаются в виде кругов. Пусть даны множества $A_1, A_2, \ldots, A_n$, $n > 1$. Начертим диаграмму Венна, изображающую эти множества таким образом, чтобы все подмножества вида $Y_1 \cap Y_2 \cap \ldots \cap Y_n$, где Y_k обозначает либо A_k, либо $\neg A_k$, были не пусты. В этом случае всевозможные комбинации $Y_1 \cap Y_2 \cap \ldots \cap Y_n$ называются составляющими системы множеств $\{A_1, A_2, \ldots, A_n\}$.

. . . . . .

Составляющие системы множеств $\{A_1, A_2, \ldots, A_n\}$ *задаются следующим индуктивным определением.*

Базис. *Составляющие* $\{A_1\}$ *суть само* A_1 *и его дополнение.*

Шаг. *Если* S *— составляющая* $\{A_1, A_2, \ldots, A_{n-1}\}$, *то* $S \cap A_n$ *и* $S \cap \cap \neg A_n$ *— составляющие* $\{A_1, A_2, \ldots, A_n\}$.

Система множеств ***независима****, если все ее составляющие не пусты.*

. . . . . .

[1] Огастес де Морган (1806–1871 гг.) — шотландский математик и логик; к своим идеям в алгебре логики пришёл независимо от Дж. Буля.

[2] Этот вид диаграмм предложил и детально разработал Джон Венн (1834–1923 гг.) — английский логик и философ.

На рисунках 3.3, 3.4 изображены независимые системы множеств. Для $n = 4$ независимая система изображается четырьмя равными эллипсами или требуются невыпуклые фигуры. Для $n > 3$ диаграмму Венна кругами изобразить невозможно.

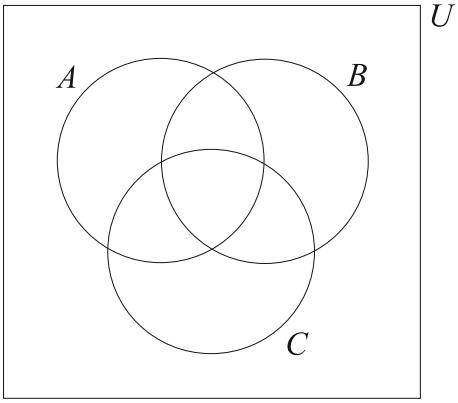


Рис. 3.3 – Диаграмма Венна для трех множеств

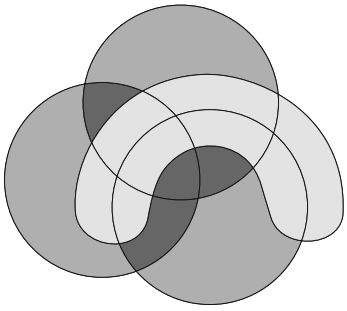


Рис. 3.4 – Диаграмма Венна для четырех множеств

Теорема 2 (Венн). Если булево тождество выполнено для некоторой независимой системы множеств, то оно выполнено для любой системы множеств.

Доказательство см. в [1, с. 79].

Теорема 3. Предложения о произвольных множествах A и B попарно эквивалентны:

1) $A \subseteq B$;
2) $A \cap B = A$;
3) $A \cup B = B$.

Доказательство. Докажем, что из первого предложения следует второе. Действительно, так как $A \cap B \subseteq A$, то достаточно показать, что в этом случае $A \subseteq A \cap B$. Но если $x \in A$, то $x \in B$, так как $A \subseteq B$, и, следовательно, $x \in A \cap B$.

Докажем, что из второго предложения следует третье. Так как $A \cap B$ равно A, то $A \cup B = (A \cap B) \cup B$. По закону поглощения (см. тождество 9) $B \cup (A \cap B) = B$. Отсюда, используя закон коммутативности, получаем равенство $A \cup B = B$.

Докажем, что из третьего предложения следует первое. Так как $A \subseteq A \cup B$, а по условию третьего предложения $A \cup B = B$, то $A \subseteq B$.

3.3 Отношения

Упорядоченная пара *<x, y> интуитивно определяется как совокупность, состоящая из двух элементов x и y, расположенных в определенном порядке. Две пары <x, y> и <u, v> считаются равными тогда и только тогда, когда x = u и y = v.*

Предыдущее определение апеллирует к таким неопределенным понятиям, как «совокупность» и «расположенные в определенном порядке». Для наших целей этого вполне достаточно. Но понятие «упорядоченная пара» можно определить точно, используя понятия «множество», «элемент» и «отношение принадлежности»[1].

Аналогично, мы определяем $<x_1, x_2, \ldots, x_n>$ — кортеж из n элементов $x_1, x_2, \ldots, x_n$, $n > 1$ (называют еще «упорядоченная n-ка»). Используется также соглашение: $<x_1, x_2, \ldots, x_n>$ совпадает по смыслу с парами

$$<<x_1, x_2, \ldots, x_{n-1}>, x_n> \text{ и } <x_1, <x_2, \ldots, x_{n-1}, x_n>>.$$

Прямое произведение

Прямым *(или* ***декартовым)*** ***произведением*** *множеств $X_1, X_2, \ldots, X_n$ называется множество всех кортежей $<x_1, x_2, \ldots, x_n>$ таких, что $x_i \in X_i$, $i = 1, 2, \ldots, n$.*

Обозначается прямое произведение множеств $X_1, X_2, \ldots, X_n$ через $X_1 \times X_2 \times \ldots \times X_n$. Если $X_1 = X_2 = \ldots = X_n = X$, то пишут $X_1 \times \times X_2 \times \ldots \times X_n = X^n$ и множество X^n называется ***n-ой декартовой степенью*** *множества X.*

Пример 3.4

1. Пусть $X = \{1, 2, 3\}$, $Y = \{0, 1\}$. Тогда $X \times Y = \{<1, 0>, <1, 1>, <2, 0>, <2, 1>, <3, 0>, <3, 1>\}$ и $Y \times X = \{<0, 1>, <0, 2>, <0, 3>, <1, 1>, <1, 2>, <1, 3>\}$. Мы указали, кроме того, такие множества X и Y, что $X \times Y \neq Y \times X$.

[1] Одно из возможных определений: упорядоченная пара $<x, y>$ есть множество $\{x, \{x, y\}\}$. Таким образом, достигается асимметрия между x и y.

2. Пусть X — множество точек отрезка [0, 1], а Y — множество точек отрезка [1, 2]. Тогда $X \times Y$ — множество точек квадрата $[0, 1] \times [1, 2]$ с вершинами в точках (0, 1), (0, 2), (1, 1) и (1, 2).

Отношением ρ *множеств* X *и* Y *называется произвольное подмножество* $X \times Y$. *Если* $<x, y> \in \rho$, *это записывается как* $x\rho y$; *при этом говорят, что* x *и* y *находятся в отношении* ρ, *или просто, что* x ***относится*** *к* y. *Элементы* x *и* y *называются* ***координатами***, *или* ***компонентами***, *отношения* ρ. *Подмножество* $\rho \subseteq X^2$ *называется* ***отношением на X***.

В общем случае произвольное множество упорядоченных n-ок называют ***n-местным отношением***, *тогда для случая* $n = 2$ *отношения называются* ***двуместными*** *или* ***бинарными***.

Если $\rho \subseteq X \times Y$, *то* ***областью определения*** *отношения* ρ *называется множество* D_ρ *всех первых координат упорядоченных пар из* ρ, *а* ***областью значений*** *отношения* ρ *называется множество* R_ρ *всех вторых координат упорядоченных пар из* ρ.

Множество D_ρ *называется также* ***проекцией*** *отношения* ρ *на* X, *а* R_ρ *— проекцией отношения* ρ *на* Y.

Пример 3.5

1. Если $A = \{1, 2, 3\}$, а $B = \{r, s\}$, так что

$$A \times B = \{<1, r>, <2, r>, <3, r>, <1, s>, <2, s>, <3, s>\},$$

тогда $\rho = \{<1, r>, <1, s>, <3, s>\}$ есть отношение множеств A и B. Можно также записать $3\rho s$, поскольку $<3, s> \in \rho$. Область определения отношения ρ есть множество $\{1, 3\}$, а область значения — множество B. Множество $A \times B$ содержит шесть элементов, поэтому существует $2^6 = 64$ подмножеств множества $A \times B$. Следовательно, существует 64 различных отношений на $A \times B$.

2. Само множество $A \times B$ есть отношение множеств A и B.

3. Отношение равенства на множестве $\mathbf{R}$ есть множество $\{<x, x> \mid x \in \mathbf{R}\}$. Для этого отношения существует специальное обозначение $=$. Область определения $D_=$ совпадает с областью значений $R_=$ и является множеством $\mathbf{R}$.

4. Отношение «меньше чем» на множестве $\mathbf{Z}$ есть множество $\{<x, y> \mid$ для целых чисел x и y найдется положительное число z такое, что $x + z = y\}$. Для этого отношения существует специальное обозначение $<$. Область определения $D_<$ совпадает с областью значений $R_<$ и является множеством $\mathbf{Z}$.

5. Пусть $A = \{1, 2, 3, 4, 5, 6\}$. Пусть отношение ρ задано на A: $x\rho y \Leftrightarrow x$ делитель y. (Символ $\Leftrightarrow$ заменяет слова «тогда и только тогда, когда».)

Тогда $\rho = \{<1, 1>, <1, 2>, <1, 3>, <1, 4>, <1, 5>, <1, 6>, <2, 2>, <2, 4>, <2, 6>, <3, 3>, <3, 6>, <4, 4>, <5, 5>, <6, 6>\}$. Имеем $D_\rho = R_\rho = A$.

6. Отношение $\{<x, y> \in \mathbf{R}^2 \mid x^2 + y^2 = 4\}$ есть бинарное отношение на **R**. Область определения и область значений равны и совпадают с множеством $\{t \mid -2 \leqslant t \leqslant 2\}$.

7. Пусть A — множество товаров в магазине. Тогда $\{<x, y> \mid x \in A, y \in \mathbf{R}$ и y — цена $x\}$ — отношение множеств A и **R**. Область определения отношения есть A, а множество значений есть подмножество множества **R**, каждый элемент которого является ценой некоторого товара в магазине.

8. Пусть A — множество женщин, а B — множество мужчин, тогда $\{<x, y> \mid y$ является мужем $x\}$ есть отношение множеств A и B. Область определения есть множество всех замужних женщин, а множество значений — множество всех женатых мужчин.

. . . . . .

Рассмотрим операции над отношениями. Конечно же, поскольку отношения являются множествами, над ними можно производить обычные булевы операции. Но есть и специальные для бинарных отношений операции.

С каждым отношением ρ на $X \times Y$ связано отношение ρ^{-1} на $Y \times X$.

Обратное отношение

. . . . . .

Пусть $\rho \subseteq X \times Y$ *есть отношение на* $X \times Y$. *Тогда отношение* ρ^{-1} *на* $Y \times X$ *определяется следующим образом:*

$$\rho^{-1} = \{<y, x> \mid x \in X, y \in Y \text{ и } <x, y> \in \rho\}.$$

Другими словами, $<y, x> \in \rho^{-1}$ *тогда и только тогда, когда* $<x, y> \in \rho$ *или, что равносильно,* $y\rho^{-1}x$ *тогда и только тогда, когда* $x\rho y$. *Отношение* ρ^{-1} *называется* ***обратным отношением*** *к данному отношению* ρ.

. . . . . .

. . . . .  Пример 3.6 . . . . . .

1. Пусть $\rho = \{<1, r>, <1, s>, <3, s>\}$, тогда $\rho^{-1} = \{<r, 1>, <s, 1>, <s, 3>\}$.

2. Пусть $\rho = \{<x, y> \mid y$ является мужем $x\}$, тогда ρ^{-1} есть отношение $\{<x, y> \mid y$ — жена $x\}$.

3. Для отношения равенства обратным является оно само, отношения $<$ и $>$ взаимно обратны.

. . . . . .

Имея два заданных отношения, можно образовать новые отношения указанным ниже способом.

Композиция отношений

Композицией отношений $\rho \subseteq X \times Y$ *и* $\varphi \subseteq Y \times Z$ *называется отношение* $\varphi \circ \rho \subseteq X \times Z$, *такое, что* $\varphi \circ \rho = \{\langle x, z\rangle \mid x \in X,\ z \in Z$ *и существует* $y \in Y$, *для которого* $\langle x, y\rangle \in \rho$ *и* $\langle y, z\rangle \in \varphi\}$.

Пример 3.7

1. Пусть ρ и φ — отношения на множестве людей A, определенные следующим образом:

- $x\rho y$, если и только если x — мать y;
- $x\varphi y$, если и только если x — отец y.

Имеем $\langle x, y\rangle \in \varphi \circ \rho$ тогда и только тогда, когда x — бабушка по линии отца для y. И $\langle x, y\rangle \in \rho \circ \varphi$, тогда и только тогда, когда x — дедушка по линии матери для y.

2. Пусть $A = \{1, 2, 3\}$, $B = \{x, y\}$, а $C = \{s, t, r, q\}$, и пусть отношения ρ на $A \times B$ и φ на $B \times C$ заданы в виде:

$$\rho = \{\langle 1, x\rangle, \langle 1, y\rangle, \langle 3, x\rangle\};$$
$$\varphi = \{\langle x, s\rangle, \langle x, t\rangle, \langle y, r\rangle, \langle y, q\rangle\}.$$

Тогда

$$\varphi \circ \rho = \{\langle 1, s\rangle, \langle 1, t\rangle, \langle 1, r\rangle, \langle 1, q\rangle, \langle 3, s\rangle, \langle 3, t\rangle\},$$

поскольку

- из $\langle 1, x\rangle \in \rho$ и $\langle x, s\rangle \in \varphi$ следует $\langle 1, s\rangle \in \varphi \circ \rho$;
- из $\langle 1, x\rangle \in \rho$ и $\langle x, t\rangle \in \varphi$ следует $\langle 1, t\rangle \in \varphi \circ \rho$;
- из $\langle 1, y\rangle \in \rho$ и $\langle y, r\rangle \in \varphi$ следует $\langle 1, r\rangle \in \varphi \circ \rho$;
- …;
- из $\langle 3, x\rangle \in \rho$ и $\langle x, t\rangle \in \varphi$ следует $\langle 3, t\rangle \in \varphi \circ \rho$.

Теорема 4. Для любых отношений выполняются следующие свойства:

$$\left(\rho^{-1}\right)^{-1} = \rho;$$
$$(\gamma \circ \varphi)^{-1} = \varphi^{-1} \circ \gamma^{-1}.$$

Доказательство. Первое свойство очевидно. Для доказательства второго свойства покажем, что множества, записанные в левой и правой частях равенства, состоят из одних и тех же элементов. Действительно, $\langle x, z\rangle \in (\gamma \circ \varphi)^{-1} \Leftrightarrow \langle z, x\rangle \in$

$\in \gamma \circ \varphi \Leftrightarrow$ существует y такое, что $\langle z, y\rangle \in \varphi$ и $\langle y, x\rangle \in \gamma \Leftrightarrow$ существует y такое, что $\langle y, z\rangle \in \varphi^{-1}$ и $\langle x, y\rangle \in \gamma^{-1}$ тогда и только тогда, когда $\langle x, z\rangle \in \varphi^{-1} \circ \gamma^{-1}$.

Теорема 5. Композиция отношений является ассоциативной операцией.

Доказательство. Пусть даны три отношения $\rho \subseteq A \times B$, $\varphi \subseteq B \times C$ и $\gamma \subseteq C \times D$. Докажем, что $(\gamma \circ \varphi) \circ \rho = \gamma \circ (\varphi \circ \rho)$. Действительно, $\langle a, d\rangle \in (\gamma \circ \varphi) \circ \rho \Leftrightarrow \langle a, b\rangle \in \in \rho$ и $\langle b, d\rangle \in \gamma \circ \varphi$ для некоторых $b \in B \Leftrightarrow \langle a, b\rangle \in \rho$ и $\langle b, c\rangle \in \varphi$ и $\langle c, d\rangle \in \gamma$ для некоторых $b \in B$ и $c \in C \Leftrightarrow \langle a, c\rangle \in \varphi \circ \rho$ и $\langle c, d\rangle \in \gamma$ для некоторых $c \in C \Leftrightarrow$ $\Leftrightarrow \langle a, d\rangle \in \gamma \circ (\varphi \circ \rho)$.

Определим некоторые свойства отношений.

- *Отношение* ρ *на множестве* X *называется* ***рефлексивным****, если для любого элемента* $x \in X$ *выполняется* $x\rho x$.
- *Отношение* ρ *на множестве* X *называется* ***симметричным****, если для любых* $x, y \in X$ *из* $x\rho y$ *следует* $y\rho x$.
- *Отношение* ρ *на множестве* X *называется* ***транзитивным****, если для любых* $x, y, z \in X$ *из* $x\rho y$ *и* $y\rho z$ *следует* $x\rho z$.
- *Отношение* ρ *на множестве* X *называется* ***антисимметричным****, если для любых* $x, y \in X$ *из* $x\rho y$ *и* $y\rho x$ *следует* $x = y$.

Замечание 1. Если для отношения ρ вообще не существует таких x, y и z, чтобы выполнялось $\langle x, y\rangle \in \rho$ и $\langle y, z\rangle \in \rho$, то отношение транзитивно.

Замечание 2. Если для отношения ρ вообще не существует таких x и y, чтобы выполнялось $\langle x, y\rangle \in \rho$ и $\langle y, x\rangle \in \rho$, то отношение антисимметрично.

Обоснование этих двух утверждений см. в параграфе 5.1 главы 5.

Пример 3.8

1. Пусть отношение ρ задано на множестве $\mathbf{R}$ и $x\rho y$, если и только если $x \leqslant y$. Тогда ρ рефлексивно, потому что $x \leqslant x$ для всех $x \in \mathbf{R}$. Отношение ρ не симметрично, например, $1 \leqslant 2$, но $2 \leqslant 1$ не выполнено. Отношение ρ, очевидно, является транзитивным, ибо если $x \leqslant y$ и $y \leqslant z$, то $x \leqslant z$. Отношение является антисимметричным, поскольку $x \leqslant y$ и $y \leqslant x$ влекут $x = y$.

2. Пусть $\rho_1 = \{\langle 1, 2\rangle, \langle 2, 3\rangle\}$, $\rho_2 = \{\langle 1, 2\rangle, \langle 1, 3\rangle\}$. Тогда отношение ρ_1 не транзитивно, так как $\langle 1, 2\rangle \in \rho_1$ и $\langle 2, 3\rangle \in \rho_1$, но $\langle 1, 3\rangle \notin \rho_1$. Но отношение ρ_2 является транзитивным, поскольку нет вообще таких элементов x, y и z, чтобы выполнялось условие $x\rho_2 y$ и $y\rho_2 z$.

3. Пусть A — непустое множество и $\rho = \varnothing$ (пустое отношение на A). Тогда отношение ρ является симметричным, транзитивным, антисимметричным. Если же $A = \varnothing$, то ρ еще и рефлексивно.

3.4 Эквивалентность и порядок

Рассмотрим два важных класса отношений: отношения эквивалентности и отношения порядка.

Отношение эквивалентности

*Рефлексивное, симметричное и транзитивное отношение ρ на множестве X называется **отношением эквивалентности** на множестве X.*

Пример 3.9

1. Отношение равенства на множестве целых чисел есть отношение эквивалентности.

2. Отношение равносильности на множестве формул логики высказываний является отношением эквивалентности.

3. Пусть $A = \mathbf{R}^2 \backslash \{<0, 0>\}$ — множество точек на плоскости за исключением начала координат. Отношение ρ на A определим так: $<a, b> \rho <c, d>$ тогда и только тогда, когда точки $<a, b>$ и $<c, d>$ лежат на одной прямой, проходящей через начало координат. Легко показать, что отношение ρ является отношением эквивалентности.

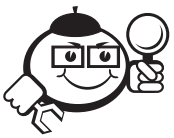
4. Отношение сравнимости по модулю натурального числа n на множестве целых чисел $\mathbf{Z}$: $x \equiv y \pmod{n}$ тогда и только тогда, когда $x - y$ делится на n. Это отношение рефлексивно на $\mathbf{Z}$, так как для любого $x \in \mathbf{Z}$ имеем $x - x$ равно нулю, и, следовательно, делится на n. Это отношение симметрично, так как если $x \equiv y \pmod{n}$, то $y \equiv x \pmod{n}$. Это отношение транзитивно, так как если $x \equiv y \pmod{n}$, то для некоторого целого t_1 имеем $x - y = t_1 n$, а если $y \equiv z \pmod{n}$, то для некоторого целого t_2 имеем $y - z = t_2 n$. Отсюда $x - z = (t_1 + t_2)n$, т. е. $x \equiv z \pmod{n}$.

5. Рассмотрим отношение ρ, определенное на множестве $\mathbf{N}$ так: $n \rho m$, если и только если n — делитель m. Отношение ρ не является отношением эквивалентности. Чтобы показать это, достаточно убедиться, что хотя бы одно из трех свойств не выполняется для ρ. Очевидно, что ρ не является симметричным отношением, так как, например, 2 — делитель 4, но 4 не является делителем 2.

6. Пусть $A = \{1, 2, 3, 4, 5, 6\}$ и отношение ρ_1 на A определено как $\rho_1 = \{<1, 1>, <2, 2>, <3, 3>, <4, 4>, <5, 5>, <6, 6>, <1, 2>, <1, 4>, <2, 1>, <2, 4>, <3, 5>, <5, 3>, <4, 1>, <4, 2>\}$. Тогда отношение рефлексивно, транзитивно и симметрично, поэтому ρ_1 есть отношение эквивалентности на множестве A.

Пусть ρ *— отношение эквивалентности на множестве* X. ***Классом эквивалентности****, порожденным элементом* x*, называется подмножество множества* X*, состоящее из тех элементов* $y \in X$*, для которых* $x\rho y$*. Класс эквивалентности, порожденный элементом* x*, обозначается* $[x]$*:*

$$[x] = \{y \mid y \in X \text{ и } x\rho y\}.$$

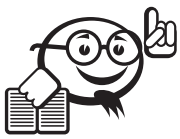


Пример 3.10

1. Отношение равенства на множестве целых чисел порождает следующие классы эквивалентности: для любого элемента $x \in \mathbf{Z}$ имеем $[x] = \{x\}$, т. е. каждый класс эквивалентности содержит только один элемент — число x.

2. Отношение сравнимости по модулю числа n на множестве целых чисел $\mathbf{Z}$ порождает следующие классы эквивалентности: вместе с любым числом $a \in \mathbf{Z}$ в этом же классе эквивалентности содержатся все числа вида $a + kn$, где k — целое. Очевидно, что все числа 0, 1, 2,…, $n - 1$ порождают различные классы эквивалентности, которые обозначим [0], [1], [2],…, $[n - 1]$. Они называются ***классами вычетов по модулю n***. Все остальные классы эквивалентности для этого отношения совпадают с ними, так как любое число $a \in \mathbf{Z}$ можно представить в виде $a = qn + r$, где $0 \leqslant r < n$.

3. Отношение $\rho_1 = \{<1, 1>, <2, 2>, <3, 3>, <4, 4>, <5, 5>, <6, 6>, <1, 2>, <1, 4>, <2, 1>, <2, 4>, <3, 5>, <5, 3>, <4, 1>, <4, 2>\}$ есть отношение эквивалентности на множестве $\{1, 2, 3, 4, 5, 6\}$. Легко видеть, что $[1] = \{1, 2, 4\} = [2] = [4]$, $[3] = \{3, 5\} = [5]$ и $[6] = \{6\}$. Всего имеется три различных класса эквивалентности: $\{1, 2, 4\}$, $\{3, 5\}$ и $\{6\}$.



Теорема 6. Пусть ρ — отношение эквивалентности на множестве X. Тогда: 1) если $x \in X$, то $x \in [x]$; 2) если $x, y \in X$ и $x\rho y$, то $[x] = [y]$ (т. е. класс эквивалентности порождается любым своим элементом).

Доказательство. Для доказательства первой части утверждения достаточно воспользоваться рефлексивностью отношения ρ: $x\rho x$ и, следовательно, $x \in [x]$. Докажем вторую часть утверждения. Пусть $z \in [y]$. Тогда $y\rho z$, и в силу транзитивности отношения ρ имеем $x\rho z$, т. е. $z \in [x]$. Отсюда $[y] \subseteq [x]$. Аналогично, в силу симметричности ρ можно показать, что $[x] \subseteq [y]$, а значит, $[y] = [x]$.

Разбиением *множества X называется множество попарно непересекающихся подмножеств X, таких, что каждый элемент множества X принадлежит одному и только одному из этих подмножеств.*

Пример 3.11

$X = \{1, 2, 3, 4, 5\}$. Тогда $\big\{\{1, 2\}, \{3, 5\}, \{4\}\big\}$ — разбиение множества X. Пусть X — множество студентов университета. Тогда разбиением этого множества является, например, совокупность студенческих групп.

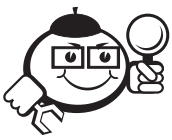
Теорема 7. Всякое разбиение множества X определяет на X отношение эквивалентности ρ: $x\rho y$ тогда и только тогда, когда x и y принадлежат одному подмножеству разбиения.

Доказательство. Рефлексивность и симметричность ρ очевидны. Пусть теперь $x\rho y$ и $y\rho z$. Тогда $x, y \in X_1$ и $y, z \in X_2$, где X_1, X_2 — подмножества из разбиения X. Поскольку $y \in X_1$, $y \in X_2$, то $X_1 = X_2$. Следовательно, $x, z \in X_1$ и $x\rho z$.

Теорема 8. Всякое отношение эквивалентности ρ определяет разбиение множества X на классы эквивалентности относительно этого отношения.

Доказательство. Докажем, что совокупность классов эквивалентности определяет разбиение множества X. В силу теоремы 6 $x \in [x]$, и, следовательно, каждый элемент множества X принадлежит некоторому классу эквивалентности. Из теоремы 6 вытекает также, что два класса эквивалентности либо не пересекаются, либо совпадают, так как если $z \in [x]$ и $z \in [y]$, то $x\rho z$, откуда $[x] = [z]$, и $y\rho z$, откуда $[y] = [z]$. Следовательно, $[x] = [y]$.

Совокупность классов эквивалентности элементов множества X по отношению эквивалентности ρ называется ***фактор-множеством*** *множества X по отношению ρ и обозначается X/ρ.*



Пример 3.12

1. Для отношения эквивалентности $\rho_1 = \{<1, 1>, <2, 2>, <3, 3>, <4, 4>, <5, 5>, <6, 6>, <1, 2>, <1, 4>, <2, 1>, <2, 4>, <3, 5>, <5, 3>, <4, 1>, <4, 2>\}$ на множестве $A = \{1, 2, 3, 4, 5, 6\}$ фактор-множество A/ρ_1 равно $\big\{\{1, 2, 4\},\ \{5, 3\},\ \{6\}\big\}$.

2. На множестве $\mathbf{N}\times\big(\mathbf{N}\backslash\{0\}\big)$ определим отношение ρ: $<x, y> \rho <u, v> \Leftrightarrow xv = yu$. Это отношение рефлексивно: $<x, y> \rho <x, y>$, так как $xy = yx$; симметрично: если $<x, y> \rho <u, v>$, то $<u, v> \rho <x, y>$, так как из $xv = yu$ следует, что и $uy = vx$; транзитивно: если выполнено $<x, y> \rho <u, v>$ и $<u, v> \rho <w, z>$, то $<x, y> \rho <w, z>$, так как, перемножая левые и правые части равенств $xv = yu$ и $uz = vw$, после сокращения получаем $xz = yw$.

Класс эквивалентности, порожденной парой $<x, y>$, для этого отношения ρ определяется соотношением $[<x, y>] = \{<u, v> \mid x/y = u/v\}$. Каждый класс эквивалентности в этом случае определяет одно положительное рациональное число. Таким образом, фактор-множество $\mathbf{N}\times\big(\mathbf{N}\backslash\{0\}\big)/\rho$ есть множество положительных рациональных чисел. Именно так строго определяются рациональные числа с помощью теории множеств.

Элементы многих множеств можно разместить в определенном порядке на основе некоторого, заранее оговоренного соглашения. Например, на любом подмножестве A множества целых положительных чисел можно договориться о таком расположении элементов, при котором меньшие элементы будут находиться левее больших. При этом можно сказать, что на множестве A определено отношение порядка $x\rho y$, где ρ есть отношение «меньше или равно».

Частичный порядок

Рефлексивное, транзитивное и антисимметричное отношение на множестве X называется ***частичного порядка на множестве X****.*

Линейный порядок

Отношение частичного порядка ρ на множестве X, для которого любые два элемента сравнимы, т. е. для любых $x, y \in X$ имеем $x\rho y$ или $y\rho x$, называется отношением ***линейного порядка****.*

Множество X с заданным на нем частичным (линейным) порядком называется ***частично (линейно) упорядоченным****.*

Пример 3.13

1. Отношение $x \leqslant y$ на множестве действительных чисел есть отношение частичного порядка, причем это линейный порядок.

2. Отношение $x < y$ на множестве действительных чисел не является отношением частичного порядка, поскольку не рефлексивно.

3. Во множестве подмножеств некоторого универсума $\boldsymbol{U}$ отношение $A \subseteq B$ есть отношение частичного порядка, но оно не является отношением линейного порядка в общем случае.

4. Схема организации подчинения в учреждении есть отношение частичного порядка на множестве должностей.

5. Отношение на множестве слов, определенное так: «слово w связано отношением ρ со словом v, если $w = v$ или w появляется в словаре перед словом v», является отношением линейного порядка (***лексикографический порядок***).

6. На множестве положительных целых чисел можно ввести различные линейные порядки, причем некоторые выглядят весьма экзотично. Будем использовать привычное обозначение $\leqslant$ для следующего порядка.

$3 \leqslant 5 \leqslant 7 \leqslant 9 \leqslant \ldots$
$\leqslant 2 \times 3 \leqslant 2 \times 5 \leqslant 2 \times 7 \leqslant 2 \times 9 \leqslant \ldots$
$\leqslant 2^2 \times 3 \leqslant 2^2 \times 5 \leqslant 2^2 \times 7 \leqslant 2^2 \times 9 \leqslant \ldots$
$\leqslant 2^3 \times 3 \leqslant 2^3 \times 5 \leqslant 2^3 \times 7 \leqslant 2^3 \times 9 \leqslant \ldots$
$\ldots$
$\ldots$
$\ldots$
$\ldots \leqslant 2^n \leqslant \ldots \leqslant 2^3 \leqslant 2^2 \leqslant 2 \leqslant 1.$

Сначала идут все нечетные числа, потом все нечетные, умноженные на 2, потом — на 4 и т. д. После бесконечного множества таких бесконечных «секций» стоит секция степеней двойки, выстроенных в обратном порядке. Такая упорядоченность натуральных чисел называется ***порядком Шарковского***, с которым связан один из ярких результатов в теории нелинейной динамики [2].

3.5 Функции

Функция из множества X во множество Y представляет собой специальное отношение на $X \times Y$, обладающее следующими свойствами:

1. Областью определения отношения является все множество X. Следовательно, для каждого элемента x из X существует элемент y из Y такой, что x и y связаны данным отношением.
2. Если x относится к y и x относится к z, то $y = z$. В терминах упорядоченных пар это утверждение означает, что если $<x, y>$ и $<x, z>$ принадлежат отношению, то $y = z$.

Такое определение понятия «функции» ввел Дирихле[1] (рис. 3.5). По сути дела, при таком определении мы отождествляем функцию с ее графиком. Это одно из возможных определений. Другое определение, когда функция рассматривается как правило вычисления некоторого значения, используется в главе 8.

Дадим более формальное определение функции.

Рис. 3.5 – Петер Дирихле

*Отношение f на $X \times Y$ называется **функцией** (или **отображением**) из X в Y и обозначается через $f: X \to Y$, если для каждого $x \in X$ существует единственный элемент $y \in Y$, такой, что $\langle x, y\rangle \in f$. (Другими словами, из $\langle x, y\rangle \in f$ и $\langle x, z\rangle \in f$ следует $y = z$.)*

*Если f — функция, то вместо $\langle x, y\rangle \in f$ пишут $y = f(x)$ и говорят, что y — **значение, соответствующее аргументу** x.*

*Если используют термин «**отображение**» вместо термина «**функция**», то y называется **образом элемента** x.*

*Множество X называется **областью определения** функции f, а множество Y называется **областью потенциальных значений**.*

*Если $A \subseteq X$, то множество $f(A) = \{y \mid f(x) = y$ для некоторого x из $A\}$ называется **образом множества** A. Образ всего множества X называется **областью значений** функции f.*

*Если $B \subseteq Y$, то множество $f^{-1}(B) = \{x \mid f(x) \in B\}$ называется **прообразом множества** B.*

*Функция $f: X \to Y$ называется также **отображением**; при этом говорят, что f отображает X в Y. Если $\langle x, y\rangle \in f$, так что $y = f(x)$, то говорят, что элемент x отображается в элемент y.*

Поскольку функции являются бинарными отношениями, то к ним применим интуитивный принцип объемности, т. е. две функции f и g равны, если они состоят из одних и тех же элементов.

Назовем f *n-местной* функцией из X в Y, если $f: X^n \to Y$. Тогда пишем $y = f(x_1, \ldots, x_n)$ и говорим, что y — значение функции при значении аргументов $x_1, \ldots, x_n$.

[1] Петер Дирихле (1805–1859 гг.) — немецкий математик, внёсший существенный вклад в математический анализ, теорию функций и теорию чисел.

Пример 3.14

1. Пусть $X = \{-2, -1, 0, 1, 2\}$, а $Y = \{0, 1, 2, 3, 4, 5\}$. Определим отношение $f \subseteq X \times Y$ как $f = \{<-2.5>, <-1.2>, <0, 1>, <1, 2>, <2, 5>\}$.

2. Пусть $X = \{-2, -1, 0, 1, 2\}$ и $Y = \{0, 1, 2, 3, 4, 5\}$. Функция $f: X \to Y$ определена соотношением $f(x) = x^2 + 1$. Если $A = \{1, 2\}$, то $f(A) = \{y \mid <x, y> \in f$ для некоторого x из $A\} = \{y \mid y = f(x)$ для некоторого x из $A\} = \{2, 5\}$ является образом A при отображении f.

Если $B = \{0, 2, 3, 4, 5\} \subseteq Y$, то $f^{-1}(B) = \{x \mid f(x) \in B\} = \{-1, 1, -2, 2\}$ является прообразом B, где $-1 \in f^{-1}(B)$, т. к. $f(-1) = 2$, $1 \in f^{-1}(B)$, т. к. $f(1) = 2$, $-2 \in f^{-1}(B)$, т. к. $f(-2) = 5$, $2 \in f^{-1}(B)$, т. к. $f(2) = 5$. Заметим, что элементы 0, 3 и 4 не вносят никаких элементов в $f^{-1}(B)$, поскольку они не принадлежат области значений функции f.

Прообраз может быть пустым. Так, например, в случае $W = \{0, 3\}$ прообраз $f^{-1}(W)$ пуст, поскольку не существует такого $x \in X$, для которого $f(x) = 0$ или $f(x) = 3$.

Область значений функции f имеет вид $f(X) = \{y \mid f(x) = y$ для некоторого x из $X\} = \{1, 2, 5\}$. Элементами $f(X)$ являются те и только те элементы области потенциальных значений Y, которые «используются» функцией f.

3. Ортогональная проекция окружности A на прямую B (рис. 3.6).

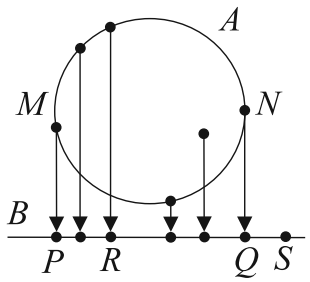


Рис. 3.6 – Ортогональная проекция

Образ окружности есть замкнутый отрезок $[P, S]$. Прообраз любой точки открытого отрезка (P, S) есть двухточечное множество на окружности; прообразы точек Q и P содержат только по одной точке, N и M соответственно; прообраз точки S есть пустое множество.

Пусть дана функция $f: X \to Y$. Подчеркнем еще раз три особенности нашего определения функции (рис. 3.7):

- несколько элементов из области определения X могут иметь один и тот же образ в области значений $(f(e) = f(d) = f(c) = 1)$;
- не все элементы из Y обязаны быть образом некоторых элементов X (нет элемента $x \in X$, такого, что $f(x) = 4$);

- для любого элемента из X, если существует образ, то он должен быть единственным (для функции недопустимо, чтобы одному элементу $x \in X$ соответствовало два разных значения $f(x)$).

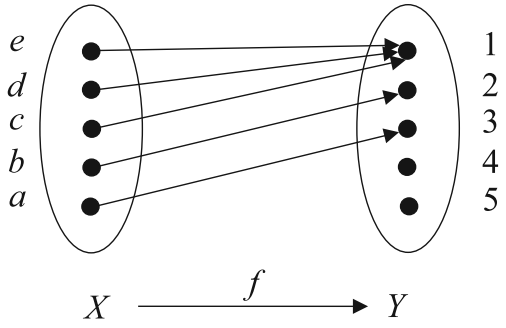


Рис. 3.7 – f: $\{a, b, c, d, e\} \to \{1, 2, 3, 4, 5\}$

Замечание 3. Общие свойства образов и прообразов множеств при любых отображениях являются следствием следующих утверждений:

Пусть $f: X \to Y$ и $A \subseteq X$ и $B \subseteq Y$, тогда имеем:

а) $y \in f(A)$ тогда и только тогда, когда существует такой $x \in A$, что $y = f(x)$;

б) $x \in f^{-1}(B)$ тогда и только тогда, когда $f(x) \in B$;

в) из $x \in A$ следует $f(x) \in f(A)$.

Утверждение, обратное в), в общем случае не выполняется. Действительно, возьмем $f(x) = x^2$ и $A = [0, 1]$. Тогда если $x = -0.5$, то имеем $f(-0.5) = 0.25 \in \in [0, 1] = f(A)$. Но $-0.5 \notin A$.

Функция $f: X \to Y$ может быть классифицирована в зависимости от того, существуют ли элементы из Y, связанные данным отношением с более чем одним элементом из X, и связан ли каждый элемент из области значений $f(X)$ с соответствующим элементом области определения X.

Инъективность

*Функция (отображение) $f: X \to Y$ называется **инъективной (инъективным)**, если для любых $x_1, x_2 \in X$, $y \in Y$ из $y = f(x_1)$ и $y = f(x_2)$ следует, что $x_1 = x_2$ (или, иначе, из $<x_1, y> \in f$ и $<x_2, y> \in f$ следует, что $x_1 = x_2$). Менее формально, функция f инъективна, если для всех x_1, x_2 выполняется: $x_1 \neq x_2$ влечет $f(x_1) \neq f(x_2)$. Инъекция также называется **вложением** (образ $f(X)$ «вкладывается» в Y).*

Сюръективность

*Функция (отображение) $f: X \to Y$ называется **сюръективной (сюръективным)**, если для любого элемента $y \in Y$ существует элемент $x \in X$, такой, что $y = f(x)$. Сюръекция называется также **наложением** (образ $f(X)$ «накладывается» на Y).*

Биективность

*Функция (отображение) f называется **биективной (биективным)**, если f одновременно инъективна и сюръективна. Если существует биекция $f: X \to Y$, то говорят, что f осуществляет **взаимно однозначное соответствие** между множествами X и Y.*

Пример 3.15

Рассмотрим четыре функции, отображающие множество действительных чисел **R** во множество действительных чисел f_i: $\mathbf{R} \to \mathbf{R}$, $i = 1, 2, 3, 4$:

1) функция $f_1(x) = e^x$ инъективна, но не сюръективна;
2) функция $f_2(x) = x^3 - x$ сюръективна, но не инъективна;
3) функция $f_3(x) = 2x + 1$ биективна;
4) функция $f_4(x) = x^2$ не является ни инъективной, ни сюръективной.

Рассмотрим три множества X, Y, Z, и пусть даны некоторые отображения $f: X \to Y$ и $g: Y \to Z$. Их можем записать в виде цепочки

$$X \xrightarrow{f} Y \xrightarrow{g} Z.$$

Рассматривая отображения f и g как отношения, мы можем применить к ним операцию композиции.

***Композиция двух функций** f и g есть отношение $g \circ f = \{<x, z> \mid$ существует такое y, что $y = f(x)$ и $z = g(y)\}$.*

Теорема 8. Композиция двух функций есть функция. При этом, если $f: X \to Y$, $g: Y \to Z$, то $g \circ f: X \to Z$.

Доказательство. Действительно, если $<x, y> \in g \circ f$ и $<x, z> \in g \circ f$, то существует такое u, что $u = f(x)$, $y = g(u)$, и существует такое v, что $v = f(x)$, $z = g(v)$. Поскольку f — функция, то $u = v$; поскольку g — функция, то $y = z$ и, следовательно, $g \circ f$ — функция. Вторая часть утверждения очевидна.

Таким образом, для любого $x \in X$ имеем $(g \circ f)(x) = g(f(x))$.

Верно также и следующее утверждение.

Теорема 9.

1. Композиция двух инъекций — инъекция.
2. Композиция двух сюръекций — сюръекция.
3. Композиция двух биекций — биекция.

Тождественным отображением *множества X в себя называется отображение e_X: $X \to X$, такое, что для любого $x \in X$ имеем $e_X(x) = x$. Тогда, если f: $X \to Y$, то $e_Y \circ f = f$, $f \circ e_X = f$.*

Пусть f^{-1} — отношение, обратное f. Выясним, при каких условиях отношение f^{-1} будет функцией. Его называют тогда ***обратной функцией*** *или, если f осуществляет отображение множества X во множество Y,* ***обратным отображением****.*

Теорема 10. Отображение f: $X \to Y$ имеет обратное отображение f^{-1}: $Y \to X$ тогда и только тогда, когда f — биекция.

Доказательство. Если f — биекция, то, поскольку f сюръективно, f^{-1} определено на множестве Y. Кроме того, f^{-1} — функция, так как если $\langle y, x_1\rangle \in f^{-1}$ и $\langle y, x_2\rangle \in f^{-1}$, то $\langle x_1, y\rangle \in f$ и $\langle x_2, y\rangle \in f$, а в силу инъективности f имеем $x_1 = x_2$.

Пусть теперь отображение f имеет обратное отображение f^{-1}, определенное на множестве Y со значениями во множестве X. Тогда f сюръективно, поскольку любой элемент $y \in Y$ имеет прообраз $x \in X$. При этом f инъективно, так как если $\langle x_1, y\rangle \in f$ и $\langle x_2, y\rangle \in f$, то $\langle y, x_1\rangle \in f^{-1}$ и $\langle y, x_2\rangle \in f^{-1}$, а поскольку f^{-1} — функция, то $x_1 = x_2$.

Пусть f: $X \to Y$. Заметим, что для того, чтобы обратное отношение f^{-1} было функцией на $f(X)$, достаточно инъективности функции f. Поэтому функция $f(x) = x^2$: $\mathbf{R} \to \mathbf{R}$, не будучи биекцией, не имеет обратной функции. Эта функция не имеет обратной, если даже она будет отображением на множество неотрицательных вещественных чисел.

Поскольку функция есть отношение, то выполняются следующие свойства инъективных функций f и g:

1) $(f^{-1})^{-1} = f$;

2) $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Если f: $X \to Y$ — биекция, то $f^{-1} \circ f = e_X$ и $f \circ f^{-1} = e_Y$.

3.6 Мощность множеств

Нетрудно установить следующий факт: *два конечных множества X и Y имеют одинаковое количество элементов тогда и только тогда, когда существует биекция X на Y*. Это утверждение является отправной точкой для следующего определения.

*Два множества называются **равномощными**, если между ними можно установить взаимно однозначное соответствие.*

Для конечных множеств это означает, что в них одинаковое число элементов, но определение имеет смысл и для бесконечных множеств. И первым здесь был Кантор — его определения и результаты о бесконечных множествах, хотя первоначально и были восприняты с трудом, но, в конце концов, нашли повсеместное применение.

Но прежде чем рассматривать отношение равномощности для бесконечных множеств, познакомимся с примером бесконечности, известным под названием «отель Гильберта». Давид Гильберт иногда начинал лекции о необычайных свойствах бесконечности с этого примера.

Отель Гильберта: «*Этот космический отель обладает уникальным свойством: число одноместных номеров в этом отеле бесконечно. Нумерация гостиничных номеров начинается с 1 и идет последовательно: 1, 2, 3,... Однажды все номера отеля оказались заняты постояльцами, а прибывает новый гость и узнает, что свободных мест нет. Портье, после некоторого размышления, уверяет гостя, что найдет для него свободный номер. Он просит каждого постояльца переселиться в соседний номер: постояльца из номера 1 переселиться в номер 2, постояльца из номера 2 — переселиться в номер 3 и т. д. Каждый из постояльцев, живших в отеле, получает новый номер, а новый гость поселяется в освободившийся номер 1.*

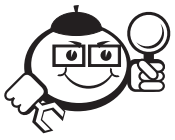
В другой раз портье сумел дополнительно поселить в целиком заполненный отель троих прибывших гостей. Для этого каждый постоялец из номера n (n = = 1, 2, 3,...) переселился в номер $n + 3$. В этом случае освободились номера 1, 2 и 3. Очевидно, что таким образом можно в целиком заполненный отель поселить новых k гостей, где k может быть как угодно велико.

Был построен еще один космический отель с бесконечным числом номеров, и вскоре он тоже оказался занятым полностью. Но, к сожалению, второй отель скоро сгорел, хотя, к счастью, все его постояльцы не пострадали. Портье первого отеля сумел расселить бесконечное множество постояльцев из второго отеля в своем отеле, где все номера были заняты. Для этого надо гостей из первого отеля из номеров n переселить в номера $2n$. Все, кто жил в отеле до прибытия новых гостей, остался в отеле, но при этом освободилось бесконечно много номеров (все те, «адреса» которых нечетны), в которых находчивый портье расселил новых гостей».

Теперь изучим понятие равномощности более строго. Во-первых, мы обнаружили парадоксальный вывод, что «бесконечная часть может иметь столько же эле-

ментов, что и целое бесконечное множество», например множество четных чисел равномощно множеству целых чисел. Точно так же отрезки $[0, 1]$ и $[0, 2]$ равномощны, поскольку отображение $x \to 2x$ является биекцией.

Отношение равномощности, очевидно, является отношением эквивалентности на множестве всех множеств (транзитивность следует из теоремы 9 (3)). Для эквивалентных бесконечных множеств мы говорим, что у них одинаковая *мощность*.



Пример 3.16

1. Два отрезка (A, B) и (C, D) имеют одинаковую мощность (рис. 3.8).

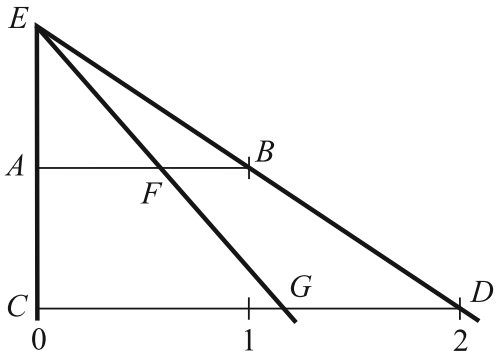


Рис. 3.8 – Биекция между двумя отрезками

2. Любые две окружности на плоскости равномощны. Любые два круга на плоскости равномощны (достаточно совместить центры окружностей и кругов и для биекции использовать гомотетию).

3. Любой открытый отрезок равномощен множеству вещественных чисел R. Для этого замечаем, что любые два отрезка равномощны. Полуокружность радиуса 1 равномощна отрезку $(-1, 1)$ (используем ортогональную биекцию полуокружности на отрезок). Полуокружность равномощна всей прямой (рис. 3.9).

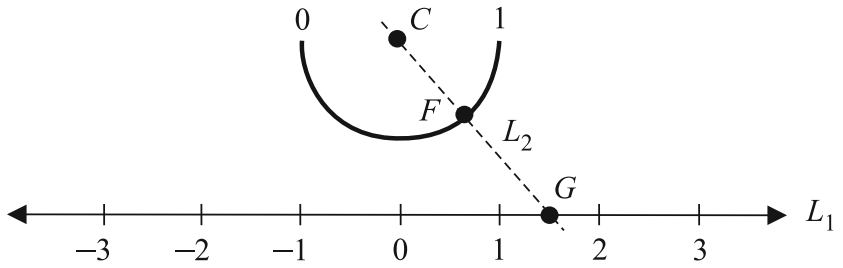


Рис. 3.9 – Полуокружность равномощна всей прямой

4. Полуинтервалы $[0, 1)$ и $(0, 1]$ имеют одинаковую мощность (используем биекцию $x \to 1 - x$).

5. Множество бесконечных последовательностей нулей и единиц равномощно множеству всех подмножеств натурального ряда. В самом деле, сопоставим с каждой последовательностью множество номеров мест, на которых стоят единицы:

например, последовательность из одних нулей соответствует пустому множеству, из одних единиц — натуральному ряду, а последовательность 10101010... — множеству четных чисел.

6. Множество бесконечных последовательностей цифр 0, 1, 2, 3 равномощно множеству бесконечных последовательностей цифр 0 и 1. В самом деле, можно закодировать цифры 0, 1, 2, 3 группами 00, 01, 10, 11. Обратное преобразование разбивает последовательность нулей и единиц на пары, после чего каждая пара заменяется на цифру от 0 до 3.

7. Множество бесконечных последовательностей цифр 0, 1, 2 равномощно множеству бесконечных последовательностей цифр 0 и 1. Это множество заключено между двумя множествами одной и той же мощности (см. предыдущий пример), и поэтому равномощно каждому из них (см. следующую теорему).

Теорема 11 (Кантора—Бернштейна). Если множество M равномощно некоторому подмножеству множества N, а множество N равномощно некоторому подмножеству множества M, то M и N равномощны (рис. 3.10).

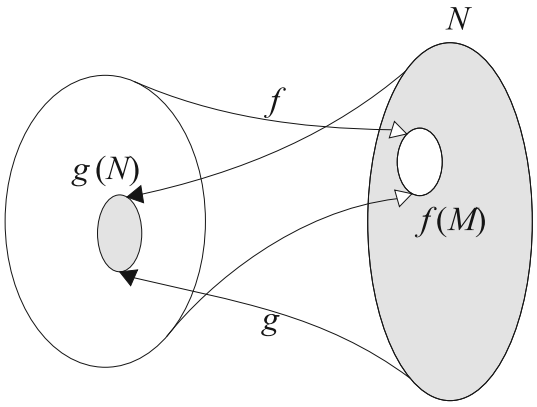


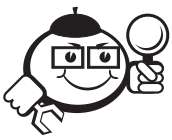
Рис. 3.10 – Теорема Кантора—Бернштейна

Доказательство см. например, в [3, с. 20–21].

Теорема Кантора—Бернштейна значительно упрощает доказательства равномощности: например, если мы хотим доказать, что бублик и шар в пространстве равномощны, то достаточно заметить, что из бублика можно вырезать маленький шар (равномощный большому), а из шара — маленький бублик.

Конечные и бесконечные множества отличаются по следующему важному признаку — определение Рассела.

Бесконечное множество *— такое множество X, что существует взаимно однозначное соответствие на какое-либо подмножество $Y \subset X$.*



Пример 3.17

Множество натуральных чисел $\mathbf{N} = \{0, 1, 2, 3, \ldots\}$ можно поставить во взаимно однозначное соответствие с множеством неотрицательных четных чисел с помощью биекции $n \to 2n$. Поскольку неотрицательные четные числа составляют собственное подмножество множества **N**, то по признаку Рассела **N** является бесконечным множеством (что мы и подозревали до этого!).

Счётное множество *— множество, равномощное множеству натуральных чисел* ***N****, т. е. если его можно представить в виде* $\{x_0, x_1, x_2, \ldots\}$ *(здесь* x_i *— элемент, соответствующий числу i; соответствие взаимно однозначно, так что* x_i *все различны).*

Например, множество целых чисел **Z** счётно, так как целые числа можно расположить в последовательность 0, 1, −1, 2, −2, 3, −3,... Мощность счетных множеств обозначается, согласно Кантору, символом $\aleph_0$ (א — «алеф» — первая буква в древнееврейском алфавите).

Теорема 12.

1. Подмножество счётного множества конечно или счётно.
2. Всякое бесконечное множество содержит счетное подмножество.
3. Объединение конечного или счётного числа конечных или счётных множеств конечно или счётно.

Доказательство.

1. Пусть B — подмножество счетного множества

$$A = \{x_0, x_1, x_2, \ldots\}.$$

Выбросим из последовательности $x_0, x_1, x_2, \ldots$ те члены, которые не принадлежат B (сохраняя порядок оставшихся). Тогда оставшиеся члены образуют либо конечную последовательность (и тогда B конечно), либо бесконечную (и тогда B счётно).

2. Пусть A бесконечно. Тогда оно не пусто и содержит некоторый элемент b_0. Будучи бесконечным, множество A не исчерпывается элементом b_0 — возьмем какой-нибудь еще элемент b_1 и т. д. Получится последовательность $b_0, b_1, \ldots$; построение не прервется ни на каком шаге, поскольку A бесконечно. Теперь множество $B = \{b_0, b_1, \ldots\}$ и будет искомым подмножеством. (Заметим, что B не обязано совпадать с A, даже если A счётно.)

3. Пусть имеется счётное число счётных множеств $A_0, A_1, \ldots$ Расположив элементы каждого из них слева направо в последовательность $\left(A_i = \{a_{i0}, a_{i1}, \ldots\}\right)$ и поместив эти последовательности друг под другом, получим таблицу

$$\begin{array}{ccccc} a_{00} & a_{01} & a_{02} & a_{03} & \ldots \\ a_{10} & a_{11} & a_{12} & a_{13} & \ldots \\ a_{20} & a_{21} & a_{22} & a_{23} & \ldots \\ a_{30} & a_{31} & a_{32} & a_{33} & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

Теперь эту таблицу можно развернуть в последовательность, например проходя по очереди диагонали:

$$a_{00}, a_{01}, a_{10}, a_{02}, a_{11}, a_{20}, a_{03}, a_{12}, a_{21}, a_{30}, \ldots$$

Если множества A_i не пересекались, то мы получили искомое представление для их объединения. Если пересекались, то из построенной последовательности надо выбросить повторения.

Если множеств конечное число или какие-то из множеств конечны, то в этой конструкции части членов не будет — и останется либо конечное, либо счётное множество.

Описанный проход по диагоналям задает взаимно однозначное соответствие между множеством всех пар натуральных чисел $\mathbf{N}^2$ и $\mathbf{N}$.

Пример 3.18

Примеры счётных множеств

Множество $\mathbf{Q}$ рациональных чисел счётно. В самом деле, рациональные числа представляются несократимыми дробями с целым числителем и знаменателем. Множество дробей с данным знаменателем счётно, поэтому $\mathbf{Q}$ представимо в виде объединения счётного числа счётных множеств. На рисунке 3.11 показано, каким образом можно задать перечисление всех положительных рациональных чисел.

Множество $\mathbf{N}^k$, элементами которого являются наборы из k натуральных чисел, счётно.

- Множество всех конечных последовательностей натуральных чисел счётно. В самом деле, множество всех последовательностей данной длины счётно (предыдущий пример), так что интересующее нас множество разбивается на счётное число счётных множеств.
- В предыдущем примере не обязательно говорить о натуральных числах — можно взять любое счётное (или конечное) множество. Например, множество всех текстов, использующих русский алфавит (текст можно считать конечной последовательностью букв, пробелов, знаков препинания и т. п.), счётно; то же самое можно сказать о множестве (всех мыслимых) компьютерных программ и т. д.

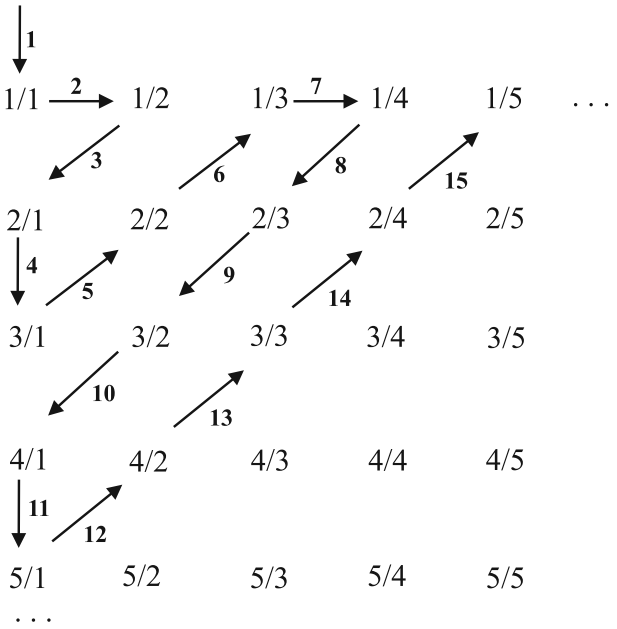


Рис. 3.11 – Множество **Q** счётно

Теорема 13. Если множество A бесконечно, а множество B конечно или счётно, то объединение $A \cup B$ равномощно A.

Доказательство. Будем считать, что B не пересекается с A (если это не так, выбросим пересечение из B, оставшееся множество будет по-прежнему конечно или счётно). Выделим в A счетное подмножество P, остаток обозначим через Q. Тогда надо доказать, что $B + P + Q$ равномощно $P + Q$ (в данном случае знак + обозначает объединение непересекающихся множеств). Поскольку $B + P$ и P оба счётны, то между ними существует биекция. Ее легко продолжить до биекции $B + P + Q$ на $P + Q$ (каждый элемент множества Q соответствует сам себе).

Существуют ли бесконечные множества, которые не являются счётными? Классический пример неравномощных бесконечных множеств дает «диагональная конструкция Кантора».

Теорема 14 (Кантора). Множество бесконечных последовательностей нулей и единиц несчётно.

Доказательство. Предположим, что оно счетно. Тогда все последовательности нулей и единиц можно перенумеровать: α_0, α_1,… Составим бесконечную вниз последовательность, строками которой будут наши последовательности:

$$\begin{array}{cccccc} \alpha_0 & = & \boldsymbol{\alpha_{00}} & \alpha_{01} & \alpha_{02} & \ldots \\ \alpha_1 & = & \alpha_{10} & \boldsymbol{\alpha_{11}} & \alpha_{12} & \ldots \\ \alpha_2 & = & \alpha_{20} & \alpha_{21} & \boldsymbol{\alpha_{22}} & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

(через α_{ij} мы обозначаем j-й член i-й последовательности). Теперь рассмотрим последовательность, образованную стоящими на диагонали членами α_{00}, α_{11}, α_{22},…; её i-й член есть α_{ii} и совпадает с i-м членом i-м последовательности. Заменив все члены на противоположные, мы получим последовательность β, у которой

$$\beta_i = 1 - \alpha_{ii},$$

так что последовательность β отличается от любой из последовательностей α_i (в позиции i) и поэтому отсутствует в таблице. А мы предположили, что таблица включает в себя все последовательности — противоречие.

Множество-степень $\boldsymbol{P}(\mathbf{N})$ — множество подмножеств натурального ряда — равномощно множеству бесконечных последовательностей нулей и единиц. Действительно, сопоставим каждому подмножеству $A \subseteq \mathbf{N}$ бесконечную последовательность α_0, α_1, α_2,…, где $\alpha_n = 1$, если $n \in A$, и $\alpha_n = 0$ в противном случае. Очевидно, такое соответствие является биекцией. Теперь мы можем переформулировать теорему 14.

Множество $\mathbf{N}$ не равномощно $\boldsymbol{P}(\mathbf{N})$.

Теорема 15. Отрезок [0, 1] равномощен множеству всех бесконечных последовательностей нулей и единиц.

Доказательство. Каждое число $x \in [0, 1]$ записывается в виде бесконечной двоичной дроби. Первый знак этой дроби равен 0 или 1 в зависимости от того, попадает ли число x в левую или правую половину отрезка. Чтобы определить следующий знак, надо выбранную половину поделить снова пополам и посмотреть, куда попадёт x, и т. д.

Это же соответствие можно описать в другую сторону: последовательности $x_0x_1x_2\ldots$ соответствует число (принадлежащее [0, 1]), являющееся суммой ряда

$$\frac{x_0}{2} + \frac{x_1}{4} + \frac{x_2}{8} + \ldots$$

Описанное соответствие не вполне взаимно однозначно: двоично-рациональные числа (вида $m/2^n$) имеют два представления. Например, $3/8 = 0.11000\ldots = 0.010111\ldots$ Соответствие станет взаимно однозначным, если отбросить дроби с единицей в периоде. Но таких дробей счётное число, поэтому на мощность это не повлияет.

Мощность множества действительных чисел называется ***мощностью континуума*** *(от латинского слова, означающего «непрерывный»; имеется в виду, что точка на отрезке может непрерывно двигаться от одного конца к другому). Мощность континуума обозначим символом* ***c****.*

Докажем следующий удивительный факт.

Теорема 16. Квадрат (с внутренностью) равномощен отрезку.

Доказательство. Квадрат равномощен множеству $[0, 1] \times [0, 1]$ пар действительных чисел, каждое из которых лежит на отрезке [0, 1] (метод координат). Мы уже знаем, что вместо чисел на отрезке можно говорить о последовательностях нулей и единиц (теорема 15). Осталось заметить, что паре последовательностей нулей и единиц ($x_0x_1x_2\ldots$, $y_0y_1y_2\ldots$) можно поставить в соответствие последовательность — смесь $x_0y_0x_1y_1x_2y_2\ldots$ и что это соответствие будет взаимно однозначным.

Можно доказать также, что любое конечномерное пространство $\mathbf{R}^n$ имеет мощность континуума.

Кантор доказал и обобщение теоремы 14.

Теорема 17. Никакое множество X не равномощно множеству $\boldsymbol{P}(X)$ всех своих подмножеств.

Доказательство. Очевидно, не существует взаимно однозначного соответствия между пустым множеством $\varnothing$ и его множеством-степенью $\boldsymbol{P}(\varnothing) = \{\varnothing\}$, содержащим один элемент. Теперь предположим, что X — не пусто и что существует биекция f между X и $\boldsymbol{P}(X)$. Покажем, что последнее предположение противоречиво.

Отображение f биективно отображает элементы множества X на подмножества множества X. Например, пусть X — множество положительных целых чисел и пусть

$f(1) = \{2, 5, 7, 9, 10\}$,
$f(2) = \{2, 4, 6, 8, \ldots\}$,
$f(3) = \varnothing$,
$f(4) = \{1, 2, 3, 4, 5, 6, 7, \ldots\}$,
$f(5) = \{1, 2\}$,
...

В некоторых случаях $n \in f(n)$. В нашем примере $2 \in f(2)$ и $4 \in f(4)$. Однако $1 \notin f(1)$, $3 \notin f(3)$, $5 \notin f(5)$.

Понятно, что любой элемент n, который функция f отображает в пустое множество, будет обладать свойством $n \notin f(n)$, а всякий элемент m, который функция f отображает во все X, будет обладать свойством $m \in f(m)$. Пусть $W = \{x \mid x \in X$

и $x \notin f(x)\}$. Поскольку отображение f сюръективно, то существует элемент $a \in X$, такой, что $f(a) = W$. Принадлежит ли a множеству W? Если $a \in W$, то a принадлежит множеству тех элементов X, которые f не отображает на множества, их содержащие. Следовательно, $a \notin f(a) = W$. Таким образом, мы приходим к противоречию. Если же $a \notin W$, то $a \notin f(a) = W$. Поэтому a удовлетворяет условию принадлежности множеству W, т. е. $a \in W$. Снова получаем противоречие. Итак, в любом случае мы приходим к противоречию. Следовательно, утверждение о существовании взаимно однозначного соответствия f между X и его множеством-степенью $\boldsymbol{P}(X)$ неверно.

Пример 3.19

Пусть $X = \{1, 2, 3, 4\}$ и
$f(1) = \{2, 4\}$,
$f(2) = \{1, 2, 3, 4\}$,
$f(3) = \{1, 3\}$,
$f(4) = \varnothing$.

Тогда $W = \{1, 4\}$ — множество из доказательства теоремы и в него не отображается никакой элемент.

Так как множество X равномощно некоторой части $\boldsymbol{P}(X)$ (биекция $x \leftrightarrow \{x\}$), а $\boldsymbol{P}(X)$ не равномощно никакому подмножеству X (в силу теоремы Кантора—Бернштейна), то можно говорить, что мощность X *меньше мощности* $\boldsymbol{P}(X)$.

Что означает ноль в обозначении $\aleph_0$? Что такое, скажем, $\aleph_1$? Обычно $\aleph_1$ обозначает наименьшую несчётную мощность. Сравнение мощностей имеет точный смысл. Дело в том, что различные мощности линейно упорядочиваются [3]. В работе Кантора 1878 года была сформулирована *континуум-гипотеза*: всякое подмножество отрезка либо конечно, либо счётно, либо равномощно всему отрезку. Другими словами, $\aleph_1 = \boldsymbol{c}$. О дальнейшей судьбе этой гипотезы см. параграф 6.7 из главы 6.

Контрольные вопросы по главе 3

1. Какие два неопределяемых понятия используются в теории множеств Кантора?
2. В чем состоит парадокс Рассела?
3. Является ли пересечение двух произвольных отношений также отношением? Тот же вопрос относительно объединения.
4. Является ли произвольная функция множеством?

5. Имеют ли одинаковую мощность множества $\boldsymbol{P}(\mathbf{Z})$ — множество-степень множества целых чисел и $\boldsymbol{P}(\mathbf{Q})$ — множество-степень множества рациональных чисел?

Рекомендуемая литература к главе 3

[1] Непейвода Н. Н. Прикладная логика : учеб. пособие / Н. Н. Непейвода. — 2-е изд., испр. и доп. — Новосибирск : Изд-во Новосиб. ун-та, 2000. — 521 с.

[2] Зюзьков В. М. Синергетика для программистов : учеб. пособие / В. М. Зюзьков. — Томск : ТУСУР, 2001. — 194 с.

[3] Верещагин Н. К. Лекции по математической логике и теории алгоритмов / Н. К. Верещагин, А. Шень. — 4-е изд., доп. — М. : МЦНМО, 2012. — Часть 1 : Начала теории множеств. — 112 с.

Глава 4

ПРОПОЗИЦИОНАЛЬНАЯ ЛОГИКА

Желтая река течет тысячи миль на север...
Затем поворачивает на восток и течет непрерывно,
Не важно, как она изгибается и поворачивается,
Её волны выходят из источника на горе.

Кунь-Лунь. Железная флейта

4.1 Высказывания и высказывательные формы

Простые высказывания

Понятие *простого* (*элементарного*) *высказывания* является первоначальным (неопределяемым) понятием в математической логике.

Под высказыванием обычно понимают повествовательное предложение, утверждающее что-либо о чем-либо, и при этом мы можем сказать, что оно должно быть истинным или ложным в данных условиях места и времени. *Логическими значениями высказываний* являются «*истина*» и «*ложь*».

Пример 4.1

Примеры простых высказываний

1. Николай Гоголь — автор повести «Тарас Бульба».
2. Литературные произведения о собаках «Каштанка», «Муму» и «Белолобый» написаны Антоном Чеховым.
3. Теорема Пифагора: в прямоугольном треугольнике сумма квадратов катетов равна квадрату гипотенузы.
4. Теорему Пифагора впервые доказал Пифагор.

5. Симфония №8 Шуберта осталась неоконченной.

6. Шуберт не смог завершить симфонию №8 потому, что его жизнь оборвалась.

Высказывания 1, 3 и 5 являются истинными. Высказывание 2 ложно. Истинности высказываний 4 и 6 неизвестны.

Следующие предложения высказываниями не являются.

7. Как пройти в библиотеку?

8. Стой, кто идет!

9. Натуральное число n является простым числом.

10 Число 10^{-6} очень мало.

11. Онегин любит Татьяну.

12. Мне кажется, что «Тараса Бульбу» написал Тарас Шевченко.

Предложения 7 и 8 не являются повествовательными. В предложении 9 не содержится никакого утверждения, и нельзя ставить вопрос об его истинности или ложности. Если подставить в это предложение вместо n какое-нибудь натуральное число, то можно тогда утверждать об его истинности или ложности. Утверждение 10 субъективно, поэтому нельзя говорить об его истинности или ложности. Утверждение 11 принципиально непроверяемое, поскольку относится к внутреннему миру человека и понимается разными людьми неодинаково. С другой стороны, предложение «Онегин сказал, что он любит Татьяну» есть истинное высказывание. Предложение 12 не имеет однозначной интерпретации и выражает отношение говорящего к высказыванию «Николай Гоголь — автор повести «Тарас Бульба».

Предложения, которые не могут иметь четкой и однозначной интерпретации, российский математик Н. Н. Непейвода называет ***квазивысказываниями*** [1, с. 18]. Квазивысказываниями являются предложения 10–12.

. . . . . .

Понятие истинного высказывания в логике согласуется с традиционным понятием истины в естественном языке. Истина объективна. В логике ложь также объективна, но в естественном языке субъективна. Человек является лгуном, если он сознательно говорит ложь. Р. Смаллиан в книге [2] приводит пример: «В одном из учебников по аномальной психологии я прочитал о следующем происшествии. Врачи в психиатрической лечебнице собирались выписать пациента, страдающего шизофренией, и решили подвергнуть его проверке при помощи детектора лжи. Среди прочих пациенту был задан вопрос: «Вы Наполеон?» Пациент ответил отрицательно. Детектор показал, что он лжет».

Именные и высказывательные формы

Буква n, входящая в предложение «Натуральное число n является простым числом», играет роль переменной. В математике ***переменная*** — это языковое выражение, служащее для обозначения произвольного объекта из некоторого фиксированного множества, называемого областью возможных значений этой переменной — ***универсумом***. Если переменная употребляется таким образом, что допускается подстановка вместо нее обозначений (*имен*) объектов универсума, то эта переменная называется ***свободной***.

Пример 4.2

1. Переменные x, y и z являются свободными в выражении $x^2 + y^2 = z^2$.
2. Переменная x в выражении $x + \sin(1/x)$ является свободной.

Однако в математике встречается и такое употребление переменных, при котором не предполагается и не допускается возможность подстановки вместо них имен конкретных объектов.

Примерами таких ситуаций являются выражения:

$$\lim_{x\to 0} \frac{\sin x}{x} = 1,$$

$$\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}.$$

В первом случае переменная x принимает численные значения из множества вещественных чисел, а во втором случае, переменная k — натуральное. Но, очевидно, подстановки чисел в эти выражения вместо x и k бессмысленны.

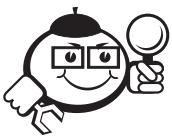
В том случае, когда по смыслу выражения, содержащего переменную, подстановка вместо неё имен конкретных объектов недопустима, эта переменная называется ***связанной***. Но мы можем без изменения смысла выражения заменить связанную переменную любой другой переменной, отсутствующей в данном выражении. Причем «новая» переменная становится также связанной. В одном выражении одна и та же переменная может употребляться и как свободная, и как связанная. Например, в выражении

$$x + \lim_{x\to 0} \frac{\sin x}{x}$$

самое левое вхождение переменной x является свободным, а все остальные вхождения переменной — связанными. Поэтому в общем случае надо говорить о свободных и связанных ***вхождениях*** переменных.

Выражение $x + \sin(1/x)$ не является именем числа, но становится таковым, после замены свободной переменной x любым не нулевым вещественным числом. Выражение $x^2 + y^2 = z^2$ не является высказыванием, поскольку не обладает истинностным значением, но становится высказыванием после замены свободных переменных x, y и z числами. Это наблюдение приводит к следующему определению.

Выражение, содержащее свободные вхождения переменных и превращающееся в имя некоторого объекта (или соответственно высказывание) всякий раз, когда вместо всех свободных вхождений каждой переменной подставляется имя какого-нибудь объекта из универсума, называется ***именной формой*** (или соответственно ***высказывательной формой***). Переменные, имеющие свободные вхождения в именную или высказывательную форму, называются ее *параметрами*. Для высказывательной формы мы часто будем употреблять обозначение вида $A(x_1, x_2, \ldots, x_n)$, явно указывая все ее параметры. Тогда, если $c_1, c_2, \ldots, c_n$ — имена каких-либо объектов из универсума возможных значений переменных $x_1, x_2, \ldots, x_n$ соответственно, то через $A(c_1, c_2, \ldots, c_n)$ обозначается высказывание, полученное из $A(x_1, x_2, \ldots, x_n)$ подстановкой c_1 вместо x_1, c_2 вместо $x_2, \ldots, c_n$ вместо x_n.



Пример 4.3

Пусть $P(n)$ обозначает высказывательную форму «n и $n+2$ — простые числа-близнецы», тогда $P(29)$ — истинное высказывание.

Сложные высказывания и логические операции

Из одних высказываний различными способами можно строить новые более сложные высказывания.

Сложные высказывания образуются из элементарных высказываний применением трех видов операций.

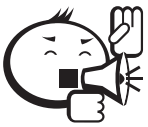
- ***Модальности*** применяются к высказываниям и изменяют наше *отношение* к ним. Получаются квазивысказывания. Например, модальностью является «По словам Сталина, Троцкий был врагом СССР». Такие квазивысказывания изучаются в *модальной логике*[1].
- ***Кванторные конструкции*** применяются к высказывательным формам и дают высказывание. Например, таковы высказывания «Для всех x выполнено $A(x)$» и «Существует x, для которого выполнено $A(x)$», где $A(x)$ — какая-то высказывательная форма.
- ***Логические связки*** (*операции*) применяются к высказываниям и дают новое высказывание, например из высказываний «Гремит гром» и «Сверкает молния» с помощью логической связки «если..., то...» образуется сложное высказывание «Если гремит гром, то сверкает молния».

Кванторные конструкции вида «Для всех...» и «Существует...» изучаются в *логике предикатов* (см. главу 5). Существуют и другие кванторные конструкции, например «Для большинства x выполнено $A(x)$». Они изучаются в модальной логике.

В *логике высказываний* используются только логические операции. Под логической операцией понимается способ построения сложного высказывания из данных высказываний, при котором истинностное значение сложного высказывания полностью определяется истинностными значениями исходных высказываний.

Более точно мы предполагаем, что для высказываний выполняются следующие два соглашения.

[1] Модальные логики изучают модальности — категории, выражающие отношение говорящего к содержанию высказывания, отношение последнего к действительности. Модальность может иметь значение утверждения, приказания, пожелания и др. Выражается специальными формами наклонений, интонацией, модальными словами (например, «возможно», «необходимо», «должен»); в логике такие слова называются модальными операторами, с их помощью указывается способ понимания суждений (высказываний).



Соглашения.

1. Имеются исходные неопределяемые понятия ***истина*** и ***ложь*** (обозначения: ***1*** и ***0*** или ***И*** и ***Л***), которые являются ***истинностными*** (***логическими***) ***значениями*** высказываний.
2. Логическое значение сложного высказывания зависит лишь от логических значений его компонент, а не от его смысла.

Рассмотрим логические операции.

Отрицание

Пусть, например, имеется высказывание

«Солнце вращается вокруг Земли». (4.1)

Мы можем образовать новое предложение, поставив перед данным предложением слова «неверно, что»:

«неверно, что Солнце вращается вокруг Земли», (4.2)

которое, очевидно, снова будет высказыванием (истинным). Обозначим высказывание (4.1) буквой A, тогда высказывание (4.2) традиционно обозначается $\neg A$ и называется ***отрицанием высказывания*** A. Символ «¬» называется ***операцией*** (***связкой***) ***отрицания***. Часто используется обозначение $\overline{A}$.

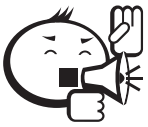
Заметим, что мы могли бы поступить по-другому для образования отрицания A, а именно, мы могли бы просто изменить сказуемое в предложении (4.1):

«Солнце не вращается вокруг Земли». (4.3)

С грамматической точки зрения (4.2) и (4.3) — это разные предложения. Но поскольку в дальнейшем мы будет интересоваться лишь истинностными значением предложений, то высказывания, подобные (4.2) и (4.3), мы будем отождествлять.

Связка отрицание словесно выражается также выражениями:

- «не A»,
- «A неверно»,
- «A ложно»,
- «A не может быть»
- и т. п.



Правило для отрицания. Утверждение $\neg A$ истинно тогда и только тогда, когда A ложно, и ложно в противном случае.

Конъюнкция

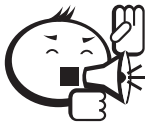
Пусть теперь имеется два высказывания: A и B. Мы можем образовать новое предложение, соединив два данных предложения союзом «и»: «A и B». Такое высказывание «A и B» естественно считать истинным только в случае, когда высказывания оба истинны. Например, мы можем построить сложное высказывание из высказываний (4.1) и (4.2), используя союз «и»:

«Солнце вращается вокруг Земли, и неверно, что Солнце вращается вокруг Земли».

Высказывание «A и B» называется ***конъюнкцией*** высказываний A и B и обозначается $A\&B$ (используется также обозначение $A \wedge B$). Заметим, что для образования конъюнкции могут быть использованы и другие союзы:

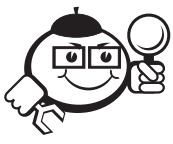
- «A, но и B также»,
- «A вместе с B»,
- «A, несмотря на B»,
- «не только A, но и B»,
- «как A, так и B»,
- «A, хотя и B»
- и т. п.

Все они записываются одинаково: $A\&B$. Разные слова здесь отражают разное отношение к факту, не меняя самого факта. Соответственно, переводя $A\&B$ на естественный язык, нужно выбирать подходящий, наиболее выразительный вариант.



Правило для конъюнкции. Утверждение $A\&B$ истинно в том и только в том случае, когда истинны как A, так и B, и ложно в остальных случаях.

В определении конъюнкции $A\&B$ высказывания A и B равноправны, но даже для этой простой связки ее математический смысл не всегда совпадает с содержательным.



Пример 4.4

Пример Клини

В самом деле, математически $A\&B$ и $B\&A$ означает одно и то же, а содержательно высказывания

«Маша вышла замуж, и у нее родился ребенок» и
«У Маши родился ребенок, и она вышла замуж»

понимаются несколько по-разному. Поскольку каждое из этих предложений выражает еще некоторую причинно-следственную связь исходных высказываний.

Пример 4.5

Вернемся к высказыванию, которое ранее приводилось в качестве простого высказывания:

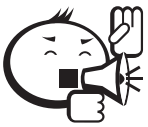
«Литературные произведения о собаках «Каштанка», «Муму» и «Белолобый» написаны Антоном Чеховым».

Не меняя смысла, мы можем преобразовать его и получить конъюнкцию[1] простых высказываний $A\&B\&C$, где A: «Антон Чехов написал «Каштанку», B: «Антон Чехов написал «Муму», C: «Антон Чехов написал «Белолобый».

Дизъюнкция

Сложное высказывание «A или B» символически записывается $A \vee B$. Знак $\vee$ называется ***дизъюнкцией***. Эта же связка применяется при переводе утверждений:

- «A или B или оба вместе»,
- «либо A, либо B»,
- «A и/или B»
- и т. п.



Правило для дизъюнкции. Утверждение $A \vee B$ ложно в том и только в том случае, когда ложны как A, так и B, и истинно в остальных случаях.

Дизъюнкция соответствует неразделительному «или» («A или B или оба вместе»). В естественном языке «или» используется также как разделительная связка: «то или другое, но не оба вместе». Например, высказывание с разделительным «или»

«Я полечу самолетом или я поеду на поезде»

нельзя записать, используя только дизъюнкцию (о представлении «разделительного или» см. замечание 2).

В соответствии с соглашением 2 мы можем применять конъюнкцию и дизъюнкцию к высказываниям, не связанным по смыслу. Поэтому следующие предложения являются высказываниями (первое — истинное, а второе — ложное):

«Снег белый или $2 \times 2 = 5$*»,*
«Снег белый и $2 \times 2 = 5$*».*

[1] Операция конъюнкции двуместная, поэтому мы должны использовать скобки и писать, например, так $(A\&B)\&C$, но в силу ассоциативности конъюнкции (теорема 3 (пункт 3) параграфа 4.3 главы 4) скобки можно опустить.

Импликация

Сложное высказывание «Из A следует B» символически записывается $A \supset B$ или $A \to B$. Знак $\supset$ (и $\to$) называется ***импликацией***. Другими вариантами содержательных утверждений, соответствующих импликации, служат:

- «A достаточное условие для B»,
- «B необходимое условие для A»,
- «A, только если B»,
- «B, если A»,
- «в случае A выполнено и B»,
- «A есть B»,
- «A влечет B».

В импликации $A \supset B$ высказывание A называют посылкой, а B — заключением.

Чтобы признать предложение «Из A следует B» высказыванием, необходимо определить его истинностные значения в зависимости от истинностных значений A и B. Если A истинно, а B ложно, то, конечно, предложение «Из A следует B» нужно считать ложным.

В других случаях правила вычисления истинностного значения $A \supset B$ нуждаются в комментариях. Правила вычисления опираются на содержательный смысл связки $\supset$: из A можно сделать вывод (вывести следствие) B и на наши гипотезы (соглашения 1–2).

Рассмотрим определенную на множестве целых чисел высказывательную форму $A(n)$:

«Если n делится на 6, то n делится на 3».

Общепризнано, что это утверждение является верным. Поэтому будут истинными и высказывания $A(6)$, $A(5)$ и $A(3)$.

Если 6 делится на 6, то 6 делится на 3.
Если 5 делится на 6, то 5 делится на 3.
Если 3 делится на 6, то 3 делится на 3.

Но пользуясь соглашением 2 и заменяя утверждения о делимости на 6 на их конкретные логические значения, получаем, что тогда должно быть

$$(\mathbf{И} \supset \mathbf{И}) = \mathbf{И}$$
$$(\mathbf{Л} \supset \mathbf{Л}) = \mathbf{И}$$
$$(\mathbf{Л} \supset \mathbf{И}) = \mathbf{И}$$

Другими словами, должны быть истинны утверждения:

Из истины следует истина. (4.4)

Из лжи следует ложь. (4.5)

Из лжи следует истина. (4.6)

Истинность $A(6)$, $A(5)$ и $A(3)$ мы должны принять, если мы желаем обеспечить возможность подстановки в доказанные теоремы конкретных значений переменных. А по соглашению 2 нам приходится принять и (4.4)–(4.6).

Определение (Л ⊃ И) = И и соответствующее ему утверждение (4.6) кажутся несколько парадоксальными. Но мы знаем, что из ложных предположений можно иногда содержательным рассуждением получить истинные следствия. Например, из ложного предположения «существуют русалки» следует истинное — «купаться ночью в одиночку в незнакомом месте опасно». Принципиально неправильная система мира Птолемея, в которой центром Вселенной служит Земля, очень точно описывает видимые движения планет. Соглашение 2 опять-таки заставляет нас распространить эту истинность на все мыслимые в математике случаи.

Правда, при этом приходится признать формально истинными и предложения типа:

«Если $2 \times 2 = 5$*, то снег черный».*

Таким образом, если считать, что истинность импликации определяется истинностью ее частей (а не наличием между ними каких-либо причинно-следственных связей), то определение импликации полностью обосновано. Такое определение импликации в философии называется «*материальная импликация*».

Правило для импликации. Утверждение $A \supset B$ ложно в том и только в том случае, когда A истинно и B ложно, и истинно во всех остальных случаях.

Эквиваленция

Связка «A тогда и только тогда, когда B» символически записывается $A \sim B$. Знак ~ называется ***эквиваленцией***. Той же связкой переводятся предложения:

- «A эквивалентно B»,
- «A необходимое и достаточное условие для B»,
- «если A, то B и наоборот»
- и т. п.

Пример эквиваленции:

«Для того, чтобы треугольник имел равные стороны, необходимо и достаточно, чтобы он имел равные углы».

Правило для эквиваленции. Утверждение $A \sim B$ истинно тогда и только тогда, когда истинностные значения A и B совпадают, и ложно в противном случае.

Очевидно, можно считать, что $A \sim B$ есть сокращенная запись формулы $(A \supset B)\ \&\ (B \supset A)$.

Заметим, что если логические связки применять к высказывательным формам, то в результате получаем снова высказывательные формы.

Все сказанное выше о правилах вычисления истинностных значений для сложных высказываний можно свести в качестве итога в следующую таблицу 4.1.

Таблица 4.1 – Правила вычисления истинностных значений для логических операций

A	B	$\neg A$	$A\&B$	$A \vee B$	$A \supset B$	$A \sim B$
И	**И**	**Л**	**И**	**И**	**И**	**И**
И	**Л**	**Л**	**Л**	**И**	**Л**	**Л**
Л	**И**	**И**	**Л**	**И**	**И**	**Л**
Л	**Л**	**И**	**Л**	**Л**	**И**	**И**

Похожесть символов, обозначающих пересечение двух множеств ($\cap$) и конъюнкцию двух высказываний ($\wedge$), а также символов, обозначающих объединение двух множеств ($\cup$) и дизъюнкцию двух высказываний ($\vee$), вовсе не случайна. Пусть множества X и Y имеют характеристические свойства P и Q соответственно. Тогда $X \cup Y = \{x \mid x \in X \vee x \in Y\}$ и $X \cap Y = \{x \mid x \in X \wedge x \in Y\}$. Дополнение множества, в свою очередь, соответствует отрицанию высказывания.

Логические операции для автореферентных высказываний

Если высказывание является автореферентным и «говорит» прямо или косвенно о своем истинностном значении, то для таких высказываний нередко не выполнены логические правила, по которым вычисляются истинностные значения сложного высказывания.

Пример 4.6

А. Операция отрицание. Истинность отрицания самоссылочного предложения не определяется только истинностью самого предложения.

- Два следующих предложения верны, несмотря на то, что одно из них является отрицанием другого:

  «Восьмым словом в этом предложении является частица «не»,

  «Восьмым словом в этом предложении не является частица «не».

- Несмотря на то, что два предложения противоположны друг другу, они оба неверны:

  «Число слов в записанном здесь предложении равно девяти»,

  «Число слов в записанном здесь предложении не равно девяти».

Б. Операция конъюнкция.

А: «У людей на руке пять пальцев» — истина;

В: «В этом предложении пять слов» — истина;

А&В: «У людей на руке пять пальцев, и в этом предложении пять слов» — ложь.

В этом случае содержательное истинностное значение (= ложь) последнего предложения отличается от истинностного значения (= истина), которое должно быть вычислено для конъюнкции двух истинных высказываний.

4.2 Язык логики высказываний

Рассмотренные нами логические понятия служат основой для превращения логики в математическую науку. Будем записывать высказывания в символическом виде. Для этого введем искусственный язык — *язык логики высказываний*.

Алфавит языка состоит из трех множеств.

1. Для обозначения логических операций (также называемых логическими связками) используются пять символов: $\neg$ («отрицание»), $\wedge$ («конъюнкция»), $\vee$ («дизъюнкция»), $\supset$ («импликация»), $\sim$ («эквиваленция»). Последние четыре символа называются ***бинарными*** логическими операциями, а первая логическая операция называется ***унарной***.
2. Счетное множество символов, называемых ***пропозициональными переменными*** (или ***высказывательными переменными***), мы будем изображать большими латинскими буквами, возможно, с индексами — натуральными числами, например Q, R, X, Y, Z, P, P_1, P_2,..., P_n,...
3. Две скобки «(», «)», соответственно называемые ***левая*** и ***правая***, будут использоваться для пунктуации.

Как видно из определения, алфавит содержит счетное множество символов.

*Понятие «**пропозициональная формула**» определяется следующими индуктивными правилами, с помощью которых мы создаем новые формулы из уже построенных формул:*

- *F_0: Каждая пропозициональная переменная есть формула.*
- *F_1: Если A есть формула, то $\neg A$ — также формула.*
- *F_2, F_3, F_4, F_5: Если A и B — формулы, то $(A\&B)$, $(A \vee B)$, $(A \supset B)$, $(A \sim B)$ — также формулы.*

Для любых формул A и B будем называть формулу $\neg A$ *отрицанием формулы* A и соответственно формулы $(A\&B)$, $(A \vee B)$, $(A \supset B)$, $(A \sim B)$ будут называться *конъюнкцией*, *дизъюнкцией*, *импликацией* и *эквиваленцией формул* A и B. В импликации $(A \supset B)$ формулу A называют посылкой, а B — заключением.

Мы будем использовать в формулах большие латинские буквы, иногда с нижними индексами.

Пример 4.7

$$A,\ C \sim \neg C,\ \neg\Big(C \supset \big(X_1 \& (B \vee X_2)\big)\Big).$$

Таким образом, мы определили ***язык логики высказываний****: это упорядоченная пара <**A**, **F**>, где **A** — алфавит логики высказываний, **F** — формулы логики высказываний.*

Когда мы, например, пишем формулу $\neg\Big(C \supset \big(X_1 \wedge (B \vee X_2)\big)\Big)$, то предполагаем, что C, X_1, X_2, B — пропозициональные переменные, именующие какие-то высказывания. Если же формула имеет вид

$$\neg\Big(C \supset \big(X_1 \wedge (B \vee X_2)\big)\Big), \tag{4.7}$$

то тогда предполагаем, что C, X_1, X_2, B — произвольные формулы[1], каждая из которых может совпадать с пропозициональной переменной, а может быть построена из пропозициональных переменных по правилам F_1, F_2, F_3, F_4, F_5. В этом случае формула (4.7) понимается безотносительно к каким-либо высказываниям, а просто как синтаксически правильное выражение, составленное из символов алфавита языка логики высказываний.

Будем для формул A и B писать $A = B$, если формулы A и B идентичны (типографски тождественны). Если какая-то формула не является ни пропозициональной переменной, ни частью другой формулы, то мы будем опускать внешние скобки. Поэтому мы будем считать, что $A = (A)$. Также для сокращения записи мы будем писать $\neg P$ вместо $\neg(P)$, если P — произвольная переменная.

Для удобства записи и чтения формальных выражений принято считать, что связки $\supset$ и $\sim$ связывают слабее, чем $\&$ и $\vee$, а $\neg$ — самая сильная связка, и поэтому формулу

$$\neg\Big((A\&B) \supset \big(C \vee \big(\neg(D)\big)\big)\Big)$$

можно переписать в форме

$$\neg(A\&B \supset C \vee \neg D).$$

До главы 5 слово «переменная» будет обозначать *пропозициональную переменную*, а слово «формула» — *пропозициональную формулу*.

Единственность декомпозиции

Может быть доказано [3, с. 103; 4], что каждая формула строится единственным образом из переменных. Точнее, для каждой формулы X только одно из следующих условий имеет место:

1. X — пропозициональная переменная.
2. Существует единственная формула Y, такая, что $X = \neg Y$.
3. Существуют единственная пара формул Y и Z и единственная бинарная операция $\square$ ($\square$ может обозначать любую логическую операцию), такие, что $X = Y \square Z$.

Поэтому $A_1 \square B_1 = A_2 \square B_2$ только в том случае, если оба вхождения $\square$ обозначают одну и ту же бинарную операцию и $A_1 = A_2$ и $B_1 = B_2$.

[1] Обратите внимание: для символов C, X_1, X_2, B используется шрифт Arial.

Подформулы формул

Определение ***подформулы****, как и определение формулы, рекурсивно.*

1. *Подформулой пропозициональной переменной является только она сама.*
2. *Подформулой формулы* $\neg A$ *является сама формула* $\neg A$*, формула* A *и любая подформула формулы* A*.*
3. *Подформулой формулы* $A \square B$ *(*$\square$ *— любая бинарная логическая связка) является сама формула* $A \square B$*, формулы* A *и* B*, любая подформула формулы* A *и любая подформула формулы* B*.*

В силу единственности декомпозиции множество всех подформул формулы определяется однозначно.

Пример 4.8

Множество подформул формулы $\neg\big(C \supset X_1 \& (B \vee X_2)\big)$ есть

$$\big\{\neg\big(C \supset X_1 \& (B \vee X_2)\big),\ C \supset X_1 \& (B \vee X_2),\ C,\ X_1 \& (B \vee X_2),\ X_1,\ B \vee X_2,\ B,\ X_2\big\}.$$

Легко проверить, что отношение «*формула* A *есть подформула формулы* B» есть отношение частичного порядка.

Введем понятие интерпретации языка логики высказываний. Интерпретировать язык логики высказываний — это значит сопоставить каждой пропозициональной переменной некоторое конкретное высказывание. Если в формуле заменить каждую пропозициональную переменную на соответствующее высказывание, то данная формула превращается в некоторое высказывание, истинностное значение которого будет зависеть лишь от истинностных значений тех высказываний, которые использованы для построения данного сложного высказывания. Но истинностное значение формулы не зависит от смысла высказываний, которые использовались.

Интерпретацией *языка логики высказываний называется любое отображение* φ*:* $\boldsymbol{P} \to \{\boldsymbol{И}, \boldsymbol{Л}\}$*, где* $\boldsymbol{P}$ *— счетное множество всех пропозициональных переменных,* $\{\boldsymbol{И}, \boldsymbol{Л}\}$ *— множество, состоящее из двух истинностных значений.*

Любую интерпретацию φ *можно продолжить до отображения* $\boldsymbol{\varphi}$*:* $\boldsymbol{F} \to \{\boldsymbol{И}, \boldsymbol{Л}\}$*, заданного на множестве всех формул рекурсивным определением.*

Для определения $\boldsymbol{\varphi}(A)$ *частично упорядочим все подформулы формулы* A *относительно порядка «быть подформулой». И далее для любой подформулы* B *используем следующие правила.*

1. *Если* B *— произвольная пропозициональная переменная, то* $\boldsymbol{\varphi}(B) = \varphi(B)$.
2. *Далее, предполагая, что* $\boldsymbol{\varphi}$ *уже определено для всех подформул формулы* B *(не совпадающих с самой* B*), определяем* $\boldsymbol{\varphi}(B)$*:*
   - *Если* $B = \neg C$*, то полагаем* $\boldsymbol{\varphi}(B) = \neg\boldsymbol{\varphi}(C)$.
   - *Если* $B = C \square D$*, то полагаем* $\boldsymbol{\varphi}(B) = \boldsymbol{\varphi}(C) \square \boldsymbol{\varphi}(D)$ *(оба вхождения* $\square$ *обозначают одну и ту же бинарную логическую связку).*

В дальнейшем мы, как правило, будем обозначать расширение интерпретации на формулы $\boldsymbol{\varphi}$ *тем же символом* φ*, как и для переменных. Будем называть* $\varphi(A)$ ***истинностным значением формулы*** A ***в интерпретации*** φ.

Пусть A *— произвольная формула и* $X_1, X_2, \ldots, X_n$, $n > 0$, *— все переменные, входящие в* A*. Присвоим каждой переменной* X_i *(*$i = 1, 2, \ldots, n$*) некоторое истинностное значение (обычно говорят, что в этом случае имеем набор* σ *истинностных значений пропозициональных переменных, входящих в формулу* A*). Таким образом, мы определяем интерпретацию языка логики высказываний. Точнее, мы имеем бесконечное множество интерпретаций, истинностные значения которых фиксированы только на переменных* $X_1, X_2, \ldots, X_n$ *и совпадают там. Обозначим через* φ *одну из таких интерпретаций. Ясно, что истинностное значение* $\varphi(A)$ *является одним и тем же для всех интерпретаций с набором* σ *истинностных значений переменных* $X_1, X_2, \ldots, X_n$.

Поэтому $\varphi(A)$ *также называют* ***истинностным значением формулы*** A ***на наборе*** σ ***истинностных значений переменных формулы*** A.

. . . . . .

Пример 4.9

Пусть

$$A = \neg\Big(\big(X \vee (\neg Y \supset X)\big) \supset \neg Y\Big)$$

и $\{\textbf{Л}, \textbf{И}\}$ — набор истинностных значений переменных X и Y соответственно. Таким образом, определена интерпретация φ, для которой $\varphi(X) = \textbf{Л}$, $\varphi(Y) = \textbf{И}$[1]. Тогда по правилам вычисления $\varphi(A)$ получаем истинностное значение

[1] Через φ обозначается произвольная интерпретация с указанными значениями на переменных X и Y.

$$\varphi(A) = \neg\varphi\Big(\big(X \vee (\neg Y \supset X)\big) \supset \neg Y\Big) = \neg\Big(\varphi\big(X \vee (\neg Y \supset X)\big) \supset \varphi(\neg Y)\Big) =$$
$$= \neg\Big(\big(\varphi(X) \vee \varphi(\neg Y \supset X)\big) \supset \neg\varphi(Y)\Big) = \neg\Big(\big(\mathbf{Л} \vee \big(\varphi(\neg Y) \supset \varphi(X)\big)\big) \supset \neg\mathbf{И}\Big) =$$
$$= \neg\Big(\big(\mathbf{Л} \vee \big(\neg\varphi(Y) \supset \mathbf{Л}\big)\big) \supset \mathbf{Л}\Big) = \neg\Big(\big(\mathbf{Л} \vee (\neg\mathbf{И} \supset \mathbf{Л})\big) \supset \mathbf{Л}\Big) =$$
$$= \neg\Big(\big(\mathbf{Л} \vee (\mathbf{Л} \supset \mathbf{Л})\big) \supset \mathbf{Л}\Big) = \neg\big((\mathbf{Л} \vee \mathbf{И}) \supset \mathbf{Л}\big) = \neg(\mathbf{И} \supset \mathbf{Л}) = \neg\mathbf{Л} = \mathbf{И}.$$

Таким образом, формула A является истинной на наборе $\{X = \mathbf{Л}, Y = \mathbf{И}\}$. И на этом же наборе формула $\big(X \vee (\neg Y \supset X)\big) \supset \neg Y$ ложна.

. . . . . .

Если нас интересуют истинностные значения формулы на всевозможных наборах истинностных значений ее переменных, то соответствующие вычисления можно представить в виде так называемой ***таблицы истинности*** этой формулы. Вот как выглядит такая таблица для формулы A из предыдущего примера.

X	Y	$\neg Y$	$\neg Y \supset X$	$X \vee (\neg Y \supset X)$	$\big(X \vee (\neg Y \supset X)\big) \supset \neg Y$	A
И	**И**	**Л**	**И**	**И**	**Л**	**И**
И	**Л**	**И**	**И**	**И**	**И**	**Л**
Л	**И**	**Л**	**И**	**И**	**Л**	**И**
Л	**Л**	**И**	**Л**	**Л**	**И**	**Л**

Данная таблица имеет четыре строки в соответствии с числом наборов истинностных значений, которые можно составить для двух переменных. Вообще, если в формулах имеется n переменных, то ее таблица истинности содержит 2^n строк. Столбцы соответствуют подформулам формулы и располагаются в таблице в соответствии с частичным порядком на подформулах слева направо, начиная с переменных. Количество столбцов может быть как угодно большое, даже для формулы с одной переменной (например, если каждая подформула есть отрицание предыдущей подформулы).

Покажем, как с помощью логики высказываний можно решать логические задачи.

Задача 1. Известны следующие факты:

1. Если A виновен и B не виновен, то C виновен.
2. C никогда не действует в одиночку.
3. A никогда не ходит на дело вместе с C.
4. Никто, кроме A, B и C, в преступлении не замешан, и, по крайней мере, один из этой тройки виновен.

Полностью доказать, кто виновен, а кто не виновен, из этих фактов не получится, но чтобы выдвинуть неопровержимое обвинение против одного из них, материала вполне достаточно.

Решение. Обозначим через пропозициональные переменные A, B и C высказывания «персона A виновна», «персона B виновна» и «персона C виновна» соответственно. Тогда факты 1–4 можно записать в виде формул:

1. $A\&\neg B \supset C$.
2. $C \supset A \vee B$.
3. $A \supset \neg C$.
4. $A \vee B \vee C$.

Для решения задачи достаточно определить, для каких значений переменных эти формулы одновременно истинны.

Первый способ решения: мы высказываем гипотезы и рассуждаем по формулам.

Пусть C — истина, тогда по формуле 2 имеем, что $A \vee B$ = **И**. Далее, если A = **И**, то по формуле 3 C = **Л**. Получили противоречие с исходным предположением. Следовательно, B = **И**.

Пусть теперь C — ложь. Тогда по формуле 1 получаем $A\&\neg B$ = **Л**. Последняя формула может быть ложной, если B = **И**. Если же B = **Л**, то тогда должно быть A = **Л**. Следовательно, в этом случае все три переменные ложны, что противоречит истинности формулы 4. Таким образом, B = **И**.

Получили, что независимо от C переменная B всегда истинна. Следовательно, B — преступник.

Второй способ — решение «в лоб»: строим таблицу истинности сразу для четырех исходных формул (столбцы для некоторых подформул опускаем).

A	B	C	$A\&\neg B$	$A \vee B$	$A\&\neg B \supset C$	$C \supset A \vee B$	$A \supset \neg C$	$A \vee B \vee C$
И	**И**	**И**	**Л**	**И**	**И**	**И**	**Л**	**И**
Л	**И**	**И**	**Л**	**И**	**И**	**И**	**И**	**И**
И	**Л**	**И**	**И**	**И**	**И**	**И**	**Л**	**И**
И	**И**	**Л**	**Л**	**И**	**И**	**И**	**И**	**И**
Л	**Л**	**И**	**Л**	**Л**	**И**	**Л**	**И**	**И**
Л	**И**	**Л**	**Л**	**Л**	**И**	**И**	**И**	**И**
И	**Л**	**Л**	**И**	**И**	**Л**	**И**	**И**	**И**
Л	**Л**	**Л**	**Л**	**Л**	**И**	**И**	**И**	**Л**

Анализируя таблицу, видим, что все четыре формулы истинны только в трех строчках и каждый раз только переменная B истинна. Следовательно, B — преступник.

Раймонд Смаллиан в нескольких своих книгах (например, в [2]) рассмотрел различные варианты оригинальных задач с рыцарями и лжецами.

Путешественник попадает на остров, где живут только рыцари и лжецы. Рыцари всегда говорят правду, лжецы всегда лгут. Путешественник встречается с различными группами островитян, задает им вопросы с целью, как правило, узнать кто перед ним, рыцарь или лжец. Требуется по ответам островитян выяснить, кто они есть.

Приведем несколько типичных задач и обсудим их решения.

Задача 1. Путешественник встретил двух островитян α и β. Островитянин α сказал: «Мы оба лжецы». Кто на самом деле α и кто β?

Решение. Рыцарь не может утверждать, что он лжец. Поэтому α лжец, но они вместе с β не могут быть оба лжецами, так как в этом случае α говорил бы правду. Поэтому получаем: α лжец, а β рыцарь.

Задача 2. Теперь α говорит другую фразу о себе и β: «По крайней мере, один из нас лжец». Кто α и кто β?

Решение. Пусть α лжец. Тогда его фраза ложь и они оба рыцари, но это противоречит исходному предположению. Поэтому α рыцарь. И из его правдивого заявления следует решение: α рыцарь, а β лжец.

Мы решали неформально. Но оказывается, можно получить ответ, используя язык логики высказываний.

Пусть α один из жителей острова. Обозначим через A высказывание «α рыцарь». Тогда $\neg A$ обозначает высказывание «α лжец». Пусть α утверждает некоторое высказывание P. Нам неизвестно, рыцарь α или нет, и так же неизвестно, высказывание P — истина или ложь. Но несомненно, если α рыцарь, то P истинно, и наоборот, если P истинно, то α рыцарь. Следовательно, формула $A \sim P$ должна всегда быть истинной. И точно так же для любого другого жителя β, говорящего какое-то высказывание Q, должна быть истинна формула $B \sim Q$, где B обозначает высказывание «β рыцарь». И решением задачи является интерпретация языка логики высказываний, в которой все таким образом составленные формулы являются истинными.

Решение задачи 1. Построим таблицу истинности для формулы $A \sim \neg A \& \neg B$, полученной из условия задачи.

A	B	$\neg A \& \neg B$	$A \sim \neg A \& \neg B$
И	**И**	**Л**	**Л**
И	**Л**	**Л**	**Л**
Л	**И**	**Л**	**И**
Л	**Л**	**И**	**Л**

По таблице получаем единственное решение: α лжец, β рыцарь.

Решение задачи 2. Построим таблицу истинности для формулы $A \sim \neg(A \& B)$, полученной из условия задачи.

A	B	$\neg(A \& B)$	$A \sim \neg(A \& B)$
И	**И**	**Л**	**Л**
И	**Л**	**И**	**И**
Л	**И**	**И**	**Л**
Л	**Л**	**И**	**Л**

По таблице получаем единственное решение: α рыцарь, β лжец.

Вернемся к автореференции, о которой шла речь в конце первого параграфа.

Крайняя опасность автореференции обыграна в ***парадоксе Карри***[1].

Пусть A — произвольное высказывание. Пусть B — высказывание «Если B, то A».

Мы не знаем, верно ли высказывание B. Но если бы высказывание B было верным, то это влекло бы истинность A. Но именно это и утверждается в высказывании B, таким образом, B — верно. Но тогда доказано и A.

Таким образом, Карри показал, что обычная импликация в любой системе с автореференцией позволяет вывести любое предложение, что является противоречием.

Переформулируем парадокс Карри на языке задач о рыцарях и лжецах.

Задача 3. В этот раз β говорит о себе и α следующее: «Если я рыцарь, то α рыцарь». Кто они?

Решение. Имеем, формула $B \sim (B \supset A)$ есть истина. Построим таблицу истинности.

[1] Карри, Хаскелл Брукс (1900–1982 гг.) — американский математик и логик.

A	B	$B \supset A$	$B \sim (B \supset A)$
И	**И**	**И**	**И**
И	**Л**	**И**	**Л**
Л	**И**	**Л**	**Л**
Л	**Л**	**И**	**Л**

Так как $B \sim (B \supset A)$ — истина, то B = **И**, A = **И**, следовательно, β и α — рыцари.

Таким образом, парадокс Карри возникает, когда мы предполагаем, что формула $B \sim (B \supset A)$ есть истина.

В большинстве случаев в задачах с рыцарями и лжецами использование таблиц истинности достаточно трудоемко. Но применение пропозициональной логики позволит быстро найти решение, если мы программным путем будем находить интерпретации, в которых истинны заданные формулы. Можно, например, использовать систему компьютерной алгебры Mathematica [5].

4.3 Тавтологии и равносильности

Определим несколько важных видов формул.

*Формула называется **выполнимой**, если существует интерпретация, в которой эта формула истинна.*

*Формула называется **опровержимой**, если существует интерпретация, в которой эта формула ложна.*

*Формула A называется **тавтологией** (или **тождественно истинной**), если формула истинна во всех интерпретациях, в этом случае мы будем использовать обозначение $\models A$.*

*Формула называется **противоречием** (или **тождественно ложной**), если формула ложна во всех интерпретациях.*

Конечно, каждое из этих определений можно эквивалентным образом сформулировать, используя понятие набора истинностных значений. Например, формула является противоречием, если она ложна независимо от того, какие значения принимают встречающиеся в ней пропозициональные переменные.

Приведем утверждения, которые являются очевидными следствиями данных определений:

- A — тавтология тогда и только тогда, когда A не является опровержимой;
- A — тождественно ложна тогда и только тогда, когда A не является выполнимой;
- A — тавтология тогда и только тогда, когда $\neg A$ — тождественно ложна;
- A — тождественно ложна тогда и только тогда, когда $\neg A$ — тавтология.

Теорема 1. Подстановка вместо пропозициональных переменных. Пусть A — формула, в которую входят только пропозициональные переменные $X_1, X_2, \ldots, X_n$, а B — формула, полученная из A одновременной подстановкой формул $C_1, C_2, \ldots, C_n$ вместо $X_1, X_2, \ldots, X_n$ соответственно. Если A — тавтология (противоречие), то B — тавтология (противоречие соответственно).

Доказательство. Рассмотрим произвольную интерпретацию φ, определенную для всех переменных $Y_1, Y_2, \ldots, Y_k$, содержащихся в формулах $C_1, C_2, \ldots, C_n$. Если A — тавтология, то докажем, что B — тавтология. От противного. Пусть $Y_1, Y_2, \ldots, Y_k$ — все переменные, содержащиеся в формулах $C_1, C_2, \ldots, C_n$. Только эти переменные являются пропозициональными переменными, присутствующими в формуле B. Рассмотрим интерпретацию φ, определенную для всех переменных $Y_1, Y_2, \ldots, Y_k$, и предположим, что формула B ложна в этой интерпретации. Тогда $\varphi(C_1), \varphi(C_2), \ldots, \varphi(C_n)$ — некоторый набор истинностных значений для переменных $X_1, X_2, \ldots, X_n$ соответственно, при которых формула A ложна (так как формула B построена из подформул $C_1, C_2, \ldots, C_n$ таким же образом, как A построена из $X_1, X_2, \ldots, X_n$). Получили противоречие. Случай, когда A — противоречие, доказывается аналогично.

Пусть имеется некоторая тавтология A. В силу теоремы 1 любая подстановка произвольных формул в формулу A вместо пропозициональных переменных дает тавтологию. Поэтому тавтологии являются схемами истинных высказываний, в которых выражаются ***логические законы***.

Пример 4.10

Перечислим некоторые важные тавтологии (A, B, C — произвольные формулы):

1. $\models A \vee \neg A$ (***закон исключенного третьего*** или ***tertium nondatur***);
2. $\models A \supset A$;
3. $\models A \supset (B \supset A)$;
4. $\models (A \supset B) \supset \big((B \supset C) \supset (A \supset C)\big)$ (***цепное рассуждение***);
5. $\models \big(A \supset (B \supset C)\big) \supset \big((A \supset B) \supset (A \supset C)\big)$;
6. $\models (A\&B) \supset A$; $(A\&B) \supset B$;
7. $\models A \supset \big(B \supset (A\&B)\big)$;
8. $\models A \supset (A \vee B)$; $B \supset (A \supset B)$;
9. $\models (\neg B \supset \neg A) \supset \big((\neg B \supset A) \supset B\big)$;
10. $\models \big((A \supset B) \supset A\big) \supset A$ (***закон Пирса***);
11. $\models \neg(B\&\neg B)$ (***закон противоречия***);
12. $\models (A \supset B) \vee (B \supset A)$.

Тавтология 12 выражает на первый взгляд парадоксальный закон: для любых высказываний A и B хотя бы одна из импликаций $A \supset B$ и $B \supset A$ является истинной.

Каждую из этих тавтологий можно обосновать, например, составив таблицу и вычислив по ней значение формулы, считая A, B и C — пропозициональными переменными.

Использование таблиц истинности является универсальным способом для установления того, является ли формула выполнимой, опровержимой, тавтологией или противоречием. Но если в формуле более трех переменных, то по мере увеличения количества переменных построение таблицы человеком становится очень трудоемким и невозможным. Использование компьютерных программ позволяет увеличить количество переменных в рассматриваемых формулах, но тоже до некоторого предела.

Тавтологичность формул некоторого вида можно установить с помощью доказательства от противного. Подробно метод доказательства от противного описан в параграфе 7.3 главы 7.

Покажем, как использовать доказательство от противного для некоторых формул $A = B \supset C$. Вы предполагаете, что формула A ложна и, делая отсюда выводы об истинном значении подформул формулы A, приходите к противоречию или определяете значения переменных, при которых формула ложна. Для формул указанного вида ложность $B \supset C$ однозначно определяет: B — истинна, а C — ложна. Этот метод эффективней, чем построение таблицы истинности, в том случае, когда истинностный анализ подформул можно произвести однозначно или с небольшим перебором.

Задача 1. Является ли формула $\big((P \supset Q)\&P\big) \supset Q$ тавтологией?

Решение. Предположим, что $\big((P \supset Q)\&P\big) \supset Q$ ложна при некоторых значениях пропозициональных переменных P и Q. Представим наши рассуждения в виде таблицы. Каждая следующая строчка таблицы есть логическое следствие предыдущей строки.

$\big((P \supset Q)\&P\big) \supset Q$ = **Л**	
$(P \supset Q)\&P$ = **И**	Q = **Л**
$P \supset Q$ = **И**, P = **И**	
И $\supset Q$ = **И** (подставили в формулу **И** вместо P)	
Q = **И**	

Получили противоречие (Q = **И** и Q = **Л** одновременно), следовательно, исходное предположение о ложности $\big((P \supset Q)\&P\big) \supset Q$ неверно, и получаем $\models \big((P \supset Q)\&P\big) \supset Q$.

Задача 2. Является ли тавтологией формула

$$\big((P \supset Q)\&(\neg R \supset \neg Q)\&(T \supset \neg R)\big) \supset (P \supset \neg T)?$$

Решение. Предположим, что формула ложна при некоторых значениях пропозициональных переменных P, Q, R и T.

$\big((P \supset Q)\&(\neg R \supset \neg Q)\&(T \supset \neg R)\big) \supset (P \supset \neg T) =$ **Л**	
$(P \supset Q)\&(\neg R \supset \neg Q)\&(T \supset \neg R) =$ **И**	$P \supset \neg T =$ **Л**
$P \supset Q =$ **И**, $\neg R \supset \neg Q =$ **И**, $T \supset \neg R =$ **И**	$P =$ **И**, $\neg T =$ **Л**
И $\supset Q =$ **И**, $\neg R \supset \neg Q =$ **И**, **И** $\supset \neg R =$ **И** (подставили в формулы **И** вместо P и T)	
$Q =$ **И**, $\neg R =$ **И**, $\neg R \supset \neg Q =$ **И**	
И $\supset \neg$**И** = **И** (подставили в формулы **И** вместо Q и $\neg R$)	
И $\supset$ **Л** = **И**. Но это невозможно!	

Пришли к противоречию, следовательно, исходная формула — тавтология.

Задача 3. Является ли формула $\big((P \supset Q)\&P\big) \supset (Q \supset \neg P)$ тавтологией?

Решение. Предположим, что формула $\big((P \supset Q)\&P\big) \supset (Q \supset \neg P)$ ложна при некоторых значениях пропозициональных переменных P и Q.

$\big((P \supset Q)\&P\big) \supset (Q \supset \neg P) =$ **Л**	
$(P \supset Q)\&P =$ **И**	$Q \supset \neg P =$ **Л**
$P \supset Q =$ **И**, $P =$ **И**	$Q =$ **И**, $\neg P =$ **Л**
И $\supset Q =$ **И** (подставили в формулу **И** вместо P)	
$Q =$ **И**	

Получили значения переменных $Q =$ **И** и $P =$ **И**, при которых формула ложна:

$$\big((P \supset Q)\&P\big) \supset (Q \supset \neg P) = \textbf{Л},$$

следовательно, эта формула не является тавтологией.

На множестве пропозициональных формул определим отношение эквивалентности.

*Формулы A и B называются **равносильными**, если эти формулы принимают одинаковые истинностные значения в любой интерпретации. Равносильность формул обозначается как $A \equiv B$.*

Установить, равносильные формулы или нет, мы можем с помощью таблицы истинности, построенной сразу для двух формул.

Пример 4.11

Рассмотрим формулы $\neg X \vee \neg Y$ и $\neg(X\&Y)$.

X	Y	$\neg X$	$\neg Y$	$\neg X \vee \neg Y$	$X\&Y$	$\neg(X\&Y)$
И	**И**	**Л**	**Л**	**Л**	**И**	**Л**
И	**Л**	**Л**	**И**	**И**	**Л**	**И**
Л	**И**	**И**	**Л**	**И**	**Л**	**И**
Л	**Л**	**И**	**И**	**И**	**Л**	**И**

Столбцы пятый и седьмой совпадают, поэтому $\neg X \vee \neg Y \equiv \neg(X\&Y)$.

Замечание 1. Из определений тавтологии и равносильности сразу следует, что $A \equiv B$ тогда и только тогда, когда $\models A \sim B$.

Теорема 2. Пусть формулы A и B равносильны, причем $X_1, X_2, \ldots, X_n$ — список всех переменных, входящих в A или в B. Пусть формулы D и E получены из A и B одновременной подстановкой формул $C_1, C_2, \ldots, C_n$ вместо $X_1, X_2, \ldots, X_n$ соответственно. Тогда $D \equiv E$.

Доказательство следует из предыдущего замечания и теоремы 1.

Теорема 3. Основные равносильности. Для любых формул A, B, C справедливы следующие равносильности:

1. $A\&B \equiv B\&A$ (коммутативность &);
2. $A\&A \equiv A$ (идемпотентность &);
3. $A\&(B\&C) \equiv (A\&B)\&C$ (ассоциативность &);
4. $A \vee B \equiv B \vee A$ (коммутативность $\vee$);
5. $A \vee A \equiv A$ (идемпотентность $\vee$);
6. $A \vee (B \vee C) \equiv (A \vee B) \vee C$ (ассоциативность $\vee$);
7. $A \vee (B\&C) \equiv (A \vee B)\&(A \vee C)$ (дистрибутивность $\vee$ относительно &);
8. $A\&(B \vee C) \equiv (A\&B) \vee (A\&C)$ (дистрибутивность & относительно $\vee$);
9. $A\&(A \vee B) \equiv A$ (первый закон поглощения);
10. $A \vee (A\&B) \equiv A$ (второй закон поглощения);
11. $\neg\neg A \equiv A$ (снятие двойного отрицания);
12. $\neg(A\&B) \equiv \neg A \vee \neg B$ (первый закон де Моргана);
13. $\neg (A \vee B) \equiv \neg A\&\neg B$ (второй закон де Моргана);
14. $A \equiv (A\&B) \vee (A\&\neg B)$ (первый закон расщепления);
15. $A \equiv (A \vee B)\&(A \vee \neg B)$ (второй закон расщепления).
16. $A \sim B \equiv (A \supset B)\&(B \supset A) \equiv (A\&B) \vee (\neg A\&\neg B)$;
17. $A \supset B \equiv \neg A \vee B \equiv \neg(A\&\neg B)$;
18. $A \vee B \equiv \neg A \supset B \equiv \neg(\neg A\&\neg B)$;
19. $A\&B \equiv \neg(A \supset \neg B) \equiv \neg(\neg A \vee \neg B)$;
20. $A \supset B \equiv \neg B \supset \neg A$ (закон контрапозиции).

Равносильности 16–19 показывают, что одни связки могут быть выражены через другие.

Все равносильности теоремы 3 легко доказываются либо с помощью таблиц истинности, либо без них. В качестве примера докажем 7 с помощью таблицы истинности.

A	B	C	$B\&C$	$A \vee (B\&C)$	$A \vee B$	$A \vee C$	$(A \vee B)\&(A \vee C)$
И	**И**	**И**	**И**	**И**	**И**	**И**	**И**
И	**И**	**Л**	**Л**	**И**	**И**	**И**	**И**
И	**Л**	**И**	**Л**	**И**	**И**	**И**	**И**
И	**Л**	**Л**	**Л**	**И**	**И**	**И**	**И**
Л	**И**	**И**	**И**	**И**	**И**	**И**	**И**
Л	**И**	**Л**	**Л**	**Л**	**И**	**Л**	**Л**
Л	**Л**	**И**	**Л**	**Л**	**Л**	**И**	**Л**
Л	**Л**	**Л**	**Л**	**Л**	**Л**	**Л**	**Л**

Докажем равносильность 12 без таблицы истинности. Пусть на некотором наборе истинностных значений переменных формула $\neg(A\&B)$ принимает значение **Л**. Тогда формула $A\&B$ принимает значение **И**, а поэтому обе формулы A и B принимают значение **И**. Но в этом случае, очевидно, и правая часть равносильности 12 принимает значение **Л**. И наоборот, пусть формула $\neg A \vee \neg B$ принимает значение **Л**. Тогда формулы $\neg A$, $\neg B$ принимают значение **Л**, а формулы A, B — значение **И**. Очевидно, что и левая часть равносильности 12 принимает значение **Л**.

Замечание 2. Пусть символ $\bullet$ обозначает бинарную операцию «исключительное или», которая выдает истину только в случае, когда один из операндов имеет значение истина. Тогда $A \bullet B \equiv (A\&\neg B) \vee (B\&\neg A)$, что можно проверить с помощью таблицы истинности.

Используя известные равносильности, можно получать новые. Об этом говорит следующая теорема.

Теорема 4. Правило равносильных преобразований. Пусть C_A — формула, содержащая A в качестве своей подформулы. Пусть C_B получается из C_A заменой A в этом вхождении на B. Тогда, если $A \equiv B$, то $C_A \equiv C_B$.

Для доказательства нам потребуются две леммы.

Лемма 1. Пусть $A \equiv B$ и C — произвольная формула. Тогда $\neg A \equiv \neg B$, $A\&C \equiv B\&C$, $C\&A \equiv C\&B$, $A \vee C \equiv B \vee C$, $C \vee A \equiv C \vee B$, $A \supset C \equiv B \supset C$, $C \supset A \equiv C \supset B$, $A \sim C \equiv B \sim C$, $C \sim A \equiv C \sim B$.

Доказательство. Докажем, например, равносильность $A \supset C \equiv B \supset C$. Пусть на произвольном наборе истинностных значений пропозициональных переменных формулы A и B принимают одинаковое истинностное значение (скажем, s). Пусть t — значение C на этом распределении истинностных значений. Обе части рассматриваемой равносильности принимают одно и то же значение $s \supset t$.

Лемма 2. Пусть $A \equiv B$ и C — формула, в которой выделено одно вхождение некоторой переменной X. Пусть C_A получается из C заменой этого вхождения X на A, а C_B — из C заменой того же вхождения X на B. Тогда $C_A \equiv C_B$.

Доказательство леммы будет проведено в параграфе 7.2 главы 7 с помощью математической индукции по построению.

Доказательство теоремы 4. Рассмотрим произвольную переменную X и получим формулу C из C_A заменой A на X. Будем считать это вхождение X в C выделенным. Тогда C, A, B, C_A, C_B удовлетворяют условиям леммы 2, а значит, $C_A \equiv C_B$.

Замечание 3. Из теоремы 4 мы сразу получаем несколько полезных следствий. Например, пусть имеется формула, содержащая только n штук операций конъюнкции. Если $n > 1$, то необходимо присутствие скобок в формуле, чтобы показать, в каком порядке выполняется бинарная операция конъюнкции. В силу ассоциативности & (равносильность 3 из теоремы 3) сразу получаем, что истинностное значение исходной n-кратной конъюнкции не зависит от расстановки скобок. Поэтому при записи такой формулы, скажем $A\&B\&C\&D\&E$, можно вообще не использовать скобки. Так как n-кратная дизъюнкция также ассоциативна, то мы можем использовать n-кратную дизъюнкцию также без скобок.

Замечание 4. Для каждой формулы можно указать равносильную ей формулу, не содержащую логических символов $\supset$ и $\sim$. В самом деле, опираясь на правило равносильных преобразований, можно в исходной формуле каждую подформулу вида $A \sim B$ заменить на $(A\&B) \vee (\neg A\&\neg B)$, а каждую подформулу вида $A \supset B$ — на $\neg A \vee B$ (см. равносильности 16 и 17 теоремы 3).

Замечание 5. Возможно, вы заметили, что основные равносильности логики высказываний и основные тождества алгебры множеств выражаются одними и теми же законами. Это не случайно: и алгебра высказываний, и алгебра множеств — это различные варианты математической структуры, называемой ***булевой алгеброй*** (см. например, [6] или любой учебник по дискретной математике).

4.4 Логическое следствие

Дадим основные определения этого параграфа.

Непустое множество формул Г будем называть ***выполнимым***[1], если существует интерпретация φ, что все формулы из Г в интерпретации φ истинны. При этом интерпретация φ называется ***моделью*** множества формул Г.

Пустое множество выполнимо, и его модель есть любая интерпретация.

Заметим, что если множество Г конечно и состоит, например, из формул A_1, $A_2, \ldots, A_n$, то невыполнимость множества Г равносильна противоречивости формулы

$$A_1 \,\&\, A_2 \,\&\, \ldots \,\&\, A_n.$$

[1]Используется также терминология: логически непротиворечивым, непротиворечивым или семантически непротиворечивым, сравните с логикой первого порядка (глава 5).

Пусть Γ *— произвольное (возможно, пустое) множество формул и* A *— какая-то формула. Будем говорить, что формула* A *является* ***логическим следствием*** *множества* Γ *и писать* $\Gamma \models A$*, если эта формула истинна в любой модели множества* Γ.

Иногда говорят, что «множество формул Γ *логически влечет* формулу A» или «формула A *логически следует* из множества формул Γ».

Если $\Gamma = \{A_1, A_2, \ldots, A_n\}$, то пишут $A_1, A_2, \ldots, A_n \models A$. Для $\Gamma = \varnothing$ пишут $\models A$, что согласуется с ранее введенным обозначением для тавтологий, поскольку тождественно истинная формула истина в любой интерпретации.

Замечание 3. В определении понятия логического следования не предполагается, что множество Γ обязательно имеет хотя бы одну модель. Просто в случае отсутствия моделей у множества Γ на формулу A не накладывается никаких ограничений и, следовательно, считается по определению, что невыполнимое множество формул логически влечет любую формулу логики высказываний.

Теорема 5.

(a) $A \models B$ тогда и только тогда, когда $\models A \supset B$.

(b) Более общо, при $n \geqslant 1$: $A_1, A_2, \ldots, A_{n-1}, A_n \models B$ тогда и только тогда, когда $A_1, A_2, \ldots, A_{n-1} \models A_n \supset B$.

Доказательство.

(a) Рассмотрим таблицы истинности для A, B и $A \supset B$ с перечнем всех фигурирующих в них переменных на входах этих таблиц. Для выяснения, имеет ли место $A \models B$, надо пренебречь строками, в которых A дает **Л**, ибо в них формула $A \supset B$ всегда принимает значение **И** (по правилу импликации). Рассмотрим прочие строки, т. е. строки, где A дает **И**. Если $A \models B$, то B дает **И** в этих строках, а по правилу для импликации и $A \supset B$ дает **И**. В остальных же строках она и так истинна. Следовательно, $\models A \supset B$. Обратно, если $\models A \supset B$, то $A \supset B$ дает **И** во всех строках, где A дает **И** (и, конечно, во всех остальных строках). Следовательно, по правилу импликации, B должно давать **И** во всех тех строках, где A дает **И**, а это значит, что $A \models B$.

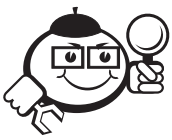
(b) Рассмотрим случай $n \geqslant 2$. Возьмем таблицы истинности для $A_1, A_2, \ldots, A_n$, B, $A_n \supset B$. Рассуждаем, как и выше, но на этот раз в качестве A фигурирует A_n: мы ограничиваемся рассмотрением тех строк, где $A_1, A_2, \ldots, A_{n-1}$ дают **И**.

Следствие. При $n \geqslant 1$ $A_1, A_2, \ldots, A_{n-1}, A_n \models B$ тогда и только тогда, когда

$$\models A_1 \supset \Big(\ldots\big(A_{n-1} \supset (A_n \supset B)\big)\ldots\Big)$$

Доказательство проводится n-кратным применением теоремы.

Таким образом, задача установления того, какие формулы являются логическими следствиями данных формул $A_1, A_2, \ldots, A_{n-1}, A_n$, сводится к задаче выяснения, какие формулы есть тавтологии. В этом, в частности, и заключается важная роль тавтологий.



Пример 4.12

Проверим, что $(P \supset Q) \models (Q \supset P)$ не выполняется. Предположим противное: $(P \supset Q) \models (Q \supset P)$, следовательно, $(P \supset Q) \supset (Q \supset P)$ — тавтология. Но если взять P = **Л**, а Q = **И**, то $(P \supset Q) \supset (Q \supset P)$ = **Л**. Противоречие говорит о том, что $Q \supset P$ не является логическим следствием $P \supset Q$.

Контрольные вопросы по главе 4

1. Чем различаются определения истинностного значения для простого и составного высказываний?
2. Какие вхождения переменной x в выражение

$$\int_0^x \sin(x) = 1 - \cos(x)$$

являются связанными, а какие — свободными?

3. Результат какой бинарной логической операции является истинным в одном случае из четырех?
4. Какое из следующих двух высказываний мог сказать житель острова рыцарей и лжецов?

   Если я лжец, то я рыцарь.
   Если я рыцарь, то я лжец.

5. Может ли формула пропозициональной логики одновременно быть выполнимой и тавтологией?

Рекомендуемая литература к главе 4

[1] Непейвода Н. Н. Прикладная логика : учеб. пособие / Н. Н. Непейвода. — 2-е изд., испр. и доп. — Новосибирск : Изд-во Новосиб. ун-та, 2000. — 521 с.

[2] Смаллиан Р. Как же называется эта книга? / Р. Смаллиан. — М. : Издательский дом Мещерякова, 2007. — 272 с.

[3] Клини С. К. Введение в метаматематику / С. К. Клини. — 2-е изд., испр. — М. : Книжный дом «Либроком», 2009. — 528 с.

[4] Черч А. Введение в математическую логику / А. Черч. — 2-е изд., испр. — М. : Книжный дом «Либроком», 2009. — Т. 1.

[5] WolframMathematica [Электронный ресурс]. — URL : http://www.wolfram.com/mathematica/ (дата обращения: 08.05.2015).

[6] Игошин В. И. Математическая логика и теория алгоритмов / В. И. Игошин. — 2-е изд., стереотип. — М. : Академия, 2008. — 448 с.

Глава 5

ЯЗЫКИ ПЕРВОГО ПОРЯДКА

> Если бы я владел знаниями, то шел бы по большой дороге. Единственная вещь, которой я боюсь, — это узкие тропинки. Большая дорога совершенна ровна, но народ любит узкие тропинки.
>
> *Лао-цзы*

Логика высказываний обладает довольно слабыми выразительными возможностями. В ней нельзя выразить даже очень простые с математической точки зрения рассуждения. Укажем примеры слабости языка логики высказываний.

1. В языке логики высказываний никак нельзя передать внутреннюю структуру математического утверждения, например такого как «для любого положительного числа x существует такое число y, что $x = y^2$». Языковые конструкции «для любого x» и «существует y» называются кванторами и широко используются в математике. Кроме того, из одной высказывательной формы мы можем создать несколько высказываний, просто подставляя вместо параметров формы различные имена элементов универсума. Но общее происхождение полученных таким образом высказываний никак нельзя передать в формулах логики высказываний.
2. Рассмотрим, например, следующее умозаключение. «Всякое целое число является рациональным. Число 2 — целое. Следовательно, 2 — рациональное число». Все эти утверждения с точки зрения логики высказываний являются атомарными. Средствами логики высказываний нельзя вскрыть внутреннюю структуру, и поэтому нельзя доказать логичность этого рассуждения в рамках логики высказываний.

Для точного описания математических утверждений нам понадобится искусственный язык. В математической логике наиболее распространены так называемые ***языки первого порядка***, которые являются расширениями языка пропозициональных формул. Языки первого порядка отличаются точностью и удобством для записи математических утверждений, и допускают сравнительно легкий перевод на обычный язык и обратно.

5.1 Предикаты и кванторы

Элементарные высказывания с точки зрения пропозициональной логики характеризуются только истинностными значениями и являются неделимыми конструкциями. Но логиков во многих случаях интересует и внутренняя структура простых предложений: *что* и *о чем* говорится в данном предложении. С точки зрения грамматики естественного языка, *субъект* (или подлежащее) — это то, о чем или о ком говорится в предложении, а *предикат* (называемый также сказуемым или группой сказуемого) выражает то, что говорится о субъекте. В математической логике произвольную высказывательную форму со свободными переменными называют также предикатом. Если мы заменим свободные переменные, входящие в эту форму, на имена объектов универсума, то получим некоторое отношение между этими объектами, которое, в зависимости от конкретных объектов-параметров, будет истинным или ложным высказыванием.

Таким образом, со всяким предикатом, понимаемым как высказывательная форма, естественным образом связана функция, которая каждому набору значений параметров сопоставляет истинное или ложное высказывание. Если мы не будем различать высказывания, имеющие одно и то же истинностное значение, то придем к следующему определению: k-местным ***предикатом*** на универсуме M называется произвольная функция

$$P\colon M^k \to \{\mathbf{И}, \mathbf{Л}\}.$$

Пример 5.1

Пусть универсум — множество натуральных чисел **N**. Определим одноместный предикат P: $\mathbf{N} \to \{\mathbf{И}, \mathbf{Л}\}$, так что $P(n) = \mathbf{И}$ тогда и только тогда, когда n есть простое число.

Пример 5.2

Пусть универсум есть произвольное множество M, элементы которого сами являются множествами. Определим двуместный предикат A: $M^2 \to \{\mathbf{И}, \mathbf{Л}\}$, так что $A(X, Y) = \mathbf{И}$ тогда и только тогда, когда $X \subseteq Y$.

В математике чаще всего встречаются одноместные и двуместные (***бинарные***) отношения. Бинарные отношения обычно записываются между своими аргументами, например $4 < 7$, $x^2+2x+1 > 0$ и т. д. Одноместные отношения в математике часто записываются при помощи символа $\in$ и символа для множества объектов, обладающих данным свойством. Например, утверждение «π — действительное число» записывается в виде $\pi \in \mathbf{R}$, где **R** обозначает множество действительных чисел. Но

в логике для единообразия мы пользуемся предикатной записью $P(t_1, \ldots, t_n)$, чтобы обозначить высказывание, образованное применением n-местного отношения P к предметам $t_1, \ldots, t_n$. В такой записи $2 = 4$ выглядит следующим образом: $=(2, 4)$.

«Предикат» и «отношение» соотносятся как имя и предмет, им обозначаемый. Но в математике эти два понятия употребляются почти как синонимы. В логических материалах мы будем пользоваться строгим термином «предикат», а в конкретных приложениях, когда это вошло в математическую традицию, использовать и слово «отношение» (например, говорить об отношении «>» в формуле $a > b$).

Вообще, всякий раз, когда речь идет о «свойствах» объектов (пример 5.1) или «отношениях» между ними (пример 5.2), свойства и отношения можно представлять как соответствующие предикаты.

Логические операции, называемые *кванторами*, позволяют из данного предиката получать предикат с меньшим числом параметров, в частности из одноместного предиката получается высказывание.

Квантор «для всех»

Пусть $A(x)$ — предикат с одним параметром, тогда высказывание «для всех x верно $A(x)$» символически записывается $\forall x A(x)$. Символ $\forall$ называется ***квантором всеобщности*** (или ***универсальным квантором***). Эта же связка используется при переводе утверждений:

«A верно при любом значении x»,
«для произвольного x имеет место $A(x)$»,
«каково бы ни было x, $A(x)$»,
«для каждого x (верно) $A(x)$»,
«всегда имеет место $A(x)$»,
«каждый обладает свойством A»,
«свойство A присуще всем»
и т. п.

Утверждение $\forall x A(x)$ истинно тогда и только тогда, когда $A(x)$ истинно при любом фиксированном значении x. Утверждение $\forall x A(x)$ ложно тогда и только тогда, когда имеется хоть один предмет c из нашего универсума (другими словами, хотя бы одно значение x), такой, что $A(c)$ ложно.

В том случае, когда универсум содержит бесконечное множество значений, нет никакой переборной процедуры, которая помогла бы проверить истинность $\forall x A(x)$; только математическое доказательство позволяет нам единым образом обозреть все это бесконечное множество и получить точный ответ.

Квантор «существует»

Пусть $A(x)$ — предикат с одним параметром, тогда высказывание «существует такое x, что $A(x)$» символически записывается $\exists x A(x)$. Знак $\exists$ называется ***квантором существования***. Эта же связка применяется при переводе утверждений:

«$A(x)$ верно при некоторых x»,
«$A(x)$ иногда верно»,
«есть такое x, при котором $A(x)$»,
«можно найти такое x, при котором $A(x)$»,
«у некоторых вещей есть признак A»,
«по крайней мере один объект есть A»
и т. п.

Высказывание $\exists x A(x)$ истинно, если в нашем универсуме найдется хотя бы одно значение c, при котором $A(c)$ истинно. $\exists x A(x)$ ложно, если при любом значении c ложно $A(c)$.

Нахождение истинностного значения $\exists x A(x)$ также может составлять проблему. Например, натуральное число n называется совершенным, если сумма его делителей (исключая самого n) равна n. Например, 6 — совершенное число, так как $6 = 1 + 2 + 3$. Проблема «существует ли нечетное совершенное число?» стоит со времен античности, и не видно способа ее решить.

Заметим, что утверждение $\exists x A(x)$ не отрицает того, что $\forall x A(x)$. И конечно, кванторы $\exists$ и $\forall$ всегда употребляются вместе с переменной и заставляют ее пробегать весь универсум.

Для предикатов с несколькими параметрами $A(x_1, x_2, \ldots, x_n)$, $n > 1$ применение квантора общности или существования по любой переменной связывает эту переменную и создает предикат с числом параметров, меньшим на единицу. Например, рассмотрим высказывательную форму $x \geqslant 0 \supset x = y^2$, которую обозначим в виде предиката $P(x, y)$. Тогда мы можем создать предикат с одной свободной переменной $\exists y P(x, y)$ и, применяя еще один квантор, получаем (истинное) высказывание $\forall x \exists y P(x, y)$. Отметим, что мы можем получить еще 7 различных высказываний, меняя кванторы, их порядок и связывая квантором разные переменные.

Применение логического языка в теории множеств

Покажем, как простое использование логических операций и предикатов дает более точное и краткое описание понятий и рассуждений в теории множеств. Например, для доказательства основных тождеств алгебры множеств (теорема 1 из главы 3) можно использовать логические равносильности.

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \text{ (дистрибутивность } \cup \text{ относительно } \cap).$$

Имеем $A \cup (B \cap C) = \{x \mid x \in A \cup (B \cap C)\}$ = (по определению объединения и пересечения множеств) $\{x \mid x \in A \vee (x \in B \,\&\, x \in C)\}$ = (дистрибутивность $\vee$ относительно $\&$) $\{x \mid (x \in A \vee x \in B) \,\&\, (x \in A \vee x \in C)\} = (A \cup B) \cap (A \cup C)$.

$$\neg(A \cup B) = \neg A \cap \neg B \text{ (законы де Моргана)}.$$

Имеем $\neg(A \cup B) = \{x \mid x \in \neg(A \cup B)\}$ = (по определению дополнения и объединения) $\{x \mid x \in U \,\&\, \neg(x \in A \vee x \in B)\}$ = (закон де Моргана для $\vee$) $\{x \mid x \in U \,\&\, \neg(x \in \in A) \,\&\, \neg(x \in B)\}$ = (определение дополнения) $\{x \mid x \in \neg A \,\&\, x \in \neg B\} = \neg A \cap \neg B$.

Следующие утверждения были приведены в главе 3, но без обоснования. Теперь мы можем воспользоваться свойствами импликации.

Замечание 1. Транзитивность описывается формулой:

$$\forall x \forall y \forall z(<x, y> \in \rho \,\&\, <y, z> \in \rho \supset <x, z> \in \rho).$$

Если для отношения ρ вообще не существует таких x, y и z, чтобы выполнялось $<x, y> \in \rho \,\&\, <y, z> \in \rho$, то импликация истинна и, следовательно, отношение транзитивно.

Замечание 2. Антисимметричность описывается формулой:

$$\forall x \forall y(<x, y> \in \rho \,\&\, <y, x> \in \rho \supset x = y).$$

Если для отношения ρ вообще не существует таких x и y, чтобы выполнялось $\langle x, y\rangle \in \rho$ & $\langle y, x\rangle \in \rho$, то импликация истинна и, следовательно, отношение антисимметрично.

Мы привели примеры использования логического языка в «наивной» теории множеств. Но чтобы доказательства в теории множеств стали более строгими и не приводили к парадоксам, необходимо ввести специальный язык первого порядка (см. главу 6, параграф 6.7).

5.2 Термы и формулы

Языки первого порядка в первую очередь используются для записи математических утверждений, причем для каждой конкретной области математики, или, как говорят, математической теории, выбирается подходящий язык. Использование языка первого порядка для записи утверждений, относящейся к данной математической теории, становится возможным, если все основные понятия теории удается разбить на три категории: «объекты», «функции» и «предикаты». При этом функции и предикаты должны быть определены только на объектах, а значениями функций являются только объекты. В частности, не допускается рассматривать предикаты, заданные на функциях, или функции, заданные на предикатах[1]. Затем для некоторых конкретных, замечательных в том или ином отношении объектов, функций и предикатов фиксируются их обозначения, которые и образуют сигнатуру языка.

Каждый язык первого порядка задается своей ***сигнатурой*** *— тройкой множеств* $\Omega = \langle$**Cnst**, **Fn**, **Pr**$\rangle$*, где*

1) **Cnst** *— множество* ***констант****;*
2) **Fn** *— множество* ***функциональных символов****;*
3) **Pr** *— множество* ***предикатных символов****.*

При этом с каждым функциональным или предикатным символом однозначно связано некоторое натуральное число — количество аргументов (или ***местность****,* ***арность****) этого символа. Арность функционального символа положительна, а предикатные символы могут быть нульместными.*

Во всяком языке первого порядка имеется счетный набор переменных. Условимся считать, что в качестве переменных во всех языках первого порядка используются строчные буквы из конца латинского алфавита, возможно с числовыми индексами.

Язык первого порядка с сигнатурой Ω будем называть языком Ω. Язык состоит из выражений, называемых термами и формулами. При этом термы играют роль имен и именных форм, а формулы роль высказываний и высказывательных форм.

[1] Из-за этих ограничений язык называется языком *первого* порядка.

Определение ***терма*** носит индуктивный характер и содержит три пункта. Первые два пункта являются базисом индукции и указывают, какие объекты языка следует непосредственно считать термами. Третий пункт представляет собой шаг индукции и задает порождающее правило, позволяющее уже из построенных термов построить новый терм.

1. *Каждая переменная есть терм.*
2. *Каждая константа есть терм.*
3. *Если f есть k-местный функциональный символ и $t_1, t_2, \ldots, t_k$ — термы, то выражение $f(t_1, t_2, \ldots, t_k)$ есть терм.*

Пример 5.3

Пусть сигнатура содержит целые числа в качестве констант, двуместные функциональные символы + и ×, и пусть x и y — переменные. Тогда выражения

$$-7 + x,\ y,\ \big((1 + 2) + (3 + 4)\big) \times (x + 10)$$

суть термы. Заметим, что функциональные символы + и × в данном случае пишутся в инфиксной форме (между аргументами).

Атомарные *(или* ***элементарные****) формулы определяются как выражения вида $P(t_1, t_2, \ldots, t_k)$, где P есть k-местный предикатный символ $(k \geqslant 1)$, а $t_1, t_2, \ldots, t_k$ — термы. Всякий 0-местный предикатный символ также считается атомарной формулой. Кроме того, имеется предикатный символ '=', обозначающий предикат «****равенство****» и используемый в инфиксном виде. Таким образом, к числу атомарных формул относятся и выражения вида $t_1 = t_2$, где t_1, t_2 — термы.*

Формулы *определяются индуктивно с помощью следующих четырех пунктов, причем первый пункт представляет из себя базис индукции, а остальные три пункта суть порождающие правила.*

1. *Каждая атомарная формула есть формула.*
2. *Если A — формула, то выражение $\neg A$ есть формула.*
3. *Если A и B — формулы, то выражения $(A\&B)$, $(A \vee B)$, $(A \supset B)$, $(A \sim B)$ суть формулы.*
4. *Если A — формула, x — переменная, то выражения $\forall xA$ и $\exists xA$ суть формулы.*

Пусть дан язык первого порядка с некоторой сигнатурой Ω. При построении формул языка используются следующие непересекающиеся множества символов: **Cnst** — множество констант, **Fn** — множество функциональных символов, **Pr** — множество предикатных символов, множество переменных, $\{\&, \vee, \supset, \sim, \neg, \forall, \exists\}$ — множество логических связок и множество, состоящее из двух круглых скобок и запятой. Объединение этих шести множеств называется ***алфавитом*** данного языка.

В любом языке первого порядка имеется только счетное число формул. Действительно, любая формула — это конечная последовательность символов из счетного алфавита, а таких последовательностей счетное число (см. главу 3, пример 3.18).

Пример 5.4

Высказывание «Григорий Чхартишвили и Борис Акунин — это один и тот же человек» в пропозициональной логике мы могли представить только в виде пропозициональной переменной. На языке первого порядка мы можем использовать равенство с константами

'Григорий Чхартишвили' = 'Борис Акунин'.

Пример 5.5

Пусть сигнатура содержит константы, функциональные символы и переменные такие же, как в примере 5.3. А среди предикатных символов присутствует двуместный символ f и одноместный символ g. Тогда следующие выражения являются формулами:

$$g(-7), \quad f\big(x, y \times (x + 10)\big), \quad y = 1 + 2, \quad g(y + 2), \quad f(3 + 4, x \times x).$$

Заметим, что пропозициональные формулы отличаются от формул языка первого порядка видом атомарных формул и кванторы могут присутствовать только в формулах языка первого порядка. Мы распространяем на формулы языков первого порядка те же соглашения об «экономии» скобок, которые действуют и для формул пропозициональной логики (глава 4).

В формулах вида $\forall xA$ и $\exists xA$ выражение $\forall x$ и $\exists x$ называется ***кванторной приставкой***, а формула A — ***областью действия*** соответствующего квантора.

В соответствии с общим введением понятий свободной и связанной переменной (глава 4, параграф 4.1) вхождение переменной x в формулу называется связанным, если оно находится в области действия квантора $\forall x$ или $\exists x$ или входит в кванторную приставку. Вхождение переменной, не являющееся связанным, называется свободным. Формула, не содержащая свободных переменных, называется ***замкнутой***.

Рассмотрим сложные высказывания на естественном (русском) языке и покажем, что языки первого порядка более точно по сравнению с пропозициональными формулами записывают эти высказывания (сигнатуру языка мы полностью не определяем).

Пример 5.6

1. Если я прикажу генералу обратиться в чайку и он не сможет выполнить приказ, то виноват буду я, а не генерал (Сент-Экзюпери. Маленький принц).

Решение.

Логика высказываний:

A: *«Я приказываю генералу обратиться в чайку».*

B: *«Генерал выполняет приказ».*

C: *«Я виноват».*

D: *«Генерал виноват».*

Формула: $(A\&\neg B) \supset (C\&\neg D)$.

Логика предикатов:

Универсум: люди. «*Я*» и «*Генерал*» — константы.

Предикат $A(x, y) \Leftrightarrow$ «человек x отдает приказ человеку y превратиться в чайку».

Предикат $B(x, y) \Leftrightarrow$ «человек x не выполняет приказ человека y».

Предикат $C(x) \Leftrightarrow$ «человек x виноват».

Формула: $\big(A(Я, Генерал)\ \&\ \neg B(Генерал, Я)\big) \supset \big(C(Я)\ \&\ \neg C(Генерал)\big)$.

2. Если учиться и не думать — запутаешься, а если думать и не учиться — впадешь в сомнение (Конфуций. Лунь юй).

Решение.

Логика высказываний:

A: *«Человек учится».*

B: *«Человек не думает».*

C: *«Человек запутывается».*

D: *«Человек впадает в сомнение».*

Формула: $(A\&\neg B \supset C)\&(\neg A\&B \supset D)$.

Логика предикатов:

Универсум: люди.

Предикат $A(x) \Leftrightarrow$ «человек x учится».

Предикат $B(x) \Leftrightarrow$ «человек x думает».

Предикат $C(x) \Leftrightarrow$ «человек x запутывается».

Предикат $D(x) \Leftrightarrow$ «человек x впадает в сомнение».

Формула: $\forall x\Big(\big(A(x)\ \&\ \neg B(x)\big) \supset C(x)\Big)\ \&\ \forall x\Big(\big(\neg A(x)\ \&\ B(x)\big) \supset D(x)\Big)$.

Приведем два языка первого порядка, играющие наиболее важную роль в математике и логике.

Язык элементарной арифметики предназначен для записи утверждений о натуральных числах. Сигнатура языка содержит единственную константу **0** и три функциональных символа: одноместный S и двуместные + и ×. Вместо $+(t_1, t_2)$ и $\times(t_1, t_2)$ принято писать $t_1 + t_2$ и $t_1 \times t_2$ соответственно. Подразумеваемый смысл введенных символов описан в следующем параграфе.

Язык теории множеств имеет сигнатуру с двуместным предикатом $\in$ (подразумевается отношение принадлежности); обычно вместо $\in (x, A)$ пишут $x \in A$. Единственной константой является $\varnothing$. Смотрите пример 5.9 в следующем параграфе.

5.3 Интерпретация формул

Пусть имеется некоторый язык первого порядка с сигнатурой Ω. Формулы и термы этого языка, по определению сигнатуры Ω — это всего лишь некоторые последовательности символов алфавита языка. Никакого другого смысла пока в них нет. Однако после того как мы определенным образом интерпретируем эти символы, выбрав некоторую предметную область D, каждая замкнутая формула языка получит определенное истинное истинностное значение и, следовательно, оно превратится в некое высказывание, имеющее отношение к элементам рассматриваемой области D.

В отличие от языка пропозициональной логики, где под интерпретацией понимается просто приписывание истинностных значений пропозициональным переменным, в логике языка первого порядка задание интерпретации предполагает наличие, прежде всего, некоторого непустого множества D (называемого в дальнейшем *носителем интерпретации*[1]), на котором и интерпретируются символы этого языка. Содержательно — это множество тех объектов, свойства отношений между которыми мы собираемся выражать и изучать в подходящим образом выбранном языке первого порядка.

Для пропозициональной формулы, задав интерпретацию переменных, мы получаем интерпретацию всей формулы. Точно также мы будем поступать и в случае формул языка первого порядка. Нам надо определить, что означает интерпретация атомарной формулы.

Перейдем теперь к точным формулировкам.

Чтобы задать ***интерпретацию*** *сигнатуры* Ω = <**Cnst**, **Fn**, **Pr**>, *нужно*

1) *фиксировать некоторое непустое множество D — носитель интерпретации (также называют универсумом);*
2) *с каждой константой $c \in$* **Cnts** *сопоставить элемент $\overline{c} \in D$;*

[1] Если интерпретация известна, то тогда носитель интерпретации называют также *универсумом*.

3) *с каждым k-местным функциональным символом* $f \in \mathbf{Fn}$ *сопоставить некоторую k-местную функцию* $\overline{f}: D^k \to D$;

4) *с каждым k-местным предикатным символом* $P \in \mathbf{Pr}$ *сопоставить k-местный предикат* $\overline{P}: D^k \to \{\boldsymbol{И}, \boldsymbol{Л}\}$.

Если P есть 0-местный предикатный символ, то с ним сопоставляется одно из двух истинностных значений ***И*** *или* ***Л****.*
Будем называть $\overline{c}, \overline{f}, \overline{P}$ *интерпретациями соответственно константы c, функционального символа f и предикатного символа P.*
Интерпретация предикатного символа «=» понимается всегда как отношения равенства элементов D.
Универсум D объявляется областью возможных значений для каждой переменной.

. . . . . .

Пример 5.7

Пусть $\Omega = <\{\mathbf{0}\}, \{S, +, \times\}, \{=\}>$ — сигнатура языка элементарной арифметики. Рассмотрим следующую интерпретацию.

Носитель интерпретации — множество натуральных чисел **N**; константа **0** интерпретируется как число 0. Функциональный символ S интерпретируется как $\overline{S}(x) = x + 1$, с привычной точки зрения $S(x)$ — это следующее за x натуральное число. Поэтому термы, имеющие вид $S(\mathbf{0})$, $S(S(\mathbf{0}))$, $S(S(S(\mathbf{0})))$ и т. д., есть имена натуральных чисел 1, 2, 3 и т. д. Функциональные символы + и × интерпретируются как операции сложения и умножения соответственно. Язык элементарной арифметики использует только предикатный символ равенства «=» (понимаемый как равенство натуральных чисел). Если t_1, t_2 — термы языка, то $t_1 = t_2$ — атомарная формула. Из атомарных формул с помощью логических связок и кванторов строятся более сложные формулы языка, причем $\exists x$ мы понимаем как «существует натуральное число», а $\forall x$ — как «для всех натуральных чисел».

Терм $S(\ldots S(\mathbf{0})\ldots)$, где символ S повторяется k раз, кратко будем обозначать $\boldsymbol{k}$. Таким образом, натуральное число k именуется термом $\boldsymbol{k}$. Термы такого рода **0**, **1**, **2**,… принято называть ***нумералами*** — стандартными обозначениями конкретных натуральных чисел. Очевидно, термы в этой интерпретации — это обозначения полиномов (от нескольких, вообще говоря, переменных) с натуральными коэффициентами. Например, терм

$$\Big((x \times x) + \big((\mathbf{2} \times x) \times y\big)\Big) + (y \times y)$$

представляет полином $x^2 + 2xy + y^2$.

Средствами языка элементарной арифметики легко записываются простейшие утверждения о свойствах натуральных чисел, например:

1) «$x < y$» соответствует $\exists z(\neg(z = \mathbf{0}) \;\&\; y = x + z)$;

2) «x — четное число» соответствует $\exists y(x = y + y)$;

3) «x — простое число» соответствует

$$\text{«}\mathbf{1} < x\text{»} \;\&\; \neg\exists y \exists z(\text{«}y < x\text{»} \;\&\; \text{«}z < x\text{»} \;\&\; x = y \times z),$$

где утверждения со знаком «<» должны быть заменены соответствующими подформулами;

4) «существует бесконечно много простых чисел» соответствует

$$\forall x \exists y(\text{«}x < y\text{»} \ \&\ \text{«}y \text{ — простое число»})$$

с уже введенными обозначениями для подформул.

Эта интерпретация называется ***стандартной интерпретацией языка элементарной арифметики***.

Пример 5.8

Сигнатура $\Omega = <\{\mathbf{0}\}, \{S, +, \times\}, \{=\}>$ остается прежней, но интерпретацию изменим.

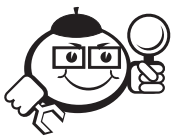
Носителем интерпретации является множество простых чисел, и **0** интерпретируется как первое простое число 2. Терм $S(x)$ интерпретируется как простое число, следующее за простым числом x. Поэтому термы, имеющие вид $S(\mathbf{0})$, $S(S(\mathbf{0}))$, $S(S(S(\mathbf{0})))$ и т. д., есть имена простых чисел 3, 5, 7 и т. д. Терм $S(\ldots S(\mathbf{0})\ldots)$, где символ S повторяется k раз, кратко будем обозначать $\boldsymbol{k}$. В этом случае термы **1**, **2**, **3**, **4**,... именуют подряд идущие простые числа 3, 5, 7, 11,...

Функциональные символы + и × интерпретируются более сложно, чем просто сложение и умножение. Пусть p_n обозначает n-е по счету простое число, например $p_5 = 13$.

1. Тогда $\overline{+(t_1, t_2)}$ — это простое число с номером $k + m$, если интерпретация термов t_1 и t_2 дает простые числа p_k и p_m.
2. Тогда $\overline{\times(t_1, t_2)}$ — это простое число с номером $k \times m$, если интерпретация термов t_1 и t_2 дает простые числа p_k и p_m.

Например, $\mathbf{0} \times (\mathbf{1} + \mathbf{2})$ интерпретируется как простое число 13, имеющее номер $5 = 1 \times (2 + 3)$. При такой интерпретации формула $x + \mathbf{0} = y$ утверждает, что x и y — простые числа-близнецы.

Эта интерпретация не имеет названия и не используется.



Пример 5.9

Пусть $\Omega = <\{\varnothing\}, \varnothing, \{=, \in\}>$ — сигнатура языка теории множеств. Пусть носитель интерпретации состоит из всех подмножеств множества **R** вещественных чисел. Константа $\varnothing$ интерпретируется как пустое множество, функциональные символы отсутствуют, и предикатный символ $\in$ интерпретируется как отношение принадлежности элемента множеству.

Примеры формул этого языка:

1) $\forall x(x \in A \supset x \in B)$. Эту формулу можно переписать в принятом виде $A \subseteq B$;
2) $\neg(x = y)$ соответствует $x \neq y$;
3) $\neg\exists x(x \in A)$ соответствует $A = \varnothing$;
4) $\forall x(x \in A \ \& \ x \in B \sim x \in C)$ соответствует $A \cap B = C$.

. . . . . .

Пусть задана интерпретация языка первого порядка. Можно ли считать, что при этом каждая формула становится именем некоторого высказывания? Другими словами, можно ли при задании интерпретации каждой формулы языка каким-то разумным способом приписать некоторое истинностное значение? Интуитивно ясно, что если формула замкнута, то она превращается в высказывание, и это высказывание имеет истинностное значение **И** или **Л**. Но в общем случае ответ будет отрицательным, поскольку формула может содержать свободные переменные, и пока этим свободным переменным не будут приписаны определенные значения из носителя интерпретации, говорить о каком-либо истинностном значении данной формулы не имеет смысла.

Чтобы придать вышесказанному точный смысл, мы вводим понятие оценки.

Пусть D — носитель интерпретации. ***Оценкой*** в этой интерпретации называется любое отображение

$$v: X \to D,$$

ставящее в соответствие каждой переменной данного языка некоторый элемент из носителя интерпретации. Элемент $v(x_i) \in D$ мы будем называть ***значением переменной*** x_i ***на оценке*** v.

Для любого терма оценка переменных, используя подстановку значений переменных в терм, однозначно дает значение терма — элемент из носителя интерпретации.

Например, при стандартной интерпретации языка элементарной арифметики и оценке $v(x) = 4$, $v(y) = 2$ терм $\big((x \times x) + \big((\mathbf{2} \times x) \times y\big) + (y \times y)\big)$ имеет в качестве значения натуральное число 36.

Интуитивно ясно, что любая формула при фиксированных интерпретации и оценке имеет истинностное значение. Рассмотрим примеры формул в стандартной интерпретации языка элементарной арифметики.

1. $\exists y(\mathbf{0} = y \times \mathbf{2})$. При оценке $v(y) = 1$ формула $\mathbf{0} = y \times \mathbf{2}$ является ложной. При оценке $v(y) = 0$ формула $\mathbf{0} = y \times \mathbf{2}$ является истинной, и поэтому формула $\exists y(\mathbf{0} = y \times \mathbf{2})$ имеет истинностное значение **И**.
2. $\forall x\exists y(x = y + y)$. При оценке $v(x) = 2$, $v(y) = 2$ формула $x = y + y$ имеет значение **Л**. При оценке $v(x) = 2$, $v(y) = 1$ формула $x = y + y$ имеет значение **И**, следовательно, формула $\exists y(x = y + y)$ имеет значение **И**. Рассмотрим теперь различные оценки, в которых $v(x) = 3$. Перебирая различные значения для y, мы получаем каждый раз, что формула $x = y + y$ имеет значение **Л**. Это позволяет нам высказать гипотезу, что формула $\mathbf{3} = y + y$ для всех y имеет ложное значение, откуда должна следовать ложность исходной формулы $\forall x\exists y(x = y + y)$. Но эта гипотеза требует доказательства.

Более строгое, с техническими подробностями, формальное определение истинностного значения формулы можно найти в различных классических учебниках (см., например, [1]).

Имеет место следующее утверждение (см., например, [1]).

Пусть A — замкнутая формула в языке первого порядка и φ — некоторая интерпретация сигнатуры языка. Тогда на любой оценке в данной интерпретации формула A имеет одно и тоже истинностное значение — оно называется ***истинностным значением формулы A в интерпретации*** φ.

5.4 Формулы общезначимые, выполнимые, логически эквивалентные

Введем некоторые термины, которые часто будем использовать в дальнейшем.

*Формула называется **общезначимой** (или **тождественно истинной**), если она истинна в любой интерпретации при любой ее оценке.*

Пример 5.10

Пусть A — произвольная формула языка первого порядка. Тогда в любой интерпретации и на любой оценке одна из двух формул A и $\neg A$ имеет значение **И**. Следовательно, формула $A \vee \neg A$ общезначима.

Пример 5.11

Формула $\forall x A(x) \supset \exists x A(x)$ является общезначимой для произвольной формулы $A(x)$ с одной свободной переменной для любой сигнатуры Ω. Действительно, возьмем произвольную интерпретацию φ сигнатуры Ω. Имеется два варианта для этой интерпретации:

а) на любой оценке $v(x)$ значение формулы $A\big(v(x)\big)$ есть **И**;

б) есть такая оценка $v(x) = c$, что значение формулы $A(c)$ есть **Л**.

В случае а) формулы $\forall x A(x)$ и $\exists x A(x)$ обе будут истинными и импликация дает **И**.

В случае б) формула $\forall x A(x)$ имеет значение **Л** и импликация снова дает **И**.

Пример 5.12

Формула $\forall x, y\big(A(x) \supset A(x) \vee A(y)\big)$ является общезначимой для произвольной формулы $A(x)$ с одной свободной переменной для любой сигнатуры Ω. Действительно, возьмем произвольную интерпретацию φ сигнатуры Ω с носителем D. Возьмем произвольные элементы $a, b \in D$ (мы не исключаем случай $a = b$), тогда формула $A(a) \supset A(a) \vee A(b)$ истинна для любых истинностных значений $A(a)$ и $A(b)$.

Пример 5.13

Принцип пьяницы

Знаменитый американский математик, автор множества логических задач, Рэймонд Смаллиан в своей книге [2, с. 226–228] описал знаменитый «Принцип пьяницы», который звучит так:

«Человек сидит у стойки в баре. Внезапно он ударяет кулаком по стойке и приказывает бармену: «Налей-ка мне и налей всем. Когда пью я, пьют все. Такой уж я человек!» Все выпивают, настроение у посетителей бара повышается.

Через какое-то время человек, сидящий у стойки, снова ударяет кулаком по стойке и заплетающимся языком отдает бармену распоряжение: «Налей мне еще и налей всем еще по одной. Когда я пью еще одну, все пьют еще по одной! Такой уж я человек!» Все выпивают еще по одной, и настроение в баре повышается еще больше.

Затем человек, сидящий у стойки, кладет на нее деньги и говорит: «А когда я плачу, платят все. Такой уж я человек!».

Вопрос: существует ли в действительности такой человек, что если он пьет, то пьют все?

Мы приведем формулу, которая дает положительный ответ на этот вопрос.

Рассмотрим универсум, состоящий из людей. Пусть предикат $P(x)$ обозначает свойство людей: «x пьет». Рассмотрим формулу:

$$\exists x\big(P(x) \supset \forall y P(y)\big).$$

Эта формула истинна в данной интерпретации при любом распределении пьющих людей в универсуме.

Действительно, любая оценка переменных означает соответствующее распределение пьющих людей. Возможно два варианта: а) все люди обладают свойством P и б) есть люди, которые не пьют. Если для любого человека m значение предиката $P(m)$ равно **И**, то формулы $\forall y P(y)$ и $P(m) \supset \forall y P(y)$ имеют значение истина, и, следовательно, переходя к квантору, $\exists x\big(P(x) \supset \forall y P(y)\big)$ имеет значение **И**. Пусть в случае б) человек m не пьет, тогда $P(m)$ ложно, но импликация $P(m) \supset \forall y P(y)$ имеет значение **И**. Снова заключаем, что формула $\exists x\big(P(x) \supset \forall y P(y)\big)$ имеет значение **И**.

В нашем примере с пьяницей мы нигде не использовали специфики интерпретации, поэтому произвольная формула $A(x)$, выражающая некоторое свойство элементов носителя интерпретации, дает общезначимую формулу:

$$\exists x \left(A(x) \supset \forall y\, A(y)\right).$$

В главе 4 было введено понятие тавтологии как пропозициональной формулы, которая превращается в истинное высказывание при любой подстановке в нее конкретных высказываний вместо пропозициональных переменных.

Если в пропозициональную формулу вместо всех пропозициональных переменных подставить какие-нибудь формулы языка первого порядка, то, очевидно, получим формулу языка первого порядка. Будем называть такую формулу также ***тавтологией***. Выше рассмотренный пример 5.10 демонстрирует одну из таких тавтологий — $A \vee \neg A$.

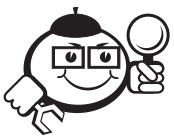
Теорема 1. Любая тавтология общезначима.

Доказательство. Пусть $B(X_1, X_2, \ldots, X_n)$ — пропозициональная формула с переменными $X_1, X_2, \ldots, X_n$, а $A_1, A_2, \ldots, A_n$ — произвольные формулы языка первого порядка. Обозначим через $B(A_1, A_2, \ldots, A_n)$ формулу, полученную подстановкой в $B(X_1, X_2, \ldots, X_n)$ формул $A_1, A_2, \ldots, A_n$ вместо $X_1, X_2, \ldots, X_n$ соответственно. Выберем произвольную интерпретацию и оценку языка первого порядка, тогда каждая формула $A_1, A_2, \ldots, A_n$ будет иметь некоторое истинностное значение. Следовательно, мы можем получить истинностное значение формулы $B(A_1, A_2, \ldots, A_n)$, такое же, как значение формулы $B(X_1, X_2, \ldots, X_n)$, где истинностные значения переменных $X_1, X_2, \ldots, X_n$ совпадают с истинностными значениями формул $A_1, A_2, \ldots, A_n$ соответственно. Но формула $B(X_1, X_2, \ldots, X_n)$ имеет значение **И**, следовательно, значение формулы $B(A_1, A_2, \ldots, A_n)$ также **И**.

Вышерассмотренные примеры 5.11–5.13 показывают, что общезначимые формулы не только те формулы, которые могут быть получены из тавтологий пропозициональной логики.

*Формула называется **выполнимой**, если она истинна хотя бы в одной интерпретации при хотя бы одной ее оценке.*

При заданной интерпретации истинностное значение замкнутой формулы постоянно на любой оценке, поэтому для замкнутой формулы можно просто говорить о выполнимости формулы A в интерпретации φ; факт выполнимости для замкнутых формул принято обозначать $\varphi \vDash A$.



Пример 5.14

Рассмотрим формулу $\exists x A(x) \vee \exists y A(y)$. Эта формула выполнима, но не общезначима. Выберите подходящие интерпретации для доказательства.

*Формулы A и B называются **логически эквивалентными**, если формула $A \sim B$ общезначима. Если A и B логически эквивалентны, то будем писать $A \equiv B$.*

Теорема 2. Пусть даны пропозициональные формулы B и C с переменными $X_1, X_2, \ldots, X_n$ и $A_1, A_2, \ldots, A_n$ — формулы языка первого порядка. Обозначим через $B(A_1, A_2, \ldots, A_n)$ и $C(A_1, A_2, \ldots, A_n)$ формулы, полученные подстановкой в B и C формул $A_1, A_2, \ldots, A_n$ вместо $X_1, X_2, \ldots, X_n$ соответственно. Тогда, если $B \equiv C$, то $B(A_1, A_2, \ldots, A_n) \equiv C(A_1, A_2, \ldots, A_n)$.

Доказательство. Так как $B \equiv C$ в логике высказываний, то $B \sim C$ — пропозициональная тавтология, следовательно, по теореме 1, формула $B(A_1, A_2, \ldots, A_n) \equiv C(A_1, A_2, \ldots, A_n)$ является общезначимой, что и требовалось доказать.

Следующее утверждение не следует из теоремы 2.

Теорема 3 [3, с. 39–40]. Какие бы ни были формулы A и B, справедливы следующие утверждения о логической эквивалентности.

1. Если B не содержит свободных вхождений переменной x, то
   а) $\exists x(A \& B) \equiv \exists x A \& B$;
   б) $\forall x(A \& B) \equiv \forall x A \& B$;
   в) $\forall x(A \vee B) \equiv \forall x A \vee B$;
   г) $\exists x(A \vee B) \equiv \exists x A \vee B$.
2. $\forall x(A \vee B) \equiv \exists x A \vee \exists x B$.
3. $\forall x(A \& B) \equiv \forall x A \& \forall x B$.
4. $\neg \exists x A \equiv \forall x \neg A$.
5. $\neg \forall x A \equiv \exists x \neg A$.

6. Если $A(x)$ не содержит y, то

   а) $\forall x A(x) \equiv \forall y A(y)$;

   б) $\exists x A(x) \equiv \exists y A(y)$.

. . . . . .

Доказательство следующих теорем смотрите в [3, с. 40–41].

. . . . . .

Теорема 4. Пусть A произвольная формула, а $B \equiv C$. Тогда

1) $A\&B \equiv A\&C$;
2) $A \vee B \equiv A \vee C$;
3) $A \supset B \equiv A \supset C$;
4) $B \supset A \equiv C \supset A$;
5) $A \sim B \equiv A \sim C$;
6) $\neg B \equiv \neg C$;
7) $\exists x B \equiv \exists x C$;
8) $\forall x B \equiv \forall x C$.

Теорема 5. Пусть A произвольная формула, а $B \equiv C$. Пусть A_1 получена из A заменой некоторых вхождений формулы B на C. Тогда $A \equiv A_1$.

. . . . . .

В языках первого порядка по определению существует предикат равенство «=». Причем общепринято предполагать, что этот предикат обладает следующим свойством[1].

Если A — произвольная формула языка первого порядка, то формула:

$$\forall x, y \left(x = y \supset \left(A(x) \supset A(y) \right) \right)$$

общезначима.

Другими словами, свойства равных объектов эквивалентны. В математических утверждениях можно заменить равные объекты друг на друга, и мы получим эквивалентное рассуждение. Например, утверждение, говорящее о числе «4», мы можем заменить эквивалентным утверждением, говорящим о выражении «2 + 2». Но в программировании не всегда так. Например, если программная переменная x имеет значение 4, то нельзя все вхождения x заменить числом 4.

Еще одно свойство равенства:

$$\forall x (x = x),$$

т. е. каждый объект равен самому себе.

Из этих двух свойств равенства выводятся другие законы равенства, например:

$$\forall x, y, z (x = y \ \& \ y = z \supset x = z);$$
$$\forall x, y (x = y \supset y = x);$$
$$\forall x, y, z (x = y \ \& \ x = z \supset y = z).$$

Докажем для образца первое из этих равенств: если первый предмет равен второму, а второй — третьему, то первый предмет равен третьему. В самом деле,

[1] Отношение равенства с перечисленными здесь свойствами используется не только в языках первого порядка — оно повсеместно встречается в математике.

пусть при конкретных произвольных x, y, z выполнено $x = y$ и $y = z$. Тогда по основному свойству равенства в $x = y$ можно y заменить на z и получим $x = z$, что и требовалось доказать.

Выразимость

*Пусть $A(x_1, x_2, \ldots, x_n)$ — формула сигнатуры Ω со свободными переменными $x_1, x_2, \ldots, x_n$, φ — интерпретация сигнатуры Ω с носителем D, а R есть n-местный предикат на D. Говорят, что формула A **выражает** предикат R в интерпретации φ, если $R(a_1, a_2, \ldots, a_n)$ = **И** тогда и только тогда, когда $\varphi \vDash A(a_1, a_2, \ldots, a_n)$ для любых значений $a_1, a_2, \ldots, a_n$ из D переменных $x_1, x_2, \ldots, x_n$.*

*Предикат R называется **выразимым** в интерпретации φ, если существует формула, его выражающая.*

*Множество $B \subset D$ называется **выразимым**, если существует одноместный выразимый предикат P, что $b \in B$ тогда и только тогда, когда $P(b)$ = **И**.*

Пример 5.15

Возьмем стандартную интерпретацию языка элементарной арифметики $<\{\mathbf{0}\}, \{S, +, \times\}, \{=\}>$. Формула $\exists y\big(y = S(x + x)\big)$ выражает предикат «x — нечетно». Формула $\exists z(y = x+z)$ выражает предикат «$x \leqslant y$». Предикат $x = 0$ можно выразить двумя разными формулами: $x = \mathbf{0}$ и $x + x = x$.

Существуют ли невыразимые в **N** множества при стандартной интерпретации элементарной арифметики? Из мощностных соображений следует, что существуют. Формул языка первого порядка лишь счетное число (параграф 5.2), а подмножеств **N** — континуум. Поскольку каждое подмножество $D \subset \mathbf{N}$ определяет соответствующий предикат $P(x) = \{x \mid x \in D\}$, то различных предикатов тоже континуум; следовательно, существуют и невыразимые предикаты.

Теорема 6. Пусть D — носитель интерпретации языка первого порядка с произвольной сигнатурой Ω. Имеем следующие свойства выразимых в D множеств.

1. Если $A \subset D$ и $B \subset D$, то $A \cap B$ выразимо.
2. Если $A \subset D$ и $B \subset D$, то $A \cup B$ выразимо.
3. Если $A \subset D$ выразимо, то $D \backslash A$ выразимо.

Доказательство. Действительно, если формулы P и Q со свободными переменными y и z выражают множества A и B соответственно, то формула $P\&Q$, в которой все свободные вхождения y и z заменены на x, выражает множество $A \cap B$. Утверждения 2 и 3 доказываются аналогично.

Логическое следование

Для пропозициональной логики мы ввели понятие логического следования. Приспособим это определение к исчислению предикатов.

Пусть Γ *— произвольное множество замкнутых формул сигнатуры* Ω. ***Моделью*** *множества* Γ *называется интерпретация* φ *сигнатуры* Ω*, в которой истинны все формулы из* Γ. *Множество* Γ *называется* ***совместным*** *(выполнимым), если оно имеет хотя бы одну модель.*

Пример 5.16

Множество формул $\{\forall x, y(x = y), \exists z, y(P(z) \ \& \ \neg P(y))\}$ несовместно потому, что любая модель в качестве носителя имеет одноэлементное множество и вторая формула всегда ложна.

Будем говорить, что замкнутая формула A *сигнатуры* Ω ***логически следует*** *(семантически следует или просто следует) из* Γ*, и писать* $\Gamma \models A$*, если* A *истинна во всех моделях множества* Γ. *В этом случае будем также говорить, что* A *является* ***логическим следствием*** *множества формул* Γ.

Пустое множество совместно, и его моделью является любая интерпретация, поэтому $\varnothing \models A$ выполнено тогда и только тогда, когда A — общезначимая формула. Обычно для общезначимых формул пишут просто $\models A$.

Теорема 6. Пусть Γ — некоторое множество замкнутых формул сигнатуры Ω, A и B — замкнутые формулы сигнатуры Ω. Тогда

а) $\Gamma \models A$ и $\Gamma \models B$ тогда и только тогда, когда $\Gamma \models A\&B$.

б) $\Gamma \cup \{A\} \models B$ тогда и только тогда, когда $\Gamma \models A \supset B$.

в) $\Gamma \models A$ тогда и только тогда, когда множество $\Gamma \cup \{\neg A\}$ несовместно.

Доказательство смотрите, например, в [3, с. 58–59].

Множество Γ *замкнутых формул сигнатуры* Ω *будем называть* ***семантически полным****, если* Γ *совместно и для любой замкнутой формулы* A *сигнатуры* Ω *выполнено* $\Gamma \models A$ *или* $\Gamma \models \neg A$.

Пример 5.17

Пусть сигнатура не содержит никаких констант, функциональных и предикатных символов (равенство присутствует). Рассмотрим одноэлементное множество $\Gamma = \{\forall x, y(x = y)\}$ формул этой сигнатуры. Это множество семантически полно, поскольку все его модели — одноэлементные множества, и любая замкнутая формула либо истинна, либо ложна в этой модели.

5.5 Перевод с естественного языка на логический и обратно

Рассмотрим рекомендации и примеры перевода высказываний на русском языке на язык логики предикатов. Исходные высказывания большей частью не являются математическими. Обратный перевод также заслуживает внимания.

Правила для перевода

Если высказывание не является математическим, то, как правило, нет необходимости полностью определять сигнатуру языка, на который мы переводим высказывание[1]. Поэтому рекомендуется руководствоваться следующими правилами.

1. При решении задач на перевод сначала следует выбрать универсум, содержащий объекты (сущности), о которых говорится в высказывании. Выбор универсума в большинстве случаев не является однозначным, тогда надо руководствоваться дополнительно правилом 2. В некоторых случаях одним универсумом не обойтись.
2. Определяем предикатные символы для обозначения свойств объектов (одноместные предикаты) и/или отношений между объектами универсума (универсумов). Важно, чтобы определяемые вами предикаты имели смысл для всех элементов универсума. Кроме того, для каждого одноместного предиката множество значений этого предиката должно быть собственным непустым подмножеством универсума. Если это не так, то предикат не нужен, без него можно обойтись.
3. Определяем используемые термы. Для этого, при необходимости, вводим функциональные символы, и когда речь идет о конкретных объектах (указаны собственные имена), то вводим константы для обозначения этих объектов.

[1] Тем более что во многих случаях это было бы сделать затруднительно или невозможно.

4. Элементарным (атомарным) высказываниям соответствуют атомарные формулы языка первого порядка. Это правило говорит о том, какие предикаты должны быть в получаемой формуле. Количество используемых предикатов, функциональных символов, констант следует минимизировать[1], но и не следует впадать в другую крайность, когда высказывание представляется одним многоместным предикатом.
5. В элементарном высказывании мы можем обнаружить кванторную конструкцию, тогда в соответствующей формуле используется квантор.
6. Если высказывание является сложным, то каждой пропозициональной связке в высказывании соответствует аналогичная связка в переводе.
7. В общем случае при переводе содержательного высказывания на формальный язык формула должна быть замкнутой, иначе она не имеет истинностного значения и мы не можем проверить перевод.
8. Если в высказывании говорится о нескольких свойствах объектов из универсума, то каждое свойство определяет соответствующее подмножество универсума. Далее мы можем при выборе пропозициональных связок руководствоваться соответствиями: пересечению подмножеств соответствует конъюнкция предикатов, объединению — дизъюнкция, включению подмножеств соответствует импликация предикатов.

Рассмотрим последнее правило подробнее.

Пусть U — универсум и $X_1 = \{x \in U \mid A(x)\}$, $X_2 = \{x \in U \mid B(x)\}$, где $A(x)$ и $B(x)$ — некоторые одноместные предикаты. Рассмотрим высказывание вида: «Все объекты x из U, обладающие свойством A, обладают свойством B». На языке множеств мы имеем $X_1 \subseteq X_2$, что мы можем представить на языке первого порядка формулой $\forall x\big(A(x) \supset B(x)\big)$.

При прежних обозначениях пусть имеется высказывание вида: «Есть объект x из U, обладающий свойствами A и B». На языке множеств мы имеем $X_1 \cap X_2, \neq \varnothing$, и мы пишем на языке первого порядка формулу $\exists x\big(A(x)\&B(x)\big)$.

Таким образом, имеем простые правила:

«Если A, то B» — пишем $\forall x\big(A(x) \supset B(x)\big)$;
«Некоторые A есть B» — пишем $\exists x\big(A(x)\&B(x)\big)$.

Пример 5.18

Некоторые свиньи не умеют летать.

Универсум: животные. Предикаты: $S(x) \equiv$ «x — свинья», $E(x) \equiv$ «x — умеет летать».

Формула: $\exists x\big(S(x)\&\neg E(x)\big)$.

[1] «Не следует создавать сущностей больше необходимого числа» — принцип «бритва Оккама». Оккам Уильям (ок. 1285–1349 гг.) — английский философ-схоласт, логик.

Пример 5.19

Все дети не любят прилежно заниматься.

Универсум: люди. Предикаты: $B(x) \equiv$ «x — ребенок», $L(x) \equiv$ «x — любит прилежно заниматься».

Формула: $\forall x\big(B(x) \supset \neg L(x)\big)$.

«Многоэтажные» кванторы. Дополнительные ограничения

Рассмотрим утверждение: «Все бешеные собаки смертельно опасны». Здесь говорится, что если данное нам животное x — собака, и причем бешеная, то x — смертельно опасное. Следовательно, если предикат $D(x)$ означает «животное x — собака», предикат $M(x)$ означает «животное x — бешеное», а предикат $Z(x)$ — «x — смертельно опасное», то формальная запись этого утверждения имеет вид

$$\forall x\big(D(x)\ \&\ M(x) \supset Z(x)\big).$$

Аналогично утверждение «Некоторые старательные студенты получают стипендию» можно записать в виде

$$\exists x\big(P(x)\ \&\ S(x)\ \&\ O(x)\big),$$

где $P(x)$ означает «x — студент»; $S(x)$ означает «x — старательный»; $O(x)$ — «x — получает стипендию».

Итак, если на значения переменной накладываются сразу несколько ограничений, то все они перечисляются через &, а затем надстраивается ограниченный квантор по обычным правилам.

Теперь рассмотрим утверждение: «произведение двух чисел, отрицательного и положительного, является отрицательным». Пусть универсум составляет множество вещественных чисел, а предикаты используем в традиционной записи: $x < 0$ (число x отрицательно), $x > 0$ (число x положительно). Произведение двух чисел представим традиционным термом. Тогда высказывание имеет несколько эквивалентных форм, все они допустимы. Выберем два варианта[1]:

$$\forall x\big(x < 0 \supset \forall y(y > 0 \supset x \times y < 0)\big),$$
$$\forall x \forall y(x < 0\ \&\ y > 0 \supset x \times y < 0).$$

Хоть эти две формы и эквивалентны, но вторая, пожалуй, несколько выразительнее и яснее подчеркивает равноправие двух чисел. Для последней формулы можно использовать сокращение

$$\exists x, y(x < 0\ \&\ y > 0 \supset x \times y < 0),$$

т. е. несколько однородных кванторов соединяются в один. Заметим, что в исходном высказывании не присутствуют явно слова («все», «любые» и т. п.), которые

[1] Какие еще варианты возможны?

бы указывали о необходимости квантора общности, но мы должны его использовать, исходя из смысла высказывания и учитывая правило 7 для перевода.

Перевод утверждения «для всякого целого числа есть меньшее целое» можно записать следующим образом:

$$\forall x\big(x \in \mathbf{Z} \supset \exists y(y \in \mathbf{Z} \;\&\; y < x)\big). \tag{5.1}$$

Заметим, что это утверждение удобнее писать, начиная с внутреннего квантора, т. е. сначала перевести, что означает «Для x есть меньшее его натуральное число», а затем расшифровать начало предложения: «для всякого x».

При переводе утверждений с вложенными кванторами необходимо тщательнейшим образом следить за порядком кванторов и их областью действия. Например, если утверждение (5.1), конечно же, истинно, то утверждение

$$\exists y\big(y \in \mathbf{Z} \;\&\; \forall x(x \in \mathbf{Z} \supset y < x)\big)$$

ложно. Оно выражает утверждение естественного языка «Существует наименьшее целое число». В самом деле, прочтем его. Читать также начинают изнутри. Внутри у нас говорится, что всякое целое число x больше y. А какое y? Пока неопределено, но, переходя к началу формулы, мы видим, что y должно быть предварительно выбрано. Но какое бы целое число y ни выбрали, внутреннее утверждение будет ложно. Следовательно, такого y не существует.

Из этого примера виден и способ чтения формальных выражений. Мы начинаем с внутренних кванторов и, прочитав утверждение «начерно», в неестественных для естественного языка формах типа «для всех x, таких, что…, существует y, такое, что…», стремимся переформулировать полученное предложение более кратко и более красиво, более выразительно. При этом по возможности изгоняется упоминание о тех переменных, которые в формальном выражении были связаны. Упоминание же о тех переменных, которые были свободны, по которым кванторов навешено не было, обязательно остается.

Например, выражение

$$\exists z(z \in \mathbf{R} \;\&\; x < z \;\&\; z < y)$$

можно прочитать как «Существует действительное число z, такое, что x меньше z, а z меньше y», и переформулировать начисто: «Между x и y есть действительное число».

И наконец, рассмотрим утверждение: «Для любого целого числа есть большее и меньшее его целые числа». Это утверждение можно представить в виде формулы:

$$\forall x \exists y,\, z(x \in \mathbf{Z} \supset y \in \mathbf{Z} \;\&\; y > x \;\&\; z \in \mathbf{Z} \;\&\; z < x),$$

но лучше всего перевод:

$$\forall x\big(x \in \mathbf{Z} \supset \exists y(y \in \mathbf{Z} \;\&\; y > x) \;\&\; \exists z(z \in \mathbf{Z} \;\&\; z < x)\big),$$

где каждый квантор относится лишь к тем утверждениям, которые он связывает.

Выводы

- Если предложение достаточно сложное, его перевод на формальный язык лучше всего писать изнутри, начиная с самой главной части данного предложения.
- Порядок кванторов часто имеет решающее значение.
- Не стесняйтесь гнаться за выразительностью: это окупается.
- При переводе на формальный язык нужно по мере возможности уменьшать области действия кванторов, чтобы каждый из них не включал в свою область утверждения, не говорящие о связываемой переменной.
- При чтении сложной формулы начинайте изнутри. Если затруднительно сразу понять ее смысл, сначала прочитайте ее начерно, а затем начисто, изгоняя явное упоминание кванторов и связанных переменных.
- Свободные переменные должны входить в окончательную словесную формулировку утверждений.

Единственность и неединственность

При изложении этого пункта следуем [4].

Исключительно важную роль в языке математики играет утверждение единственности x, удовлетворяющего данному условию A (например, часто приходится доказывать, что решение задачи единственно).

На самом деле обычно подразумевается не только то, что решение задачи единственно, но и то, что она имеет решение, т. е. доказывается не только единственность, а существование и единственность объекта, удовлетворяющего свойству A. При аккуратных формулировках это необходимо оговаривать.

Единственность «в чистом виде» выражается следующим образом:

$$\forall x, y\ (A(x)\ \&\ A(y) \supset x = y).$$

Заметим, что утверждение «x, удовлетворяющее A, единственно», вообще говоря, *не предполагает, что оно существует*, что задача вообще имеет решение. Чисто формально, предыдущая формула истинна и в том случае, когда x, удовлетворяющих A, вообще нет. Поэтому эту формулу точнее читать «есть не более одного x, удовлетворяющего $A(x)$».

А утверждение «существует единственное x, такое, что $A(x)$» выражается в форме

$$\exists x A(x)\ \&\ \forall x, y\big(A(x)\ \&\ A(y) \supset x = y\big).$$

Но это не самая выразительная запись утверждения о единственности. Гораздо выразительнее $\exists x \forall y (A(y) \supset x = y)$.

Итак, то, что существует единственное x, удовлетворяющее $A(x)$, означает, что условие $A(x)$ на самом деле сводится к равенству этому единственному x.

В задачах, где идет речь о количестве каких-то объектов, следует использовать предикат равенство.

Общий способ получить утверждение «существует не более n таких x, что $A(x)$»:

$$\exists x_1, \ldots, x_n \big(\forall y \, (A(y) \sim x_1 = y \vee \ldots \vee x_n = y) \big).$$

Но здесь мы не утверждаем, что этих различных x ровно n: если x и y обозначены по-разному, то это отнюдь не означает, что они принимают различные значения: они имеют право принимать разные значения, но имеют право принять и одинаковые.

Итак, мы приходим к необходимости уметь формулировать различие. Если $x = y$ означает равенство, неразличимость, совпадение предметов, то соответственно $\neg(x = y)$, обычно обозначаемое $x \neq y$, — их различие. Итак, сказать, что есть не менее двух различных решений задачи, очень просто:

$$\exists x, y \big(x \neq y \;\&\; A(x) \;\&\; A(y) \big).$$

Так же просто сказать и то, что их ровно два:

$$\exists x, y \Big(x \neq y \;\&\; \forall z \big(A(z) \sim z = x \vee z = y \big) \Big).$$

А вот как записывается, что решений не более двух:

$$\forall x, y, z \Big(x \neq y \;\&\; x \neq z \;\&\; y \neq z \supset \neg \big(A(x) \;\&\; A(y) \;\&\; A(z) \big) \Big).$$

Подобным образом можно написать формулы и для большего числа решений.

Контрольные вопросы по главе 5

1. Пусть предикат $P(x, y)$ обозначает высказывательную форму $x \geqslant 0 \supset x = y^2$. Мы можем связать переменные x и y кванторами $\exists$ и $\forall$ в различных комбинациях и в различном порядке. Предполагая, что значениями переменных являются вещественные числа, мы получаем всего 8 различных высказываний о числах x и y (например, $\exists x \forall y P(x, y)$ и $\forall x \forall y P(x, y)$). Найдите истинностное значение для каждого такого высказывания.
2. Как на языке первого порядка для теории множеств (пример 5.9) записать утверждение $A \cup B = C$?
3. Следующее физическое утверждение:

   «Тело движется равномерно и прямолинейно в том и только в том случае, когда на него не действуют силы или равнодействующая действующих на тело сил равна нулю».

   На языке логики высказываний можно представить так:

A: *«Тело движется равномерно и прямолинейно».*

B: *«На тело не действуют силы».*

C: *«Равнодействующая действующих на тело сил равна нулю».*

Формула: $A \sim (B \vee C)$.

Как это записать на языке логики предикатов?

4. Переведите на язык логики предикатов высказывание:

   Все, что сделано из золота, драгоценно.

5. Переведите на язык логики предикатов высказывание:

   Чтобы не быть собакой, достаточно быть кошкой.

Рекомендуемая литература к главе 5

[1] Колмогоров А. Н. Математическая логика / А. Н. Колмогоров, А. И. Драгалин. — 3-е изд. — М. : КомКнига, 2006. — 240 с.

[2] Смаллиан Р. Как же называется эта книга? / Р. Смаллиан. — М. : Издательский Дом Мещерякова, 2007. — 272 с.

[3] Успенский В. А. Вводный курс математической логики / В. А. Успенский, Н. К. Верещагин, В. Е. Плиско. — М. : ФИЗМАТЛИТ, 2004. — 128 с.

[4] Непейвода Н. Н. Прикладная логика : учеб. пособие / Н. Н. Непейвода. — 2-е изд., испр. и доп. — Новосибирск : Изд-во Новосиб. ун-та, 2000. — 521 с.

Глава 6

АКСИОМАТИЧЕСКИЙ МЕТОД

> . . .эмпирические системы утрачивают свою актуальность, математические же — никогда. Их бессмертие — в их «пустоте».
>
> *Станислав Лем. Сумма технологии*

6.1 Предварительные понятия и простые примеры

Человеческому мышлению свойственны мыслительные процессы двух видов: осознанные и неосознанные. Осознанные рассуждения допускают в большинстве случаев передачу другому лицу в письменном виде или в виде речи. В идеале читатель может понять их. Бессознательные процессы явно не осознаются, но иногда их результаты воспринимаются сознанием.

Если существуют бессознательные процессы мышления, то должны существовать и неосознанные «разумные принципы», регулирующие это мышление (ведь оно приводит не только к беспорядочным сновидениям, но и к разумному решению реальных проблем).

То же самое справедливо для математического мышления. Мы часто имеем дело с определенным комплексом бессознательных принципов, которые неосознанно регулируют наши рассуждения. Такие бессознательные регулирующие факторы, вырабатываемые в ходе интенсивных умственных занятий в определенной области, обычно называют ***интуицией***.

Общее биологическое развитие людей, взаимодействие в общем внешнем мире, общая культурная среда приводят к тому, что механизмы интуиции являются общими для большинства людей. Но одной интуиции недостаточно.

В процессе становления математики интуитивные представления уточнялись, и в результате появились строгие понятия и утверждения. В математике справедливость утверждений устанавливается с помощью доказательств.

Понятие математического доказательства исторически менялось. В Древнем Египте уже применялись правила для сложения и умножения целых положительных чисел и обратных им дробей. Также для нахождения площадей некоторых геометрически простых земельных участков применялись определенные правила. Но эти правила никак не обосновывались. Доказательством справедливости этих правил служил сам факт их наличия, факт того, что они были записаны.

В Древней Индии для доказательства нередко использовались математические рисунки. Доказательство теоремы, которую мы сейчас называем теоремой Пифагора, сводилось у индийского математика Бхаскары (1114–1185 гг.) к рисунку 6.1 с пояснением в одно слово «Смотри!»[1].

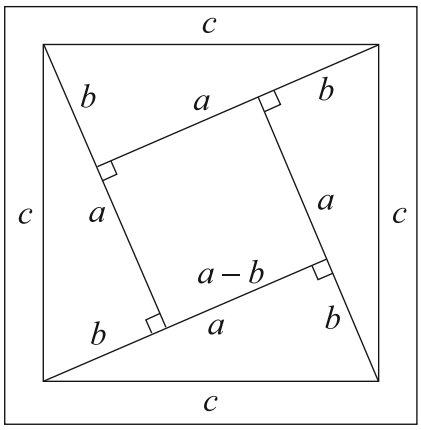


Рис. 6.1 – Доказательство Бхаскары

Современные доказательства опираются на аксиоматический метод[2]. Как говорилось в главе 2, уже в «Началах» Евклид использовал аксиоматический метод. Аксиоматический метод — это такой способ построения математической теории, при котором в основу кладутся основные положения теории, принимаемые без доказательства, а все остальные выводятся из них при помощи доказательств. Исходные положения называются ***аксиомами***, а те, которые из них выводятся, ***теоремами***.

Остановимся на двух особенностях применения аксиоматического метода.

1. В «Началах» Евклида аксиомы — это очевидные истины, принимаемые без доказательства. В XIX веке это понятие сильно изменилось, потому что аксиомы перестали быть очевидными, они по-прежнему принимаются без доказательства, но могут быть в принципе совершенно произвольными утверждениями. За этим небольшим, на первый взгляд, изменением стоит достаточно радикальная смена философской позиции — отказ от признания одной-единственной возможной математической реальности[3].

[1]Историки-математики считают, что Бхаскара выражал площадь квадрата, построенного на гипотенузе, как сумму площадей четырех треугольников $(4ab/2)$ и площади квадрата $(a-b)^2$. Следовательно: $c^2 = 4ab/2 + (a-b)^2$, потом $c^2 = 2ab + a^2 - 2ab + b^2$ и, наконец, $c^2 = a^2 + b^2$.

[2]Кроме аксиоматичекого метода используется также генетический подход [1, с. 17–18]. В этом случае пытаются моделировать интуицию средствами другой теории (которая сама может также быть интуитивной).

[3]См. неевклидову геометрию (параграф 6.4), континуум-гипотезу и аксиому выбора (параграф 6.7).

2. Доказательства при аксиоматическом методе могут быть неформальными и формальными. Первое понятие — традиционное, и оно было единственным до становления математической логики. Наряду с неформальным, его можно назвать и психологическим доказательством, поскольку психологии в нем не меньше, чем математики.

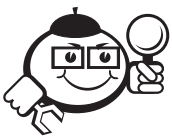
Неформальное (содержательное, психологическое) доказательство *— это рассуждение, которое нас убеждает настолько в истинности некоторого высказывания, что мы можем после этого убедить других с помощью того же рассуждения.*

Примерами неформальных доказательств служат все доказательства, рассмотренные до этой главы.

Математическая логика уточнила (формализовала) понятие содержательного доказательства и выработала понятие формального доказательства. В отличие от неформального аксиоматического метода формальный аксиоматический метод отличается тем, что совершенно четко определяет записанные в виде аксиом исходные положения, но и дозволенные способы рассуждений. Точно указываются допустимые логические переходы. Отметим, что все это определяется в виде синтаксических правил, поэтому формальные доказательства можно делать чисто механически, не вникая в их содержание. Проверять правильность формальных доказательств можно с помощью компьютера.

Неформальные доказательства можно записывать, используя любой естественный язык, формальные доказательства требуют только формального языка.

Формальные доказательства являются математическими объектами, следовательно, можно изучать математически формальные доказательства, что и делается в разделе математической логики, называемым теорией доказательств. Эти формализации психологических доказательств могут быть различными, но все они подчиняются некоторым общим требованиям. При радикальном применении формальных доказательств математика сводится к чистой логике, из нее изгоняются такие вещи, как интуиция, наглядные геометрические представления, индуктивные рассуждения и так далее.



Пример 6.1

Доказательство от противного (см. [2]). Пусть дано утверждение B. Надо доказать утверждение A.

При неформальном доказательстве из двух утверждений 1 и 2:

1) B;

2) из отрицания утверждения A следует отрицание утверждения B — вытекает утверждение A.

При формальном доказательстве указанное содержательное рассуждение начинается с записи утверждений A и B в виде формул A и B соответственно. После

этого применяется правило: если доказаны формулы B и $\neg A \supset \neg B$, то считается доказанным и A.

Аксиоматический метод позволяет построить математические теории на четко выделенных математических утверждениях, из которых прочие получаются с помощью доказательств. Полученные таким образом математические теории называются аксиоматическими.

Создание формальных аксиоматических теорий возможно только при использовании ***формальных языков*** для записи на них доказываемых утверждений и самих доказательств. Обычно для этой цели широко используются языки первого порядка.

Но в любом случае в первую очередь задается синтаксис формального языка, который описывает построение правильных выражений (к ним относятся обычно термы, формулы, доказательства).

Как правило, формальный язык наделяется еще и семантической системой, или дедуктивной системой, или и той и другой.

***Семантическая система**, или просто семантика, какого-либо языка выделяет среди всех формул этого языка те, которые объявляются истинными; говорят также, что им приписываются значения **И**. Для этого обычно используется интерпретация правильных выражений языка.*

О формальных доказательствах можно говорить лишь тогда, когда утверждения, которые мы доказываем, и доказательства представляют собой тексты, организованные по совершенно точным синтаксическим правилам, т. е. записанные на формальном языке.

***Дедуктивная система** какого-либо языка выделяет среди всех формул те, которые объявляются доказуемыми. Обычно доказуемость задается индуктивно при помощи аксиом и правил вывода. Это делается так. Некоторые формулы объявляются аксиомами. Каждое **правило вывода** применяется к одной или нескольким формулам и указывает, как из этих формул можно получить новую формулу. **Доказуемыми формулами** называются все аксиомы и формулы, которые можно получить из доказуемых с помощью правил вывода. Доказуемые формулы, которые не являются аксиомами, называются **теоремами**.*

Замечание 1. Дедуктивная система задается таким образом, что для формального доказательства должны существовать:

1) алгоритм распознавания, является ли данная последовательность формул формальным доказательством;

2) алгоритм, который по данному формальному доказательству находит доказываемую формулу.

Рассмотрим два примера аксиоматической теории — серьёзный и несерьёзный [3]. В качестве несерьезного примера можно взять игру в шахматы — назовем это теорией ***Ch***. Формулами в ***Ch*** будем считать ***позиции*** (всевозможные расположения фигур на доске вместе с указанием «ход белых» или «ход черных»). В шахматах используется шахматная нотация, которая позволяет точно описать любую позицию. Введем дедуктивную систему. Аксиомой теории ***Ch*** естественно считать ***начальную позицию***, а правилами вывода — ***правила игры***, которые определяют, какие ходы допустимы в каждой позиции. Правила позволяют получать из одних формул другие. В частности, отправляясь от нашей единственной аксиомы, мы можем получать теоремы ***Ch***. Общая характеристика теорем ***Ch*** состоит, очевидно, в том, что это — всевозможные позиции, которые могут получиться, если передвигать фигуры, соблюдая правила. Запись в шахматной нотации партии мы можем рассматривать как доказательство теоремы — той позиции, в которой партия остановлена.

В чем выражается формальность теории ***Ch***? Если некто предлагает нам «математический текст» и утверждает, что это — доказательство теоремы A в теории ***Ch***, то ясно, что речь идет о непроверенной записи шахматной партии, законченной (или отложенной) в позиции A. Проверка не является, однако, проблемой: правила игры сформулированы настолько точно, что можно составить программу для компьютера, которая будет осуществлять такие проверки. (Еще раз напомним, что речь идет о проверке правильности записи шахматной партии, а не о проверке того, можно ли заданную позицию получить, играя по правилам, — эта задача намного сложнее!)

Несколько серьезнее другой пример формальной теории. Формулами в теории ***L*** являются всевозможные строки, составленные из букв a, b, например a, aa, aba, $abaab$. Дедуктивную систему теории определим следующим образом. Единственной аксиомой ***L*** является строка a, наконец, в ***L*** имеется два правила вывода:

$$\frac{X}{Xb} \quad \text{и} \quad \frac{X}{aXa}.$$

Такая запись означает, что в теории ***L*** из строки X непосредственно выводятся Xb и aXa. Примером теоремы ***L*** является строка $aababb$; вывод (доказательство) для нее есть

$$a,\ ab,\ aaba,\ aabab,\ aababb.$$

Аксиоматические теории являются не просто игрой ума, а всегда представляют собой модель какой-то реальности (либо конкретной, либо математической). Вначале математик изучает реальность, конструируя некоторое абстрактное представление о ней, т. е. некоторую аксиоматическую теорию. Затем он доказывает теоремы этой аксиоматической теории. Вся польза и удобство аксиоматических теорий как раз и заключаются в их абстрагировании от конкретной реальности. Благодаря этому одна и та же аксиоматическая теория может служить моделью многочисленных конкретных ситуаций. Наконец, он возвращается к исходной точке всего построения и дает интерпретацию теорем, полученных при формализации.

6.2 Формальные аксиоматические теории

Дадим предварительные определения важных понятий, связанных с аксиоматическими теориями, наделенными семантической и дедуктивной структурами. Эти определения будут уточнены в дальнейшем в случае теорий с языками первого порядка.

Определение формальной аксиоматической теории

Как правило, понятие «*теория*» используется, когда в языке присутствует дедуктивная система. Обычно она определяется следующим образом.

Формальная теория T *считается определенной, если:*

- *задано некоторое счетное множество* A *символов — символов теории* T*; конечные последовательности символов теории* T *называются* ***выражениями*** *теории* T *(множество выражений обозначают через* A^**);*
- *имеется подмножество* $F \subset A^*$ *выражений теории* T*, называемых* ***формулами*** *теории* T*;*
- *выделено некоторое множество* $B \subset F$ *формул, называемых* ***аксиомами*** *теории* T*;*
- *имеется конечное множество* $\{R_1, R_2, \ldots, R_m\}$ *отношений между формулами, называемых* ***правилами вывода****. Правила вывода позволяют получать из некоторого конечного множества формул другое множество формул.*

Множество символов A — ***алфавит теории*** — может быть конечным или бесконечным. Обычно для образования символов используют конечное множество букв, к которым, если нужно, приписывают в качестве индексов натуральные числа.

Множество формул F обычно задается индуктивным определением, например с помощью формальной грамматики. Как правило, это множество бесконечно. Множества A и F в совокупности определяют ***язык формальной теории***.

Множество аксиом B может быть конечным или бесконечным. Если множество аксиом бесконечно, то, как правило, оно задается с помощью конечного множества ***схем аксиом*** и правил порождения конкретных аксиом из схемы аксиом[1]. Обычно для формальной теории имеется алгоритм, позволяющий по данному выражению определить, является ли оно формулой. Точно так же чаще всего существует алгоритм, выясняющий, является ли данная формула теории T аксиомой; в таком случае T называется ***эффективно аксиоматизированной*** теорией.

[1] Каждая аксиома получается из схемы заменой переменных в схеме, как правило, на произвольные формулы.

Выводимость

*Пусть $A_1, A_2, \ldots, A_n, A$ — формулы теории **T**. Если существует такое правило вывода R, что $<A_1, A_2, \ldots, A_n, A> \in R$, то говорят, что формула A **непосредственно выводима** из формул $A_1, A_2, \ldots, A_n$ по правилу вывода R. Обычно этот факт записывают следующим образом:*

$$\frac{A_1, A_2, \ldots, A_n}{A} R,$$

*где формулы $A_1, A_2, \ldots, A_n$ называются **посылками**, а формула A — **заключением**.*

***Выводом** формулы A из множества формул Γ в теории **T** называется такая последовательность формул $F_1, F_2, \ldots, F_k$, что $A = F_k$, а любая формула F_i $(i < k)$ является либо аксиомой, либо $F_i \in \Gamma$, либо непосредственно выводима из ранее полученных формул $F_{j_1}, \ldots, F_{j_n}$ $(j_1, \ldots, j_n < i)$. Если в теории **T** существует вывод формулы A из множества формул Γ, то это записывается следующим образом:*

$$\Gamma \vdash_{\boldsymbol{T}} A,$$

*где формулы из Γ называются **гипотезами** вывода, а формула A — **выводимой** из множества Γ. Если теория **T** подразумевается, то её обозначение обычно опускают.*

Если множество Γ конечно: $\Gamma = \{B_1, B_2, \ldots, B_n\}$, то вместо

$$\{B_1, B_2, \ldots, B_n\} \vdash A$$

*пишут $B_1, B_2, \ldots, B_n \vdash A$. Если Γ есть пустое множество $\varnothing$, то A называют **теоремой** (или **доказуемой** формулой) и в этом случае используют сокращенную запись $\vdash A$ («A есть теорема»).*

Отметим, что в соотношении {теоремы} $\subset$ {формулы} $\subset$ {выражения} включение множеств является строгим.

Обычно дедуктивная система удовлетворяет требованиям, сформулированным в замечании 1 (параграф 6.1).

Приведем несколько простых свойств понятия выводимости из посылок.

1. Если $\Gamma \subseteq \Sigma$ и $\Gamma \vdash A$, то $\Sigma \vdash A$.

   Это свойство выражает тот факт, что если A выводимо из множества гипотез Γ, то оно остается выводимым, если мы добавим к Γ новые гипотезы.

2. $\Gamma \vdash A$ тогда и только тогда, когда в Γ существует конечное подмножество Σ, для которого $\Sigma \vdash A$.

Часть «тогда» утверждения 2 вытекает из утверждения 1. Часть «только тогда» этого утверждения очевидна, поскольку всякий вывод A из Γ использует лишь конечное число гипотез из Γ.

3. Если $\Sigma \vdash A$ и $\Gamma \vdash B$ для любого B из множества Σ, то $\Gamma \vdash A$.

Смысл этого утверждения прост: если A выводимо из Σ и любая формула из Σ выводима из Γ, то A выводима из Γ.

Понятие формальности можно определить в терминах теории алгоритмов: теорию $\boldsymbol{T}$ можно считать формальной, если построен алгоритм[1] для проверки правильности рассуждений с точки зрения принципов теории $\boldsymbol{T}$. Это значит, что если некто предлагает математический текст, являющийся, по его мнению, доказательством некоторой теоремы в теории $\boldsymbol{T}$, то, применяя алгоритм, мы можем проверить, действительно ли предложенный текст соответствует стандартам правильности, принятым в $\boldsymbol{T}$. Таким образом, стандарт правильности рассуждений для теории $\boldsymbol{T}$ определен настолько точно, что проверку его соблюдения можно передать компьютеру (следует помнить, что речь идет о *проверке правильности* готовых доказательств, а не об их поиске!). Если проверку правильности доказательств в какой-либо теории нельзя передать компьютеру и она доступна в полной мере только человеку, значит, еще не все принципы теории аксиоматизированы (то, что мы не умеем передать компьютеру, остается в нашей интуиции и «оттуда» регулирует наши рассуждения).

Интерпретация, модель

Семантическую систему теории вводим с помощью следующих понятий.

Понятие интерпретации аксиоматической теории определяется как обобщение интерпретации языков первого порядка. Это позволяет ввести понятие истинности.

Следующие понятия есть просто обобщение понятий, введенных для языков первого порядка.

*Формула P называется **общезначимой**, если она истинна в каждой интерпретации теории (обозначается $\vDash P$).*

*Формула P называется **противоречием**, если формула P ложна во всякой интерпретации теории.*

Формализация задается не только синтаксисом и семантикой формального языка (эти компоненты как раз чаще всего берутся традиционными из хорошо известного крайне ограниченного набора), но и множеством утверждений, которые считаются истинными. Именно эта формулировка базисных свойств, аксиом, описывающих некоторую предметную область, обычно рассматривается как математическое описание объектов. Таким образом, практически нас интересуют не все интерпретации данной теории, а лишь те из них, на которых выполнены аксиомы.

[1] Пока мы можем довольствоваться нашим интуитивным пониманием алгоритмов. Точное определение понятия алгоритма смотрите в главе 8.

При рассмотрении аксиоматических теорий в общем виде любое множество замкнутых формул данного языка может быть принято в качестве системы аксиом. Пусть Г — произвольное множество замкнутых формул языка.

Интерпретация называется ***моделью множества формул*** Г*, если все формулы этого множества истинны в данной интерпретации. Множество* Г *называется* ***совместным****, если оно имеет хотя бы одну модель.*

Если в аксиоматической теории вводят семантическую и дедуктивную систему, то это делают таким образом, чтобы доказуемые формулы были истинными. В этом случае говорят, что дедуктивная система *корректна* относительно семантической системы.

- ***Моделью теории*** *называется такая интерпретация, в которой истинны все теоремы теории (для этого достаточно, чтобы были истинны все аксиомы теории).*
- *Формула P называется* ***логическим следствием*** *(семантическим следствием) множества формул* Г*, если P выполняется в любой модели* Г *(обозначается* $\Gamma \models P$*).*
- *Формула B является* ***логическим следствием*** *формулы A (обозначение:* $A \models B$*), если формула B выполнена в любой интерпретации, в которой выполнена формула A.*
- *Формулы A и B* ***логически эквивалентны*** *(обозначение:* $A \equiv B$*), если они являются логическим следствием друг друга.*

При изучении аксиоматических теорий нужно различать теоремы аксиоматической теории и теоремы об аксиоматической теории, или ***метатеоремы***. Это различие не всегда явно формализуется, но всегда является существенным.

Множество теорем аксиоматической теории является точно определенным объектом (обычно бесконечным), и поэтому можно доказывать утверждения, относящиеся ко всем теоремам одновременно. Например, в теории ***Ch*** (параграф 6.1) множество всех теорем оказывается, правда, конечным (хотя конечность эта с практической точки зрения ближе к бесконечности). Легко доказать следующее утверждение, относящееся ко *всем* теоремам ***Ch***: ни в одной теореме белые не имеют 10 ферзей. В самом деле, достаточно заметить, что в аксиоме ***Ch*** белые имеют одного ферзя и восемь пешек и что по правилам игры белым ферзем может стать только белая пешка. Следовательно, $1 + 8 < 10$. Таким образом, мы подметили в системе аксиом и правил вывода теории ***Ch*** особенности, которые делают справедливым наше общее утверждение о теоремах ***Ch***.

Аналогичные возможности имеем в случае теории ***L*** (параграф 6.1). Можно доказать, например, следующее утверждение, относящееся ко всем теоремам ***L***: если X — теорема, то aaX — тоже теорема (см. пример 7.5 в параграфе 7.2 главы 7).

*Формальная теория **T** с языком первого порядка называется **противоречивой**, если существует формула A, доказуемая вместе со своим отрицанием ¬A. Теория называется **непротиворечивой**, если она не является противоречивой. В другой терминологии говорят также, что теория **синтаксически** (или **дедуктивно**) **непротиворечива**.*

Формальная теория пригодна для описания тех предметных областей, которые являются ее моделями. Справедлива теорема 1.

Теорема 1. Модель для формальной теории ***T*** существует тогда и только тогда, когда ***T*** синтаксически непротиворечива.

Полнота, независимость и разрешимость

Пусть универсум M, рассматриваемый с соответствующей интерпретацией, является моделью формальной теории ***T***.

*Формальная теория **T** называется **полной** (относительно данной интерпретации), если каждому истинному высказыванию об объектах M соответствует теорема теории **T**.*

*Если для предметной области M существует формальная полная непротиворечивая теория **T**, то M называется **аксиоматизируемой** (или **формализуемой**).*

*Система аксиом (или аксиоматизация) непротиворечивой теории **T** называется **независимой**, если никакая из аксиом не выводима из остальных по правилам вывода теории **T**.*

Одним из первых вопросов, которые возникают при задании формальной теории, является вопрос о том, возможно ли, рассматривая какую-нибудь формулу формальной теории, определить, является ли она доказуемой или нет. Другими словами, речь идет о том, чтобы определить, является ли данная формула теоремой или *не теоремой* и как это доказать.

*Формальная теория **T** называется **разрешимой**, если существует алгоритм, который для любой формулы теории определяет, является ли эта формула теоремой теории.*

*Формальная теория **T** называется **полуразрешимой**, если существует алгоритм, который для любой формулы P теории выдает ответ «да», если P является теоремой теории, и выдает «нет» или, может быть, не выдает никакого ответа, если P не является теоремой (т. е. алгоритм применим не ко всем формулам).*

Для первоначального знакомства с аксиоматическими теориями познакомимся с простыми учебными примерами, взятыми из книги Дугласа Хофштадтера[1] (рис. 6.2) «Гёдель, Эшер, Бах: эта бесконечная гирлянда» [3].

Рис. 6.2 – Дуглас Хофштадтер

Формальная система *MIU*

Алфавит: M, I, U.

Формулы = $\{M, I, U\}^*$.

Определим дедуктивную систему.

Аксиома: MI.

Правила вывода:

1) $xI \to xIU$ (продукция);
2) $Mx \to Mxx$ (продукция);
3) $III \to U$ (правило переписывания);
4) $UU \to \varnothing$ (правило переписывания, $\varnothing$ обозначает пустую строку).

Продукция — это правило, применяемое к формулам, рассматриваемым как единое целое, а правило переписывания — правило, которое может применяться к любой подформуле формулы.

Приведем типичный вывод в этой теории:

MI	Аксиома
MII	Правило 2
MIIII	Правило 2
MUI	Правило 3
MUIU	Правило 1
MUIUUIU	Правило 2
MUIIU	Правило 4

Любые утверждения о свойствах этой теории являются метатеоремами. Читателю предлагается задача: «Найдите вывод *MU* или докажите, что он невозможен».

Формальная система *PR*

Алфавит: $\{P, R, -\}$.

Выражения — элементы $\{P, R, -\}^*$.

Формулы — строки вида $xPyRz$, где x, y и z — строки, состоящие только из тире.

Определим дедуктивную систему.

Схема аксиом:

$xP-Rx-$ является аксиомой, когда x состоит только из тире (каждое из двух вхождений x замещает одинаковое число тире).

Правило вывода (схема).

Пусть x, y и z — строки, состоящие только из тире. Пусть $xPyRz$ является теоремой. Тогда $xPy-Rz-$ также будет теоремой.

В системе *PR* используются только удлиняющие правила, т. е. количество символов в формуле в результате применения правила вывода увеличивается.

[1] Дуглас Роберт Хофштадтер (род. 1945 г.) — американский физик и информатик. Получил всемирную известность благодаря книге «Гёдель, Эшер, Бах: эта бесконечная гирлянда», опубликованной в 1979 году и в 1980 году получившей Пулитцеровскую премию в категории «Нехудожественная литература».

Определим семантическую структуру. Выберем следующую интерпретацию системы *PR* (одну из возможных).

- Универсум — множество целых положительных чисел.
- Строка, состоящая из *n* тире, интерпретируется как число *n*.
- *P* интерпретируется как символ +.
- *R* интерпретируется как символ =.

Нетрудно убедиться, что указанная интерпретация теореме *xPyRz* ставит в соответствие истинное утверждение о целых положительных числах «$x + y = z$» и поэтому данная интерпретация является моделью системы *PR*.

Теперь мы можем использовать более простой разрешающий алгоритм для теории *PR*: формула *xPyRz* является теоремой тогда и только тогда, когда $x + y = z$ — истина.

В модели теоремы и истины совпадают — т. е. между теоремами и фрагментами реального мира существует изоморфизм.

Грубо говоря, изоморфизм есть преобразование, сохраняющее информацию. Слово «изоморфизм» применимо к тем случаям, когда две сложные структуры могут быть отображены одна в другую таким образом, что каждой части одной структуры соответствует какая-то часть другой структуры («соответствие» здесь означает, что эти части выполняют в своих структурах сходные функции).

При данной интерпретации есть изоморфизм между системой *PR* и сложением натуральных чисел.

Формальная система *UR*

Алфавит: $\{U, R, -\}$.

Выражения — элементы $\{U, R, -\}^*$.

Формулы — строки вида *xUyRz*, где *x*, *y* и *z* — строки, состоящие только из тире.

Определим дедуктивную систему.

Схема аксиом:

xU−Rx является аксиомой, когда *x* состоит только из тире (каждое из двух вхождений *x* замещает одинаковое число тире).

Правило вывода (схема).

Пусть *x*, *y* и *z* — строки, состоящие только из тире. Пусть *xUyRz* является теоремой. Тогда *xUy−Rzx* также будет теоремой.

Определим семантическую структуру. Выберем следующую интерпретацию системы *UR*.

- Универсум — множество целых положительных чисел.
- Строка, состоящая из *n* тире, интерпретируется как число *n*.
- *P* интерпретируется как символ ×.
- *R* интерпретируется как символ =.

Нетрудно убедиться, что указанная интерпретация теореме *xUyRz* ставит в соответствие истинное утверждение о целых положительных числах «$x \times y = z$» и поэтому данная интерпретация является моделью системы *UR*.

Формальная система *PR*1

Алфавит: $\{P, R, -\}$.

Выражения — элементы $\{P, R, -\}^*$.

Формулы — строки вида $xPyRz$, где x, y и z — строки, состоящие только из тире.

Определим дедуктивную систему.

Схемы аксиом:

1) $xP{-}Rx{-}$ является аксиомой, когда x состоит только из тире (каждое из двух вхождений x замещает одинаковое число тире).
2) $xP{-}Rx$ является аксиомой, когда x состоит только из тире (каждое из двух вхождений x замещает одинаковое число тире).

Правило вывода (схема).

Пусть x, y и z — строки, состоящие только из тире. Пусть $xPyRz$ является теоремой. Тогда $xPy{-}Rz{-}$ также будет теоремой.

Рассмотрим различные интерпретации системы $PR1$.

1. Выберем интерпретацию системы $PR1$ такую же, как для PR.

- Универсум — множество целых положительных чисел.
- Строка, состоящая из n тире, интерпретируется как число n.
- P интерпретируется как символ +.
- R интерпретируется как символ =.

Указанная интерпретация теореме $xPyRz$ ставит в соответствие утверждение о целых положительных числах «$x + y = z$». Но эти утверждения могут быть и ложными, поэтому данная интерпретация не является моделью системы $PR1$.

2. Вторая интерпретация системы $PR1$ отличается от первой только тем, как интерпретируется символ R.

- R интерпретируется как «равняется или больше на 1».

Указанная интерпретация теореме $xPyRz$ ставит в соответствие истинное утверждение о целых положительных числах

$$«x + y = z + 1 \vee x + y = z»,$$

и поэтому данная интерпретация является моделью системы $PR1$. Более того, любое истинное утверждение

$$«x + y = z + 1 \vee x + y = z»$$

описывается в виде теоремы $xPyRz$ теории $PR1$. То есть теория с данной интерпретацией является полной.

3. В последней интерпретации символ R понимается снова по-другому.

- R интерпретируется как символ «$\geqslant$».

Указанная интерпретация теореме $xPyRz$ ставит в соответствие истинное утверждение о целых положительных числах «$x + y \geqslant z$», и поэтому данная интерпретация является моделью системы $PR1$. Но мы сейчас имеем существенное отличие от предыдущей интерпретации: не все истинные утверждения вида $x + y \geqslant z$ являются теоремами в $PR1$. Так, например, формула $-P-R-$ имеет истинную интерпретацию $2 + 1 \geqslant 1$, но это не теорема.

6.3 Исчисление высказываний

Мы опишем применение аксиоматического метода к пропозициональной логике. В результате получим формальную аксиоматическую теорию, называемую

исчислением высказываний. Семантическая система в языке пропозициональной логики уже введена, введем дедуктивную систему.

Исчислением высказываний *называется формальная теория с языком логики высказываний, со схемами аксиом*

A_1) $A \supset (B \supset A)$;

A_2) $\big(A \supset (B \supset C)\big) \supset \big((A \supset B) \supset (A \supset C)\big)$;

A_3) $(\neg B \supset \neg A) \supset \big((\neg B \supset A) \supset B\big)$

*и правилом вывода MP (**modus ponens** — обычно переводится как **правило отделения**):*

$$\frac{A,\ A \supset B}{A}\ MP.$$

Здесь A, B и C — *любые* пропозициональные формулы[1]. Таким образом, множество аксиом исчисления высказываний бесконечно, хотя задано тремя схемами аксиом. Множество правил вывода также бесконечно, хотя оно задано только одной схемой.

Пример 6.2

Для любой формулы A построим вывод формулы $A \supset A$, т. е. $A \supset A$ — теорема.

Подставляем в схему аксиом A_2 вместо B формулу $A \supset A$ и вместо C формулу A, получаем аксиому

$$\big(A \supset \big((A \supset A) \supset A\big)\big) \supset \big(\big(A \supset (A \supset A)\big) \supset (A \supset A)\big). \tag{6.1}$$

Подставляем в A_1 вместо формулы B формулу $A \supset A$, получаем аксиому

$$A \supset \big((A \supset A) \supset A\big). \tag{6.2}$$

Из формул (6.1) и (6.2) по правилу *MP* получаем

$$\big(A \supset (A \supset A)\big) \supset (A \supset A). \tag{6.3}$$

Подставляем в A_1 вместо формулы B формулу A, получаем аксиому

$$A \supset (A \supset A). \tag{6.4}$$

Из формул (6.3) и (6.4) по правилу *MP* получаем $A \supset A$.

[1] До конца этого параграфа под словом «формула» мы будем понимать только пропозициональные формулы.

Теорема 2. Пусть Г — произвольное множество гипотез. Если $\Gamma \vdash \vdash A \supset B$ и $\Gamma \vdash A$, то $\Gamma \vdash B$.

Доказательство. Пусть $A_1, A_2, \ldots, A_n$ — вывод формулы A из Г, где A_n совпадает с A. Пусть $B_1, B_2, \ldots, B_m$ — вывод формулы $A \supset B$ из Г, где B_n совпадает с $A \supset B$. Тогда $A_1, A_2, \ldots, A_n, B_1, B_2, \ldots, B_m, B$ — вывод формулы B из Г. Последняя формула в этом выводе получена применением правила *MP* к формулам A_n и B_m.

В исчислении высказываний импликация очень тесно связана с выводимостью.

Теорема 3 (о дедукции, Эрбран)[1]. Пусть Г — множество формул. Имеем $\Gamma \cup \{A\} \vdash B$, тогда и только тогда, когда $\Gamma \vdash A \supset B$.

Следствие:

1. $A \supset B, B \supset C \vdash A \supset C$.
2. $A \supset (B \supset C), B \vdash A \supset C$.

Доказательство 1.

(a) $A \supset B$ гипотеза.

(b) $B \supset C$ гипотеза.

(c) A гипотеза.

(d) B применяя *MP* из (a) и (c).

(e) C применяя *MP* из (b) и (d).

Таким образом, $A \supset B, B \supset C, A \vdash C$. И по теореме дедукции, $A \supset (B \supset C), B \vdash A \supset C$.

Доказательство 2.

(a) $A \supset (B \supset C)$ гипотеза.

(b) B гипотеза.

(c) A гипотеза.

(d) $B \supset C$ применяя *MP* из (a) и (c).

(e) C применяя *MP* из (b) и (d).

Таким образом, $A \supset (B \supset C), B, A \vdash C$. И по теореме дедукции, $A \supset (B \supset C), B \vdash A \supset C$.

Пример использования теоремы о дедукции см. в параграфе 7.3 главы 7.

Полнота, разрешимость и непротиворечивость исчисления высказываний

В исчислении высказываний у нас есть два понятия, касающиеся формул: теорема и тавтология. Аксиомы и правило вывода придуманы так, что эти два понятия совпадают.

[1] Жак Эрбран (1908–1931 гг.) — французский математик и логик.

Наша цель — показать, что формула исчисления высказываний является тавтологией тогда и только тогда, когда она есть теорема. В одну сторону это совсем просто.

Теорема 4.

1. Любая аксиома в исчислении высказываний является тавтологией.
2. Любая теорема в исчислении высказываний является тавтологией.

Доказательство. То, что каждая аксиома A_1–A_3 является тавтологией, легко проверить с помощью таблиц истинности. Для доказательства п. 2 теоремы достаточно доказать, что правило *MP*, примененное к тавтологиям, приводит к тавтологиям.

Действительно, пусть при произвольном распределении истинностных значений формулы A и $A \supset B$ являются тавтологиями. Тогда формула A истинна и, по свойствам импликации, B истинно. Следовательно, B — тавтология. Доказательства обратного утверждения смотрите в [4].

Теорема 5 (Поста[1]*, 1921 г.)*. Формула A в исчислении высказываний является теоремой тогда и только тогда, когда A — тавтология.

Интерпретация формул исчисления высказываний проста — область интерпретации состоит из двух значений «истина» и «ложь»; поэтому пропозициональная переменная принимает только значения **И** и **Л** и интерпретация составной формулы вычисляется по известным законам с помощью логических операций над истинностными значениями. Поскольку любая формула содержит только конечное число пропозициональных переменных, то формула обладает только конечным числом различных интерпретаций. Следовательно, исчисление высказываний является, очевидно, разрешимой формальной теорией.

Легко убедиться, что исчисление высказываний является непротиворечивой теорией. Действительно, все теоремы исчисления высказываний суть тавтологии. Следовательно, никакая опровержимая формула не может быть доказана.

Другие аксиоматизации исчисления высказываний

Теория, определенная для пропозициональной логики, не является единственно возможной аксиоматизацией исчисления высказываний. Её основное достоинство — лаконичность при сохранении определенной наглядности. Действительно, в теории всего две связки, три схемы аксиом и одно правило. Известны и многие другие аксиоматизации исчисления высказываний, предложенные различными авторами [4, с. 48–51]. В классической логике все аксиоматизации приводят к одному множеству выводимых формул.

Например, оставив *MP* как единственное правило вывода, можно объявить схемами аксиом следующие формулы:

[1] Эмиль Леон Пост (1897–1954 гг.) — американский математик и логик.

- $A \supset (B \supset A)$;
- $\big(A \supset (B \supset C)\big) \supset \big((A \supset B) \supset (A \supset C)\big)$;
- $A \,\&\, B \supset A$;
- $A \,\&\, B \supset B$;
- $A \supset (B \supset A \,\&\, B)$;
- $A \supset A \vee B$;
- $B \supset A \vee B$;
- $(A \supset C) \supset \big((B \supset C) \supset (A \vee B \supset C)\big)$;
- $\neg A \supset (A \supset B)$;
- $(A \supset B) \supset \big((A \supset \neg B) \supset \neg A\big)$;
- $A \vee \neg A$.

Последняя аксиома $A \vee \neg A$, называемая «***законом исключенного третьего***» и иногда читаемая как «третьего не дано» (*tertium non datur* в латинском оригинале), вызвала в первой половине XX века большое количество споров.

6.4 Аксиоматизация геометрии

«Начала» Евклида не были достаточно последовательными с точки зрения воплощения даже неформального аксиоматического метода. Трактат начинается с определений таких геометрических понятий, как «точка», «прямая», «плоскость» и др. Но это все не определения, а пояснения понятий. При современном изложении геометрии данные понятия не определяются. Евклид дает 19 аксиом [5], которым удовлетворяют точки, прямые и плоскости, но этих аксиом недостаточно. Он иногда опирается на утверждения, не входящие в список аксиом. Многие рассуждения Евклида апеллировали к зрительной интуиции. Но тем не менее следует отдать должное древнегреческим математикам, и в частности Евклиду, что впервые более двух тысяч лет назад была поставлена задача логического обоснования математики и в большей части удовлетворительно решена.

Изложение геометрии, основанное на «Началах» Евклида, постепенно улучшалось усилиями многих математиков. Были добавлены отсутствующие аксиомы, и некоторые аксиомы стали теоремами. Очень много усилий было потрачено математиками на освобождение геометрии Евклида от его ***аксиомы о параллельных прямых***. Часть аксиом Евклид называл ***постулатами*** — они были связаны с какими-то геометрическими построениями и аксиома о параллельных более известна как пятый постулат Евклида. В современном и более простом, но математически равносильном, виде аксиома о параллельности гласит:

«В плоскости через точку, не лежащую на данной прямой, можно провести одну и только одну прямую, параллельную данной».

За два тысячелетия было предложено много доказательств этой аксиомы, но в каждом из них рано или поздно обнаруживался порочный круг: оказывалось, что среди явных или неявных посылок содержится утверждение, которое не удаётся доказать без использования того же пятого постулата.

Глубокое исследование аксиомы о параллельных, основанное на совершенно оригинальном принципе, провёл в 1733 году итальянский монах-иезуит, преподаватель математики Джироламо Саккери. Он опубликовал труд под названием «Евклид, очищенный от всех пятен, или же геометрическая попытка установить самые первые начала всей геометрии». Идея Саккери состояла в том, чтобы заменить пятый постулат противоположным утверждением («через точку, взятую вне данной прямой, можно провести более одной прямой, параллельной данной»), вывести из новой системы аксиом как можно больше следствий, тем самым построив «ложную геометрию», и найти в этой геометрии противоречия или заведомо неприемлемые положения. Тогда справедливость аксиомы о параллельных будет доказана от противного [6]. Но ему не удалось получить противоречие.

Рис. 6.3 – Николай Лобачевский

В первой половине XIX века по пути, проложенному Саккери, пошли Карл Гаусс, венгерский математик Янош Бойяи и российский математик Николай Лобачевский (рис. 6.3). Но цель у них была уже иная — не разоблачить неевклидову геометрию как невозможную, а, наоборот, построить альтернативную геометрию и выяснить её возможную роль в реальном мире. На тот момент это была совершенно еретическая идея; никто из учёных ранее не сомневался, что физическое пространство евклидово. Гаусс не решился опубликовать работу на эту тему, но его черновые заметки и несколько писем подтверждают глубокое понимание неевклидовой геометрии.

Лобачевский и Бойяи проявили большую смелость, чем Гаусс, и почти одновременно (Лобачевский — в докладе 1826 года и публикации 1829 года; Бойяи — в письме 1831 года и публикации 1832 года), независимо друг от друга, опубликовали изложение того, что сейчас называется геометрией Лобачевского. Лобачевский продвинулся в исследовании новой геометрии дальше всех, и она в настоящий момент носит его имя.

Приведем примеры теорем, которые имеют место в геометрии Лобачевского. Прежде всего заметим, что все теоремы, доказываемые без использования аксиомы параллельности, сохраняются и в геометрии Лобачевского. Например, вертикальные углы конгруэнтны (равны), углы при основании равнобедренного треугольника конгруэнтны; из данной точки можно опустить на данную прямую только один перпендикуляр. Теоремы же евклидовой геометрии, при доказательстве которой применяется аксиома параллельности, в геометрии Лобачевского видоизменяются. Например, теорема о сумме углов треугольника: *сумма величин углов любого треугольника меньше* π.

Разность $\delta = \pi - (\angle A + \angle B + \angle C)$ называется дефектом треугольника ABC. Лобачевский доказал, что в его геометрии площадь треугольника пропорциональна дефекту, $S = k \cdot \delta$, где коэффициент k зависит от выбора единицы измерения площадей.

Интересно, что в геометрии Лобачевского существуют три прямые, попарно параллельные друг другу в различных направлениях (рис. 6.4).

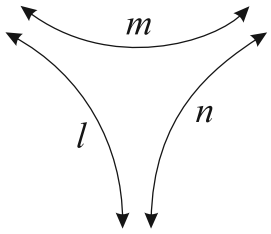


Рис. 6.4 – Треугольник из параллельных прямых

У треугольника, образованного этими прямыми, вершины как бы находятся в бесконечности, причем мера каждого угла равна 0. Отсюда следует, что дефект этого «треугольника» равен π и, следовательно, этот бесконечный «треугольник» имеет конечную площадь.

Главная заслуга Лобачевского в том, что он поверил в новую геометрию и имел мужество отстаивать своё убеждение.

При этом Лобачевский действовал «синтаксически», манипулируя с аксиомами чисто формально, без какого бы то ни было визуального сопровождения, ибо никто в те времена не мог себе представить, как неевклидову геометрию можно реализовать.

Доказать непротиворечивость новой геометрии ни Лобачевский, ни Бойяи не сумели — тогда математика ещё не располагала необходимыми для этого средствами. Только спустя 40 лет появились модель Феликса Клейна и модель Пуанкаре, реализующие аксиоматику геометрии Лобачевского на базе евклидовой геометрии. В модели Клейна (рис. 6.5) плоскость — внутренность круга k, прямые — хорды. Через точку P проходит целый пучок хорд, не пересекающих прямую a.

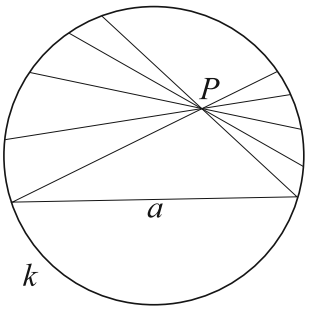


Рис. 6.5 – Модель Клейна

Таким образом, геометрия Лобачевского непротиворечива, если непротиворечива евклидова геометрия.

Первая последовательная и полная аксиоматическая теория для евклидовой геометрии была создана Давидом Гильбертом в самом конце XIX века, после того как Мориц Паш и Гильберт обнаружили все утверждения, которые Евклид не сформулировал в виде аксиом, но использовал при доказательствах [7].

Дадим представление об аксиоматике Гильберта в неформальном виде. Полное описание аксиом и понятий и примеры доказательств геометрических теорем смотрите в [5]. Восемь понятий считаются неопределенными: «точка», «прямая», «плоскость», отношение «точка лежит на прямой», отношение «точка лежит на

плоскости», отношение «точка B лежит между точками A и C», отношение равенства для углов, отношение равенства для отрезков. На основе исходных неопределяемых понятий определяются новые понятия «пересекаться» (о прямых и плоскостях), «лежать на», «принадлежать», «проходить через» (о прямой и плоскости) и т. п.

Аксиомы делятся на пять групп.

Аксиомы связи (8 аксиом)

Аксиомы связи, или аксиомы принадлежности, говорят о том, в каких отношениях точки, прямые и плоскости могут находиться друг с другом. При интерпретации этих аксиом на естественном языке мы обычно используем выражения «точка лежит на плоскости», «прямая проходит через две данные точки» и т. п.

Пример аксиомы из этой группы:

Если две различные точки лежат на некоторой прямой и на некоторой плоскости, то всякая точка, лежащая на этой прямой, лежит и на этой плоскости.

Аксиомы порядка (6 аксиом)

Аксиомы порядка описывают расположение точек прямой на основе отношения «между».

В качестве примера аксиомы из этой группы приведем аксиому Паша (Мориц Паш открыл эту аксиому в 1882 г.). Эта аксиома в неформальном изложении такова:

Прямая, расположенная в плоскости треугольника и пересекающая одну из сторон этого треугольника, обязательно пересекает и какую-то другую сторону.

Аксиомы конгруэнтности (6 аксиом)

В этих аксиомах определяется равенство отрезков, углов, треугольников.

Но предварительно эти новые понятия должны быть определены через неопределяемые и уже введенные понятия.

Пример аксиомы:

Всякий угол равен самому себе.

Аксиомы непрерывности (2 аксиомы)

Приведем вольные формулировки этих двух аксиом.

Аксиома Архимеда утверждает, что, шагая по прямой равномерными шагами, можно рано или поздно перешагнуть через любую точку на этой прямой.

Аксиома Кантора утверждает, что для любой последовательности вложенных друг в друга отрезков найдется точка, лежащая внутри каждого из этих отрезков.

Последняя группа состоит из одной аксиомы.

Аксиома о параллельных

Через всякую точку, не лежащую на какой-либо прямой p, проходит не более одной прямой, параллельной прямой p.

Утверждение, что через точку вне данной прямой можно провести прямую, параллельную данной, есть теорема, вытекающая из остальных аксиом геометрии, так что нет нужды провозглашать ее аксиомой.

Аксиоматику Гильберта можно полностью описать на языке первого порядка, и аксиомы Гильберта образуют независимую систему аксиом. Что касается непротиворечивости системы аксиом, то Гильберт построил ее модель, опирающуюся

на теорию действительных чисел. Что касается теории действительных чисел, то ее непротиворечивость (как показывают модели, построенные Кантором и Дедекиндом) сводится к непротиворечивости рациональных чисел, что, в свою очередь, сводится к непротиворечивости теории элементарной арифметики ***EA*** (параграф 6.6).

Правомочен вопрос: какая из аксиом о параллельности, Евклида или Лобачевского, точнее описывает те представления о структуре реального физического пространства, которые отражаются в геометрических образах? Строгий ответ на этот вопрос: неизвестно. Однако можно с уверенностью утверждать, что в доступных нашему наблюдению областях пространства евклидова геометрия соблюдается с высокой степенью точности. Так что, когда мы говорим о неизвестности, мы имеем в виду очень большие области пространства.

6.5 Теории первого порядка

Языки первого порядка используются в формальных теориях первого порядка.

Синтаксические свойства истинности теорий с языками первого порядка

Пусть нам дана некоторая формальная теория $\boldsymbol{T}$ с языком первого порядка Ω и задана интерпретация φ этого языка. Обозначим через $\boldsymbol{F}_\varphi$ множество всех формул теории $\boldsymbol{T}$, истинных в данной интерпретации. Множество $\boldsymbol{F}_\varphi$ обладает определенными свойствами, которые отражают заложенную в языки первого порядка логику, не зависящую от конкретных особенностей интерпретации.

Предварительно надо определить следующее понятие. Пусть дана формула P, свободное вхождение переменной x в P и терм t. Мы говорим, что ***данное вхождение*** x ***не связывает*** t ***в*** P, если оно не лежит в области действия ни одного квантора вида $\forall y$ и $\exists y$, где y — переменная, входящая в t.

Иными словами, после подстановки t вместо данного вхождения x все переменные, входящие в t, останутся свободными в P.

Чаще всего приходится подставлять терм вместо каждого из свободных вхождений данной переменной. Важно, что такая операция переводит термы в термы и формулы в формулы. Если каждое свободное вхождение x в P не связывает t, мы будем говорить просто, что ***терм*** t ***свободный для*** x ***в*** P.

Пример 6.3

1. Терм y свободен для переменной x в формуле $P(x)$, но тот же терм y не свободен для переменной x в формуле $\forall y P(x)$.

2. Терм $f(x, z)$ свободен для переменной x в формуле $\forall y P(x, y) \supset Q(x)$, но тот же терм $f(x, z)$ не свободен для переменной x в формуле $\exists z \forall y P(x, y) \supset Q(x)$.

Теперь мы готовы перечислить свойства $\boldsymbol{F}_\varphi$.

1. Для любой замкнутой формулы P либо $P \in \boldsymbol{F}_\varphi$, либо $\neg P \in \boldsymbol{F}_\varphi$.

2. Множество $\boldsymbol{F}_\varphi$ не содержит противоречия, т. е. ни для какой формулы P не может быть, чтобы одновременно выполнялось $P \in \boldsymbol{F}_\varphi$ и $\neg P \in \boldsymbol{F}_\varphi$.
3. Множество $\boldsymbol{F}_\varphi$ содержит все тавтологии языка Ω (см. главу 5, параграф 5.4).
4. Множество $\boldsymbol{F}_\varphi$ содержит следующие общезначимые формулы:
   а) $\forall x A(x) \supset A(t)$,
   где $A(t)$ есть формула теории $\boldsymbol{T}$ и t есть терм теории $\boldsymbol{T}$, свободный для x в $A(x)$. Условие, чтобы t был свободен для x, — гигиеническое правило при перемене обозначений;
   б) $\forall x\big(A \supset B(x)\big) \supset \big(A \supset \forall x B(x)\big)$,
   где A не содержит свободных вхождений переменной x;
   в) $\big(\forall x \neg A(x)\big) \sim \big(\neg \exists x A(x)\big)$.
5. Множество $\boldsymbol{F}_\varphi$ замкнуто относительно правил вывода modus ponens и обобщения. По определению это означает, что если $A \in \boldsymbol{F}_\varphi$ и $A \supset B \in \boldsymbol{F}_\varphi$, то также $B \in \boldsymbol{F}_\varphi$; если $A \in \boldsymbol{F}_\varphi$, то $\forall x A \in \boldsymbol{F}_\varphi$ для любой переменной x.

Определение теорий первого порядка

Теорией первого порядка называется теория с языком Ω первого порядка, обладающая всеми описанными в предыдущем пункте свойствами истинности. Теории первого порядка различаются сигнатурами Ω и аксиомами.

Аксиомы теории первого порядка $\boldsymbol{T}$ разбиваются на два класса: логические аксиомы (вместе с аксиомами равенства) и собственные (или нелогические).

Логические аксиомы: каковы бы ни были формулы A, B и C теории $\boldsymbol{T}$, следующие формулы являются логическими аксиомами теории $\boldsymbol{T}$:

$\boldsymbol{A}_1$. $A \supset (B \supset A)$.

$\boldsymbol{A}_2$. $\big(A \supset (B \supset C)\big) \supset \big((A \supset B) \supset (A \supset C)\big)$.

$\boldsymbol{A}_3$. $(\neg B \supset \neg A) \supset \big((\neg B \supset A) \supset B\big)$.

$\boldsymbol{A}_4$. $\forall x A(x) \supset A(t)$, где $A(t)$ есть формула теории $\boldsymbol{T}$ и t есть терм теории $\boldsymbol{T}$, свободный для x в $A(x)$. Заметим, что t может совпадать с x, и тогда мы получаем аксиому $\forall x A(x) \supset A(x)$.

$\boldsymbol{A}_5$. $\forall x\big(A \supset B(x)\big) \supset \big(A \supset \forall x B(x)\big)$, где A не содержит свободных вхождений переменной x.

Аксиомы равенства.

$\boldsymbol{A}_6$. $t_1 = t_1$.

$\boldsymbol{A}_7$. $t_1 = t_2 \supset t_2 = t_1$.

$\boldsymbol{A}_8$. $t_1 = t_2 \;\&\; t_2 = t_3 \supset t_1 = t_3$.

$\boldsymbol{A}_9$. $t_1 = s_1 \;\&\; \ldots \;\&\; t_n = s_n \supset f(t_1, \ldots, t_n) = f(s_1, \ldots, s_n)$.

$\boldsymbol{A}_{10}$. $t_1 = s_1 \;\&\; \ldots \;\&\; t_n = s_n \supset P(t_1, \ldots, t_n) \equiv P(s_1, \ldots, s_n)$.

В этих аксиомах $t_1, \ldots, t_n$, $s_1, \ldots, s_n$ — любые термы, f — любой n-местный функциональный символ из Ω, P — любой n-местный предикатный символ из Ω.

Собственные аксиомы: таковые не могут быть сформулированы в общем случае, ибо меняются от теории к теории.

Правилами вывода во всякой теории первого порядка являются:

1. Modus ponens:

$$\frac{A,\ A \supset B}{B}\ MP.$$

2. Правило обобщения:

$$\frac{A(x)}{\forall x A(x)}\ Gen.$$

Формула B называется ***непосредственным следствием формул*** A, $A \supset B$ ***по правилу modus ponens***. Формула $\forall x A(x)$ называется ***непосредственным следствием формулы*** $A(x)$ ***по правилу обобщения***.

Интуитивный смысл правил вывода следующий. Правило modus ponens отвечает элементарному рассуждению типа: если верно A и верно, что из верности A следует верность B, то верно B. Правило обобщения соответствует практике записи тождества или универсально верных утверждений в математике. Когда мы пишем $(a + b)^2 = a^2 + 2ab + b^2$ или «в прямоугольном треугольнике квадрат гипотенузы равен сумме квадратов катетов», кванторы $\forall ab$, $\forall$ (треугольник) опускаются.

Теория первого порядка, которая не содержит собственных аксиом, называется ***исчислением предикатов первого порядка***. ***Чистым исчислением предикатов*** называется исчисление предикатов первого порядка, не содержащее предметных констант и функторов.

Аксиомы $\boldsymbol{A}_1$–$\boldsymbol{A}_3$ являются также аксиомами исчисления высказываний, поэтому с помощью правила modus ponens выводимы все тавтологии языка Ω. Аксиомы $\boldsymbol{A}_4$–$\boldsymbol{A}_5$ называются «логическими аксиомами с кванторами». Аксиома $\boldsymbol{A}_4$ (***аксиома специализации***) означает, что если $A(x)$ верна для любого x, то $A(t)$ верна для любого t, где t — имя любого объекта.

Пример 6.4

Теории первого порядка с собственными аксиомами широко распространены в математике. Некоторые из них применяются в логическом программировании [8, 9]. Логическое программирование является, пожалуй, наиболее впечатляющим примером применения идей и методов математической логики (точнее, одного из ее разделов — теории логического вывода) в программировании.

Идея использования языка логики предикатов первого порядка в качестве языка программирования возникла еще в 60-е годы, когда создавались многочисленные системы автоматического доказательства теорем и основанные на них вопросно-ответные системы. Суть этой идеи заключается в том, чтобы программист не указывал машине последовательность шагов, ведущих к решению задачи, как это делается во всех процедурных языках программирования, а описывал на логическом языке свойства интересующей его области, иначе говоря, описывал мир своей задачи. Другие свойства и удовлетворяющие им объекты машина находила бы сама путем построения логического вывода.

Первые компьютерные реализации систем автоматического доказательства теорем появились в конце 50-х годов, а в 1965 г. Дж. Робинсон[1] предложил метод резолюций [10], который и по сей день лежит в основе большинства систем поиска логического вывода.

[1] Джон Алан Робинсон (англ. *John Alan Robinson*; род. 1930 г.) — английский философ и логик.

Наиболее распространен язык логического программирования Пролог. Составляя программу на языке Пролог, программист тем самым создает прикладную теорию первого порядка — записывает собственные аксиомы теории и ничего больше. Причем эти аксиомы пишутся в таком виде, что программировать может даже человек, не знающий математической логики. Интерпретатор с языка Пролог содержит все остальные (логические) аксиомы и пытается доказать формулы, предлагаемые программистом.

Теорема 6. Если теория первого порядка противоречива, то в ней выводима любая формула.

Доказательство. В самом деле, пусть формулы A и $\neg A$ выводимы в теории. Формула $\neg A \supset (A \supset B)$ является тавтологией в исчислении высказываний, следовательно, она выводима. Её вывод, поскольку он содержит только *MP*, остается выводом и в любой теории первого порядка. Поэтому формула $\neg A \supset (A \supset B)$ выводима в теории первого порядка. Дважды применяя *MP*, мы получаем вывод произвольной формулы B.

Таким образом, для доказательства непротиворечивости какой-либо теории первого порядка достаточно установить недоказуемость в этой теории хотя бы одной формулы.

В теориях первого порядка импликация очень тесно связана с выводимостью.

Теорема 7 (о дедукции). Если $\Gamma \cup A \vdash B$, то $\Gamma \vdash A \supset B$.

Доказательство см., например, в [11, с. 70].

Теорема 8. Пусть T — теория первого порядка и логические аксиомы $\boldsymbol{A}_1$–$\boldsymbol{A}_5$ теории являются подмножеством множества формул S. Тогда если $S \vdash P$, то либо S — противоречиво, либо P общезначима.

Доказательство см., например, в [11, с. 64].

Теорема 8 говорит о корректности исчисления предикатов: для любой формулы P из $\vdash P$ следует $\vDash P$.

Теорема 9 (Гёделя о полноте). Пусть T — теория первого порядка и логические аксиомы теории являются подмножеством множества формул. Тогда:

а) формула P выводима из S в том и только том случае, когда либо S — противоречиво, либо P общезначима;

б) формула P независима от S в том и только том случае, когда $S \cup \{P\}$ и $S \cup \{\neg P\}$ непротиворечивы.

Доказательство см., например, в [12, с. 64–69; 11, с. 84–86].

Следствие. Если теория первого порядка непротиворечива, то она полна. В частности, исчисление предикатов — полная теория.

Другими словами, в исчислении предикатов доказуемы все общезначимые формулы и только они.

Теорема 10. Замкнутая формула A является логическим следствием замкнутого множества замкнутых формул Γ тогда и только тогда, когда $\Gamma \vdash A$.

Доказательство см., например, в [11, с. 87].

Аксиоматические теории можно различать в зависимости от того, какая система, семантическая или дедуктивная, лежит в основе определения теории.

Множество замкнутых формул, которые логически следуют из данного множества аксиом, называется ***неформальной аксиоматической теорией***.

Множество замкнутых формул, которые доказуемы в теории первого порядка из данного множества аксиом, называется ***формальной аксиоматической теорией***.

Переформулируем теорему 10 в новых терминах: неформальная аксиоматическая теория с аксиомами Γ совпадает с формальной аксиоматической теорией с аксиомами Γ.

Полнота исчисления предикатов никак не облегчает жизнь в отношении разрешимости.

Теорема 11 (Чёрч)[1]. Исчисление предикатов неразрешимо.

Доказательство см. в [13, с. 297–300].

6.6 Аксиоматика Пеано

Теория элементарной арифметики ***EA*** явилась началом использования в математике формальных аксиоматических теорий первого порядка. Язык элементарной арифметики — язык первого порядка — имеет сигнатуру, состоящую из одной константы **0**, одноместного функционального символа S и двух двуместных функциональных символов + и ×. Стандартная интерпретация этого языка имеет своим

[1] Алонзо Чёрч (1903–1995 гг.) — выдающийся американский математик и логик, внесший значительный вклад в основы информатики.

носителем множество натуральных чисел $\mathbf{N}$, константу $\mathbf{0}$, функциональные символы интерпретируются как сложение и умножение, а $S(x)$ обозначает $x+1$.

Собственные аксиомы ***EA*** суть формулы следующих видов.

$\boldsymbol{P}_1$. $\Big(P(\mathbf{0}) \;\&\; \forall x\big(P(x) \supset P\big(S(x)\big)\big)\Big) \supset \forall z P(z)$

(принцип математической индукции, P — произвольная формула),

$\boldsymbol{P}_2$. $S(t_1) = S(t_2) \supset t_1 = t_2$,

$\boldsymbol{P}_3$. $\neg(S(t) = \mathbf{0})$,

$\boldsymbol{P}_4$. $t + \mathbf{0} = t$,

$\boldsymbol{P}_5$. $t_1 + S(t_2) = S(t_1 + t_2)$,

$\boldsymbol{P}_6$. $\mathbf{0} \times t = \mathbf{0}$,

$\boldsymbol{P}_7$. $S(t_1) \times t_2 = t_1 \times t_2 + t_2$.

Аксиомы $\boldsymbol{P}_2$ и $\boldsymbol{P}_3$ обеспечивают существование нуля и операции «непосредственно следующий». Аксиомы $\boldsymbol{P}_4$–$\boldsymbol{P}_7$ представляют собой рекурсивные равенства, служащие определениями операций сложения и умножения.

С помощью правила *MP* из схемы аксиом $\boldsymbol{P}_1$ мы можем получить следующее правило индукции: из $P(\mathbf{0})$ и $\forall x\big(P(x) \supset P\big(S(x)\big)\big)$ выводится $\forall x P(x)$.

Аксиомы $\boldsymbol{P}_1$–$\boldsymbol{P}_3$ ввел Пеано[1] (1891 г.) для аксиоматизации натурального ряда.

Среди логических аксиом для теории первого порядка (параграф 6.4) присутствует аксиома:

$\boldsymbol{A}_4$. $\forall x A(x) \supset A(t)$, где $A(t)$ есть формула теории $\boldsymbol{T}$ и t есть терм теории $\boldsymbol{T}$, свободный для x в $A(x)$.

Сейчас удобно на примере системы ***EA*** пояснить, почему необходима аксиома $\boldsymbol{A}_4$ для определения теории первого порядка, — она предотвращает коллизию переменных.

Рассмотрим теорию ***EA***. Пусть $A(x)$ есть формула $\exists b(b = x+1)$. Тогда $\forall x A(x)$, обозначающая формулу $\forall x \exists b(b = x+1)$, — истинная формула при стандартной интерпретации ***EA***. Возьмем терм $t \equiv b$, тогда для терма t имеем формулу $\forall x \exists b(b = x+1) \supset \exists b(b = b+1)$. Формула $\exists b(b = b+1)$ ложна при стандартной интерпретации ***EA***, следовательно, формула $\forall x A(x) \supset A(t)$ ложна.

Основным средством вывода теорем в теории ***EA*** является, как и следовало ожидать, схема индукции. Рассмотрим в качестве примера вывод формулы $\mathbf{0} + x = x$ (она отличается от аксиомы $x + \mathbf{0} = x$). Обозначим $\mathbf{0} + x = x$ через $A(x)$. Сначала мы должны доказать $A(\mathbf{0})$, т. е. $\mathbf{0} + \mathbf{0} = \mathbf{0}$, но это частный случай упомянутой аксиомы. Теперь можем доказать $A(x) \supset A\big(S(x)\big)$. Предполагая воспользоваться теоремой дедукции, возьмем $A(x)$ в качестве гипотезы:

- $A(x)$ или $\mathbf{0} + x = x$ (гипотеза);
- $\mathbf{0} + S(x) = S(\mathbf{0} + x)$ (частный случай аксиомы);
- $\mathbf{0} + x = x \supset S(\mathbf{0} + x) = S(x)$ (свойство равенства);
- $S(\mathbf{0} + x) = S(x)$ (modus ponens);
- $\mathbf{0} + S(x) = S(x)$ или $A\big(S(x)\big)$ (транзитивность равенства).

[1] Джузеппе Пеано (1858–1932 гг.) — итальянский математик. Внёс вклад в математическую логику, аксиоматику, философию математики.

По теореме 7 (о дедукции) отсюда следует $\vdash A(x) \supset A\big(S(x)\big)$, а затем $\vdash \forall x\Big(A(x) \supset \supset A\big(S(x)\big)\Big)$. Так как $A(\mathbf{0})$ уже доказано, то по схеме индукции получаем $\vdash \forall x A(x)$ или $\vdash \mathbf{0} + x = x$.

Аналогично доказываются другие простые теоремы ***EA***. Следует помнить, однако, что перед тем как доказывать какую-либо теорему (например, коммутативность умножения: $x \times y = y \times x$), полезно уже знать некоторые теоремы. Таким образом, даже доказательство простых теорем ***EA*** содержит в себе творческий момент — он состоит в наиболее рациональном выборе порядка, в котором эти теоремы следует доказывать.

Следующее утверждение является эмпирически установленным фактом: все рассуждения обычной (интуитивной) теории чисел, которые не апеллируют к произвольным действительным числам и функциям, могут быть формально воспроизведены в ***EA***.

Язык теории ***EA*** (как и любой язык теории первого порядка) можно расширить, введя новые функциональные символы и константы, которые «доказуемо выразимы» в языке. Это просто формальный вариант «введения новых обозначений». Их добавление к алфавиту сокращает формульные выводы и записи формул, но не увеличивает множество выводимых формул.

> У логики один недостаток: она не останавливается на полпути.
>
> *Д. Уиндем. День триффидов*

6.7 Аксиоматика Цермело—Френкеля

Язык первого порядка Цермело—Френкеля предназначен для описания теории множеств. Сигнатура языка содержит единственную константу $\varnothing$ (имя пустого множества при интерпретации) и два предикатных символа: = (равенство) и символ принадлежности $\in$.

Аксиоматика Цермело—Френкеля обычно называется системой ***ZF*** или ***ZFC***, где ***C*** подчеркивает присутствие в системе аксиомы выбора. Прежде чем начать описывать аксиомы, сразу укажем, что является стандартной интерпретацией языка. В качестве носителя интерпретации определяется универсум фон Неймана. Это более ограниченный класс множеств, чем канторовский универсум. Часть ограничений вызвана желанием избежать парадоксов наивной теории множеств, другая часть определяется желанием, чтобы рассматриваемый класс множеств был замкнут относительно всех математических конструкций, необходимых для реализации как возможно большей части содержательной математики.

В универсуме фон Неймана $\boldsymbol{V}$ элементами множеств могут быть только множества. Любое множество строится из пустого множества — «из ничего». Не всякая совокупность множеств является множеством, в частности, совокупность всех множеств универсума $\boldsymbol{V}$ множеством не является. Поэтому точно формулируются те операции, которые не выводят за пределы $\boldsymbol{V}$. Символы переменных языка являются только именами множеств. Полное описание универсума $\boldsymbol{V}$ [12, с. 100–108] требует знаний, не входящих в курс элементарной логики, и поэтому мы остановимся только на примерах.

Универсум строится индуктивно, начиная с пустого множества последовательным применением операции $\boldsymbol{P}$: «множество всех подмножеств». Таким образом, первые множества следующие:

- $V_0 = \varnothing$,
- $V_1 = \boldsymbol{P}(V_0) = \{\varnothing\}$,
- $V_2 = \boldsymbol{P}(V_1) = \{\varnothing, \{\varnothing\}\}$,
- ...
- $V_{n+1} = \boldsymbol{P}(V_n)$,
- ...

Имеем $V_n \subset V_{n+1}$. Множество V_n состоит из $2^{2^{\cdot^{\cdot^{2}}}}$ ($n-1$ двоек) конечных множеств, элементами которых, в свою очередь, являются конечные множители, и т. д. Выйти за пределы конечных множеств нельзя, если не обратиться к рассмотрению всех V_n как «уже построенных», к объединению которых снова применяется операция $\boldsymbol{P}$.

Перечислим аксиомы ***ZFC***, которые являются истинными в стандартной интерпретации с носителем $\boldsymbol{V}$.

1. *Аксиома пустого множества*

$$\forall x \neg (x \in \varnothing).$$

2. *Аксиома пары*

$$\forall x, y\ \exists X \forall z (z \in X \sim z = x \vee z = y).$$

3. *Аксиома объединения множества множеств*

$$\forall X \exists Y \forall y \big(y \in Y \sim \exists x (x \in X\ \&\ y \in x)\big).$$

Множество Y обозначается просто $\cup X$.

4. *Аксиома множества всех подмножеств*

$$\forall X \exists Y \forall Z \big(Z \in Y \sim \forall x (x \in Z \supset x \in X)\big).$$

Множество Y есть множество всех подмножеств множества X.

5. *Аксиома объемности*

$$\forall X,\ Y \big(\forall z (z \in X \sim x \in Y) \supset X = Y\big).$$

Если множества имеют одни и те же элементы, то они равны.

6. *Аксиома регулярности*

$$\forall X \exists x \big(x \in X\ \&\ \neg \exists y (y \in x\ \&\ y \in X)\big).$$

Суть ее в том, чтобы запретить ситуации вида $x \in x$.

7. *Аксиома бесконечности*

В этой и следующей аксиомах мы для ясности формулировок свободно пользуемся переменными для функций, поскольку уже знаем, как определять функции через множества.

$$\exists X \exists f \left(\begin{array}{l} f\colon X \to X \ \& \\ \forall x, y\big(x \in X \ \& \ y \in X \in f(x) = f(y) \supset x = y\big) \ \& \\ \exists y\Big(y \in X \ \& \ \forall x\big(x \in X \supset f(x) \neq y\big)\Big) \end{array} \right).$$

Аксиома утверждает, что существует бесконечное множество. Для этого используется свойство, выполняемое только для бесконечных множеств: существует биекция множества на его собственное подмножество.

8. *Аксиома подстановки*

Пусть $A(x, y)$ — произвольная формула языка Цермело—Френкеля, X — множество и $\forall x\big(x \in X \supset \exists 1 y A(x, y)\big)$, то $\big\{y \mid \exists x\big(x \in X \ \& \ A(x, y)\big)\big\}$ также множество.

Подформула $\exists 1 y A(x, y)$ является сокращенной записью формулы, которая утверждает, что существует только одно значение y, для которого выполнено $A(x, y)$.

9. *Аксиома выбора* ***AC***

$$\forall X \left(\begin{array}{l} \forall Y\big(Y \in X \supset \exists y(y \in Y)\big) \supset \\ \exists f(f\colon X \to \cup X) \ \& \ \forall Y\big(Y \in X \supset f(Y) \in Y\big) \end{array} \right).$$

Аксиома утверждает, что для каждого множества X существует функция выбора на X, т. е. функция f, сопоставляющая всякому подмножеству $Y \in X$ элемент $f(Y) \in Y$.

Использование аксиомы выбора в математике происходит повсеместно и, как правило, неосознанно. Каждый раз как только что-либо допускается по поводу бесконечных множеств, в замаскированной глубине обычно возникает аксиома выбора, без которой «все рассыпается». Рассмотрим доказательство утверждения (глава 3, теорема 12.3).

Объединение счётного числа счётных множеств счётно.

Доказательство. Пусть имеется счётное число счётных множеств $A_1, A_2, \ldots$ Расположив элементы каждого из них слева направо в последовательность $\big(A_i = \{a_{i_0}, a_{i_1}, \ldots\}\big)$ и поместив эти последовательности друг под другом, получим таблицу

$$\begin{array}{ccccc} a_{00} & a_{01} & a_{02} & a_{03} & \ldots \\ a_{10} & a_{11} & a_{12} & a_{13} & \ldots \\ a_{20} & a_{21} & a_{22} & a_{23} & \ldots \\ a_{30} & a_{31} & a_{32} & a_{33} & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

Теперь эту таблицу можно развернуть в последовательность, например проходя по очереди диагонали:

$$a_{00}, a_{01}, a_{10}, a_{02}, a_{11}, a_{20}, a_{03}, a_{12}, a_{21}, a_{30}, \ldots$$

Если множества A_i не пересекались, то мы получили искомое представление для их объединения. Если пересекались, то из построенной последовательности надо выбросить повторения.

По первому впечатлению доказательство дает нужный результат без каких бы то ни было предположений. Но без аксиомы выбора не удается фиксировать таблицу, потому что из множества возможных нумераций каждой последовательности[1] A_i требуется выбрать каждый раз конкретную нумерацию, что нельзя сделать без аксиомы ***AC***.

Можно надеяться выйти из положения окольным путем. Но, оказывается, никакая другая схема доказательства не работает, хотя это устанавливается уже не так просто [14, с. 64].

Исключение ***AC*** изымает из математического арсенала массу удобных и привычных инструментов. Например, эквивалентность (ε, δ)-определения непрерывности определению с помощью сходимости последовательностей.

Невинная с виду аксиома выбора знаменита «невероятными» следствиями[2].

Теорема 12 (Банаха–Тарского). Шар $B \subset \mathbf{R}^3$ допускает разбиение на конечное число непересекающихся множеств $B_1, B_2, \ldots, B_k$, из которых можно составить передвижением B_j, как твердых тел (перенос плюс поворот), либо два шара того же радиуса, либо шар удвоенного радиуса.

Хотя утверждение теоремы 12 называют также парадоксом Банаха–Тарского, но это не парадокс. Подробное и элементарное доказательство можно посмотреть в книге [15]. Хотя теорема выглядит шокирующее, но она не противоречит возможности измерять объемы тел. Представляется «естественным», что всякое (по крайней мере ограниченное) подмножество пространства имеет объем. Но из теоремы следует, что это не так.

Курт Гёдель доказал (1940 г.), что аксиома выбора не противоречит системе аксиом ***ZF***. Точнее, если ***ZF*** непротиворечива, то и ***ZFC*** непротиворечива. Пол Коэн[3] в свою очередь доказал (1963 г.), что если ***ZF*** непротиворечива, то и ***ZF*** плюс отрицание ***AC*** также непротиворечива.

В теорию множеств ***ZF*** можно добавлять и другие аксиомы, лишь бы они не противоречили с существующими. В связи с этим рассмотрим сейчас гипотезу континуума. Доказав, что мощность отрезка [0, 1] превосходит мощность множества натуральных чисел **N** (параграф 3.6 главы 3), естественно задаться вопросом: существует ли множество, промежуточное по мощности? Для ответа можно пытаться найти подмножество из [0, 1] промежуточной мощности. Широкую известность получило канторово множество C, получаемое последовательным выбрасыванием третей из [0, 1]. Сначала отрезок [0, 1] делится на три равных части и средняя часть (интервал) удаляется. С каждой из оставшихся частей повторяется аналогичная операция — и так до бесконечности. В пределе от [0, 1] почти ничего не остается, что и называется ***канторовым множеством*** C. Длина выброшенных третей равна

[1] Наличие таких нумераций гарантирует счетность последовательности.

[2] Бертран Рассел так отозвался об аксиоме выбора: «Сначала она кажется очевидной; но чем больше вдумываешься, тем более странными кажутся выводы из этой аксиомы; под конец же вообще перестаешь понимать, что же она означает».

[3] Пол Джозеф Коэн (1934–2007 гг.) — американский математик.

$$\frac{1}{3}\cdot\left(1+\frac{2}{3}+\left(\frac{2}{3}\right)^2+\ldots\right)=1,$$

т. е. «вся длина» выбрасывается, но тем не менее C оказывается равномощно континууму.

Рис. 6.6 – Множество Кантора

В результате многих безуспешных попыток Кантор пришел к убеждению справедливости следующего утверждения.

Гипотеза континуума (ГК)

Не существует множества, промежуточного по мощности между **N** и [0, 1], т. е. вслед за счетным множеством сразу идет континуум.

Эту гипотезу не могли доказать в течение сотни лет. В итоге оказалось, что гипотезу с равным успехом можно принять или отвергнуть как аксиому. Гёдель доказал (1940 г.), что если теория ***ZF*** непротиворечива, то ***ГК*** не противоречит аксиоматике ***ZF*** и поэтому её можно добавить как аксиому. И снова Коэн доказал (1963 г.), что если теория ***ZF*** непротиворечива, то ***ГК*** не является теоремой ***ZF***, т. е. к ***ZF*** можно добавить отрицание гипотезы континуума.

Получается, что мы обладаем, по крайней мере, четырьмя различными теориями множеств (с гипотезой континуума или без неё, с аксиомой выбора или без нее) и все они в одинаковой степени непротиворечивы.

А как же дело обстоит с непротиворечивостью аксиоматике ***ZF***? Неизвестно, и мы можем только догадываться. Российский математик Ю. И. Манин замечает: «Вопрос о формальной непротиворечивости аксиом Цермело—Френкеля должен оставаться предметом веры, пока и поскольку не продемонстрирована их противоречивость. Все те доказательства, которые были основаны на них, до настоящего момента не привели к противоречию, но развернули перед нами богатый мир классической и современной математики. Этот мир обладает некоторой реальностью и внутренней жизнью, мало зависящими от формализмов, призванных его описывать.

Обнаружение противоречия в любом из этих формализмов, буде оно и произойдет, послужит лишь прояснению, уточнению и, возможно, перестройке наших представлений, но не их крушению, как это многократно случалось в прошлом» [12].

Немаловажно отметить, что арифметика может быть погружена в систему ***ZFC***. В результате арифметические аксиомы Пеано становятся теоремами ***ZFC***, в том числе и математическая индукция, — ибо аксиома $\boldsymbol{P}_1$ (параграф 6.6 главы 6) является частным случаем трансфинитной индукции, каковая в ***ZFC*** не постулируется, а доказывается [14, с. 66–67].

Подведя итог рассмотрению аксиоматизации геометрии и теории множеств, мы видим, что у математиков есть выбор, считать ли следующие утверждения ак-

сиомами или к таковым отнести их отрицания: аксиома о параллельных, аксиома выбора и гипотеза континуума. Тем самым правомочно утверждать о существовании различных математических реальностей.

Контрольные вопросы по главе 6

1. Для чего формальный язык наделяется семантической и дедуктивной системами?
2. Что такое модель аксиоматической теории?
3. В каком случае аксиоматическая теория называется полной относительно данной интерпретации?
4. В каком случае аксиоматическая теория называется разрешимой?
5. Почему формальная система, имеющая только удлиняющие правила (параграф 6.2 главы 6), имеет разрешающий алгоритм.

Рекомендуемая литература к главе 6

[1] Подниекс К. М. Вокруг теоремы Гёделя / К. М. Подниекс. — Рига, 1981.

[2] Успенский В. А. Апология математики / В. А. Успенский. — СПб. ; Амфора, 2009. — 554 с.

[3] Хофштадтер Д. Гёдель, Эшер, Бах: эта бесконечная гирлянда / Д. Хофштадтер. — Самара : Изд. дом «Бахрах-М», 2001. — 752 с.

[4] Мендельсон Э. Введение в математическую логику / Э. Мендельсон. — М. : Наука, 1976. — 320 с.

[5] Успенский В. А. Что такое аксиоматический метод? / В. А. Успенский. — Ижевск : НИЦ Регулярная и хаотическая динамика, 2001 — 96 с.

[6] История математики : в 3 т. / под ред. А. П. Юшкевича. — М. : Наука, 1972. — Т. III. — С. 215–217.

[7] Гильберт Д. Основания геометрии : пер. с нем. / Д. Гильберт ; под ред. А. В. Васильева. — Л. : Сеятель, 1923. — 152 с.

[8] Братко И. Алгоритмы искусственного интеллекта на языке PROLOG : пер. с англ. / И. Братко. — 3-е изд. — М. : Вильямс, 2004. — 640 с.

[9] Логический подход к искусственному интеллекту: От классической логики к логическому программированию : пер. с франц. / А. П. Тейз [и др.]. — М. : Мир, 1990. — 432 с.

[10] Robinson J. A. A machine-oriented logic based on resolution principle // Journal of the ACM. — 1965. — N 12 — P. 23–41.

[11] Успенский В. А. Вводный курс математической логики / В. А. Успенский, Н. К. Верещагин, В. Е. Плиско. — М. : ФИЗМАТЛИТ, 2004. — 128 с.

[12] Манин Ю. И. Доказуемое и недоказуемое / Ю. И. Манин. — М. : Мир ; Советское радио, 1979. — 168 с.

[13] Клини С. К. Математическая логика / С. К. Клини. — 2-е изд. — М. : Едиториал УРСС, 2005. — 480 с.

[14] Босс В. Лекции по математике : учеб. пособие / В. Босс. — М. : Книжный дом «Либроком», 2011. — Т. 16 : Теория множеств: От Кантора до Коэна. — 208 с.

[15] Губа В. С. «Парадокс» Банаха—Тарского / В. С. Губа, С. М. Львовский. — М. : МЦНМО, 2012. — 48 с.

Глава 7

МАТЕМАТИЧЕСКОЕ ДОКАЗАТЕЛЬСТВО

> Со времен греков говорить «математика» — значит говорить «доказательство».
>
> *Николя Бурбаки. Теория множеств*

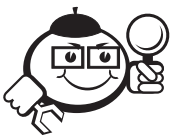
> Хорошее доказательство — это рассуждение, которое делает нас умнее.
>
> *Ю. И. Манин. Доказуемое и недоказуемое*

В этой главе доказательство в математике исследуется с разных сторон. Уточняются данные ранее определения различных видов математических доказательств. Рассматриваются и другие методы доказательств.

7.1 Индукция

В математическом творчестве основные части: это догадка и доказательство. Догадка может быть направлена на получение гипотезы — предположения, истинность которого мы ожидаем. В этом случае, получив гипотезу, мы нуждаемся в ее доказательстве. Но нам необходимо также догадаться, как провести безупречное доказательство. Также решение серьезной математической задачи во многих случаях требует математического открытия (хотя бы для того, кто решает задачу). И в этом случае часто мы должны догадаться. В первой главе мы упомянули о двух видах логических рассуждений: индукции и дедукции. Рассмотрим подробно индукцию.

Индуктивное рассуждение — процесс получения общего утверждения на основе изучения частных примеров. Когда мы рассматриваем конечную последовательность чисел и предсказываем, каким будет следующее число, мы обнаруживаем некоторый образец, шаблон, которому удовлетворяют известные члены последовательности. Это типичная индукция.



Пример 7.1

Используйте индуктивное рассуждение, чтобы предсказать наиболее вероятное следующее число в последовательностях:

a. 3, 6, 9, 12, 15, ?

b. 1, 3, 6,10, 15, ?

Решение:

a. Каждое последующее число на 3 больше чем предыдущее, поэтому мы предсказываем, что после 15 должно следовать 18.

b. Первые два числа отличаются на 2. Разность между третьим и вторым равна 3. Рассмотрение следующих разностей приводит нас к мысли, что разности между соседними членами последовательно возрастают на 1. Поэтому логично предположить, что следующее число за 15 будет 21.

Пример 7.2

Используйте индуктивное рассуждение, чтобы предсказать наиболее вероятное следующее число в последовательности a_n:

2, 7, 24, 59, 118, 207, ?

Решение:

Ниже строки чисел данной последовательности выпишем разности соседних чисел:

2 7 24 59 118 207

5 17 35 59 89

Полученную последовательность обычно называют последовательностью *первых разностей* последовательности a_n. Но для первых разностей мы можем найти «свои» разности — вторые разности для последовательности a_n:

5 17 35 59 89

12 18 24 30

Теперь находим третьи разности для последовательности a_n:

12 18 24 30

6 6 6

Это позволяет определить очередную вторую разность 30 + 6 = 36, потом — очередную первую разность 89 + 36 = 125 и, наконец, 207 + 125 = 332 — очередной член последовательности a_n.

Примеры 7.1 и 7.2 являются учебными, так как, очевидно, любая конечная последовательность имеет бесконечное множество продолжений. В примерах речь идет о естественных, очевидных продолжениях. В математических задачах индукция возникает, когда имеется несколько частных случаев, для которых мы устано-

вили частные утверждения о каком-то математическом объекте, и нам хотелось бы получить общий закон. Очевидно, наш выбор догадок ограничен, так как математики проверяют свои гипотезы.

Пример 7.3

Многоугольные числа, по мнению пифагорейцев, играют важную роль в структуре мироздания. Поэтому их изучением занимались многие математики античности. Большой интерес к фигурным числам проявили индийские математики и первые математики средневековой Европы. В Новое время многоугольными числами занимались Ферма, Эйлер, Лангранж, Гаусс и другие. В классической интерпретации многоугольными числами мы называем числа, которые можно изобразить на плоскости в виде правильного многоугольника с помощью точек или шаров одинакового размера (рис. 7.1).

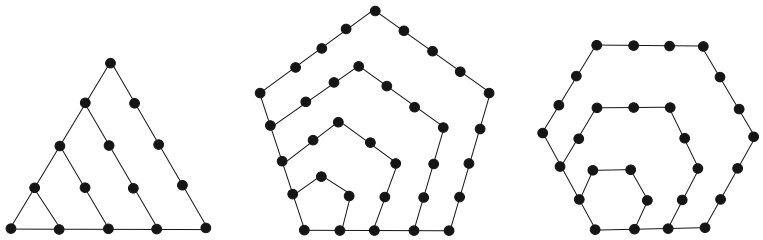


Рис. 7.1 – Треугольное, пятиугольное и шестиугольное числа

Наглядность многоугольных чисел способствовала с помощью индукции предсказывать многие утверждения. Ферма сформулировал в 1654 г. «золотую» теорему: любое натуральное число представимо в виде суммы n n-угольных чисел. Гипотезу Ферма доказал Коши только в 1815 году [1, с. 62–65].

Треугольное число — это число кружков, которые могут быть расставлены в форме правильного треугольника. На рисунке 7.2 изображены первые пять треугольных числа S_n, $n = 1, 2, 3, 4, 5$.

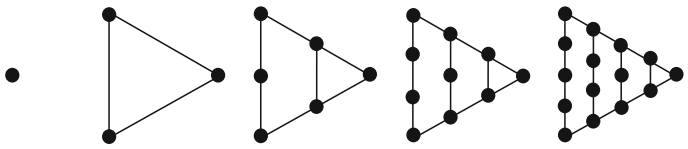
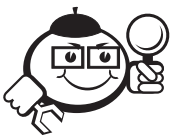


Рис. 7.2 – $S_1 = 1$, $S_2 = 3$, $S_3 = 6$, $S_4 = 10$, $S_5 = 15$

Очевидно, с чисто арифметической точки зрения, n-е треугольное число — это сумма n первых натуральных чисел. Поэтому получаем

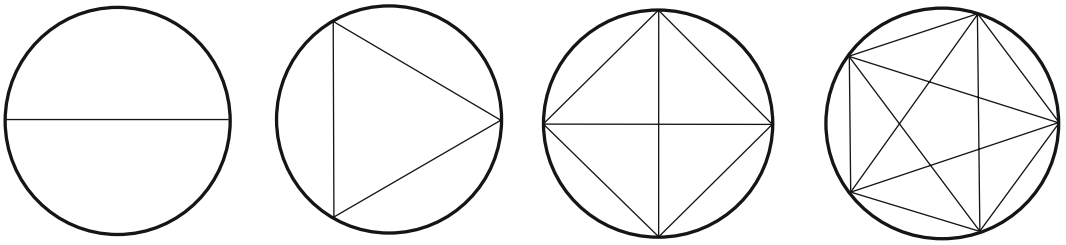
$$S_n = \frac{n \cdot (n+1)}{2}.$$

Заключение, основанное на индуктивном рассуждении, может быть некорректно.



Пример 7.4

Известна задача [30, с. 50] об определении числа R_n областей, образуемых $n(n-1)/2$ хордами, которые соединяют n фиксированных точек на окружности, при предположении, что никакие три хорды не пересекаются внутри круга (рис. 7.3).



$R_2 = 2$ $R_3 = 4$ $R_4 = 8$ $R_5 = 16$

Рис. 7.3 – Хорды в круге

Результат при n = 2, 3, 4, 5 наводит на мысль, что $R_n = 2^{n-1}$, но R_6 = 31 (рис. 7.4).

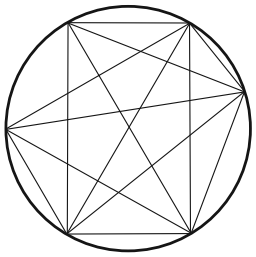


Рис. 7.4 – Контрпример: R_6 = 31

Частный случай, показывающий ложность утверждения, истинность которого предполагалась в общем случае, называется ***контрпримером*** (общего утверждения). Наличие контрпримера опровергает доказываемое утверждение и заставляет выдвинуть новое предположение. На самом деле правильной формулой будет

$$R_n = 1 + \frac{n \cdot (n-1)}{2} + \frac{n \cdot (n-1)(n-2)(n-3)}{24}. \qquad (7.1)$$

Парадокс Гемпеля[1]

В науке широко используется *принцип индукции*, который утверждает, что: «Наблюдение явления X, которое соответствует теории T, дополнительно подтверждает теорию T».

Предположим, биолог ищет доказательства своей гипотезы «Все во́роны — черные». Но для этого ему нет необходимости отправляться в экспедиции. Ибо в силу закона контрапозиции $A \supset B \equiv \neg B \supset \neg A$, дополнительным свидетельством гипотезы

[1] Карл Густав Гемпель (1905–1997 гг.) — немецкий и американский философ.

является всякий нечерный предмет, найденный биологом дома (конечно, если он не окажется вороном).

Логика бессильна формализовать индукцию (но, см. [2], том 2), тем не менее она совершенно не препятствует использованию индукции в науке и в жизни: мы пользуемся ею чаще, чем всеми принципами формальной логики, вместе взятыми.

Логика очень важна в математике, однако она не настолько тесно связана с открытиями и изобретениями, как может показаться. Логика не указывает путь и не подсказывает, как найти решение. Этот путь открывают эксперимент, аналогия и интуиция, а затем логика превращает эти нехоженые тропинки в широкую магистраль, по которой может проехать любой.

7.2 Математическая индукция

Рис. 7.5 – Дьердь Пойа

Математическая индукция является приемом доказательства, часто полезным для подтверждения математических предположений, к которому мы пришли с помощью некоторого процесса индукции.

В книге [2] Д. Пойа[1] (рис. 7.5) рассказывает, как с помощи индукции можно найти формулу для суммы n первых квадратов

$$1 + 4 + 9 + 16 + \ldots + n^2.$$

Он сравнивает эту сумму с суммой первых n натуральных чисел с известной формулой

$$1 + 2 + 2 + \ldots + n = \left[n \cdot (n+1)\right] \Big/ 2.$$

Он говорит о том, что естественно попытаться обнаружить какого-то рода параллелизм между этими двумя суммами и рассмотреть их совместно:

n	1	2	3	4	5	6	…
$1 + 2 + 3 + \ldots + n$	1	3	6	10	15	21	…
$1 + 4 + 9 + \ldots + n^2$	1	5	14	30	55	91	…

Далее он пишет:

«Как связаны две последние строки? Нам может прийти в голову идея исследовать их отношение:

n	1	2	3	4	5	6	…
$\dfrac{1^2 + 2^2 + \ldots + n^2}{1 + 2 + \ldots + n}$	1	$\dfrac{5}{3}$	$\dfrac{7}{3}$	3	$\dfrac{11}{3}$	$\dfrac{13}{3}$	…

[1] Дьёрдь Пойа (англ. *George Polya* — Джордж Полиа; 1887–1985 гг.) — венгерский и американский математик с мировым именем. Основные результаты — в теории чисел, функциональном анализе, математической статистике и комбинаторике. Знамениты его книги о том, как решать задачи и как надо учить решать задачи.

Здесь правило очевидно, и если отношение во второй строке записать следующим образом:

$$\frac{3}{3}\ \frac{5}{3}\ \frac{7}{3}\ \frac{9}{3}\ \frac{11}{3}\ \frac{13}{3},$$

его почти невозможно не заметить. Едва ли мы сможем удержаться и не сформулировать предположение, что

$$\frac{1^2 + 2^2 + \ldots + n^2}{1 + 2 + \ldots + n} = \frac{2n + 1}{3}.$$

Пользуясь значением знаменателя в левой части, которое мы считаем известным, можем высказать наше предположение в форме

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n \cdot (n + 1)(2n + 1)}{6}.$$

Верно ли это? То есть, всегда ли это верно?»

Далее Д. Пойя дополнительно проверяет эту формулу, в частности, получает неоспоримое следствие из предполагаемой формулы, что серьезно подтверждает его догадку. И наконец, приводит следующее доказательство.

«Предположительно верно, что

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n \cdot (n + 1)(2n + 1)}{6}.$$

Неоспоримо верно, что

$$(n + 1)^2 = \frac{(n + 1)(n + 2)(2n + 3)}{3} - \frac{n \cdot (n + 1)(2n + 1)}{6}.$$

Следовательно, верно, что

$$1^2 + 2^2 + 3^2 + \ldots + n^2 + (n + 1)^2 = \frac{(n + 1)(n + 2)(2n + 3)}{6}$$

(мы сложили два предыдущих равенства). Это означает: если наше предположение верно для некоторого целого числа n, то оно непременно остается верно для следующего целого числа $n + 1$.

Однако мы знаем, что предположение верно для $n = 1, 2, 3, 4, 5, 6, 7$. Будучи верным для 7, оно должно быть верным и для следующего числа 8; будучи верным для 8, оно должно быть верно и для 9; так как оно верно для 9, оно верно и для 10, а значит, и для 11 и т. д. Предположение верно для всех целых чисел, нам удалось доказать его в полной общности».

Далее Д. Пойа показывает, что предыдущее рассуждение может быть упрощено, если воспользоваться важным методом доказательства, называемым «*математическая индукция*». При этом бесконечное множество переходов от фиксированного натурального числа n к следующему числу $n + 1$ (признаком бесконечности служат слова «и т. д.») в доказательстве заменяется на одно общее рассуждение.

Приступим сейчас к рассмотрению разнообразных вариантов математической индукции. Современное развитие принципа математической индукции началось с аксиом Пеано для теории формальной арифметики ***EA***. Аксиома математической индукции (см. главу 6, параграф 6.6) в стандартной интерпретации ***EA*** выражается формулой:

$$\Big(P(0)\ \&\ \forall x\big(P(x) \supset P(x+1)\big)\Big) \supset \forall n P(n). \tag{7.2}$$

Из аксиомы (7.2) следует предложение 1.

Предложение 1 (Принцип математической индукции). Пусть $P(n)$ — свойство натуральных чисел, выразимых в теории ***EA***.

Если

(1) выполнено $P(0)$ и

(2) для каждого $k \geqslant 0$ из $P(k)$ следует $P(k+1)$,

то для каждого $n \geqslant 0$ справедливо $P(n)$.

Доказательство. Из истинности формул $P(0)$ и $\forall x\big(P(x) \supset P(x+1)\big)$ в силу аксиомы (7.2) следует $\forall n P(n)$.

В математической индукции имеется ***индуктивный базис*** — утверждение, что свойство выполнено для самого маленького из рассматриваемых чисел, и ***индуктивный шаг*** — обоснование перехода от числа n к числу $n+1$.

Пример 7.5

Приведем с помощью математической индукции доказательство справедливости формулы для суммы квадратов

$$1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n \cdot (n+1)(2n+1)}{6}. \tag{7.3}$$

Пусть $P(n)$ обозначает равенство (7.3). Очевидно, базис индукции выполнен, $0^2 = 0 \times 2 \times 3/6 = 0$. Докажем индуктивный переход от $P(n)$ к $P(n+1)$: добавим к обеим частям равенства (7.3) слагаемое $(n+1)^2$. Тогда слева будет сумма первых $n+1$ квадратов, а справа получаем

$$\frac{n \cdot (n+1)(2n+1)}{6} + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6},$$

что и требовалось доказать.

Задача 1. Пусть дана последовательность 1, 1, 2, 3, 5, 8,… чисел Фибоначчи $f(n)$ (см. главу 1, параграф 1.3). Докажите формулу Кассини

$$f(n+1) \cdot f(n-1) - f(n)^2 = (-1)^n$$

при $n > 1$.

Решение. Определим $P(n)$ как $f(n+1) \cdot f(n-1) - f(n)^2 = (-1)^n$ при $n > 1$.

Базис индукции выполняется для $n = 2$: $f(3) \cdot f(1) - f(2)^2 = (-1)^2$.

Шаг индукции. Пусть для $k \geqslant 2$ выполнено $P(k)\colon f(k+1)\cdot f(k-1)-f(k)^2 = (-1)^k$. Докажем $P(k+1)$. Имеем

$$f(k+2)\cdot f(k) = \big(f(k+1)+f(k)\big)\cdot f(k) = f(k+1)\cdot f(k)+f(k)^2 =$$
$$= f(k+1)\cdot f(k)+f(k+1)\cdot f(k-1)-(-1)^k \ \big(\text{в силу } P(k)\big) =$$
$$= f(k+1)\cdot\big(f(k)+f(k-1)\big)-(-1)^k = f(k+1)\cdot f(k+1)-(-1)^k = f(k+1)^2-(-1)^k.$$

Отсюда получаем $f(k+2)\cdot f(k) = f(k+1)^2+(-1)^{k+1}$, т. е. $f(k+2)\cdot f(k)-f(k+1)^2 = (-1)^{k+1}$. По принципу математической индукции имеем $f(n+1)\cdot f(n-1)-f(n)^2 = (-1)^n$ при $n > 1$.

Формула Кассини объясняет софизм с числами Фибоначчи, рассмотренный в главе 1, параграф 1.3.

Выполнение базиса индукции необходимо для индуктивного доказательства.

Пример 7.6

Пусть $P(n)$ есть

$$\sum_{i=0}^{n}(2i-1) = n^2+5.$$

Тогда $P(0)$ ложно, а из $P(n)$ следует $P(n+1)$. И $P(n)$ ложно для всех натуральных чисел.

Пример 7.7

Для любого натурального n число n^2+5n+1 — четное. И в этом случае верности одного индуктивного перехода недостаточно.

Базис в математической индукции может быть любым натуральным числом.

Предложение 2. Принцип математической индукции с базисом, большим 0. Пусть $P(n)$ — свойство натуральных чисел, выразимых в теории ***EA***.

Если

(1) для некоторого $k \geqslant 0$ выполнено $P(k)$ и

(2) для каждого $m \geqslant k$ из $P(m)$ следует $P(m+1)$,

то для каждого $n \geqslant k$ справедливо $P(n)$.

Доказательство. Положим $T(n) = P(n+k)$. Тогда имеем

(1a) выполнено $T(0)$ и

(2a) для каждого $m \geqslant 0$ из $T(m)$ следует $T(m+1)$, и предложение 1 дает для каждого $n \geqslant 0$ истинность $T(n)$, что влечет справедливость $P(n)$ для всех $n \geqslant k$.

Предложение 3. Принцип математической индукции эквивалентен существованию наименьшего элемента в любом непустом подмножестве **N**.

Доказательство.

1. Пусть в любом непустом подмножестве **N** существует минимальный элемент. Докажем выполнимость принципа математической индукции. Пусть $P(n)$ — некоторое свойство натуральных чисел, для которого

(1) выполнено $P(0)$ и

(2) для каждого $k \geqslant 0$ из $P(k)$ следует $P(k+1)$.

Будем рассуждать от противного: множество $B = \{n \mid \neg P(n)\}$ не пусто. Тогда существует наименьший элемент $m \in B$. Так как $P(0)$, по базису индукции, — истина, то $m > 0$. Следовательно, $m - 1 \in \mathbf{N}$ и $P(m-1)$, поэтому по индуктивному переходу выполнено P для m. Но это противоречит $m \in B$, следовательно, B пусто. И поэтому для всех $n \geqslant 0$ справедливо $P(n)$.

2. Пусть справедлив принцип математической индукции и B — непустое подмножество **N**. Докажем, что в B существует наименьший элемент. От противного: пусть в B нет наименьшего элемента. Определим предикат

$$P(n) - \text{«}\forall m(m \leqslant n \supset m \notin B)\text{»}.$$

Имеем $0 \notin B$, иначе 0 был бы наименьшим элементом в B. Поэтому выполнено $P(0)$ — базис индукции для $P(n)$. Покажем истинность индуктивного перехода. Пусть для k выполнено $P(k)$, т. е. для всех $m \leqslant k$ имеем $m \notin B$, в частности $k \notin B$. Отсюда следует, что $k+1 \notin B$, иначе $k+1$ был бы наименьшим элементом в B. Поскольку для всех $m \leqslant k+1$ выполнено $m \notin B$, то $P(k+1)$ — истина. Тем самым мы доказали верность индуктивного перехода и, по принципу математической индукции, получили, что для всех $n \geqslant 0$ справедливо $P(n)$. Последнее означает, что $B = \varnothing$. Полученное противоречие говорит о том, что B имеет наименьший элемент.

Возвратная индукция — один из вариантов математической индукции. Здесь индуктивный переход происходит не от одного значения к следующему, а от всех предыдущих значений к последующему; шаг индукции переводит не от $P(x)$ к $P(x+1)$, а от $P(y)$ для всех $y < x$ к $P(x)$. При таком переходе не требуется базиса индукции. В самом деле, поскольку условие $x < 0$ тождественно ложно, то, поскольку из лжи следует все, что угодно, имеем

$$\forall x\big(x < 0 \supset P(x)\big),$$

а отсюда по индуктивному переходу имеем $P(0)$.

Предложение 4. Возвратная индукция. Пусть $P(n)$ — свойство натуральных чисел, выразимых в теории ***EA***.

Если для всех x утверждение $\forall y\big(y < x \supset P(y)\big)$ влечет $P(x)$, то для каждого $n \geqslant 0$ справедливо $P(n)$.

Еще одна переформулировка метода математической индукции.

Предложение 5. Принцип бесконечного спуска. Пусть $P(n)$ — свойство натуральных чисел, выразимых в теории ***EA***.

Если для каждого натурального числа, удовлетворяющего свойству $P(n)$, найдется меньшее, удовлетворяющее этому же свойству, то чисел n, для которых выполнено $P(n)$, вообще нет.

Формально:

$$\forall n\Big(P(n) \supset \exists m\big(m < n \;\&\; P(m)\big)\Big) \supset \forall n \neg P(n).$$

Теорема 1. Следующие пять свойств множества **N** натуральных чисел эквивалентны:

(a) принцип математической индукции (предложение 1);
(b) любое непустое подмножество **N** имеет наименьший элемент;
(c) всякая строго убывающая последовательность натуральных чисел конечна;
(d) возвратная индукция (предложение 4);
(e) принцип бесконечного спуска (предложение 5).

Доказательство.

$(a) \Leftrightarrow (b)$: эквивалентность (a) и (b) доказана в предложении 3.

$(b) \Leftrightarrow (c)$: если $x_0 > x_1 > x_2 > \ldots$ — бесконечная убывающая последовательность, то, очевидно, множество ее значений не имеет наименьшего элемента (для каждого элемента следующий еще меньше). Поэтому из (b) следует (c). Напротив, если B — непустое множество, не имеющее наименьшего элемента, то бесконечную убывающую последовательность можно построить так. Возьмем произвольный элемент $b_0 \in B$. По предположению, он не является наименьшим, так что можно найти $b_1 \in B$, для которого $b_0 > b_1$. По тем же причинам можно найти $b_2 \in B$, для которого $b_1 > b_2$, и т. д. Получается бесконечная убывающая последовательность.

$(b) \Leftrightarrow (d)$: выведем метод возвратной индукции из существования наименьшего элемента в любом подмножестве. Пусть $P(n)$ — свойство натуральных чисел, для которого справедливо утверждение индуктивного перехода

«для всех x утверждение $\forall y\big(y < x \supset P(y)\big)$ влечет $P(x)$». (7.4)

Рассуждаем от противного: пусть $P(n)$ справедливо не для всех n. Рассмотрим непустое множество B тех элементов, для которых свойство P неверно. Пусть x — наименьший элемент множества B. По условию меньших элементов во множестве B нет, поэтому для всех $y < x$ свойство $P(y)$ выполнено. Но тогда в силу (7.4) должно быть выполнено и $P(x)$, что противоречит $x \in B$. Следовательно, $P(n)$ справедливо для всех n.

Докажем существование наименьшего элемента в любом непустом множестве с помощью возвратной индукции. Пусть B — множество, в котором нет наименьшего элемента. Докажем по индукции, что B пусто; для этого в качестве $P(x)$ возьмем свойство $x \notin B$. В самом деле, если $P(y)$ верно для всех $y < x$, то никакой элемент, меньший x, не лежит в B. Значит, если бы x лежал в B, то он бы был там минимальным, а таких нет. Полученное противоречие доказывает существование минимального элемента в любом непустом множестве.

$(c) \Leftrightarrow (e)$: если бы некоторая убывающая последовательность натуральных чисел была бы бесконечна, то это противоречило бы принципу бесконечного спуска. Теперь выведем принцип бесконечного спуска из конечности убывающих последовательностей. Если бы для каждого n_k, удовлетворяющего свойству $P(n_k)$, нашлось бы меньшее его n_{k+1}, удовлетворяющее этому же свойству, то получившаяся последовательность была бы бесконечно убывающей, чего не может быть. Таким образом, от противного обоснован принцип бесконечного спуска.

Проиллюстрируем применение принципа бесконечного спуска.

Задача 2. Пусть k — натуральное число, и $\sqrt{k}$ — не целое. Докажите, что $\sqrt{k}$ — иррациональное число.

Решение. Предположим, что можно представить $\sqrt{k}$ в виде отношения натуральных чисел m и n. Обозначим через q наибольшее натуральное число, не превосходящее $\sqrt{k}$. Имеем равенства

$$\sqrt{k} = \frac{m}{n} = \frac{m(\sqrt{k}-q)}{n(\sqrt{k}-q)} = \frac{m\sqrt{k}-mq}{n\sqrt{k}-nq} = \frac{nk-mq}{m-nq} = \frac{m'}{n'}.$$

Перед последним равенством первое m в числителе заменили произведением $n\sqrt{k}$, а $\sqrt{k}$ заменили отношением m/n.

Мы получили из дроби m/n равную ей новую дробь m'/n', причем $m' < m$ и $n' < n$ (исходные числитель и знаменатель умножили на число меньшее 1 и упростили независимо так, чтобы снова получились целые числа). С новой дробью m'/n' мы можем повторить подобное преобразование и получим дробь с еще меньшими числителями и знаменателями и т. д. По принципу бесконечного спуска следует, что таких чисел m и n вообще нет.

При доказательстве основной теоремы арифметики обычно используется возвратная индукция.

Теорема 2. Основная теорема арифметики. Всякое натуральное число, большее 1, единственным образом (с точностью до порядка сомножителей) разложимо в произведение простых чисел.

Доказательство.

1. Сначала докажем, что натуральное число, большее 1, разложимо на простые множители. Пусть $P(n)$ есть утверждение «n — произведение простых чисел».

Индуктивный шаг. Возьмем некоторое $m \geqslant 2$ и допустим, что для каждого k, удовлетворяющего неравенству $2 \leqslant k < m$, утверждение $P(k)$ истинно. Если m — простое число, то $P(m)$ — истина. Если m — составное число, то существуют r и s, для которых выполнено $2 \leqslant r < m$, $2 \leqslant s < m$ и $r \cdot s = m$. Так как $P(r)$ и $P(s)$ выполнено, то r и s — произведения простых чисел. Поэтому $r \cdot s$ есть произведение простых чисел. В силу возвратной индукции, мы получаем, что любое n разложимо в произведение простых чисел.

2. Покажем единственность разложения, следуя [3, с. 17–18]. Пусть $S(n)$ утверждает, что n имеет единственное представление (с точностью до порядка сомножителей) в виде произведения простых чисел. Возьмем некоторое $m \geqslant 2$ и допустим, что для каждого k, удовлетворяющего неравенству $2 \leqslant k < m$, утверждение $S(k)$ истинно. Если m — простое число, то $S(m)$ — истина. Предположим, что m — составное и имеется два различных представления m в виде произведения простых, скажем,

$$m = pqr\ldots = p'q'r'\ldots,$$

где p, q, r,… и p', q', r',… — простые. Одно и тоже простое число не может встретиться в двух разложениях, так в этом случае мы сократили бы на это простое и получили бы два различных разложения меньшего числа, а это противоречит индуктивному предположению.

Не нарушая общности, можно предполагать, что p — наименьшее из простых, встречающихся в первом разложении. Так как m — составное, имеется по меньшей мере один множитель в разложении, помимо p; поэтому $m \geqslant p^2$. Аналогично $m \geqslant p'^2$. Так как p и p' не одинаковы, то по крайней мере одно из этих неравенств строгое и, следовательно, $pp' < m$. Рассмотрим теперь число $m - pp'$. Это натуральное число меньше m, следовательно, оно может быть представлено, как произведение простых, одним и только одним способом. Так как p делит m, оно делит также $m - pp'$, поэтому p должно входить в разложение $m - pp'$.

(Мы пользуемся следующим вспомогательным утверждением: если разложение числа n на простые множители единственно, то каждый простой множитель n должен входить в это разложение. Действительно, пусть a — какое-нибудь простое число, делящее n, тогда $n = ab$, где b — некоторое целое число; разложение n можно получить из разложения b, добавив простой множитель a. Так как по предположению имеется только одно разложение n на простые, то a должно встретиться в нем.)

Аналогично убеждаемся, что в это разложение должно входить и p'. Следовательно, разложение $m - pp'$ имеет вид

$$m - pp' = pp'QR\ldots,$$

где Q, R,… — простые числа. Отсюда следует, что число pp' делит m. Но $m = pqr\ldots$, поэтому (после сокращения на p) получается, что p' делит $qr\ldots$ Ввиду вспомогательного утверждения, приведенного выше в скобках, это невозможно, ибо $qr\ldots$ — число, меньшее m, и p' не является одним из простых q, r,…, входящих в его

разложение. Это противоречие доказывает, что для m выполнено $S(m)$. В силу возвратной индукции мы получаем, что любое n разложимо в произведение простых чисел единственным образом (с точностью до порядка сомножителей).

Индуктивное рассуждение можно применять различными способами.

Например, если

(1) базис индукции: $P(0)$ и $P(1)$ истинно,

(2) индуктивный шаг: для любого $n \geqslant 0$ из $P(n)$ следует $P(n+2)$,

то для всех $n \geqslant 0$ справедливо $P(n)$.

В действительности, два отдельных индуктивных доказательства комбинируются в одно (одно для четных чисел и другое для нечетных чисел). Приведем пример, где три индуктивных доказательства свернуты в одно.

Задача 3. Докажите, что если натуральное $n > 13$, то существуют такие натуральные числа a и b, что $n = 3a + 8b$.

Решение. Пусть $P(n)$ есть утверждение «$n = 3a+8b$ для некоторых натуральных a и b». Будем использовать математическую индукцию.

Базис индукции. $P(14)$, $P(15)$ и $P(16)$ истинны, так как $14 = 2 \cdot 3 + 8$, $15 = 5 \cdot 3 + 0 \cdot 8$ и $16 = 0 \cdot 3 + 2 \cdot 8$.

Индуктивный шаг $\big(P(k) \supset P(k+3)\big)$. Пусть для некоторого натурального $k > 13$ выполнено $P(n)$, т. е. существуют такие a и b, что $k = 3a + 8b$. Тогда $k + 3 = 3(a+1) + 8b$, т. е. выполнено $P(k+3)$.

В силу принципа математической индукции для всех $n > 13$ имеем $P(n)$. Действительно, здесь есть три отдельных доказательства: первое доказательство для последовательности чисел 14, 17, 20,…; второе — для последовательности 15, 18, 21,… и третье — для последовательности 16, 19, 22,…

Индуктивное доказательство может быть также проведено, когда индуктивный базис есть $P(m)$ и $P(m+1)$ для фиксированного натурального числа m и индуктивный переход есть $P(k)$ & $P(k+1) \supset P(k+2)$ для произвольного $k \geqslant m$. Тогда в результате для всех $n \geqslant m$ справедливо $P(n)$.

Задача 4. Докажите, что для любого $n \geqslant 1$ выполнено неравенство

$$f(n) \leqslant \left(\frac{5}{3}\right)^{n-1}.$$

Решение. Пусть $P(n)$ есть утверждение $f(n) \leqslant (5/3)^{n-1}$ для $n \geqslant 1$.

Базис индукции. Имеем $P(1)$: $1 \leqslant 1$ — истина и $P(2)$: $1 \leqslant 5/3$ — истина.

Индуктивный шаг. Пусть $k \geqslant 1$ и $P(k)$ & $P(k+1)$ — истина. Тогда

$$f(k+2) = f(k) + f(k+1) \leqslant \left(\frac{5}{3}\right)^{k-1} + \left(\frac{5}{3}\right)^{k} \text{ (в силу } P(k) \text{ и } P(k+1)) =$$

$$= \left(\frac{5}{3}\right)^{k-1} \cdot \left(1 + \frac{5}{3}\right) = \left(\frac{5}{3}\right)^{k-1} \cdot \left(\frac{8}{3}\right) < \left(\frac{5}{3}\right)^{k-1} \cdot \left(\frac{25}{9}\right) = \left(\frac{5}{3}\right)^{k+1}.$$

Мы доказали $P(k+2)$. Поэтому $P(n)$ справедливо для $n \geqslant 1$.

Парадоксы и софизм при математической индукции

1. **Парадокс неожиданной казни**. Мы уже встретились с этим парадоксом, в главе 1, параграф 1.3. Кажется, до сих пор не существует удовлетворительного разрешения этого парадокса, однако см. книгу Р. Смаллиана [4, с. 16–20].

2. **Парадокс Ришара**. Рассмотрим этот парадокс в иной форме по сравнению с оригинальным описанием в [5, с. 41].

Предложение 5. Каждое натуральное число *определяется* на русском языке фразой, содержащей менее 14 слов.

Доказательство. Пусть $P(n)$ будет утверждением:

«n определяется на русском языке фразой, содержащей менее четырнадцати слов».

Базис индукции. $n = 0$ определяется как «наименьшее натуральное число». Поскольку эта фраза содержит менее 14 слов, то $P(0)$ выполнено.

Индуктивный шаг. Пусть $k \geqslant 0$ фиксировано и допустим, что имеет место $P(0), P(1), \ldots, P(k-1)$, т. е. каждое число, меньшее k, определяется на русском языке фразой, содержащей менее 14 слов. Если k не определяется, то его можно определить как «наименьшее натуральное число, которое определяется на русском языке фразой, содержащей менее четырнадцати слов», — фраза состоит из 13 слов, и поэтому k становится определенным после этого. Это противоречие доказывает индуктивный шаг.

Следовательно, по математической индукции $P(n)$ справедливо для всех n, так что доказательство закончено.

В этом виде парадокс Ришара очень близок парадоксу Берри, описанному в параграфе 1.3 главы 1.

3. **Софизм**. **Все лошади одной масти**. То, что все лошади одной масти, можно доказать индукцией по числу лошадей в определенном табуне.

Доказательство. Если существует только одна лошадь, то она своей масти, так что база индукции тривиальна. Для индуктивного перехода предположим, что существует $n+1$ лошадь (с номерами от 1 до $n+1$). По индуктивному предположению лошади с номерами от 1 до n одинаковой масти и, аналогично, лошади с номерами от 2 до $n+1$ имеют одинаковую масть. Но лошади посередине с номерами от 2 до n не могут изменять масть в зависимости от того, как они сгруппированы — это лошади, а не хамелеоны. Поэтому лошади с номерами от 1 до n также должны быть одинаковой масти. Таким образом, все n лошадей одинаковой масти. Что и требовалось доказать.

Объяснение софизма. Поскольку базис индукции доказан для $n = 1$, то индуктивный переход от n к $n+1$ должен быть выполнен для всех $n \geqslant 1$. Но это невозможно, поскольку пересечение двух множеств $\{1, 2, \ldots, n\}$ и $\{2, 3, \ldots, n+1\}$ пусто при $n = 1$.

4. **Парадокс изобретателя**. Попробуем доказать методом математической индукции неравенство

$$\frac{1 \cdot 3 \cdot \ldots \cdot (2n-1)}{2 \cdot 4 \cdot \ldots \cdot 2n} < \frac{1}{\sqrt{n}}, \quad n \geqslant 1.$$

Базис индукции:

$$\frac{1}{2} < \frac{1}{\sqrt{1}}.$$

По предположению индукции:

$$\frac{1\cdot 3\cdot \ldots\cdot (2k-1)\cdot (2k+1)}{2\cdot 4\cdot \ldots\cdot 2k\cdot (2k+2)} = \frac{1\cdot 3\cdot \ldots\cdot (2k-1)}{2\cdot 4\cdot \ldots\cdot 2k}\cdot \frac{2k+1}{2k+2} < \frac{1}{\sqrt{k}}\cdot \frac{2k+1}{2k+2},$$

и нам остается доказать, что

$$\frac{2k+1}{2k+2} \leqslant \frac{1}{\sqrt{k+1}}. \tag{7.5}$$

Возводя обе части неравенства в квадрат и избавляясь от знаменателей, приходим к эквивалентному неравенству

$$(k+1)(2k+1)^2 \leqslant k(2k+2)^2. \tag{7.6}$$

И далее, раскрывая скобки, — к неравенству

$$4k^3 + 8k^2 + 5k + 1 \leqslant 4k^3 + 8k^2 + 4k.$$

Это неравенство неверно! Следовательно, неверны и неравенства (7.6) и (7.5). Можно считать, что неверно исходное неравенство?

Нет нельзя. Неудача говорит лишь о том, что не годится конкретный метод доказательства — индукция.

Попробуем теперь доказать неравенство:

$$\frac{1\cdot 3\cdot \ldots\cdot (2n-1)}{2\cdot 4\cdot \ldots\cdot 2n} < \frac{1}{\sqrt{n+1}}, \quad n \geqslant 1. \tag{7.7}$$

Неравенство (7.7) сильнее нашего исходного неравенства, и казалось бы, что доказывать его тем же методом — индукцией — дело безнадежное. Все же попробуем.

Базис индукции:

$$\frac{1}{2} < \frac{1}{\sqrt{1+1}}.$$

По предположению индукции:

$$\frac{1\cdot 3\cdot \ldots\cdot (2k-1)\cdot (2k+1)}{2\cdot 4\cdot \ldots\cdot 2k\cdot (2k+2)} = \frac{1\cdot 3\cdot \ldots\cdot (2k-1)}{2\cdot 4\cdot \ldots\cdot 2k}\cdot \frac{2k+1}{2k+2} < \frac{1}{\sqrt{k+1}}\cdot \frac{2k+1}{2k+2},$$

и нам надо доказать, что

$$\frac{1}{\sqrt{k+1}}\cdot \frac{2k+1}{2k+2} \leqslant \frac{1}{\sqrt{k+2}}.$$

Снова возводя обе части неравенства в квадрат, избавляясь от знаменателей и раскрывая скобки, приходим к эквивалентному неравенству

$$4k^3 + 12k^2 + 9k + 2 \leqslant 4k^3 + 12k^2 + 12k + 4.$$

Это неравенство верно.

Следовательно, мы доказали (методом математической индукции) неравенство (7.7), из которого немедленно выводим наше первоначальное неравенство.

Как же это получается? Дело в том, что хотя во втором случае нам и пришлось доказывать более сильное заключение, но мы могли пользоваться и более сильным предположением индукции. Подобная ситуация получила название «***парадокс изобретателя***».

Этот термин ввел в научный оборот Дьёрдь Пойа [6, с. 138]. Он использовал наблюдение, что при доказательстве по математической индукции часто необходимо усиливать доказываемое предложение и индуктивное утверждение становится намного сложнее конечного результата. Эта необходимость усиливать результат, чтобы его строго обосновать, на первый взгляд кажется парадоксальной. Парадокс изобретателя используется для описания явлений в области математики, программирования и логики, а также в других областях, связанных с творческим мышлением.

Парадокс изобретателя связан со следующей логической и методологической проблемой. В доказательствах порою встречаются вспомогательные утверждения, более сложные, чем извлекаемые из них следствия. Можно ли хотя бы в принципе устранить окольные пути в доказательствах, когда мы доказываем лемму лишь затем, чтобы в дальнейшем применить ее в частных случаях? Доказательства без окольных путей называют также прямыми.

Н. Н. Непейвода в [7, с. 868–869; 8, с. 323–325] пишет, что даже в принципе в математических доказательствах внешне простых предложений нельзя обойтись без сложных лемм. Парадокс изобретателя показывает полную методологическую несостоятельность редукционизма и эмпиризма[1]. Человечество не может обойтись без концепций и идей высших уровней в логике и программировании.

Математическая индукция по построению

С методом математической индукции связано понятие индуктивного определения.

. . . . . .

Базис индукции. *Выражение вида A есть B.*

Индуктивный переход. *Если мы имеем выражения* $A_1, \ldots, A_n$ *типа B, то C, построенное из них, также есть выражение типа B.*

C каждым индуктивным определением связан ***принцип индукции по построению объекта*** *типа B.*

Базис индукции. *Каждый объект вида A обладает свойством* θ.

Индуктивный переход. *Если* $A_1, \ldots, A_n$ *обладают свойством* θ*, то и C им обладает.*

Заключение индукции. *Тогда любой объект типа B обладает свойством* θ.

. . . . . .

Этот принцип является логическим выражением следующего неявного пункта, присутствующего в любом индуктивном определении: никаких других объектов типа *B*, кроме полученных применением правил его определения, нет. Иными сло-

[1] Редукционизм — методологический принцип, согласно которому сложные явления могут быть полностью объяснены с помощью законов, свойственных явлениям более простым.

Эмпиризм — направление в теории познания, признающее чувственный опыт источником знания и считающее, что содержание знания может быть представлено либо как описание этого опыта, либо сведено к нему.

вами, множество объектов типа B — минимальное из тех, которые включают базисные объекты и замкнуты относительно индуктивного перехода. В простых определениях эту минимальность можно выразить следующим образом: объект должен получаться из базисных конечным числом применений шагов определения.

Стоит отметить, что логическая индукция по построению вовсе не требует однозначности представления объекта в форме, соответствующей одному из пунктов его определения. Но для задания функций индукцией по построению такая однозначность необходима.

Пример 7.8

Примеры индуктивного определения по построению

Таковыми являются определение пропозициональной формулы (глава 4, параграф 4.2), определение термов и формул языка первого порядка (глава 5, параграф 5.2).

Доказательство леммы 2 для теоремы 4 из параграфа 4.3 главы 4 было отложено. Сейчас мы проведем доказательство этой леммы с помощью математической индукции по построению.

Лемма 2. Пусть $A \equiv B$ и C — формула, в которой выделено одно вхождение некоторой переменной X. Пусть C_A получается из C заменой этого вхождения X на A, а C_B — из C заменой того же вхождения X на B. Тогда $C_A \equiv C_B$.

Доказательство. Для доказательства мы будем использовать математическую индукцию по построению формулы C.

Базис индукции. Если формула C является просто пропозициональной переменной, то она должна совпадать с X (так как в ней имеется вхождение переменной X). В этом случае C_A есть A, C_B есть B, $C_A \equiv C_B$ — не что иное, как $A \equiv B$.

Шаг индукции. Пусть теперь формула C является составной. Она имеет вид $\neg D$, или $D \,\&\, E$, или $D \vee E$, или $D \supset E$, или $D \sim E$, причем в первом случае выделенное вхождение X содержится в D, а в остальных случаях — либо в D, либо в E, но не в D и E сразу. Рассмотрим, например, случай, когда C имеет вид $D \supset E$ и выделенное вхождение X содержится в D. По индуктивному предположению утверждение леммы справедливо для D. Заменяя X в этом вхождении в D на A и B, получаем соответственно формулы D_A и D_B. Ясно, что C_A есть $D_A \supset E$, а C_B есть $D_B \supset E$. Имеем $D_A \equiv D_B$. Применим теперь лемму 1 (для теоремы 4 в параграфе 4.3 главы 4) в случае $A \supset C \equiv B \supset C$, где в роли A выступает D_A и в роли $B - D_B$, в роли $C - E$. В результате получаем $C_A \equiv C_B$. Другие случаи рассматриваются аналогично.

Пример 7.9

В главе 6 была определена теория ***L***. Формулами в теории ***L*** являются всевозможные строки, составленные из букв *a*, *b*. Единственной аксиомой ***L*** является строка *a*, наконец, в ***L*** имеется два правила вывода:

$$\frac{X}{Xb} \quad \text{и} \quad \frac{X}{aXa}.$$

Была сформулирована в параграфе 6.3 главы 6 метатеорема: если X — теорема, то aaX — тоже теорема.

Докажем, используя математическую индукцию по построению.

Базис индукции. X — аксиома a. Тогда, применяя второе правило вывода, получаем aaa — это формула aaX.

Шаг индукции. Пусть формула X — теорема и X получена из формулы Y по одному из правил вывода, причем мы предполагаем, что aaY — теорема. Докажем, что aaX также имеет логический вывод. Рассмотрим два случая:

1) $X = Yb$, тогда $aaX = aaYb$ выводится из aaY;
2) $X = aYa$, тогда $aaX = aaaYa$ выводится из aaY.

По принципу математической индукции по построению заключаем, что если X — теорема, то aaX — тоже теорема.

7.3 Различные виды доказательств в математике

Понятие доказательства не принадлежит математике, математике принадлежит лишь его математическая модель — формальное доказательство.

Рассмотрим, как соотносятся неформальные доказательства и логический вывод. Логический вывод напоминает процесс мышления, но при этом мы не должны считать, что его правила суть правила человеческой мысли. Доказательство — это нечто неформальное; иными словами, это продукт нормального мышления, записанный на человеческом языке и предназначенный для человеческого потребления. В доказательствах могут использоваться всевозможные сложные мыслительные приемы, и хотя интуитивно они могут казаться верными, можно усомниться в том, возможно ли доказать их логически. Именно поэтому мы нуждаемся в формализации. Вывод — это искусственное соответствие доказательства: его назначение — достичь той же цели, на этот раз с помощью логической структуры, методы которой не только ясно выражены, но и очень просты.

Обычно формальный вывод бывает крайне длинен по сравнению с соответствующей «естественной» мыслью. Это, конечно, плохо — но это та цена, которую приходится платить за упрощение каждого шага. Часто бывает, что вывод и доказательство «просты» в дополнении друг к другу. Доказательство просто в том смысле, что каждый шаг «кажется правильным», даже если мы и не знаем точно, почему; логический вывод прост, потому что каждый из многочисленных его шагов так

прост, что сомнения в правильности этих шагов не возникают, и поскольку весь вывод состоит из таких шагов, мы предполагаем, что он безошибочен. Каждый тип простоты, однако, привносит свой тип сложности. В случае доказательств — это сложность системы, на которую они опираются, а именно, человеческого языка; в случае логических выводов — это их грандиозная длина, делающая их почти невозможными для понимания.

Формальные доказательства в математике (в том числе и в математической логике) в большинстве случаев являются доказательствами вида «$\Gamma \vdash P$» или «не $\Gamma \vdash P$» для разных теорий первого порядка, множеств Γ и разных (классов) формул P.

Результат «$\Gamma \vdash P$» может доказываться посредством предъявления описания вывода формулы P из Γ. Однако в мало-мальски сложных случаях оно оказывается настолько длинным, что заменяется инструкцией по составлению такого описания, более или менее полной. Наконец, доказательство «$\Gamma \vdash P$» может вообще не сопровождаться предъявлением вывода P из Γ, хотя бы и неполного. В этом случае мы «не доказываем P, а доказываем, что существует доказательство P».

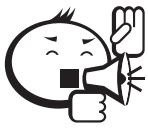
Результат «не $\Gamma \vdash P$» в редких случаях может устанавливаться чисто синтаксическим рассуждением, но обычно доказательство опирается на конструкцию модели, т. е. интерпретации, в которой Γ истинно, а P ложно.

Многие математики критикуют аксиоматический метод за то, ради чего он был создан: он избавляет математику от смысла. Потому что сначала мы избавляем математику от разных геометрических представлений, от интуиции. Переходя к формальной аксиоматической теории, мы, в общем-то, и логику изгоняем из математики. И в результате от содержательного доказательства остается лишь скелет, состоящий из формальных символов. Преимущество последнего ровно в том, что мы не знаем, что такое «смысл» и «интуиция», но зато точно знаем, что такое манипуляции с конечными строками символов. Это и позволяет нам построить точную математическую модель сложного явления — доказательства — и подвергнуть ее математическому анализу.

Математическое доказательство изначально было психологическим процессом убеждения собеседника в верности того или иного утверждения. В формальной системе это не так: все свелось к чисто механическому процессу. Этот механический процесс способен выполнять компьютер. Однако, как и всякая модель, механический процесс передает лишь некоторые черты реальных доказательств. У такой модели есть свои границы применимости. Неверно думать, что формальные доказательства и есть «настоящие» математические доказательства или что математики на самом деле работают в рамках определенных формальных систем.

По словам Ю. И. Манина [9, с. 54], «в качестве средства общения, открытия, фиксации материала никакой формальный язык не способен конкурировать со смесью национального математического арго и формул, привычной для каждого работающего математика».

Отдельно стоит сказать о преподавании математики. Нет ничего хуже, чем строить обучение школьников и студентов на выполнении механических действий (алгоритмов) или же на построении формальных логических выводов. Так можно загубить в человеке любое творческое начало. Соответственно, при обучении математике не стоит подходить с позиции строгого аксиоматического метода в смысле Гильберта — не для того он был создан.



Определение доказательства было уточнено Н. Н. Непейводой. ***Доказательство*** — конструкция, синтаксическая правильность которой гарантирует семантическую.

Под это определение попадают все формальные доказательства. Но и некоторые неформальные доказательства. Например, использование диаграмм Венна для обоснования тождеств алгебры множеств (глава 3, параграф 3.2). В этих диаграммах нет предложений, нет правил вывода, не видно умозаключений, но они доказывают на хорошо подобранных системах множеств.

Перечислим различные методы математических доказательств. Надо, конечно, учитывать, что в сложном доказательстве могут сразу присутствовать несколько методов.

С точки зрения общего движения мысли все доказательства подразделяются на *прямые* и *косвенные*.

При прямом доказательстве задача состоит в том, чтобы подыскать такие убедительные аргументы, из которых по логическим правилам получается заключение. Другими словами, истинность утверждения выводится из истинности посылок без введения дополнительных предположений.

Непрямое (косвенное) доказательство истинности или ложности некоторого утверждения состоит в том, что оно достигается посредством опровержения некоторых других высказываний, несовместимых с доказываемым. Косвенные доказательства применяются в основном в математике.

1. **Аксиоматический метод**. Подразделяется на формальный и неформальный (см. главу 6, параграф 6.1).

2. **Доказательство методом перебора**. Такой метод часто применяют, когда количество вариантов незначительно для проверки данного утверждения, например, утверждения о каком-то свойстве натуральных чисел в ограниченном диапазоне. С использованием систем компьютерной алгебры проверка может быть проделана для очень больших чисел. Например, самая старая открытая проблема со времен античности: существуют ли нечетные совершенные числа? На конец 2014 года проверены все нечетные числа, меньшие 10^{300}. Нечетное совершенное число не обнаружено[1].

3. **Использование теоремы о дедукции**. Теорема о дедукции справедлива для исчисления высказываний (глава 6, параграф 6.3, теорема 3) и для теорий первого порядка (глава 6, параграф 6.5, теорема 7). Теорема служит обоснованием следующего приема, который часто используют в математических доказательствах. Для того чтобы доказать утверждение «Если A, то B», предполагают, что справедливо A и доказывают справедливость B.

[1] Натуральное число n называется совершенным, если сумма его всех делителей равна $2n$.

Пример 7.10

Докажите, что для каждого целого n, если n четное, то n^2 тоже четное.

Доказательство. Так как n четное, то его можно представить в виде $n = 2m$, где m — целое число. Поэтому $n^2 = (2m)^2 = 4m^2 = 2(2m^2)$, где $2m^2$ — целое число, т. е. n^2 четное.

4. **Доказательство импликаций с помощью контрапозиции**. Рассмотрим условное высказывание вида $A \supset B$, где A — конъюнкция посылок, B — заключение. Иногда удобнее вместо доказательства истинности этой импликации установить логическую истинность некоторого другого высказывания, равносильного исходному. Такие формы доказательства относятся к косвенным методам.

Контрапозицией формулы $A \supset B$ называется равносильная формула $\neg B \supset \neg A$. Поэтому если мы установим истинность контрапозиции, то тем самым докажем истинность исходной импликации.

Пример 7.11

На основе контрапозиции докажите, что если m и n — произвольные положительные целые числа, такие, что $m \times n \leqslant 100$, то либо $m \leqslant 10$, либо $n \leqslant 10$.

Доказательство. Контрапозицией исходному утверждению служит следующее высказывание: «Если $m > 10$ и $n > 10$, то $m \times n > 100$», что очевидно.

Преимущества метода доказательства с помощью контрапозиции проявляются при автоматизированном способе доказательства, т. е. когда доказательство совершает компьютер с помощью специальных программных систем доказательства теорем (например, с помощью языка программирования Пролог).

При построении выводов не всегда целесообразно ждать появления искомого заключения, просто применяя правила вывода. Именно такое часто случается, когда мы делаем допущение A для доказательства импликации $A \supset B$. Мы применяем цепное правило и *modus ponens* к A и другим посылкам, чтобы в конце получить B. Однако можно пойти по неправильному пути, и тогда будет доказано много предложений, большинство из которых не имеет отношения к нашей цели. Этот метод носит название *прямой волны* и имеет тенденцию порождать лавину промежуточных результатов, если его запрограммировать для компьютера и не ограничить глубину.

Другая возможность — использовать контрапозицию и попытаться, например, доказать $\neg B \supset \neg A$ вместо $A \supset B$. Тогда мы допустим $\neg B$ и попробуем доказать $\neg A$. Это позволяет двигаться как бы назад от конца к началу, применяя правила так, что старое заключение играет роль посылки. Такая организация поиска может лучше

показать, какие результаты имеют отношение к делу. Она называется *поиском от цели*.

5. **Доказательство с помощью противоречия (от противного)**. Частным случаем косвенных методов доказательства является приведение к противоречию (от противного). Метод доказательства основывается на следующем утверждении.

Если $\Gamma, \neg S \vdash F$, где F — любое противоречие (тождественно ложная формула), то $\Gamma \vdash S$.

В этом методе используются следующие равносильности:

- $A \supset B \equiv \neg(A \supset B) \supset (C\&\neg C) \equiv (A\&\neg B) \supset (C\&\neg C)$,
- $A \supset B \equiv (A\&\neg B) \supset \neg A$,
- $A \supset B \equiv (A\&\neg B) \supset B$.

Используя вторую из приведенных равносильностей для доказательства $A \supset B$, мы допускаем одновременно A и $\neg B$, т. е. предполагаем, что заключение ложно:

$$\neg(A \supset B) \equiv \neg(\neg A \vee B) \equiv A\&\neg B.$$

Теперь мы можем двигаться и вперед от A, и назад от $\neg B$. Если B выводимо из A, то, допустив A, мы доказали бы B. Поэтому, допустив $\neg B$, мы получим противоречие. Если же мы выведем $\neg A$ из $\neg B$, то тем самым получим противоречие с A. В общем случае мы можем действовать с обоих концов, выводя некоторое предложение C, двигаясь вперед, и его отрицание $\neg C$, двигаясь назад. В случае удачи это доказывает, что наши посылки ***несовместимы*** или ***противоречивы***. Отсюда мы выводим, что дополнительная посылка $A\,\&\,\neg B$ должна быть ложна, а значит, противоположное ей утверждение $A \supset B$ истинно. Метод доказательства от противного — один из самых лучших инструментов математика. «Это гораздо более «хитроумный» гамбит, чем любой шахматный гамбит: шахматист может пожертвовать пешку или даже фигуру, но математик жертвует *партию*» [10, с. 61].

Мы уже применяли в параграфе 4.3 главы 4 метод от противного при доказательстве тавтологичности некоторых импликаций. Следующие примеры более знамениты.

Теорема 3. Школа Пифагора. Докажем, что диагональ единичного квадрата является иррациональным числом.

Доказательство. Используя теорему Пифагора, переформулируем утверждение: *Не существуют два таких целых числа p и q, чтобы выполнялось отношение*

$$\sqrt{2} = \frac{p}{q}.$$

В самом деле, тогда мы приходим к равенству $p^2 = 2q^2$. Мы можем считать, что дробь p/q несократима, иначе мы с самого начала сократили бы ее на наибольший общий делитель чисел p и q. С правой стороны имеется 2 в качестве множителя, и потому p^2 есть четное число, и, значит, само p — также четное, так как квадрат нечетного числа есть нечетное число. В таком случае можно положить $p = 2r$. Тогда равенство принимает вид:

$$4r^2 = 2q^2, \quad \text{или} \quad 2r^2 = q^2.$$

Так как с левой стороны теперь имеется 2 в качестве множителя, значит q^2, а следовательно, и q — четное. Итак, и p, и q — четные числа, т. е. делятся на 2, а это противоречит допущению, что дробь p/q несократима. Итак, равенство $p^2 = 2q^2$ невозможно и $\sqrt{2}$ не может быть рациональным числом.

Теорема 4 (Евклида). Доказать, что простых чисел бесконечно много.

Доказательство. Предположим, что существует конечное множество простых чисел и p есть наибольшее из них: 2, 3, 5, 7, 11,..., p. Определим число $N = p! + 1$. Число N при делении на любое из чисел 2, 3, 5, 7, 11,..., p дает в остатке 1. Каждое число, которое не является простым, делится, по крайней мере, на одно простое число. Число N не делится ни на одно простое число, следовательно, N — само простое число, причем $N > p$. Таким образом, мы пришли к противоречию, которое доказывает, что простых чисел бесконечно много.

Софизм. Единица — наибольшее натуральное число.

Доказательство. От противного. Пусть $k > 1$ будет наибольшим натуральным числом; тогда имеем $k \cdot k = k^2 > k \cdot 1 = k$. Неравенство показывает, что k не является наибольшим натуральным числом. Следовательно, никакое целое число $k > 1$ не может быть наибольшим натуральным числом. Остается принять, что наибольшим натуральным числом является 1, так как только в этом случае мы не приходим к противоречию.

Попробуйте разобраться самостоятельно.

6. **Доказательство контрпримером**. Многие математические гипотезы имеют в своей основе форму: «Все объекты со свойством A обладают свойством B». Мы можем записать это в виде формулы:

$$\forall x\big(A(x) \supset B(x)\big),$$

где $A(x)$ обозначает предикат «x обладает свойством A», $B(x)$ — «x обладает свойством B». Если число возможных значений x является конечным, то в принципе доказательство может быть проведено с помощью разбора случаев, то есть непосредственной проверкой выполнимости гипотезы для каждого объекта. В случае если число объектов не является конечным, то такой возможности не существует даже в принципе. Однако для доказательства ложности гипотезы достаточно привести хотя бы один пример (называемый в этом случае *контрпримером*), для которого гипотеза не выполнима.

Знаменитых контрпримеров множество. Перечислим некоторые из них.

Пример 7.12

Ферма[1] предполагал, что все числа вида

$$p_k = 2^{2^k} + 1$$

[1] Пьер Ферма (1601–1665 гг.) — французский математик, один из создателей аналитической геометрии, математического анализа, теории вероятностей и теории чисел.

простые. Первые пять чисел для $k = 0, 1, 2, 3, 4$ являются простыми. Он не смог проверить число $p_5 = 4\ 294\ 967\ 297$. Ферма был неправ, возможно, почти совсем неправ, дело в том, что все остальные числа, которые удалось проверить на простоту, оказались составными. Число p_5 было разложено на множители Эйлером.

Пример 7.13

Эйлер предположил (1769 г.), что для любого натурального числа $n > 2$ никакую n-ю степень натурального числа нельзя представить в виде суммы $(n-1)$ n-х степеней других натуральных чисел. То есть, уравнения:

$$\sum_{k=1}^{n-1} a_k^n = a_n^n$$

не имеют решения в целых числах. В 1966 году был найден для $n = 5$ контрпример

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

Для $n = 4$ контрпример был найден в 1986 году:

$$2\ 682\ 440^4 + 15\ 365\ 639^4 + 1\ 879\ 760^4 = 206\ 156\ 734^4.$$

Пример 7.14

В 1806 году Ампер[1] предпринял попытку доказать, что всякая «произвольная» функция дифференцируема всюду, за исключением «исключительных и изолированных» значений аргумента. Один из контрпримеров был найден в 1930 году ван дер Варденом[2] — пример непрерывной, но нигде не дифференцируемой функции:

$$v(x) = \sum_{n=0}^{\infty} \frac{\{10^n x\}}{10^n},$$

где фигурные скобки означают взятие дробной части.

7. **Метод математической индукции**. Дедукция как общенаучный метод является основным методом математики. Математическая индукция явно восходит к этой же идее. Аксиома индукции Пеано постулирует писать только первый и общий шаги доказательства и, таким образом, является по существу первым метаматематическим принципом. Хотя аксиома индукции формулируется для формальной арифметики, но, в сущности, она является фундаментальным архетипом математического мышления.

[1] Андре-Мари Ампер (1775–1836 гг.) — знаменитый французский физик и математик.

[2] Бартель ван дер Варден (1903–1996 гг.) — голландский математик.

Отметим, что математическая индукция очень часто используется для доказательства гипотез, полученных с помощью индукции.

Доказательство становится таковым только в результате социального акта «принятия доказательства». Это относится к математике в той же мере, что и к физике, лингвистике или биологии. Представление о математическом доказательстве меняется со временем (см. [11, с. 370–390]). Однако со времени Евклида неизменной остается идеальная структура математического доказательства «неочевидной истины»: переход к ней от «очевидных» или установленных ранее посылок посредством серии явно выписанных «очевидно законных» элементарных умозаключений.

Формальный метод является хорошим приближением к традиционным математическим доказательствам. О различиях по форме и восприятию их человеком мы уже сказали. Но есть и другие серьезные различия, о которых пишет Ю. И. Манин [9, с. 54–55].

а) *Надежность принципов*. Не только математика, заложенная в специальные аксиомы теории множеств и арифметики Пеано, но даже логика языков первого порядка не является общепризнанной. В частности, после Брауэра[1] оспаривается закон исключенного третьего. С этих крайне критических позиций наши «доказательства» в лучшем случае выводят бессмыслицу из лжи. Быть совершенно глухим к этой критике математик не может себе позволить: вдумываясь в нее, следует по крайней мере осознать, что существуют объективно различные «степени доказательности» доказательств.

б) *Уровни доказательности*. Каждое предложенное доказательство апробируется на приемлемость математиками, иногда нескольких поколений. При этом подлежит уточнению и само доказательство, и его результат. Чаще всего доказательство является более или менее краткой схемой формального вывода в подходящем языке. Однако как уже было отмечено, иногда утверждение P устанавливается посредством доказательства того, что доказательство P существует. Эта иерархия доказательств существования доказательств в принципе может быть как угодно высокой. Мы снимаем ее с помощью высших логических или теоретико-множественных принципов, с которыми, однако, можно не соглашаться. Работы по конструктивной математике пестрят утверждениями типа: «не может не существовать алгоритма, вычисляющего x» там, где классический математик сказал бы просто «x существует» или, в крайнем случае, «x существует и эффективно вычислим».

в) *Ошибки*. Особенности человеческой психики делают формальные выводы практически не поддающимися проверке, даже если согласиться, что это идеальный вид доказательности. Два обстоятельства действуют в одну сторону с губительным эффектом: формальные выводы гораздо длиннее текстов на арго; скорость их сознательного чтения человеком гораздо ниже.

[1] Лёйтзен Брауэр (1881–1966 гг.) — голландский философ и математик. Положил начало новому направлению в математике — интуиционизму. Он подверг сомнению неограниченную приложимость в математических рассуждениях классического закона исключенного третьего и косвенных методов доказательства.

Нередко доказательство одной теоремы занимает пять, пятнадцать и даже сотни страниц. Длина соответствующих формальных выводов не поддается воображению.

Поэтому отсутствие ошибок в математической работе (если они не обнаружены), как и в других естественных науках, часто устанавливается по косвенным данным: имеет значение соответствие с общими ожиданиями, использование аналогичных аргументов в других работах. Разглядывание «под микроскопом» отдельных участков доказательства, даже репутация автора; словом, воспроизводимость в широком смысле слова, непонятные доказательства могут сыграть очень полезную роль, стимулируя поиски более доступных рассуждений.

> Лучший способ в чём-то разобраться до конца — это попробовать научить этому компьютер.
>
> *Дональд Кнут*

7.4 Компьютерные доказательства

Заслуживают отдельного рассмотрения доказательства с помощью компьютера. Но прежде чем говорить о компьютерных доказательствах, рассмотрим некоторые вопросы применения компьютеров в математике.

История математики до компьютерной эры содержит много примеров трудоемких вычислений. Некоторые вычисления сводились к сложным и громоздким преобразованиям формул, другие вычисления использовали небольшие формулы, но требовали выполнения операций с большим количеством цифр в числах.

Великий Леонард Эйлер был непревзойдённым мастером формальных выкладок и преобразований, в его трудах многие математические формулы и символика получили современный вид (например, ему принадлежат обозначения для e и π). Наглядными примерами мастерства Эйлера служат его вычисление суммы обратных квадратов и получение необычайной формулы, связывающей суммы делителей натуральных чисел [2, с. 40–43, 112–122].

В XIX веке очень много вычислений было проделано в астрономии. Например, французский математик Урбен Леверье проводил громоздкие расчеты орбиты Нептуна, основанные на аналитических вычислениях возмущенной орбиты Урана (что и позволило открыть Нептун).

Впечатляющие вычисления с карандашом и бумагой проделал французский астроном Чарльз-Евгений Делоне для вычисления орбиты Луны. Он вывел около 40 000 формул. На их вывод потребовалось 10 лет и еще 10 лет ушло на проверку формул. Окончательная формула занимала 128 страниц его книги с результатами работы. Проверка его аналитических преобразований было проведена двумя американскими математиками с помощью компьютера в 70-е годы XX века. Компьютеру потребовалось двое суток работы.

Большие усилия тратили математики на определение числа π, вручную вычисляя большое количество цифр. Так, например, наилучший результат к концу XIX века был получен англичанином Вильямом Шенксом. Он потратил 15 лет для того, чтобы вычислить 707 цифр, хотя из-за ошибки только первые 527 были верными. Он использовал формулу Мэчина (Johm Machin, 1680–1751 гг.):

$$\frac{\pi}{4} = 4\,\mathrm{arctg}\,\frac{1}{5} - \mathrm{arctg}\,\frac{1}{239}.$$

Ошибку Шенкса обнаружил в 1944 году Фергюсон (D. E. Ferguson); он считал по формуле, подобной формуле Мэчина,

$$\frac{\pi}{4} = 3\,\mathrm{arctg}\,\frac{1}{4} + \mathrm{arctg}\,\frac{1}{20} + \mathrm{arctg}\,\frac{1}{1985}$$

на настольном механическом калькуляторе.

В начале 50-х годов стали появляться первые программы, производящие частично аналитические вычисления. В 1951 году с помощью компьютера EDSAC 1 было открыто наибольшее известное простое число $180(2^{127} - 1)^2 + 1$ с 79 десятичными цифрами. В 1952 году математики Эмиль Артин и Джон фон Нейман проделали большие вычисления, связанные с эллиптическими кривыми, на компьютере MANIAC. В 1953 году было показано, как алгоритмы в теории групп могут быть реализованы на компьютере.

В 60-х годах XX века стали создаваться первые системы компьютерной алгебры. Система компьютерной алгебры (computer algebra system) — программа для выполнения символьных (математических) вычислений. Основная определяющая функциональность таких систем — это операции с выражениями в символьной форме.

Первые системы были ограничены по своим возможностям и предназначались для какой-то отдельной области математики. Системы компьютерной алгебры общего назначения (универсальные) — это те, в которых реализованы основные математические алгоритмы и есть возможность пользователю самому создать новые алгоритмы на языке программирования системы.

В настоящее время применяется несколько систем компьютерной алгебры общего назначения. Отметим одну из них.

Mathematica — система компьютерной алгебры, используется во многих научных, инженерных, математических и вычислительных областях. Система была задумана Стивеном Вольфрамом (физик, математик и программист) и в дальнейшем разработана в компании Wolfram Research (Шампейн, штат Иллинойс, США). Начало разработки — 1986 г.; первая версия — 1988 г.; последняя 10-я версия — 2014 г. [12].

Применение Mathematica позволяет эффективно вычислять математические объекты, что проливает свет на используемые математические понятия. Причем использование Mathematica не требует глубоких знаний программирования. Только человек, по роду своей деятельности имеющий дело с математическими вычислениями, глубоко понимающий их специфику и потребности, мог создать подобный программный продукт.

Пример 7.15

В параграфе 7.1 главы 7, пример 7.4, мы рассматривали задачу об определении числа R_n областей, образуемых $n(n-1)/2$ хордами, которые соединяют n фиксированных точек на окружности, при предположении, что никакие три хорды не пересекаются внутри круга. Эмпирически были установлены значения R_n для

$n = 1, 2, \ldots, 6$ — это числа 1, 2, 4, 8, 16, 31. Mathematica может определить закономерность этой последовательности:

```
FindSequenceFunction[{1, 2, 4, 8, 16, 31}, n]
```

$$\frac{1}{24} \cdot \left(24 - 18n + 23n^2 - 6n^3 + n^4\right).$$

В настоящее время развивается экспериментальная математика: открытие новых математических закономерностей путем компьютерной обработки большого числа примеров. Такой подход не столь убедителен, как короткое доказательство, но может быть убедительнее длинного, сложного доказательства и в некоторых случаях вполне приемлем. В прошлом данную концепцию отстаивали и Дьердь Пойа [2, 13], и Лакатос[1] [14], убежденные сторонники эвристических методов и квазиэмпирической природы математики.

Экспериментальной математике посвящены книги [15, 16]. Методы экспериментальной математики в естественно-научных дисциплинах, в первую очередь в физике, применяются и обосновываются в книге «Новый вид науки» Стивена Вольфрама [17].

Компьютеры иногда позволяют получить неформальные аргументы в пользу того или иного предположения, а иногда, наоборот, опровергнуть казавшиеся правдоподобными гипотезы. Компьютерные вычисления также поставляют первичную информацию, позволяющую обнаруживать новые свойства изучаемых объектов и выдвинуть новые гипотезы.

Можно ли компьютер использовать более существенным образом, а именно полностью поручить ему весь процесс доказательства математического результата?

Аксиоматический метод открывает для этого некоторые возможности. Формальное доказательство, в конечном счете, есть последовательность формул, получаемых из аксиом по чисто синтаксическим правилам. Поэтому в принципе для этого можно использовать компьютер. Но большинство полезных математических теорий являются неразрешимыми, т. е. для таких теорий не существует алгоритма, который нашел бы доказательство для теоремы. Что компьютер может — это постепенно в результате процесса вычисления порождать всё новые утверждения, выводимые в данной формальной системе, и этот процесс потенциально никогда не заканчивается. Так как мы не можем заранее знать, встретится или нет в этом перечислении интересующий нас результат, мы не можем рассчитывать и на построение его формального доказательства за конечное время.

Тем не менее некоторые рутинные части повседневной работы математиков очень хотелось бы отдать компьютеру. Но вот то, как это сделать, представляет собой значительную техническую проблему, которая связана не только с развитием математики и исследованиями логических теорий, но также и с развитием определенных компьютерных технологий.

Приблизительно лет пятнадцать-двадцать назад развитие компьютерных технологий достигло такого уровня, когда стало возможно всерьез надеяться на создание систем, которые действительно могли бы помочь работе математика при построении и проверке математических доказательств, то есть фактически взять на себя

[1] Имре Лакатос (1922–1974 гг.) — английский философ венгерского происхождения.

часть его интеллектуальной работы. На данный момент эта область очень быстро развивается, и существует больше десятка различных систем, предназначенных для автоматического и полуавтоматического, то есть интерактивного, доказательства теорем. Для этих систем появилось специфическое название theorem prover (система поиска вывода, «прувер») [18].

Пруверы делятся на два класса: автоматические (automated theorem prover), которые ищут доказательства совершенно независимо от человека, и интерактивные (proof-assistant = interactive theorem prover), которые взаимодействуют с человеком; он помогает компьютеру находить эти доказательства. Интерактивные системы наиболее перспективны для формализации реальных математических доказательств. На основе этих систем были уже получены полностью формализованные доказательства целого ряда знаменитых математических результатов.

Пример 7.16

Теорема Жордана о кривой. Если J — простая замкнутая кривая в $\mathbf{R}^2$, то $\mathbf{R}^2 \backslash J$ имеет две компоненты («внутреннюю» и «внешнюю») с J в качестве общей границы [19].

В 2005 году были независимо созданы два формальных доказательства этой теоремы с помощью пруверов HOL Light и Mizar [20].

Пример 7.17

Теорема Гёделя о неполноте (см. главу 2, параграф 2.3). Формализованные доказательства этой теоремы были созданы в 1986 году с помощью системы Nqthm [21] и в 2003 году с помощью системы Coq [22].

Пример 7.18

Теорема о распределении простых чисел [23]. Было формализовано два известных доказательства этой теоремы: в 2005 г. с помощью прувера Isabelle и в 2009 г. с помощью прувера HOL Light [24].

В предыдущих примерах были получены компьютерные доказательства теорем, для которых были уже известны неформальные доказательства. Но компьютеры уже применяются и там, где без них не удается провести доказательства. Расскажем об первом крупном результате, для доказательства которого был применен компьютер.

Теорема о четырех красках

Что такое теорема о четырех красках? Она долгое время была недоказанной математической гипотезой и состояла в том, что каждую карту на плоскости можно раскрасить правильным образом в четыре цвета. «Правильным образом» — это означает, что разные страны на этой карте, если они имеют общий участок границы, должны быть покрашены в разные цвета. Если исключить некоторые патологические ситуации, то хорошие карты на плоскости в соответствии с этой теоремой о четырех красках всегда можно раскрасить в четыре цвета.

Впервые эту гипотезу высказал один любитель математики по фамилии Гутри (Francis Guthrie) в 1852 г. Первые доказательства были предложены Кемпе (Alfred Kempe) в 1879 г. и Томасом (Peter Thomas) в 1880 г. Через 10 лет были найдены ошибки в обоих доказательствах.

Эта известная математическая гипотеза оставалась недоказанной в течение более ста лет. Первое доказательство этой гипотезы было получено с помощью компьютеров американскими математиками Аппелем и Хакеном в 1976 г. [25].

Аппель и Хакен свели доказательство этого результата к перебору более 1476 различных графов и проверки для них некоторого условия на компьютере.

Само сведение к более тысячи случаев было далеко не тривиальным и в общем занимало 400 страниц, т. е. это был очень сложный математический результат, сопровождаемый еще сложным компьютерным перебором, потребовавшим 1000 часов машинного времени.

Как математическое сообщество отнеслось к такому доказательству? Согласно традиционным представлениям, прочно утвердившимся в XX веке, смысл опубликованного доказательства некоторой задачи заключается в том, чтобы каждый математик мог прочесть доказательство, оценить его обоснованность, если нужно — проверить доказательство, высказать свои сомнения и возражения, если они у него есть. Только после того как опубликованное доказательство прошло подобное испытание среди математического сообщества, оно считается окончательно признанным.

Не все математики признали теорему о четырех красках доказанной, как раз из-за использования компьютера. Возражения были следующего рода.

Как найти ошибку в доказательстве, проведенном компьютером? Как можно понять такое доказательство, оценить его смысл и те связи, которые оно выявляет между различными сторонами исследуемой математической модели? Разобраться в деталях чужой сложной программы практически невозможно. Компьютеру придется просто доверять.

Во-первых, компьютер мог дать сбой при вычислениях. Даже если результат проверен несколько раз, это лишь повышает вероятность правильности доказательства, но не сделает его абсолютно надежным.

Во-вторых, в процессоре и вспомогательных программах (компиляторе, библиотеках и т. п.) могут содержаться (и даже наверняка содержатся) ошибки и невозможно полностью исключить их влияние на правильность доказательства.

И, наконец, самое главное: программа, которая была написана для поиска или проверки доказательства, тоже может содержать ошибки. Строго математически убедиться в том, что она в полной мере соответствует спецификации, настолько же сложно, как и проверить вручную выполненное с ее помощью доказательство (а возможно, и сложнее).

И проблемы с этим доказательством действительно начались, но они оказались не в компьютерной части, а в человеческой. В доказательстве были найдены недочеты. В начале 1980-х годов Ульрих Шмидт исследовал доказательство Аппеля и Хакена и обнаружил пропуски в математической части доказательства.

В 1989 году Аппель и Хакен напечатали дополненное и исправленное доказательство теоремы [26]. Все обнаруженные Шмидтом пропуски вариантов были устранены, были исправлены и прочие ошибки, найденные другими математиками. К доказательству был приложен полный текст программы.

Вслед за этим известные специалисты по теории графов Робертсон, Сандерс, Сеймур и Томас, упростили доказательство Аппеля и Хакена и свели эту задачу к перебору 633 случаев, причем ими был найден более эффективный по времени алгоритм проверки условия [27]. Тем не менее без помощи компьютера добиться решения этой проблемы не удавалось.

И по-прежнему, поскольку компьютер участвовал в этом процессе, у математиков не было доверия к полученному решению. После этого за дело взялись специалисты по формальной математике, потому что было понятно, что здесь как раз тот случай, когда построение полностью формализованного и проверенного (как говорят в таких случаях, «верифицированного») доказательства теоремы может спасти положение и убедить всех в ее корректности. А такую верификацию можно также было сделать только с помощью компьютера.

В 2004 году группа французских ученых под руководством Жоржа Гонтье полностью формализовала с помощью системы интерактивного поиска вывода Coq компьютерную часть на основе доказательства Робертсона и его соавторов. Работа включает как верификацию содержательного сведения, так и компьютерного перебора. Фактически была написана верифицированная в Coq программа перебора (и не нужно было вводить 633 случая от руки) [28].

Прежде чем обсудить надежность компьютерного доказательства, остановимся на надежности человеческого доказательства. Современная математика переживает кризис переусложненности: доказательства стали настолько длинными и сложными, что ни один ученый не взял бы на себя смелость однозначно подтвердить или оспорить их правильность. Например, доказательство двух гипотез Бернсайда из теории конечных групп занимает около пятисот страниц каждое. Понятно, что такой длины сложный текст, конечно, может содержать ошибки.

Человек может прочитать чужое доказательство и проверить, правильное оно или нет. Но если вы читаете чужое достаточно длинное доказательство и в нем есть ошибка, то есть все шансы, что вы ее не заметите. Почему? В первую очередь потому, что раз сам автор доказательства сделал эту ошибку — значит, она психологически обоснована. То есть он не просто так ее сделал, по случайности — это в принципе такое место, где типичный человек может сделать такую ошибку. Значит, и вы можете сделать ту же самую ошибку, читая это место и соответственно ее не заметив.

И вот с этой проблемой — найти ошибку в записанном людьми математическом тексте, — становится все труднее справиться, а иногда и вообще невозможно — это серьезная проблема современной математики.

Насколько надежны компьютерные доказательства? Л. Беклемишев[1] считает, что достаточно надежны. Приведем его аргументы.

1. Степень надежности зависит от прувера, его интерфейса и внутренней архитектуры. Абсолютной надежности (по целому ряду не зависящих друг от друга причин) не гарантирует ни один прувер. Несмотря на это, в целом компьютерные доказательства намного надёжнее всего остального.
2. Идеальное техническое решение основывается на принципе де Брейна (de Bruijn), который состоит в следующем.
   - В основе прувера лежит логическое ядро — формальная аксиоматическая система, в которой записываются логические выводы. Логическое ядро должно быть обозримым — достаточно малым и простым. Например, аксиоматика Пеано и Цермело—Френкеля удовлетворяет этому условию.
   - Прувер — который в принципе может быть сколь угодно сложной системой, — в результате работы конструирует явный формальный вывод в языке своего ядра.
   - Верификатор (независимо от прувера) проверяет корректность данного вывода на соответствие правилам ядра.
   - Простота ядра гарантирует простоту верификатора. Более того, каждый желающий может сам написать свой собственный верификатор и убедиться в корректности каждого конкретного формального доказательства.
3. Надежность доказательства определяется только надежностью ядра и верификатора. Остальные части прувера не влияют на правильность доказательства. Такое построение системы дает лучшую гарантию надежности, чем любые другие методы, в том числе традиционное «ручное» доказательство теорем.

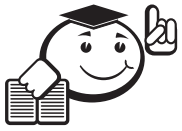
Для формального доказательства теоремы о четырех красках Ж. Гонтье с коллегами верифицировали как содержательную часть доказательства, сведение к перебору, так и формально доказали корректность алгоритма той программы, которая осуществляла перебор. В этом было принципиальное отличие их работы от предыдущих доказательств этой теоремы: компьютерное вычисление было снабжено компьютерным же доказательством его корректности. Конечно, это был успех, потому что формальные верифицированные математические доказательства имеют гораздо большую надежность, чем любое сколько-нибудь объемное доказательство, полученное человеком.

Таким образом, теорему о четырех красках, при всей ее громоздкости, можно считать на данный момент одним из наиболее тщательно проверенных и надежно установленных математических результатов [29].

[1] Лев Дмитриевич Беклемишев (р. 1967 г.) — российский математик, доктор физико-математических наук. Имеет работы в области математической логики.

Контрольные вопросы по главе 7

1. У математиков-профессионалов иногда при доказательстве каких-то теорем встречается фраза «предположим для простоты». Что это означает: а) автор может сделать то, что требуется, и без упрощения, но щадит читателя; б) автор должен был упростить задачу, чтобы он сам мог ее решить?
2. Попробуйте разобраться, в чем заключается ошибка при доказательстве софизма: «Единица — самое большое натуральное число».
3. В чем заключается математическая индукция по построению?
4. О чем говорит теорема дедукции?
5. Какие формы доказательств не используются при компьютерных доказательствах?



Рекомендуемая литература к главе 7

[1] Деза Е. И. Специальные числа натурального ряда : учеб. пособие / Е. И. Деза. — М. : Книжный дом «ЛИБРОКОМ», 2011. — 240 с.

[2] Пойа Д. Математика и правдоподобные рассуждения / Д. Пойа. — 3-е изд. — М. : Книжный дом «ЛИБРОКОМ», 2010. — Т. 1, 2. — 464 с.

[3] Дэвенпорт Г. Высшая арифметика: Введение в теорию чисел. : пер. с англ. / Г. Дэвенпорт. — 2-е изд. — М. : Книжный дом «ЛИБРОКОМ», 2010. — 176 с.

[4] Смаллиан Р. Вовеки неразрешимое. Путь к Гёделю через занимательные загадки / Р. Смаллиан. — М. : Канон, 2013. — 303 с.

[5] Клини С. К. Введение в метаматематику / С. К. Клини. — 2-е изд., испр. — М. : Книжный дом «ЛИБРОКОМ», 2009. — 528 с.

[6] Пойа Д. Как решать задачу : пер. с англ. / Д. Пойа. — 4-е изд. — М. : Книжный дом «ЛИБРОКОМ», 2010. — 208 с.

[7] Непейвода Н. Н. Основания программирования [Электронный ресурс] / Н. Н. Непейвода, И. Н. Скопин. — Москва-Ижевск : НИЦ «Регулярная и хаотическая динамика». — 2003. — 913 с. — URL : http://ulm.uni.udm.ru/~nnn/ (дата обращения: 08.05.2015).

[8] Непейвода Н. Н. Прикладная логика : учеб. пособие / Н. Н. Непейвода. — 2-е изд., испр. и доп. — Новосибирск : Изд-во Новосиб. ун-та, 2000. — 512 с.

[9] Манин Ю. И. Доказуемое и недоказуемое / Ю. И. Манин. — М. : Мир ; Советское радио, 1979. — 168 с.

[10] Харди Г. Г. Апология математики / Г. Г. Харди. — Ижевск : НИЦ «Регулярная и хаотическая динамика», 2000. — 104 с.

[11] Успенский В. А. Апология математики / В. А. Успенский. — СПб. ; Амфора, 2009. — 554 с.

[12] WolframMathematica [Электронный ресурс]. — URL : http://www.wolfram.com/mathematica/ (дата обращения: 08.05.2015).

[13] Пойа Д. Математическое открытие: Решение задач: основные понятия, изучение и преподавание / Д. Пойа. — 3-е изд. — М. : КомКнига, 2010. — 448 с.

[14] Лакатос И. Доказательства и опровержения: Как доказываются теоремы / И. Лакатос. — 2-е изд. — М. : Изд.-во ЛКИ, 2010. — 152 с.

[15] Bailey D. Mathematics by Experiment: Plausible Reasoning in the 21st Century / D. Bailey. — Wellesley, MA: A K Peters, 2003.

[16] Borwein J. Experimentation in Mathematics / J. Borwein, D. Bailey, R. Gkgensohn. — Wellesley, MA: A K Peters, 2003. — 358 p.

[17] Wolfram S. A New Kind of Science / S. Wolfram. — Champaign, Illinois: Wolfram Media, Inc., 2002. — 1197 p.

[18] Wiedijk F. (ed): The Seventeen Provers of the World // Lecture Notes in Artificial Intelligence. — 2006. — Vol. 3600.

[19] Спеньер Э. Алгебраическая топология / Э. Спеньер. — М. : Мир, 1971. — 680 с.

[20] Hales Thomas C. The Jordan curve theorem, formally and informally // The American Mathematical Mounthly. — 2007. — Vol. 114 (10). — P. 882–894.

[21] Shankar N. Metamathematics, Machines and Gödel's Proof // Cambridge tracts in theoretical computer science. — 1994. — Vol. 38.

[22] O'Connor R. Essential Incompleteness of Arithmetic Verified by Coq // Lecture Notes in Computer Science. — 2005. — Vol. 3603. — P. 245–260.

[23] Дербишир Д. Простая одержимость. Бернхард Риман и величайшая нерешенная проблема в математике / Д. Дербишир. — М. : Астрель, 2010. — 464 с.

[24] Harrison J. Formalizing an analytic proof of the Prime Number Theorem // Journal of Automated Reasoning. — 2009. — Vol. 43. — P. 243–261.

[25] Appel K. The Solution of the Four-Color Map Problem / K. Appel, W. Haken // Sci. Amer. — 1977. — Vol. 237. — P. 108–121.

[26] Appel K. Every Planar Map is Four-Colorable // K. Appel, W. Haken // Amer. Math. Soc. — 1989.

[27] A New Proof of the Four Colour Theorem. Electron. Res. Announc / N. Robertson [and others] // Amer. Math. Soc. — 1996. — N 2. — P. 17–25.

[28] Gonthier G. Formal Proof — The Four-Color Theorem // Notices of the American Mathematical Society. — 2008. — Vol. 55 (11). — P. 1382–1393.

[29] Wilson R. Four Colors Suffice: How the Map Problem Was Solved / R. Wilson. — Princeton, NJ: PrincetonUniversityPress, 2004.

[30] Кострикин А. И. Введение в алгебру : В 3-х ч. Ч. I: Основы алгебры. — М. : МЦНМО, 2009. — 272 с.

Глава 8

АЛГОРИТМЫ И ВЫЧИСЛИМЫЕ ФУНКЦИИ

Удобства — это вопрос жизни и смерти математической дисциплины.

Владимир Босс

8.1 Понятие алгоритма и неформальная вычислимость

Под ***алгоритмом*** понимается способ преобразования представления информации. Слово «*algorithm*» — произошло от имени аль-Хорезми — автора известного арабского учебника по математике (от его имени произошли также слова «алгебра» и «логарифм»).

Интуитивно говоря, алгоритм — некоторое формальное предписание, действуя согласно которому, можно получить решение задачи.

Алгоритмы типичным образом решают не только частные задачи, но и классы задач. Подлежащие решению частные задачи, выделяемые по мере надобности из рассматриваемого класса, определяются с помощью параметров. Параметры играют роль исходных данных для алгоритма.

Основные особенности алгоритма

Определенность. *Алгоритм разбивается на отдельные шаги (этапы), каждый из которых должен быть простым и локальным.*

Ввод. *Алгоритм имеет некоторое (быть может, равное нулю) число входных данных, т. е. величин, заданных ему до начала работы.*

Вывод. *Алгоритм имеет одну или несколько выходных величин, т. е. величин, имеющих вполне определенное отношение к входным данным.*

***Детерминированность**. После выполнения очередного шага алгоритма однозначно определено, что делать на следующем шаге.*

Обратите внимание, что мы не требуем, чтобы алгоритм заканчивал свою работу для любых входных данных.

Примеры алгоритмов широко известны: изучаемые в школе правила сложения и умножения десятичных чисел или, скажем, алгоритмы сортировки массивов. Для алгоритмически разрешимой задачи всегда имеется много различных способов ее решения, т. е. различных алгоритмов.

Данное здесь определение алгоритма не является, конечно, строгим, но оно интуитивно кажется вполне определенным. К сожалению, для решения некоторых задач не существует алгоритма. Установление таких фактов требует введения строгого понятия алгоритма.

Мы будем рассматривать алгоритмы, имеющие дело только с натуральными числами. Можно доказать, что это не является потерей общности, так как объекты другой природы можно закодировать натуральными числами. Для пользователей компьютеров такое утверждение должно быть очевидным.

*Пусть **N** обозначает множество натуральных чисел* $\{0, 1, 2, \ldots\}$. *Объекты, которые мы будем рассматривать, будут функциями с областью определения* $D_f \subseteq \mathbf{N}^k$ *(k — целое положительное число) и с областью значений* $R_f \subseteq \mathbf{N}$. *Такие функции будем называть **k-местными частичными**. Слово «частичная» должно напомнить о том, что функция определена на подмножестве* $\mathbf{N}^k$ *(конечно, в частном случае может быть* $D_f = \mathbf{N}^k$, *тогда функция называется **всюду определенной**).*

Назовем k-местную функцию $f: \mathbf{N}^k \to \mathbf{N}$ ***вычислимой**, если существует алгоритм A, её вычисляющий, т. е. такой алгоритм A, что:*

1. *Если на вход алгоритма A поступил вектор* $\boldsymbol{x} = \langle x_1, x_2, \ldots, x_k \rangle$ *из* D_f, *то вычисление должно закончиться после конечного числа шагов и выдать* $f(\boldsymbol{x})$.
2. *Если на вход алгоритма A поступил вектор* $\boldsymbol{x}$, *не принадлежащий области определения* D_f, *то алгоритм A никогда не заканчивается.*

Несколько замечаний по поводу этого определения.

1. Понятие вычислимости определяется здесь для частичных функций (областью определения которых является некоторое подмножество натурального ряда). Например, нигде не определенная функция вычислима, в качестве A надо взять программу, которая всегда зацикливается.
2. Можно было бы изменить определение, сказав так: «если $f(\boldsymbol{x})$ не определено, то либо алгоритм A не останавливается, либо останавливается, но ничего не печатает на выходе». На самом деле от этого ничего бы не из-

менилось (вместо того, чтобы останавливаться, ничего не напечатав, алгоритм может зацикливаться).

3. Входами и выходами алгоритмов могут быть не только натуральные числа, но и двоичные строки (слова в алфавите $\{0, 1\}$), конечные последовательности слов и вообще любые, как говорят, «конструктивные объекты».
4. Множество вычисляемых функций мы не отождествляем с множеством «практически вычисляемых» функций, так как не накладываем на первое множество никаких ограничений, связанных с современными вычислительными машинами. Хотя каждое входное натуральное число должно быть конечным, тем не менее не предполагается верхняя граница размера этого числа, так, например, количество цифр числа может быть больше числа электронов во Вселенной. Точно так же нет никакой верхней границы на число шагов, которые может сделать алгоритм для конкретных $\boldsymbol{x}$ из области определения.

Рассматривая теорию алгоритмов, мы можем ссылаться на программистский опыт, говоря об алгоритмах, программах, интерпретаторах и т. д. Это позволяет нам игнорировать детали построения тех или иных алгоритмов под тем предлогом, что читатель их легко восстановит (или хотя бы поверит). Но в некоторых случаях этого недостаточно, поэтому мы собираемся дать строгое определение нового множества функций, которое в некотором смысле будет совпадать с множеством вычислимых функций. Мы дадим две формализации понятия вычислимой функции.

8.2 Частично рекурсивные функции

Мы познакомились с неформальными определениями алгоритма и вычислимой функции. Но для математического изучения этих понятий вычислимость следует формализовать. В 30-е годы XX века и позже было предложено несколько точных определений понятия алгоритма и вычислимой функции. Опишем подход Гёделя и Клини[1] (рис. 8.1), предложенный ими в 1936 г.

Рис. 8.1 – Стивен Клини

Основная идея состояла в том, чтобы получить все вычислимые функции из существенно ограниченного множества базисных функций с помощью простейших алгоритмических средств.

Множество *исходных* функций таково:

- постоянная функция $0(\boldsymbol{x}) = 0$;
- одноместная функция следования $s(x) = x + 1$;
- функция проекции pr_i, $1 \leqslant i \leqslant k$, $pr_i(\boldsymbol{x}) = x_i$.

[1] Стивен Коул Клини (1909–1994 гг.) — американский математик, логик.

Нетривиальные вычислительные функции можно получать с помощью композиции (суперпозиции) уже имеющихся функций. Этот способ явно алгоритмический.

1. **Оператор суперпозиции**. Говорят, что k-местная функция $f(\boldsymbol{x})$ получена с помощью суперпозиции из m-местной функции $\varphi(y_1, y_2, \ldots, y_m)$ и k-местных функций $g_1(\boldsymbol{x}), g_2(\boldsymbol{x}), \ldots, g_m(\boldsymbol{x})$, если $f(\boldsymbol{x}) = \varphi\big(g_1(\boldsymbol{x}), g_2(\boldsymbol{x}), \ldots, g_m(\boldsymbol{x})\big)$.

   Второй (несколько более сложный) способ действует так.

2. **Примитивная рекурсия**. При $n \geqslant 0$ из n-местной функции f и $(n+2)$-местной функции g строится $(n+1)$-местная функция h по следующей схеме:

   - $h(\boldsymbol{x}, 0) = f(\boldsymbol{x})$,
   - $h(\boldsymbol{x}, y+1) = g\big(\boldsymbol{x}, y, h(\boldsymbol{x}, y)\big)$.

   При $n = 0$ получаем (a — константа):

   - $h(0) = a$;
   - $h(y+1) = g\big(y, h(y)\big)$.

   Два упомянутых способа позволяют задать только всюду определенные функции. Частично-определенные функции порождаются с помощью третьего гёделева механизма.

3. **Оператор минимизации**. Эта операция ставит в соответствие частичной функции $f\colon \boldsymbol{N}^{k+1} \to \boldsymbol{N}$ частичную функцию $h\colon \boldsymbol{N}^k \to \boldsymbol{N}$, которая определяется так ($\boldsymbol{x} = \langle x_1, \ldots, x_k \rangle$):

   - область определения $D_h = \{\boldsymbol{x} \mid$ существует $x_{k+1} \geqslant 0$, $f(\boldsymbol{x}, x_{k+1}) = 0$ и $\langle \boldsymbol{x}, y \rangle \in D_f$ для всех $y \leqslant x_{k+1}\}$;
   - $h(\boldsymbol{x})$ = наименьшее значение y, при котором $f(\boldsymbol{x}, y) = 0$.

Оператор минимизации обозначается так: $h(\boldsymbol{x}) = \mu y\big[f(\boldsymbol{x}, y) = 0\big]$. Очевидно, что даже если f всюду определено, но нигде не обращается в 0, то $\mu y\big[f(\boldsymbol{x}, y) = 0\big]$ нигде не определено. Естественный путь вычисления $h(\boldsymbol{x})$ состоит в подсчете значения $f(\boldsymbol{x}, y)$ последовательно для $y = 0, 1, 2, \ldots$ до тех пор, пока не найдется y, обращающее $f(\boldsymbol{x}, y)$ в 0. Этот алгоритм не остановится, если $f(\boldsymbol{x}, y)$ нигде не обращается в 0.

В общих чертах роль оператора минимизации состоит во введении функций, заданных «неявно». Кроме того, минимизация позволяет вводить в вычисление перебор объектов для отыскания объекта в бесконечном семействе. Важно отметить две особенности оператора минимизации.

Выбор минимального числа y, для которого $f(\boldsymbol{x}, y) = 0$ требуется для обеспечения однозначности функции h.

Область определения функции h: на первый взгляд представляется искусственно суженной: если, скажем, $f(\boldsymbol{x}, 1) = 0$, а $f(\boldsymbol{x}, 0)$ не определено, мы считаем функцию $h(\boldsymbol{x})$ неопределенной, а не равной 1. Причина этого состоит в желании сохранить интуитивную вычислимость функции h.

Все функции, которые можно получить из базисных функций за конечное число шагов только с помощью трех указанных механизмов, называются ***частично рекурсивными****. Если функция получается всюду определенная, то тогда она называется* ***общерекурсивной****. Если функция получена без механизма минимизации, то в этом случае она называется* ***примитивно рекурсивной****.*

Любую примитивно рекурсивную функцию можно вычислить с помощью цикла в форме *for*, так как верхнюю границу для числа повторений можно указать заранее. Оператор минимизации позволяет описать функции, которые нельзя вычислить за заранее ограниченное число итераций, для вычисления их значений требуется цикл в форме *while*.

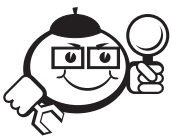
Можно легко показать [1, с. 28], что введение фиктивных переменных, а также перестановка и отождествление переменных не выводят за пределы класса примитивно рекурсивных функций и класса частично рекурсивных функций. Это проще всего объяснить на примерах.

Введение фиктивных переменных. Если $g(x_1, x_3)$ — примитивно рекурсивная функция и $f(x_1, x_2, x_3) = g(x_1, x_3)$, то $f(x_1, x_2, x_3)$ — примитивно рекурсивная функция.

Перестановка переменных. Если $g(x_1, x_2)$ — примитивно рекурсивная функция и $f(x_2, x_1) = g(x_1, x_2)$, то f есть также примитивно рекурсивная функция.

Отождествление переменных. Если $g(x_1, x_2, x_3)$ — примитивно рекурсивная функция и $f(x_1, x_2) = g(x_1, x_2, x_1)$, то $f(x_1, x_2)$ есть также примитивно рекурсивная функция.

Рассмотрим примеры частично рекурсивных функций. Все эти примеры и много других можно найти в [1, 2].



Пример 8.1

Примеры рекурсивности

Сложение двух чисел

sum: $<x, y> \to x + y$.

Эта функция является общерекурсивной в силу примитивной рекурсии

$sum(x, 0) = pr_1(x) = x$,

$sum(x, y + 1) = s\big(sum(x, y)\big) = sum(x, y) + 1$.

Считая известным частичную рекурсивность функции *sum*, легко убедиться с помощью примитивной рекурсии и композиции в частичной рекурсивности функции $(x_1, x_2, \ldots, x_n) \to x_1 + x_2 + \ldots + x_n$.

Умножение двух чисел

prod: $<x, y> \to xy$.

Используем примитивную рекурсию

$prod(x, 0) = 0(x) = 0$,

$prod(x, y + 1) = sum(prod(x, y), x)$.

Считая известным частичную рекурсивность функции *prod*, легко убедиться с помощью примитивной рекурсии и композиции в частичной рекурсивности функции $(x_1, x_2, \ldots, x_n) \to x_1 \cdot x_2 \cdot \ldots \cdot x_n$.

Усеченное вычитание 1

$\delta(x) = x - 1$, если $x > 0$,

$\delta(0) = 0$.

Эта функция примитивно рекурсивна, действительно,

$\delta(0) = 0 = 0(x)$,

$\delta(y + 1) = y = pr_2(<x, y>)$.

Усеченная разность

$x \div y = x - y$, если $x \geqslant y$,

$x \div y = 0$, если $x < y$.

Эта функция примитивно рекурсивна, действительно,

$x \div 0 = x$,

$x \div (y + 1) = \delta(x \div y)$.

Модуль разности

$|x - y| = x - y$, если $x \geqslant y$,

$|x - y| = y - x$, если $x < y$.

Эта функция примитивно рекурсивна в силу суперпозиции

$|x - y| = (x \div y) + (y \div x)$.

Факториал

Действительно,

$0! = 1$,

$(y + 1)! = prod(y!, y + 1)$.

$\min(x, y)$ — *наименьшее из чисел x и y.*

В силу суперпозиции: $\min(x, y) = x \div (x \div y)$.

Знак числа

$sg(x) = 0$, если $x = 0$,

$sg(x) = 1$, если $x > 1$.

В силу рекурсии

$sg(0) = 0$,

$sg(y + 1) = 1$.

$rm(x, y)$ — *остаток от деления y на x, если* $x \neq 0$, *и y, если* $x = 0$.

В силу рекурсии и суперпозиции

$rm(x, 0) = 0$,

$$rm(x, y + 1) = prod\Big(s\big(rm(x, y)\big),\ sg\Big(\big|x - s\big(rm(x, y)\big)\big|\Big)\Big).$$

. . . . . .

Используя функции, для которых уже установлено, что они являются частично рекурсивными, мы получаем все новые и новые частично рекурсивные функции. Существуют критерии, которые позволяют установить частичную рекурсивность сразу для обширных классов функций (см., например, [2, с. 135–150]).

Используя минимизацию (μ-оператор), можно получать частично определенные функции из всюду определенных функций.

Пример 8.2

Пусть $f(x, y)$ есть частично рекурсивная функция $|x - y^2|$, тогда $g(x) = \mu y\left[f(x, y) = 0\right]$ — не всюду определенная функция:

$$g(x) = \sqrt{x},$$

если x есть точный квадрат, и неопределенна в противном случае.

Таким образом, тривиально используя μ-оператор вместе с суперпозицией и рекурсией, можно построить больше функций, исходя из основных, чем только с помощью суперпозиции и рекурсии (так как эти операции порождают из всюду определенных функций всюду определенные). Существуют, однако, и общерекурсивные (всюду определенные) функции, для построения которых нельзя обойтись без минимизации.

Приведем пример функции, не являющейся примитивно рекурсивной, хотя и вычислимой в интуитивном смысле.

Определим последовательность одноместных функций F_n: $\mathbf{N} \to \mathbf{N}$, $n \in \mathbf{N}$, следующим образом:

$F_0(x) = x + 1$,

$F_{n+1}(x) = F_n\Big(F_n\big(\ldots F_n(1)\ldots\big)\Big)$ (F_n повторяется $x + 1$ раз).

Поэтому $F_1(x) = x + 2$, $F_2(x) = 2x + 3$, $F_3(x) = 2^{x+3} - 3$,

$F_4(x) = 2^{2^{\cdot^{\cdot^{2}}}} - 3$ (башня из $x + 3$ двойки) и т. д.

Имеем следующие свойства:

1) для каждого n функция $x \to F_n(x)$ является примитивно рекурсивной;
2) $F_n(x) > 0$;
3) $F_n(x + 1) > F_n(x)$;
4) $F_n(x) > x$;
5) $F_{n+1}(x) \geqslant F_n(x + 1)$;
6) для каждой k-местной примитивно рекурсивной функции $f(x_1, x_2, \ldots, x_k)$ существует такое n, что F_n мажорирует f, т. е.

$$f(x_1, x_2, \ldots, x_k) \leqslant F_n\big(\max(x_1, x_2, \ldots, x_k)\big)$$

для всех $x_1, x_2, \ldots, x_k$;

7) функция $A(n, x) = F_n(x)$ не является примитивно рекурсивной [3, с. 53] (эта функция известна как ***функция Аккермана***[1]).

Функцию Аккермана можно определить и в традиционной записи:

- $f(0, y) = y + 1$,

[1] Вильгельм Фридрих Аккерман (1896–1962 гг.) — немецкий математик и логик.

- $f(x+1, 0) = f(x, 1)$,
- $f(x+1, y+1) = f\big(x, f(x+1, y)\big)$.

Позднее мы приведем доводы в пользу правдоподобности того, что понятие частично рекурсивной функции есть точный математический эквивалент интуитивной идеи (эффективно) вычислимой функции.

8.3 Машины Тьюринга

Рассмотрим еще один способ определения вычислимых функций, следуя в изложении [4, с. 12–14]. Формулировка, выраженная в терминах воображаемой вычислительной машины, была дана английским математиком Аланом Тьюрингом в 1936 г. Главная трудность при нахождении этого определения была в том, что Тьюринг искал его до создания реальных цифровых вычислительных машин. Познание шло от абстрактного к конкретному: фон Нейман был знаком с работой Тьюринга, и сам Тьюринг позднее сыграл вдохновляющую роль в развитии вычислительных машин.

На неформальном уровне мы можем описывать машину Тьюринга как некий черный ящик с лентой. Лента разбита на ячейки, и каждая ячейка может содержать пустой символ 0 либо непустой символ 1. Лента потенциально бесконечна в обе стороны в том смысле, что мы никогда не придем к ее концу, но в любое время лишь конечное число ячеек может быть непустым. В начале лента содержит числа входа, в конце — число-выход. В промежуточное время лента используется как пространство памяти для вычисления.

Если мы откроем черный ящик, то обнаружим, что он устроен очень просто. В любой момент времени он может обозревать лишь одну ячейку памяти. Устройство содержит конечный список инструкций (или *состояний*) $q_0, q_1, \ldots, q_n$. Каждая инструкция может указать два возможных направления действий; одного нужно придерживаться, если на обозреваемой ячейке ленты находится 0, а другого — если там находится 1. В любом случае следующее действие может состоять из таких трех типов элементарных шагов:

- символ (возможно, такой же, как старый) пишется на обозреваемой ячейке ленты, при этом предыдущий символ стирается;
- лента сдвигается на одну ячейку влево или вправо;
- указывается следующая инструкция.

Таким образом, список инструкций определяет некоторую функцию перехода, которая по данной инструкции и обозреваемому символу указывает три компоненты того, что нужно делать. Мы можем формализовать эти идеи, взяв в качестве машины Тьюринга эту функцию перехода.

Машина Тьюринга *— это функция M, такая, что для некоторого натурального числа n область определения этой функции есть подмножество множества* $\{0, 1, \ldots, n\} \times \{0, 1\}$*, а область значений есть подмножество множества* $\{0, 1\} \times \{Л, П\} \times \{0, 1, \ldots, n\}$.

Например, пусть $M(3, 1)$ = <0, Л, 2>. Подразумеваемый смысл этого состоит в том, что как только машина дойдет до инструкции q_3, а на обозреваемой ячейке написан символ 1, она должна стереть 1 (оставляя на ячейке 0), передвинуть ленту так, чтобы обозреваемой ячейкой стала левая соседняя ячейка от той, которая обозревалась, и перейти к следующей инструкции q_2. Если $M(3, 1)$ не определено, тогда как только машина дойдет до инструкции q_3, а на обозреваемой ячейке написан символ 1, то машина останавливается. (Это единственный путь остановки вычисления.)

Такая подразумеваемая интерпретация не включена в формальное определение машины Тьюринга, но она мотивирует и подсказывает формулировки всех следующих определений. В частности, можно определить, что означает для машины M передвижение (за один шаг) от одной конфигурации до другой. Нам не нужно здесь давать формальных определений, так как они являются простыми переводами наших неформальных идей.

Входные и выходные данные — это строчки из 1, разделенные 0. Пусть $<n>$ будет строчкой из 1 длины $n + 1$. Тогда

$$<n_1>\ 0\ <n_2>\ 0\ \ldots\ 0\ <n_k>$$

получено комбинацией k строчек из 1, каждая отделена от другой 0.

Наконец, мы можем определить вычислимость.

Пусть $D_f \subseteq \mathbf{N}^k$ — область определения k-местной функции f: $D_f \to \mathbf{N}$. Функция f называется ***вычислимой по Тьюрингу****, если существует машина Тьюринга M, такая, что как только M начинает с инструкции q_0, обозревая самой левый символ строки*

$$<n_1>\ 0\ <n_2>\ 0\ \ldots\ 0\ <n_k>,$$

(вся остальная часть ленты пуста), тогда:

- *если $f(n_1, n_2, \ldots, n_k)$ определено, то M, в конце концов, остановится, обозревая самый левый символ строки $<f(n_1, n_2, \ldots, n_k)>$, при этом часть, находящаяся справа от этой строчки, пустая;*
- *если $f(n_1, n_2, \ldots, n_k)$ не определено, то M никогда не останавливается.*

Заметим, что имеется бесконечное множество машин Тьюринга, для каждой вычислимой функции своя. Более того, для любой вычислимой функции имеется бесконечное множество машин Тьюринга, вычисляющих эту функцию.

Пример 8.3

Построим машину Тьюринга, вычисляющую сумму $n_1 + n_2$. Зададим функцию M следующим образом:

$M(0, 1) = <1, П, 0>$;
$M(0, 0) = <1, П, 1>$;
$M(1, 1) = <1, П, 1>$;
$M(1, 0) = <0, Л, 2>$;
$M(2, 1) = <0, Л, 3>$;
$M(3, 1) = <0, Л, 4>$;
$M(4, 1) = <1, Л. 4>$;
$M(4, 0) = <0, П, 5>$.

Посмотрим, как происходит сложение 1 + 1. В текущей строке символов обозреваемый символ выделен.

Номер инструкции	Текущая строка символов	Комментарий
0	0***1***10110	Прохождение через первое слагаемое
0	01***1***0110	
0	011***0***110	Заполнение промежутка
1	0111***1***10	Прохождение через второе слагаемое
1	01111***1***0	
1	0111110	Конец второго слагаемого
2	01111***1***0	Стирание 1
3	0111***1***00	Стирание второй 1
4	011***1***000	Движение назад
4	01***1***1000	
4	0***1***11000	
4	0111000	Остановка
5	0***1***11000	

Мы должны заметить, что многие детали нашего определения машины Тьюринга до некоторой степени произвольны. Если бы было более одной ленты, то класс вычислимых функций остался бы неизменным, хотя некоторые функции могли бы быть вычислены более быстро. Аналогично, мы могли бы допускать больше символов, чем 0 и 1, или же у нас могла бы быть лента, бесконечная только в одну сторону от начальной точки, вместо имеющейся бесконечной в обоих направлениях. Ни одно из этих изменений не затрагивает класса вычислимых функций. Что действительно существенно в этом определении — это разрешение произвольно большого количества материала для запоминающего устройства и произвольно длинных вычислений.

8.4 Тезис Чёрча

За последние 70 лет было предложено много различных математических уточнений интуитивного понятия алгоритма. Два из этих подходов мы разобрали. Перечислим некоторые другие альтернативные способы, которые предлагались следующими авторами:

- Ламбда-исчисление Чёрча [5] — представляет класс (частичных) функций (λ-определимые функции), который характеризует неформальное понятие вычислимой функции.
- Гёдель—Эбран—Клини. Общерекурсивные функции, определенные с помощью исчисления рекурсивных уравнений [2, с. 261–278].
- Пост. Функции, определяемые каноническими дедуктивными системами [3, с. 66–72].
- Марков. Функции, задаваемые некоторыми алгоритмами (известные под названием «нормальные алгоритмы») над конечным алфавитом [6].
- Шепердсон—Стерджис. МНР-вычислимые функции [3].

Между этими подходами (в том числе и двумя рассмотренными выше) имеются большие различия; каждый из них имеет свои преимущества для соответствующего описания вычислимости. Следующий замечательный результат получен усилиями многих исследователей.

Теорема 1 (основной результат) [3, с. 57]. Каждое из вышеупомянутых уточнений вычислимости приводит к одному и тому же классу вычислимых функций.

Вопрос: насколько хорошо неформальное и интуитивное понятие вычислимой функции отражено в различных формальных описаниях?

Чёрч, Тьюринг и Марков, каждый в соответствии со своим подходом, выдвинули утверждение (тезис) о том, что класс определенных ими функций совпадает с неформально определенным классом вычислимых функций. В силу основного результата все эти утверждения логически эквивалентны.

А. Чёрч был первым, кто осознал, что одно конкретное и, казалось бы, весьма специальное определение может адекватно отражать основополагающее понятие алгоритма. Название «*тезис Чёрча*» теперь применяется к этим и аналогичным им утверждениям.

***Тезис Чёрча**. Интуитивно и неформально определенный класс вычислимых функций совпадает с классом частично-рекурсивных функций.*

Здесь мы встретились с таким редким в математике объектом, как тезис. Что же это такое? Это не теорема, ибо тезис Чёрча не имеет доказательства. Это не гипотеза, ибо он и не может быть доказан. Это даже не аксиома, которую мы вольны

принимать или не принимать. Всё это так из-за того, что тезис Чёрча не является точным математическим утверждением, ибо он связывает строгое понятие вычислимости с нестрогим понятием вычислимости в интуитивном смысле.

Тезис скорее является утверждением, которое принимается на веру, причем вера подкрепляется следующими аргументами [3, с. 75–76]:

- Фундаментальный результат: многие независимые инварианты уточнения интуитивного понятия вычислимости привели к одному и тому же классу функций.
- Обширное семейство вычислимых функций принадлежит этому классу. Конкретные функции, рассмотренные в параграфе 8.2 главы 8, образуют исходную часть этого семейства, которую можно расширять до бесконечности методами из параграфа 8.2 главы 8 или более мощными и сложными методами.
- Никто еще не нашел функцию, которую можно было признать вычислимой в неформальном смысле, но которую нельзя было бы построить, используя один из формальных методов.

> . . .Найти задачу — не меньшая радость, чем отыскать решение.
>
> *Томас де Куинси*

> — Это же проблема Бен Бецалеля. Калиостро же доказал, что она не имеет решения. . . Как же искать решения, когда его нет? Бессмыслица какая-то. . .
>
> — Бессмыслица — искать решение, если оно и так есть. Речь идет о том, как поступать с задачей, которая решения не имеет.
>
> *А. и Б. Стругацкие. Понедельник начинается в субботу*

8.5 Некоторые алгоритмически неразрешимые проблемы

Решение вопроса о том, обладают ли натуральные числа данным свойством, является часто встречающейся задачей математики. Поскольку свойства чисел можно выразить с помощью подходящего предиката, то решение задачи сводится к выяснению того, является ли данный предикат ***разрешимым*** или нет (т. е. существует ли алгоритм, который позволил бы распознать, является ли предикат истинным или ложным; см. параграф 5.1 главы 5). Задачи с произвольными универсумами во многих случаях можно переформулировать в виде задач с натуральными числами, если использовать подходящее кодирование. В контексте разрешимости предикаты часто называются ***проблемами***.

Имея точное определение вычислимости, удалось доказать, что некоторые проблемы неразрешимы. Как мы уже знаем (глава 6, теорема 11), Алонзо Чёрч доказал, что не существует алгоритма, который для любой формулы логики предикатов устанавливает, общезначима она или нет.

Теорема 2. Проблема остановки неразрешима.

Этот результат, доказанный впервые независимо друг от друга Тьюрингом (используя машины Тьюринга) и Чёрчем (с помощью ламбда-исчисления) точно формулируется в следующем виде.

Не существует никакого общего алгоритма, позволяющего установить, остановится ли некоторая конкретная программа (на любом языке программирования), запущенная после введения в неё некоторого конкретного набора данных. Смысл этого утверждения для теоретического программирования очевиден: не существует совершенно общего метода проверки программ на наличие в них бесконечных циклов.

С использованием аналогичных идей получены и следующие результаты о неразрешимости. Не существует никакого общего алгоритма, позволяющего установить, вычисляет ли некоторая конкретная программа (на любом языке программирования) постоянную нулевую функцию [3, с. 110]. То же самое справедливо и для любой другой конкретной вычислимой функции. И как следствие, можно утверждать, что вопрос о том, вычисляют ли две данные программы одну и ту же одноместную функцию, также неразрешим. Тем самым получаем, что в области тестирования компьютерных программ мы имеем принципиальные ограничения.

Диофантовы уравнения

Пусть $p(z_1, \ldots, z_n)$ — полином с целыми коэффициентами типа

$$p(z_1, z_2) = z_1^5 - 4z_1z_2^3 + 32.$$

Диофантовы уравнения $p(z_1, \ldots, z_n) = 0$ подразумевают решение в целых числах. Первым диофантовые уравнения систематизировал и изучил греческий математик Диофант в третьем веке нашей эры. Ниже приводится пример системы диофантовых уравнений:

$$\begin{cases} 6w + 2x^2 - y^3 = 0, \\ 5xy - z^2 + 6 = 0, \\ w^2 - w + 2x - y + z - 4 = 0. \end{cases}$$

Вот еще один пример:

$$\begin{cases} 6w + 2x^2 - y^3 = 0, \\ 5xy - z^2 + 6 = 0, \\ w^2 - w + 2x - y + z - 3 = 0. \end{cases}$$

Решением первой системы является, в частности, следующее:

$$w = 1,\ x = 1,\ y = 2,\ z = 4,$$

тогда как вторая система вообще не имеет решения. В самом деле, судя по первому уравнению, число y должно быть четным, судя по второму уравнению, число z также должно быть четным, однако это противоречит третьему уравнению, причем при любом w, поскольку значение разности $w^2 - w$ — это всегда четное число, а число 3 нечетно.

Со времени Диофанта специалисты по теории чисел нашли решения огромного количества диофантовых уравнений и установили отсутствие решений у массы других уравнений, однако при этом для разных классов уравнений или даже отдельных уравнений приходилось изобретать свой особый метод.

В 1900 году на Парижском международном математическом конгрессе Давид Гильберт выступил с докладом, в котором перечислил 23 наиболее сложные, по его мнению, не решенные на тот момент математические проблемы. В 10-й проблеме предлагалось найти универсальный метод для распознавания разрешимости диофантовых уравнений.

После 20-летних усилий многих математиков советский математик Ю. Матиясевич в 1970 году доказал:

Теорема 3 (отрицательное решение 10-й проблемы Гильберта). Существует такой полином $P(x_1, x_2, \ldots, x_k)$, что неразрешимость уравнения

$$P(x_1, x_2, \ldots, x_k) - y = 0$$

по $x_1, x_2, \ldots, x_k$ при любом положительном y алгоритмически непроверяема.

Для таких полиномов можно указать следующие значения (суммарной) степени n и числа m переменных x: ($n = 9$, $m \approx 1{,}6 \cdot 10^{45}$), (58,4), (38,2), (32,12), (24,36), (19,2668).

Контрольные вопросы по главе 8

1. Почему медицинские и кулинарные рецепты во многих случаях нельзя рассматривать как алгоритмы?
2. Покажите, что функция $rm(x, y)$ из параграфа 8.2 главы 8 действительно вычисляет остаток от деления.
3. Существует ли примитивно-рекурсивная функция для вычисления неполного частного при делении с остатком натуральных чисел?
4. Тезис Чёрча говорит о вычислимых функциях. Справедливо ли аналогичное утверждение об алгоритмах?
5. Существует ли какое-нибудь ограниченное множество программ, для которых проблема остановки разрешима?

Рекомендуемая литература к главе 8

[1] Манин Ю. И. Вычислимое и невычислимое / Ю. И. Манин. — М. : Советское радио, 1980. — 128 с.

[2] Мендельсон Э. Введение в математическую логику / Э. Мендельсон. — М. : Наука, 1976. — 320 с.

[3] Катленд Н. Вычислимость. Введение в теорию рекурсивных функций : пер. с англ. / Н. Катленд. — М. : Мир, 1983. — 256 с.

[4] Справочная книга по математической логике : в 4 ч. : пер. с англ. / под ред. Дж. Барвайса. — М. : Наука, 1982. — Ч. 3: Теория рекурсии. — 360 с.

[5] Барендрегт Х. Ламбда-исчисление. Его синтаксис и семантика / Х. Барендрегт. — М. : Мир, 1985. — 606 с.

[6] Марков А. А. Теория алгоритмов // Труды Мат. ин-та АН СССР. — 1954. — Т. 42.

Глава 9

СЛОЖНОСТЬ ВЫЧИСЛЕНИЙ

Применение математики во многих приложениях требует, как правило, использования различных алгоритмов. Для решения многих задач нетрудно придумать комбинаторные алгоритмы, сводящиеся к полному перебору вариантов. Но здесь вступает в силу различие между математикой и информатикой: в информатике недостаточно высказать утверждение о существовании некоторого объекта в теории и даже недостаточно найти конструктивное доказательство этого факта, т. е. алгоритм. Мы должны учитывать ограничения, навязываемые нам миром, в котором мы живем: необходимо, чтобы решение можно было вычислить, используя объем памяти и время, приемлемые для человека и компьютера.

Если дана задача, как найти для её решения эффективный алгоритм? А если алгоритм найден, как сравнить его с другими алгоритмами, решающими ту же задачу? Как оценить его качество? Вопросы такого рода интересуют и программистов, и тех, кто занимается теоретическим исследованием вычислений.

9.1 Асимптотические обозначения

Введем в первую очередь обозначение, связанное с асимптотической оценкой функций. Хотя во многих случаях эти обозначения используются неформально, полезно начать с точных определений (см. [1] или [2]).

Пусть даны две функции $f(n)$ и $g(n)$ натурального аргумента n, значениями которого являются положительные действительные числа. Говорят, что функция g ***мажорирует*** функцию f (или «f растет не быстрее g»), если существует действительное положительное число c и натуральное число n_0, такое, что $f(n) \leqslant cg(n)$ для всех $n \geqslant n_0$. Если g мажорирует f, это обозначается как $f(n) = O\big(g(n)\big)$. Символ $O\big(g(n)\big)$ читается как «O ***большое от*** $g(n)$»; при этом говорят, что $f(n)$ имеет порядок O большое от $g(n)$. Также говорят, что функция g является асимптотически верхней оценкой для функции f.

Другими словами, $f = O(g)$ означает, что отношение $f(n)/g(n)$ ограничено сверху некоторой константой.

Пример 9.1

Проверим, что $(1/2)n^2 - 3n = O(n^2)$. Согласно определению надо указать положительную константу c и число n_0 так, чтобы неравенство

$$\frac{n^2}{2} - 3n \leqslant cn^2$$

выполнялось для всех $n \geqslant n_0$. Разделим на n^2:

$$\frac{1}{2} - \frac{3}{n} \leqslant c.$$

Видно, что для выполнения неравенства достаточно положить $c = 1/2$ и $n_0 = 1$.

Пример 9.2

При $a > 0$ можно записать $an + b = O(n^2)$ (положим, $c = a + |b|$ и $n_0 = 1$).

Пример 9.3

Покажем, что $6n^3 \neq O(n^2)$. В самом деле, пусть найдутся такие c и n_0, что $6n^3 \leqslant cn^2$ для всех $n \geqslant n_0$. Но тогда $n \leqslant c/6$ для всех $n \geqslant n_0$, что невозможно.

Определение $O\big(g(n)\big)$ предполагает, что функции $f(n)$ и $g(n)$ асимптотически неотрицательны, т. е. неотрицательны для достаточно больших значений n. Заметим, что если f и g строго положительны, то можно исключить n_0 из определения (изменив константу c так, чтобы для малых n неравенство также выполнялось).

Отыскивая асимптотически верхнюю оценку для суммы, мы можем отбрасывать члены меньшего порядка, которые при больших n становятся малыми по сравнению с основным слагаемым. Заметим также, что коэффициент при старшем члене роли не играет (он может повлиять только на выбор константы c). Например, рассмотрим квадратичную функцию $f(n) = an^2 + bn + d$, где a, b и d — некоторые константы и $a > 0$. Отбрасывая члены младших порядков и коэффициент при старшем члене, находим, что $f(n) = O(n^2)$. Чтобы убедиться в этом формально, можно положить $c = 3 \times \max(a, b, d)$ и $n_0 = 1$.

Упомянем важный частный случай использования O-обозначений: $O(1)$ обозначает ограниченную сверху функцию.

Обозначение $O(\cdot)$ можно считать аналогом $\leqslant$. Аналоги для $\geqslant$ и $=$ также существуют: $f(n) = \Omega\big(g(n)\big)$ (f растет не медленее g, с точностью до константы) означает $g(n) = O\big(f(n)\big)$; $f(n) = \Theta\big(g(n)\big)$ (f и g имеют одинаковый порядок роста) означает что $f(n) = O\big(g(n)\big)$ и $g(n) = O\big(f(n)\big)$.

Работая с символами O, Ω и Θ, мы имеем дело с *односторонними* равенствами — эти символы могут стоять только справа от знака $=$.

Отношение «O большое» для функций обладает рефлексивностью и транзитивностью: $f(n) = O\big(f(n)\big)$, $f(n) = O\big(g(n)\big)$ и $g(n) = O\big(h(n)\big)$ влечет $f(n) = O\big(h(n)\big)$. Очевидно, такие же свойства у отношений $f(n) = \Omega\big(g(n)\big)$ и $f(n) = \Theta\big(g(n)\big)$, но последнее еще симметрично.

Рассмотрим отношение «O большое» для сравнения асимптотического роста конкретных функций.

Для положительных целых чисел r и s следующую теорему можно доказать методом индукции. Справедливость утверждения теоремы для положительных рациональных чисел r и s можно показать, не используя логарифмы.

Теорема 1. Если r и s — действительные числа, $r \leqslant s$ и $n > 1$, тогда $n^r \leqslant n^s$. Следовательно, $n^r = O(n^s)$.

Доказательство. Функция $\ln(x)$ — возрастающая, поэтому $a \leqslant b$ тогда и только тогда, когда $\ln(a) \leqslant \ln(b)$. Отсюда $n^r \leqslant n^s$ тогда и только тогда, когда $\ln(n^r) \leqslant \ln(n^s)$, что, в свою очередь, выполняется тогда и только тогда, когда $r\ln(n) \leqslant s\ln(n)$, т. е. тогда и только тогда, когда $r \leqslant s$, поскольку $\ln(n)$ для $n > 1$ — величина положительная.

Следующие теоремы показывают, что свойство функции иметь порядок $O\big(g(n)\big)$ замкнуто относительно операций сложения и умножения на число.

Теорема 2. Если $f(n) = O\big(g(n)\big)$, то $kf(n) = O\big(g(n)\big)$.

Доказательство. По определению, $f(n) \leqslant cg(n)$ для некоторого положительного действительного числа c и всех $n \geqslant n_0$. Поэтому

$$kf(n) \leqslant ckg(n)$$

и $cf(n) = O\big(g(n)\big)$.

Теорема 3. Если $f(n) = O\big(g(n)\big)$ и $h(n) = O\big(g(n)\big)$, то $(f + h)(n) = O\big(g(n)\big)$.

Доказательство. По определению, для некоторого постоянного k и некоторого целого числа m_1 имеем $f(n) \leqslant kg(n)$ для всех $n > m_1$. Опять же по определению, для некоторого постоянного l и некоторого целого числа m_2 имеем $h(n) \leqslant lg(n)$ для всех $n > m_2$. Пусть $m = \max(m_1, m_2)$. Следовательно, для всех $n > m$

$$f(n) + h(n) \leqslant kg(n) + lg(n) = (k + l)g(n)$$

и $(f + g)(n) = O\big(g(n)\big)$.

Теорема 4. Если $f(n) = O\big(g(n)\big)$ и $h(n) = O\big(e(n)\big)$, то $(f \times h)(n) = O(g \times e)(n)$.

Доказательство. По определению, для некоторого постоянного k и некоторого целого числа m_1 имеем $f(n) \leqslant kg(n)$ для всех $n > m_1$. Опять же по определению, для некоторого постоянного l и некоторого целого числа m_2 имеем $h(n) \leqslant le(n)$ для всех $n > m_2$. Пусть $m = \max(m_1, m_2)$. Следовательно, для всех $n > m$

$$f(n) \times h(n) \leqslant kg(n)le(n) = (kl)g(n) \times e(n)$$

и $(f \times g)(n) = O(g \times e)(n)$.

Следующая теорема устанавливает мажоранту для полинома.

Теорема 5.

Если $p(n) = a_k n^k + a_{k-1} n^{k-1} + \ldots + a_1 n + a_0$, то $p(n) = O(n^k)$.

Доказательство.

$$p(n) \leqslant |a_k n^k + a_{k-1} n^{k-1} + \ldots + a_1 n + a_0| \leqslant$$

(в силу неравенства треугольника: $|A + B| \leqslant |A| + |B|$)

$$\leqslant |a_k n^k| + |a_{k-1} n^{k-1}| + \ldots + |a_1 n| + |a_0| =$$

$$= |a_k| n^k + |a_{k-1}| n^{k-1} + \ldots + |a_1| n + |a_0| \leqslant \text{ (по теореме 1)}$$

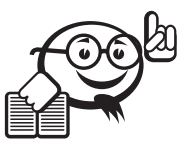
$$\leqslant |a_k| n^k + |a_{k-1}| n^k + \ldots + |a_1| n^k + |a_0| n^k = (|a_k| + |a_{k-1}| + \ldots + |a_1| + |a_0|) n^k$$

и $p(n) = O(n^k)$.

Теорема 6. Для целых чисел a и b, больших единицы, $\log_a(n) = O\big(\log_b(n)\big)$.

Доказательство. Следует непосредственно из равенства

$$\log_a(n) = \frac{\log_b(n)}{\log_a(b)}.$$



Теорема 7. Пусть n — неотрицательное целое число. Тогда $n < 2^n$ и, следовательно, $n = O(2^n)$.

Доказательство. Воспользуемся индукцией, имея для $n = 0$, $0 < 2^0 = 1$. Допустим, что $k < 2^k$, тогда

$$k + 1 \leqslant k + k \leqslant 2^k + 2^k = 2^{k+1}$$

и, по индукции, $n < 2^n$.

Следующие теоремы дают ответ на вопрос о том, какие функции могут выступать в роли мажорант для других функций.

Теорема 8. Для целых чисел a, больших единицы, $\log_a(n) = O(n)$.

Доказательство. Согласно теореме 7 имеет место неравенство $n < 2^n$. Поэтому $\log_2(n) < \log_2(2^n) = n$ и $\log_2(n) = O(n)$. Поскольку по теореме 6 имеем $\log_a(n) = O\big(\log_2(n)\big)$, то по транзитивности получаем $\log_a(n) = O(n)$.

Теорема 9. Пусть n — неотрицательное целое число, тогда $n! < n^n$ и, следовательно, $n! = O(n^n)$.

Теорема 10. Пусть $a > 1$ и n — неотрицательное целое число, тогда $\log_a(n!) \leqslant n \log_a(n)$ и, следовательно, $\log_a(n!) = O\big(n \log_a(n)\big)$.

Благодаря введенной символике мы можем заменить $7n^2 + 3n + 1$ на $\Theta(n)$, пренебрегая остальными слагаемыми. Вот несколько общих правил такого рода замен:

1. Постоянные множители можно опускать. Например, $\pi n^2 + \varepsilon n^3$ можно заменить на n^3.
2. Любая экспонента растет быстрее любого полинома. Так, например, 2^n растет быстрее n^{1000}.
3. Любой полином растет быстрее любого логарифма. Например, n (и даже $\sqrt{n}$) растет быстрее $(\log n)^3$.

Покажем теперь, как мы можем использовать O-обозначения для оценки количества определенных действий в алгоритмах.

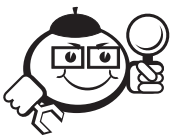
Пример 9.4

Определим число арифметических операций, необходимых для сложения двух матриц.

Пусть матрицы имеют размеры $m \times k$. Тогда алгоритм сложения матриц $A + B = C$ можно описать на Паскале следующим образом:

```
for i := 1 to m do
    for j := 1 to k do
        C[i, j] := A[i, j] + B[i, j];
```

Как видим, сложение выполняется для каждого i и каждого j. Поскольку i принимает m значений, а j принимает k значений, то выполняется mk операций сложения. Пусть $n = \max(m, k)$. Тогда число выполняемых арифметических операций имеет порядок $O(n^2)$.



Пример 9.5

Определим число арифметических операций, необходимых для умножения двух матриц.

Пусть матрицы A и B имеют размеры $m \times p$ и $p \times k$ соответственно. Тогда алгоритм умножения матриц $A \times B = C$ можно описать на Паскале следующим образом:

```
for i := 1 to m do
    for j := 1 to k do
        begin
        C[i,j] := 0;
        for s := 1 to p do
            C[i, j] := C[i, j] + A[i, s] * B[s, j];
        end;
```

Поскольку s принимает значения от 1 до p, то выполняется p операций сложения и p операций умножения. Величина s изменяется от 1 до p для каждого i и каждого j, поэтому s пробегает значения от 1 до pmk раз. Таким образом, выполняется mkp операций сложения и столько же операций умножения. Следовательно, всего выполняется $2mkp$ операций. Пусть $n = \max(m, k, p)$. Тогда число выполняемых арифметических операций имеет порядок $O(n^3)$.

Пример 9.6

Сравним количество операций, которое требуется для непосредственного вычисления значения многочлена традиционным способом и по схеме Горнера.

Пусть требуется вычислить $p(c)$, где $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$. Если $p(c)$ вычисляется непосредственно, то для подсчета c^k требуется выполнить $k - 1$ операций умножения. Еще одна операция нужна для умножения на a_k, так что вычисление $a_k x^k$ требует k операций умножения. Таким образом, нужно выполнить $1 + 2 + \ldots + n = n(n-1)/2$ умножений. Для того чтобы найти сумму $n + 1$ слагаемых, требуется выполнить n сложений, так что общее число арифметических операций равно $n(n-1)/2 + n$ и имеет порядок $O(n^2)$.

При вычислении полинома $a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ по схеме Горнера мы переписываем полином в виде $x \cdot \Big(x \cdot \big(x \cdot (a_4x + a_3) + a_2\big) + a_1\Big) + a_0$ и замечаем, что выражение включает четыре операции умножения и четыре операции сложения. Очевидно, в общем случае

$$p(x) = x \cdot \Big(x \cdot \big(\ldots\big(x \cdot (a_n x + a_{n-1}) + a_{n-2}\big) + \ldots a_2\big) + a_1\Big) + a_0$$

включает n операций сложения и n операций умножения. Таким образом, общее число арифметических операций равно $2n$ и имеет порядок $O(n)$.

9.2 Алгоритмы и их сложность

Класс однородных вычислительных задач мы будем называть ***проблемой*** (также используется понятие «***массовая задача***» или «***абстрактная задача***»). Индивидуальные случаи проблемы Q мы будем называть ***частными случаями*** проблемы Q. Мы можем, например, говорить о проблеме умножения матриц. Частные случаи этой проблемы суть пары матриц, которые нужно перемножить.

Более формально мы принимаем следующую абстрактную модель вычислительной задачи. Абстрактная задача есть произвольное бинарное отношение Q между элементами двух множеств — множества ***условий*** (или входных данных) I и множества ***решений*** S. Например, в задаче умножения матриц входными данными являются две конкретные матрицы-сомножители, а матрица-произведение является решением задачи. В задаче поиска кратчайшего пути между двумя заданными вершинами некоторого неориентированного графа[1] $G = (V, E)$ условием (элементом I) является тройка, состоящая из графа и двух вершин, а решением (элементом S) — последовательность вершин, составляющих требуемый путь в графе. При этом один элемент множества I может находиться в отношении Q с несколькими элементами множества S (если кратчайших путей между данными вершинами несколько).

Нам бы хотелось связать с каждым частным случаем проблемы некоторое число, называемое его ***размером***, которое выражало бы меру количества входных данных. Например, размером задачи умножения матриц может быть наибольший размер матриц-сомножителей. Размером задачи о графах может быть число ребер данного графа.

Решение задачи на компьютере можно осуществлять с помощью различных алгоритмов. Прежде чем подавать на вход алгоритма исходные данные (т. е. элемент множества I), надо договориться о том, как они представляются «в понятном для компьютера виде»; мы будем считать, что исходные данные закодированы последовательностью битов. Формально говоря, ***представлением*** элементов некоторого множества M называется отображение e из M во множество битовых строк. Например, натуральные числа 0, 1, 2, 3,… обычно представляют битовыми строками 0, 1, 10, 11, 100,… (при этом, например, $e(17) = 10001$).

Фиксировав представление данных, мы превращаем абстрактную задачу в ***строковую***, для которой входным данным является битовая строка, представляющая исходное данное абстрактной задачи. Естественно считать размером строковой задачи длину строки.

*Будем говорить, что алгоритм A **решает** строковую задачу за **время** $O(T(n))$, если на входном данном битовой строки длины n алгоритм работает время $O(T(n))$. Будем называть оценку $O(T(n))$ **асимптотической временной сложностью** алгоритма A.*

[1] О графах смотрите, например [3].

В качестве временной оценки работы алгоритма вместо общего числа шагов мы можем подсчитывать число шагов некоторого вида, таких как арифметические операции при алгебраических вычислениях, число сравнений при сортировке или число обращений к памяти.

Можно подумать, что колоссальный рост скорости вычислений, вызванный появлением нынешнего поколения компьютеров, уменьшит значение эффективных алгоритмов. Однако происходит в точности противоположное. Так как компьютеры работают все быстрее и мы можем решать все большие задачи, именно сложность алгоритма определяет то увеличение размера задачи, которое можно достичь с увеличением скорости машины.

Следуя [4], рассмотрим это более подробно. Допустим, у нас есть пять алгоритмов $A_1, A_2, \ldots, A_5$ с временными сложностями соответственно: $O(n)$, $O(n\log n)$, $O(n^2)$, $O(n^3)$, $O(2^n)$.

Пусть единицей времени будет 1 мс и мультипликативные константы в точных оценках временной сложности во всех алгоритмах равны 1. Тогда алгоритм A_1 может обработать за 1 с вход размера 1000, в то время как A_5 — вход размера не более 9. В таблице 9.1 приведены размеры задач, которые можно решить за 1 с, 1 мин и 1 ч каждым из этих пяти алгоритмов.

Таблица 9.1 – Границы размеров задач, определяемые скоростью роста сложности

Алгоритм	**Асимптотическая временная сложность**	**Максимальный размер задачи**		
		1 с	1 мин	1 ч
A_1	$O(n)$	1000	6×10^4	$3{,}6 \times 10^6$
A_2	$O(n\log n)$	140	4893	$2{,}0 \times 10^5$
A_3	$O(n^2)$	31	244	1897
A_4	$O(n^3)$	10	39	153
A_5	$O(2^n)$	9	15	21

Предположим, что следующее поколение компьютеров будет в 10 раз быстрее нынешнего. В таблице 9.2 показано, как возрастут размеры задач, которые мы сможем решить благодаря этому увеличению скорости.

Таблица 9.2 – Эффект десятикратного ускорения

Алгоритм	**Асимптотическая временная сложность**	**Максимальный размер задачи**	
		до ускорения	**после ускорения**
A_1	$O(n)$	S_1	$10S_1$
A_2	$O(n\log n)$	S_2	Примерно $10S_2$ для больших S_2
A_3	$O(n^2)$	S_3	$3{,}16S_3$
A_4	$O(n^3)$	S_4	$2{,}15S_4$
A_5	$O(2^n)$	S_5	$S_5 + 3{,}3$

Заметим, что для алгоритма A_5 десятикратное увеличение скорости увеличивает размер задачи, которую можно решить, только на три, тогда как для алгоритма A_3 размер задачи более чем утраивается.

Вместо эффекта увеличения скорости рассмотрим теперь эффект применения более действенного алгоритма. Вернемся к таблице 9.1. Если в качестве основы для сравнения взять 1 мин, то, заменяя алгоритм A_4 алгоритмом A_3, можно решить задачу в 6 раз большую, а заменяя A_4 на A_2, можно решить задачу, большую в 125 раз. Эти результаты производят гораздо большее впечатление, чем двукратное улучшение, достигаемое за счет десятикратного увеличения скорости. Если в качестве основы для сравнения взять 1 ч, то различие оказывается еще значительнее. Отсюда мы заключаем, что асимптотическая скорость алгоритма служит важной мерой качественности алгоритма, причем такой мерой, которая обещает стать еще важнее при последующем увеличении скорости вычислений.

Несмотря на то, что основное внимание здесь уделяется порядку роста величин, надо понимать, что больший порядок сложности алгоритма может иметь меньшую мультипликативную постоянную, чем малый порядок роста сложности другого алгоритма. В таком случае алгоритм с быстро растущей сложностью может оказаться предпочтительнее для задач с малым размером — возможно, даже для всех задач, которые нас интересуют.

9.3 Сложность задач

Сложность задачи *— это асимптотическая временная сложность наилучшего алгоритма, известного для ее решения.*

Основной вопрос теории сложности: насколько успешно или с какой стоимостью может быть решена заданная проблема Q? Мы не имеем в виду никакого конкретного алгоритма решения Q. Наша цель — рассмотреть все возможные алгоритмы решения Q и попытаться сформулировать утверждение о вычислительной сложности, внутренне присущей Q. В то время как всякий алгоритм A для Q дает верхнюю оценку величины сложности Q, нас интересует нижняя оценка. Знание нижней оценки представляет интерес математически и, кроме того, руководит нами в поиске хороших алгоритмов, указывая, какие попытки заведомо будут безуспешны.

Быстрыми являются линейные алгоритмы, которые обладают сложностью порядка $O(n)$, где n — размерность входных данных. К линейным алгоритмам относится школьный алгоритм нахождения суммы десятичных чисел, состоящих из n_1 и n_2 цифр. Сложность этого алгоритма — $O(n_1+n_2)$. Есть алгоритмы, которые быстрее линейных, например алгоритм двоичного поиска в линейном упорядоченном массиве имеет сложность $O(\log n)$, где n — длина массива.

Другие хорошо известные алгоритмы — деление, извлечение квадратного корня, решение систем линейных уравнений и др. — попадают в более общий класс полиномиальных алгоритмов.

Полиномиальным алгоритмом (или алгоритмом полиномиальной временной сложности, или алгоритмом принадлежащим классу ***P***) называется алгоритм, у которого временная сложность равна $O(n^k)$, где k — положительное целое число. Алгоритмы, для временной сложности которых не существует такой оценки, называются ***экспоненциальными***, и такие задачи считаются ***труднорешаемыми***. Понятие

полиномиально разрешимой задачи принято считать уточнением идеи «практически разрешимой» задачи. Чем объясняется такое соглашение?

Во-первых, используемые на практике полиномиальные алгоритмы обычно действительно работают довольно быстро. Конечно, трудно назвать практически разрешимой задачу, которая требует времени $\Theta(n^{100})$. Однако полиномы такой степени в реальных задачах почти не встречаются.

Второй аргумент в пользу рассмотрения класса полиномиальных алгоритмов — тот факт, что объем этого класса не зависит от выбора конкретной модели вычислений (для достаточно широкого класса моделей) [5]. Например, класс задач, которые могут быть решены за полиномиальное время на последовательной машине с произвольным доступом (RAM), совпадает с классом задач, полиномиально разрешимых на машинах Тьюринга. Класс будет тем же и для моделей параллельных вычислений, если, конечно, число процессоров ограничено полиномом от длины входа.

В-третьих, класс полиномиально разрешимых задач обладает естественными свойствами замкнутости. Например, композиция двух полиномиальных алгоритмов (выход первого алгоритма подается на вход второго) также работает полиномиальное время. Объясняется это тем, что сумма, произведение и композиция многочленов снова есть многочлен.

Приведем примеры классификации задач по их сложности.

Класс *P*

- Рассортировать множество из n чисел. Сложность поведения в среднем порядка $O(n\log n)$ для быстрого алгоритма Хоара [1, с. 198–219].
- Найти эйлеровый цикл на графе из m ребер. В силу теоремы Эйлера мы имеем необходимое и достаточное условие для существования эйлерова цикла и проверка этого условия есть алгоритм порядка $O(m)$.
- Задача Прима—Краскала. *Дана плоская страна и в ней n городов. Нужно соединить все города телефонной связью так, чтобы общая длина телефонных линий была минимальной*. В терминах теории графов задача Прима—Краскала выглядит следующим образом: *Дан граф с n вершинами; длины ребер заданы матрицей* $(d[i,j])$, $i,j = 1,\ldots,n$. *Найти остовное дерево минимальной длины*. Эта задача решается с помощью жадного алгоритма сложности $O(n\log n)$ [1, с. 644–661].
- Кратчайший путь на графе, состоящем из n вершин и m ребер. Сложность алгоритма $O(mn)$ [2, с. 105–120].
- Связные компоненты графа. Определяются подмножества вершин в графе (связные компоненты), такие, что две вершины, принадлежащие одной и той же компоненте, всегда связаны цепочкой дуг. Если n — количество вершин, а m — количество ребер, то сложность алгоритма $O(n+m)$ [6, с. 364–365].
- Быстрое преобразование Фурье [2, с. 61–74], требующее $O(n\log n)$ арифметических операций, — один из наиболее часто используемых алгоритмов в научных вычислениях.
- Умножение целых чисел. Алгоритм Шёнхаге—Штрассена [4, с. 304–308]. Сложность алгоритма порядка $O(n\log n\log\log n)$. Отметим, что школьный

метод для умножения двух n-разрядных чисел имеет сложность порядка $O(n^2)$.

- Умножение матриц. Алгоритм Штрассена [2, с. 60] имеет сложность порядка $O(n^{\log 7})$ для умножения двух матриц размера $n \times n$. Очевидный алгоритм имеет порядок сложности $O(n^3)$.
- Тест на простоту натурального числа. Алгоритм *AKS* (Агравал, Кайл и Саксен — авторы алгоритма, [7, с. 228–242]) имеет сложность порядка $O(\log^{7,5} n)$, где n — количество цифр в числе.

Класс *E*: задачи, экспоненциальные по природе

К экспоненциальным задачам относятся задачи, в которых требуется построить множество всех подмножеств данного множества, все полные подграфы некоторого графа или же все поддеревья некоторого графа.

Существует масса примеров задач с экспоненциальной сложностью. Например, чтобы вычислить $2^{(2^k)}$ для заданного натурального k, нам только для записи конечного ответа потребуется около 2^n шагов (где n — число цифр в двоичной записи k), не говоря даже о самом вычислении.

Задачи, не попадающие ни в класс *P*, ни в класс *E*

На практике существуют задачи, которые заранее не могут быть отнесены ни к одному из рассмотренных выше классов. Хотя в их условиях не содержатся экспоненциальные вычисления, однако для многих из них до сих пор не разработан эффективный (т. е. полиномиальный) алгоритм.

К этому классу относятся следующие задачи:

- задача о выполнимости: существует ли для данной булевской формулы такое распределение истинностных значений, что она имеет значение «истина»;
- задача коммивояжера (Коммивояжер хочет объехать все города, побывав в каждом ровно по одному разу, и вернуться в город, из которого начато путешествие. Известно, что переезд из города i в город j стоит $c(i, j)$ руб. Требуется найти путь минимальной стоимости.);
- решение диофантовых систем уравнений;
- составление расписаний, учитывающих определенные условия;
- размещение обслуживающих центров (телефон, телевидение, срочные службы) для максимального числа клиентов при минимальном числе центров;
- оптимальная загрузка емкости (рюкзак, поезд, корабль, самолёт) при наименьшей стоимости;
- оптимальный раскрой (бумага, картон, стальной прокат, отливки), оптимизация маршрутов в воздушном пространстве, инвестиций, станочного парка;
- факторизация — разложение натурального числа на множители [7, с. 254–288].

Заметим, что все эти задачи весьма важны с точки зрения приложений. Поэтому знание того, что полиномиальные алгоритмы для них не найдены, помогут не тратить время на безуспешные поиски точных эффективных алгоритмов, а сосредоточить усилия на создании приближенных или эвристических алгоритмов.

Контрольные вопросы по главе 9

1. Останется ли справедливой теорема 6, если символ O заменить символом Θ?
2. Пусть функции f, g и h таковы, что $f = \Theta(h)$ и $f = \Theta(g)$. Следует ли из этого равенство $g = h$?
3. Пусть $G(n) = A(n, n)$, где $A(n, x)$ — функция Аккермана из параграфа 8.2 главы 8 и $f(n)$ — произвольная примитивно-рекурсивная функция. Справедливо ли отношение $f(n) = O\big(G(n)\big)$?
4. Полиномиально разрешимую задачу принято считать «практически разрешимой» задачей. Чем объясняется такое соглашение?
5. К какому классу задач относится задача распознания простоты натурального числа?

Рекомендуемая литература к главе 9

[1] Кормен Т. Алгоритмы: построение и анализ / Т. Кормен, Ч. Лейзерсон, Р. Ривест. — М. : МЦНМО, 2001. — 960 с.

[2] Дасгупта С. Алгоритмы / С. Дасгупта, Х. Пападимитриу, У. Вазирани. — М. : МЦНМО, 2014. — 320 с.

[3] Андерсон Д. Дискретная математика и комбинаторика / Д. Андерсон. — М. : Вильямс, 2003. — 960 с.

[4] Ахо А. Построение и анализ вычислительных алгоритмов / А. Ахо, Дж. Хопкрофт, Дж. Ульман. — М. : Мир, 1979. — 536 с.

[5] Катленд Н. Вычислимость. Введение в теорию рекурсивных функций : пер. с англ. / Н. Катленд. — М. : Мир, 1983. — 256 с.

[6] Рейнгольд Э. Комбинаторные алгоритмы. Теория и практика : пер. с англ. / Э. Рейнгольд, Ю. Нивергельт, Н. Део. — М. : Мир, 1980. — 478 с.

[7] Крэндалл Р. Простые числа: Криптографические и вычислительные аспекты / Р. Крэндалл, К. Померанс. — М. : Книжный дом «ЛИБРОКОМ», 2011. — 664 с.

ЗАКЛЮЧЕНИЕ

Это учебное пособие, по сути, является введением в математическую логику. Если Вы в дальнейшем связываете свою профессиональную деятельность с программированием, то надо прочесть дополнительную литературу.

Можно рекомендовать следующие книги:

1. Непейвода Н. Н. Прикладная логика : учеб. пособие. 2-е изд., испр. и доп. — Новосибирск: Изд-во Новосиб. ун-та, 2000. — 512 с.

Эта хорошо написанная книга дает широкий обзор тех логических областей, которые являются необходимыми в современной информатике и программировании.

2. Кормен Т., Лейзерсон Ч., Ривест Р. Алгоритмы: построение и анализ. — М. : МЦНМО, 2001. — 960 с.

Если вы хотите познакомиться с современными алгоритмами, то это книга будет очень полезна.

3. Хофштадтер Д. Гёдель, Эшер, Бах: эта бесконечная гирлянда. — Самара: Изд. дом «Бахрах-М», 2001. — 752 с.

4. Братко И. Алгоритмы искусственного интеллекта на языке PROLOG, 3-е изд.: пер. с англ. — М. : Изд. дом «Вильямс», 2004. — 640 с.

Две последние книги необходимы тем, кто интересуется различными вопросами искусственного интеллекта.

Желаю успеха!

В. М. Зюзьков

ГЛОССАРИЙ

Абсолютным дополнением множества A называется множество $\overline{A}$ всех тех элементов x, которые не принадлежат множеству A.

Антисимметричное отношение. Отношение ρ на множестве X называется антисимметричным, если для любых $x, y \in X$ из $x\rho y$ и $y\rho x$ следует $x = y$.

Бесконечное множество — такое множество X, что существует взаимно однозначное соответствие на какое-либо подмножество $Y \subset X$.

Выполнимая формула логики высказываний — это такая формула, для которой существует интерпретация, в которой эта формула истинна.

Вычислимые функции.

Назовем k-местную функцию f: $\boldsymbol{N}^k \to \boldsymbol{N}$ *вычислимой*, если существует алгоритм A, её вычисляющий, т. е. такой алгоритм A, что:

- Если на вход алгоритма A поступил вектор $\boldsymbol{x} = \langle x_1, x_2, \ldots, x_k \rangle$ из D_f, то вычисление должно закончиться после конечного числа шагов и выдать $f(\boldsymbol{x})$.
- Если на вход алгоритма A поступил вектор $\boldsymbol{x}$, не принадлежащий области определения D_f, то алгоритм A никогда не заканчивается.

Дедуктивная система какого-либо языка выделяет среди всех формул те, которые объявляются доказуемыми. Обычно доказуемость задается индуктивно при помощи аксиом и правил вывода.

Дизъюнкция. Высказывание «A или B» называется дизъюнкцией высказываний A и B и обозначается $A \vee B$.

Доказательство — это рациональный логический переход от принятой точки зрения (предпосылки) к тому рубежу, где ее необходимо обосновать или подтвердить (вывод).

Импликация. Высказывание «если A, то B» называется импликацией высказываний A и B и обозначается $A \supset B$.

Интуитивный принцип абстракции означает, что «любое характеристическое свойство $A(x)$ определяет некоторое множество X, а именно множество тех и только тех предметов x, для которых выполнено свойство $A(x)$».

Интуитивный принцип объемности означает, что «множества A и B считаются равными, если они состоят из одних и тех же элементов».

Композицией отношений $\rho \subseteq X \times Y$ и $\varphi \subseteq Y \times Z$ называется отношение $\varphi \circ \rho \subseteq X \times \times Z$, такое, что $\varphi \circ \rho = \{<x, z> \mid x \in X,\ z \in Z$ и существует $y \in Y,$ для которого $<x, y> \in \in \rho$ и $<y, z> \in \varphi\}$.

Конъюнкция. Высказывание «A и B» называется конъюнкцией высказываний A и B и обозначается $A\&B$.

Логика — наука об анализе доказательств, аргументов и установлении принципов, на основании которых могут быть сделаны надежные рассуждения.

Математическая логика — логика по предмету, математика по методу.

Множество — не определяется формально, можно представлять как любое собрание определенных и различимых между собою объектов, мыслимое как единое целое. Эти объекты называются *элементами множества* S.

Мощность континуума — мощность множества действительных чисел.

n-местное отношение — произвольное множество упорядоченных n-ок.

Обратное отношение. Пусть $\rho \subseteq X \times Y$ есть отношение на $X \times Y$. Тогда обратное отношение ρ^{-1} на $Y \times X$ для отношения ρ определяется следующим образом: $\rho^{-1} = = \{<y, x> \mid x \in X,\ y \in Y$ и $<x, y> \in \rho\}$.

Объединением множеств A и B называется множество $A \cup B$, все элементы которого являются элементами множества A или/и B.

Опровержимая формула логики высказываний — это такая формула, для которой существует интерпретация, в которой эта формула ложна.

Относительным дополнением множества A до множества X называется множество $X \backslash A$ всех тех элементов множества X, которые не принадлежат множеству A.

Отношением ρ множеств X и Y называется произвольное *подмножество* прямого произведения $X \times Y$.

Отношение принадлежности — не определяется формально, говорят, что объекты, составляющие множества, «принадлежат» этому множеству.

Отношение частичного порядка на множестве X — это рефлексивное, транзитивное и антисимметричное отношение на множестве.

Отношением эквивалентности на множестве X называется рефлексивное, симметричное и транзитивное отношение ρ на множестве X.

Отрицанием высказывания A называется высказывание $\neg A$, которое истинно тогда и только тогда, когда A ложно, и ложно в противном случае.

Парадокс — рассуждение либо высказывание, в котором, пользуясь средствами, не выходящими (по видимости) за рамки логики, приходят к заведомо неприемлемому результату, обычно к противоречию.

Пересечением множеств A и B называется множество $A \cap B$, элементы которого являются элементами обоих множеств A и B.

Подмножество — множество A есть подмножество множества B (обозначается $A \subseteq B$), если каждый элемент A есть элемент B; т. е. если $x \in A$, то $x \in B$.

Принцип математической индукции.

Пусть $P(n)$ — свойство натуральных чисел, выразимых в теории ***EA***.

Если

(1) выполнено $P(0)$ и

(2) для каждого $k \geqslant 0$ из $P(k)$ следует $P(k+1)$,

то для каждого $n \geqslant 0$ справедливо $P(n)$.

В математической индукции имеется *индуктивный базис* — утверждение, что свойство выполнено для самого маленького из рассматриваемых чисел, и *индуктивный шаг* — обоснование перехода от числа n к числу $n+1$.

Противоречие — формула логики высказываний, которая ложна во всех интерпретациях.

Равномощность — два множества называются равномощными, если между ними можно установить взаимно однозначное соответствие.

Равносильные формулы — формулы A и B называются *равносильными*, если эти формулы принимают одинаковые истинностные значения в любой интерпретации.

Рефлексивное отношение — отношение ρ на множестве X называется рефлексивным, если для любого элемента $x \in X$ выполняется $x \rho x$.

Семантическая система, или просто семантика, какого-либо языка выделяет среди всех формул этого языка те, которые объявляются истинными; говорят также, что им приписываются значения **И**. Для этого обычно используется интерпретация правильных выражений языка.

Симметрическая разность $A \Delta B$ — состоит из элементов, которые принадлежат ровно одному из множеств A и B.

Симметричное отношение — отношение ρ на множестве X называется симметричным, если для любых $x, y \in X$ из $x \rho y$ следует $y \rho x$.

Сложность задачи — это асимптотическая временная сложность наилучшего алгоритма, известного для ее решения.

Софизм (от греч. sophisma — уловка, выдумка, головоломка) — мнимое доказательство, в котором обоснованность заключения кажущаяся, порождается чисто субъективным впечатлением, вызванным недостаточностью логического или семантического анализа.

Счётное множество — множество, равномощное множеству натуральных чисел **N**.

Тавтология — формула логики высказываний, которая истинна во всех интерпретациях.

Тезис Чёрча — интуитивно и неформально определенный класс вычислимых функций совпадает с классом частично рекурсивных функций.

Транзитивное отношение — отношение ρ на множестве X называется транзитивным, если для любых $x, y, z \in X$ из $x\rho y$ и $y\rho z$ следует $x\rho z$.

Формальная теория $\boldsymbol{T}$ считается определенной, если:

- задано некоторое счетное множество $\boldsymbol{A}$ символов — символов теории $\boldsymbol{T}$; конечные последовательности символов теории $\boldsymbol{T}$ называются *выражениями* теории $\boldsymbol{T}$ (множество выражений обозначают через $\boldsymbol{A}^*$);
- имеется подмножество $\boldsymbol{F} \subset \boldsymbol{A}^*$ выражений теории $\boldsymbol{T}$, называемых *формулами* теории $\boldsymbol{T}$;
- выделено некоторое множество $\boldsymbol{B} \subset \boldsymbol{F}$ формул, называемых *аксиомами* теории $\boldsymbol{T}$;
- имеется конечное множество $\{R_1, R_2, \ldots, R_m\}$ отношений между формулами, называемых *правилами вывода*. Правила вывода позволяют получать из некоторого конечного множества формул другое множество формул.

Функция (или *отображение*) — отношение f на $X \times Y$ называется функцией (или отображением) из X в Y и обозначается через $f: X \to Y$, если для каждого $x \in X$ существует единственный элемент $y \in Y$, такой, что $<x, y> \in f$.

Частично рекурсивные функции — все функции, которые можно получить из базисных функций за конечное число шагов только с помощью суперпозиции, примитивной рекурсии и минимизации.

Эквиваленция — высказывание «A тогда и только тогда, когда B» называется эквиваленцией высказываний A и B и обозначается $A \sim B$.

ПРЕДМЕТНЫЙ И ПЕРСОНАЛЬНЫЙ УКАЗАТЕЛЬ

Учебное издание

Зюзьков Валентин Михайлович

МАТЕМАТИЧЕСКАЯ ЛОГИКА
И ТЕОРИЯ АЛГОРИТМОВ

Учебное пособие

Корректор Осипова Е. А.
Компьютерная верстка Мурзагулова Н. Е.

Подписано в печать 16.06.15. Формат 60x84/8.
Усл. печ. л. 27,44. Тираж 100 экз. Заказ

Издано в ООО «Эль Контент»
634029, г. Томск, ул. Кузнецова д. 11 оф. 17
Отпечатано в Томском государственном университете
систем управления и радиоэлектроники.
634050, г. Томск, пр. Ленина, 40
Тел. (3822) 533018.