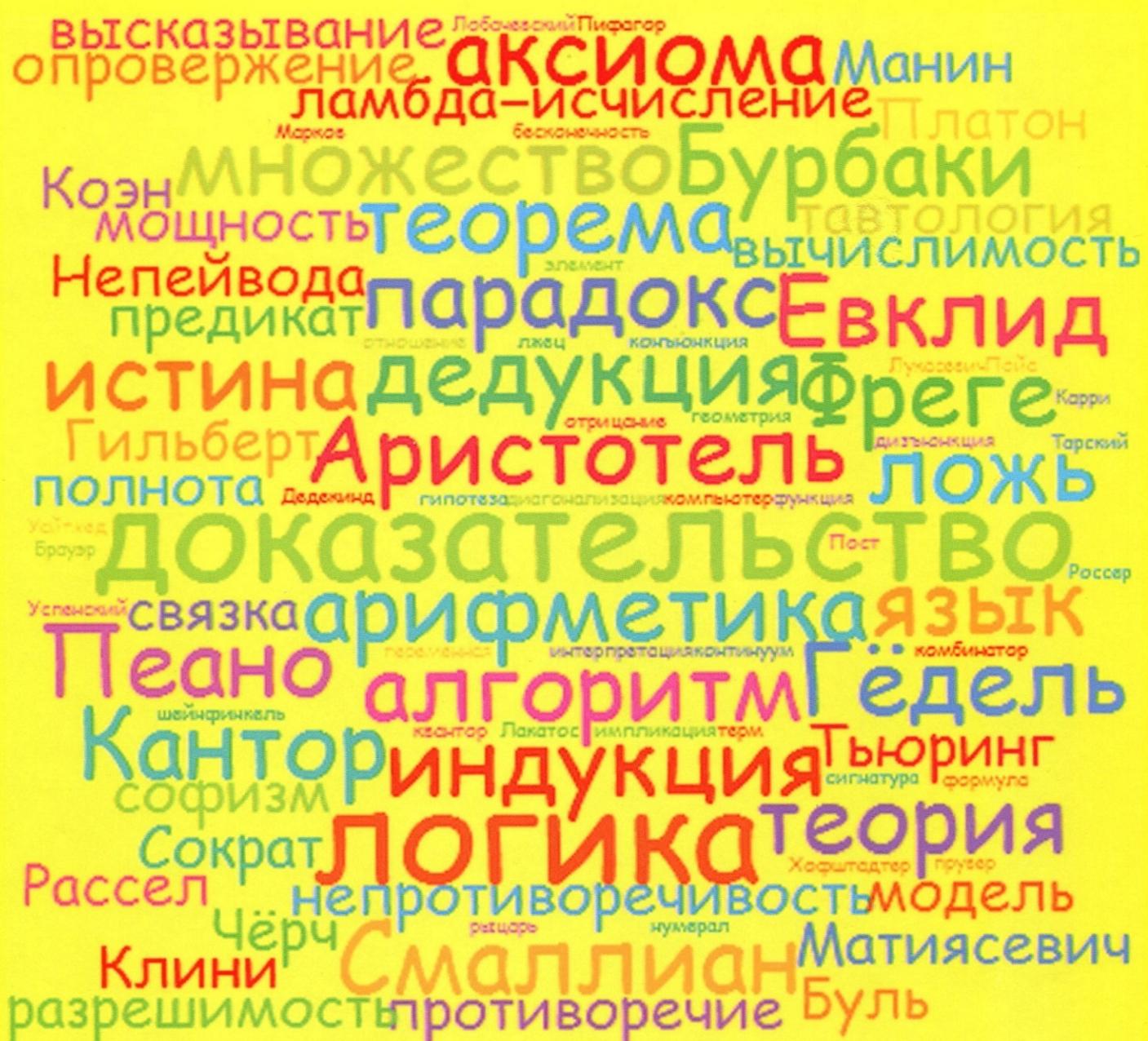


В.М. Зюзьков

ВВЕДЕНИЕ В МАТЕМАТИЧЕСКУЮ ЛОГИКУ



НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

В.М. Зюзьков

**Введение
в математическую логику**

Учебное пособие

Томск
Издательский Дом Томского государственного университета
2017

УДК 510.2+510.5+510.6

ББК 22.12я73

398

Зюзьков В.М.

398 Введение в математическую логику : учеб. пособие. – Томск : Издательский Дом Томского государственного университета, 2017. – 258 с.

ISBN 978-5-94621-617-3

Учебное пособие начинается с рассмотрения отношений между логикой, математикой, математической логикой и реальным миром. Кратко излагается история математической логики. К традиционным разделам предмета относятся: основы теории множеств, пропозициональная логика и язык предикатов, аксиоматические теории и теория вычислимости. Значительное место занимают изложение ламбда-исчисления и рассмотрение различных видов математических доказательств. Приводятся доказательства теорем Гёделя о полноте. Пособие содержит задачи, для некоторых из них приведены решения.

Для студентов математических направлений университетов, преподавателей математики и компьютерных наук высших учебных заведений.

УДК 510.2+510.5+510.6

ББК 22.12я73

Рецензент

доктор физико-математических наук, профессор *П.А. Крылов*

Оглавление

Предисловие	5
Глава 1. Миссия математической логики	6
§ 1. Логика	6
§ 2. Математика	10
§ 3. Софизмы и парадоксы	14
§ 4. Математическая логика	19
Задачи	23
Глава 2. Краткая история логики	24
§ 1. Становление логики	24
§ 2. Начало математической логики	29
§ 3. Математическая логика в своем блеске и великолепии	33
Глава 3. Основы теории множеств	41
§ 1. «Интуитивная» теория множеств	41
§ 2. Операции над множествами. Диаграммы Эйлера–Венна	43
§ 3. Отношения	49
§ 4. Эквивалентность и порядок	54
§ 5. Функции	58
§ 6. Мощность множеств	62
Задачи	69
Глава 4. Пропозициональная логика	73
§ 1. Высказывания и высказывательные формы	73
§ 2. Язык логики высказываний	80
§ 3. Тавтологии и равносильности	87
§ 4. Логическое следование	91
§ 5. Булевы алгебры	92
Задачи	97
Глава 5. Языки первого порядка	100
§ 1. Предикаты и кванторы	100
§ 2. Термы и формулы	103
§ 3. Интерпретация формул	106
§ 4. Формулы общезначимые, выполнимые и логически эквивалентные	110
§ 5. Перевод с естественного языка на логический и обратно	115
Задачи	120
Глава 6. Аксиоматические теории	123
§ 1. Предварительные понятия и простые примеры	123
§ 2. Формальные аксиоматические теории	126
§ 3. Исчисление высказываний	132
§ 4. Аксиоматизация геометрии	137
§ 5. Теории первого порядка	141
§ 6. Аксиоматика Пеано	145
§ 7. Аксиоматика Цермело–Френкеля	146
Задачи	150
Глава 7. Математическое доказательство	151
§ 1. Индукция	151
§ 2. Математическая индукция	154
§ 3. Различные виды доказательств в математике	164

§ 4. Компьютерные доказательства	172
Задачи	177
Глава 8. Неформально о вычислимости	180
§ 1. Понятие алгоритма и неформальная вычислимость	180
§ 2. Перечислимые и разрешимые множества	182
§ 3. Универсальные функции и неразрешимые множества	185
Глава 9. Формализации вычислимости	188
§ 1. Частично-рекурсивные функции	188
§ 2. Машины Тьюринга	192
§ 3. Ламбда-исчисление	195
Задачи	206
Глава 10. Алгоритмически неразрешимые проблемы	208
§ 1. Ламбда-определенные функции	208
§ 2. Тезис Чёрча и алгоритмическая неразрешимость	219
Задачи	225
Глава 11. Теоремы Гёделя о неполноте	227
§ 1. Гёделева нумерация	227
§ 2. Первая теорема Гёделя о неполноте: семантическая версия	229
§ 3. Первая теорема Гёделя о неполноте: синтаксическая версия	231
§ 4. Обобщения и вторая теорема Гёделя	234
§ 5. Теорема Гудстейна	238
Решения избранных задач	242
Задачи из главы 3	242
Задачи из главы 4	243
Задачи из главы 5	243
Задачи из главы 6	245
Задачи из главы 7	246
Задачи из главы 9	247
Задачи из главы 10	247
Литература	248
Предметный и персональный указатели	253

Книга должна быть либо ясной, либо строгой,

Совместить эти два требования невозможно.

Берtrand Рассел

Предисловие

Данное пособие написано в первую очередь для студентов-математиков. Но это не учебник в строгом смысле слова, хотя имеет многие особенности учебника, в частности присутствует много задач с решениями. Отличия от учебника – в выборе содержания и способа изложения материала.

Все рассматриваемые понятия тщательно обсуждаются с помощью большого числа примеров. Некоторые теоремы приводятся без доказательств. Для этого может быть одна из двух причин: 1) доказательство не требует дополнительных понятий и знаний сверх имеющихся в книге, но полное приведение технических деталей, кроме увеличения объема текста, не приносит никаких новых идей и «не делает читателей умнее» (см. эпиграф к главе 7); 2) требуется использование достаточно сложного материала, не входящего в книгу. В любом случае добавляется ссылка на источник с доступным доказательством.

Наиболее очевидным преимуществом такого упущения деталей является то, что эта книга способна охватить гораздо больше материала, чем если бы это был стандартный учебник того же размера. И принятое изложение текста также призвано помочь читателю сосредоточиться на панорамной картине, на основных идеях математической логики, не погрязнуть в мелочах.

Читатель, без предыдущего знания логики и теории множеств, но обучавшийся университетской математике в течение года, способен усвоить большую часть книги без обращения к внешним источникам.

Автор надеется, что книгу будут читать с удовольствием. Но она не может превратить абстрактную науку в приятное времяпрепровождение. Стремитесь получить удовольствие и от интеллектуальных усилий. Излагаются две достаточно сложные темы. Это ламбда-исчисление – одна из формализаций вычислимости, имеющая не только теоретическое значение, но и широкое практическое применение. И книга заканчивается доказательствами теорем Геделя о неполноте математики.

Читатель вправе решить, насколько слова Бертрана Рассела справедливы по отношению к данной книге.

...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

Глава 1. Миссия математической логики

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 польза от математики?

Логические и математические рассуждения нередко сопровождаются ошибками. В § 3 описываются классические софизмы и парадоксы.

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

...логика – это дама, стоящая у выхода магазина самообслуживания и проверяющая стоимость каждого предмета в большой корзинке, содержимое которой отбиралось не ею.

Дж. Пойа. Математическое открытие

§ 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 Локк¹:

«Логика есть анатомия мышления».

Джон Стюарт Милль² [84]:

«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 Кэрролл³:

«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).

¹ Джон Локк (John Locke; 1632–1704) – английский философ.

² Джон Стюарт Милль (John Stuart Mill; 1806–1873) – английский философ.

³ Льюис Кэрролл (Lewis Carroll, настоящее имя Charles Lutwidge Dodgson; 1832–1898) – английский писатель, математик, логик.

Джеймс Тёрбер⁴ [29]:

«If you can touch the clocks and never start them, then you can start the clocks and never touch them. That's logic, as I know and use it».⁵

Амброд Бирс⁶ [40]:

«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».

Берtrand Рассел⁷ [96]:

«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».

Герман Вейль⁸:

«Логика – это своего рода гигиена, позволяющая математику сохранять свои идеи здоровыми и сильными» (цит. по: [63. С. 368]).

Непейвода Н.Н.⁹ [86]:

«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 – це-

⁴ Джеймс Тёрбер (James Thurber; 1894–1961) – американский художник газетных сатирических комиксов, писатель и юморист.

⁵ Если вы можете трогать часы и никогда не завести их, то вы можете завести часы, их не трогая (перевод мой. – В.З.).

⁶ Амброд Бирс (Ambrose Bierce; 1842–1913) – американский писатель, журналист, автор юмористических и «страшных» рассказов.

⁷ Берtrand Рассел (Bertrand Russell; 1872–1970) – британский философ и математик.

⁸ Герман Вейль (Hermann Weyl; 1885–1955) – немецкий математик и физик-теоретик.

⁹ Непейвода Николай Николаевич (р. 1949) – советский и российский математик, учёный в области теоретической информатики и математической логики.

мент, скрепляющая 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: 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 (цит. по: [88. 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: **байтельрате** – 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 **латтенгиттерветтеркоттэр-байтельратте**.

Однажды в тех местах, в городе Шраттертrottэле, 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 **шраттертrottэльхоттентотенмуттераттэнтэтэр**, 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... Байтельратте? 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! – возмущался негр, положил на землю лук и стрелы, набрал в грудь воздуха и выпалил:
 - Я поймал *щраттертроттэльхомтентенмуттэрраттэнтэтэрлаттен-гиттерветтеркоттэрбейтельратте!* 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 логические 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.

Но рассуждение может быть неправильным, хотя и вывод верен, как в следующем примере.

Некоторые цветы быстро вянут.

Розы – это цветы.

Следовательно, некоторые розы быстро вянут.

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 детенышь, 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 утконос – опровергает казавшееся таким правдивым заключение. Индуктивное доказательство всегда выходит за рамки предпосылки, которая не влечет за собой обязательную истинность заключения, но предполагает его возможность. Индуктивные доказательства – это обобщения и всевозможные экстраполяции от частного к общему; от наблюданного к ненаблюданному; от прошлого и настоящего – к будущему.

Ошибки при индуктивном доказательстве могут приводить к серьезным последствиям. Г. Попов считает¹⁰, что индуктивное доказательство о классовом расколе крестьян в России, сделанное В.И. Лениным в книге «Развитие капитализма в России» на базе статистических отчетов и обследований, является ошибочным [94] (Г. Попов сообщает о характерной детали личности В.И. Ленина: он отлично владел дедукцией, но был слабым в индукции – единственная оценка «хорошо» в школьном аттестате Ленина была как раз по логике).

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

¹⁰ 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 гг.

Заботливый кредитор [111. С. 31]:

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, все правильно!

Ирландец и пиво [62. С. 39]:

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.

– Я знаю, – отзыается 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 пришлоось бросить пить.

Математик это сделает лучше.
Универсальный принцип Гуга Штейнгауза¹¹

Математик так же, как художник или поэт, создает 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 Харди¹²

§ 2. Математика

Возникновение логики как науки о дедуктивных рассуждениях связано с именем Аристотеля (384–322 гг. до н.э.)¹³. Но развитие логики по-настоящему произошло лишь в XX в., когда математика, как писал Н.Н. Непейвода, «доросла до того, чтобы применять свои мето-

¹¹ Гуга Дионисий Штейнгауз (1887–1972) – 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.

¹² Годфри Харольд Харди (Godfrey Harold Hardy; 1877–1947) – английский математик.

¹³ См. следующую главу, посвященную истории логики.

ды для анализа своей собственной структуры, и таким образом первой из наук перешла со стадии экстенсивного роста на стадию рефлексии»¹⁴.

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.

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

На наш взгляд, здесь можно полностью согласиться с мнением В.А. Успенского¹⁵. Перескажем извлечения из его работы [110].

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

Эта цель заключается не столько в сообщении знаний и даже в 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 способствовать математические занятия. Называем их в порядке возрастания важности:

- 1) умение отличать истинное от ложного (или доказанное от недоказанного);
- 2) умение отличать имеющее смысл от бессмыслицы;
- 3) 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. Она содержала правдоподобный, 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 4 500 рублей статья была принята в печать, получив положительный отзыв рецензента о том, что «статья принята с небольшими замечаниями» [58].

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 демократичная.

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

Математика обладает свойством опережать экспериментальные знания и позволяет 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 в. в движении этой планеты стали выявляться

¹⁴ Рефлексия – самоанализ, в науке – применение методов данной науки к ней самой.

¹⁵ Владимир Андреевич Успенский (р. 1930, Москва) – российский математик.

непонятные аномалии – она то «отставала» от расчетного 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 г. 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 в. существовали некоторые физические законы, полученные экспериментально: математически выраженный закон Кулона, который говорил о том, как электрические заряды притягиваются; 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 изолированно и более-менее сами по себе. Джеймс Максвелл¹⁶ 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 математической.¹⁷

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

Это не так. Станислав Лем¹⁸ весьма образно описывает, чем занимается математик. Приведем отрывок из его книги «Сумма технологий» [72]:

«Давайте представим 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 “штанами”. 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 возни-

¹⁶ Джеймс Клерк Максвелл (James Clerk Maxwell; 1831–1879) – британский физик и математик.

¹⁷ В начале нашего века шведско-американский космолог Макс Тегмарк опубликовал ряд научных и популярных работ, посвященных математической гипотезе Вселенной, которая утверждает, что наша физическая реальность является математической структурой, иными словами, наша Вселенная не просто описывается математикой – она и есть сама математика [103].

¹⁸ Станислав Лем (1921–2006) – польский писатель, философ, фантаст и футуролог.

кало 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...»

Математиков часто обвиняют в том, что они сидят в башне из слоновой кости, не смотрят в окно, не выглядывают наружу и занимаются своим делом. Но потом рано или поздно выясняется, что почему-то где-то в природе оказывается реализована часть того, что было построено внутри математики. Опыт развития математики убеждает, что самые, казалось бы, оторванные от практики ее разделы находят важные применения. Приведем несколько примеров.

1. Теория чисел, одна из древнейших в математике, долгое время считалась чем-то вроде «игры в бисер»¹⁹. 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 и в функциональном программировании – язык Haskell (реализация монад) [59].

Г. Штейнгауз предложил следующую оригинальную классификацию «математика» [119. 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 большинство людей никогда не имеют дела с математикой, иной, нежели «δ». Огромное 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 представлен в § 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 [86]:

¹⁹ 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 неявно, к добру или к злу, малейшего изменения в благоустройстве мира» [116].

«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 права 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».

О значении математики для человеческой цивилизации очень ярко написал Эдуард Френкель²⁰:

«Одно из распространенных заблуждений, касающихся математики, заключается в том, что ее можно использовать только как “инструмент”. Так, например, биолог ставит эксперименты, собирает данные, а затем пытается построить математическую модель, соответствующую этим данным (возможно, при участии математика). Хотя такой формат сотрудничества важен, математика в действительности предлагает нам намного больше: она позволяет совершать фундаментальные прорывы, делать открытия, означающие полную смену парадигмы, которые без ее помощи были бы попросту невозможны. Например, когда Альберт Эйнштейн понял, что гравитация вызывает искривление пространства, он не пытался описать с помощью уравнений какие-то данные. На самом деле таких данных вовсе не было. В то время никто даже представить себе не мог, что наше пространство искривлено: все “знали”, что мы живем в плоском мире! Однако Эйнштейн понял, что это единственный способ обобщить его специальную теорию относительности на безынерционные системы в сочетании с его догадкой о том, что гравитация и ускорение оказывают одинаковое влияние. Это был интеллектуальный скачок высочайшего уровня в сфере математики, который Эйнштейн мог совершиТЬ, только лишь полагаясь на работу математика Бернарда Римана, сделанную пятьюдесятью годами ранее. Человеческий мозг запрограммирован таким образом, что мы не в состоянии вообразить искривленные пространства размерностью больше двух; единственный способ изучения и описания их – посредством математики. И что вы думаете? Эйнштейн оказался прав! Наша Вселенная действительно искривлена; более того, она расширяется. Вот она, мощь математики, о которой я веду речь!» [114. С. 10].

Математик – это человек, который не только сразу же схватывает чужую мысль, но и видит, из какой логической ошибки она вытекает.

Хальмар Нар (р. 1931), немецкий математик

§ 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.

²⁰ Эдуард Владимирович Френкель (р. 1968, Коломна, СССР), после получения диплома в Российском университете нефти и газа был приглашён в Гарвардский университет в качестве преподавателя. В настоящее время он работает профессором математики в Калифорнийском университете в Беркли.

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 гр. sophisma – уловка, выдумка, головоломка) – мнимое доказательство, в котором обоснованность заключения кажущаяся, порождается чисто субъективным впечатлением, вызванным недостаточностью логического или семантического анализа.

Надо уметь отличать софизм от логической ошибки. Хорошим примером логической ошибки в рассуждениях служит следующая история [62. С. 54–55]:

«Осень. Индейцы в резервации интересуются у нового вождя, холодной ли будет предстоящая зима. Вождь, однако, был современным человеком и ничего не знал о том, как его предки узнавали, будет ли зима теплой или холодной. На всякий случай он приказал всем индейцам запасать дрова и готовиться к холодной зиме. Через несколько дней ему в голову, хоть и с опозданием, пришла мысль позвонить в Национальную метеорологическую службу и поинтересоваться прогнозом на зиму.

Метеорологи сообщили, что зима действительно ожидается очень холодная. Тогда он велел своим людям еще активнее заниматься заготовкой дров. Через пару недель он решил уточнить прогноз у метеорологов.

– Вы все еще предсказываете нам холодную зиму? – поинтересовался он.

– Да, конечно! – ответили ему. – Зима, похоже, будет чрезвычайно морозной!

После этого вождь приказал индейцам тащить в запасы каждую щепку, которую им удастся подобрать. И вновь через пару недель он позвонил в Национальную метеорологическую службу, дабы узнать поточнее, что специалисты думают о предстоящей зиме.

– Мы предполагаем, что эта зима будет одной из самых холодных за всю историю наблюдений! – ответили ему.

– Неужели? – поразился вождь. – Откуда вы знаете?

– Да индейцы запасаются дровами, как сумасшедшие! – ответили метеорологи».

Данная логическая ошибка называется **порочный круг в доказательстве**.

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 именовали себя некоторые древнегреческие философы IV–V вв. до н.э., достигшие большого искусства в логике. Они учили красноречию и целью своей деятельности называли приобретение и распространения мудрости. Среди софистов были выдающиеся учёные своего времени, но некоторые были готовы научить убедительно защищать любую точку зрения, какая только могла понадобиться ученику, при этом вполне допускались логические передержки, применение противоречивых норм, 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» [74]. Сочинение Протагора «Тяжба о плаче» было посвящено знаменитому софизму, относящемуся к спору Протагора с его учеником Эватлом. Последний заключил договор с Протагором, что он уплатит ему значительную сумму денег за учение, если выиграет первое дело в суде. Спустя некоторое время Протагор

потребовал от Эватла платы. Эватл отказался платить, говоря: «Но я еще ни разу не защищал дела в суде». Протагор заявил: «Если я подам в суд на тебя и выиграю дело, то ты должен будешь мне заплатить по решению суда. Если же ты выиграешь дело на суде, то ты должен будешь мне уплатить согласно договору». Эватл на это отвечал: «Ни в том ни в другом случае я не заплачу. Если решение суда будет в твою пользу, то я не стану платить согласно нашему договору. Если же суд откажет тебе, то я не буду платить согласно решению 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 ее $1/n$ 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 ошибку.

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

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

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

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 на самом деле? Посмотрите на следующее 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 $x = c$: первое слагаемое станет равным 1, а второе и третье содержат множитель $(x - c)$, поэтому обращаются в 0. Таким образом, при $x = c$ получаем равенство $1 = 1$, т.е. $x = c$ – корень этого уравнения. Совершенно аналогично проверяется, что $x = b$ и $x = a$ тоже являются корнями. Значит, это уравнение имеет три различных корня.

3. Числа Фибоначчи²¹. 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). Стороны прямоугольника $f(8) = 21$ и $f(6) = 8$. Площадь квадрата равна 169, а площадь прямоугольника равна 168. Площади равносоставленных четырехугольников оказались неравными.

Теперь возьмем квадрат со стороной $f(8) = 21$. Разрежем его на аналогичные 4 части и составим из них прямоугольник (рис. 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.

Аналогичное построение можно провести для любых трех последовательных чисел Фибоначчи.

²¹ Леонардо из Пизы (ок. 1170–1250 гг.), известный как Фибоначчи, был первым из великих математиков Европы позднего Средневековья.

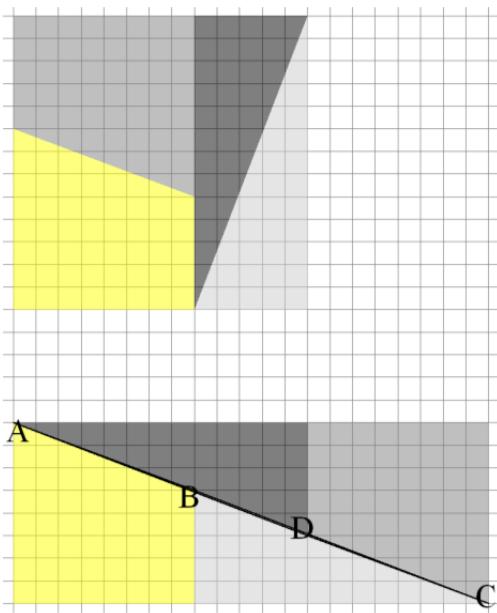


Рис. 1. $f(7)^2$ и $f(6) \times f(8)$

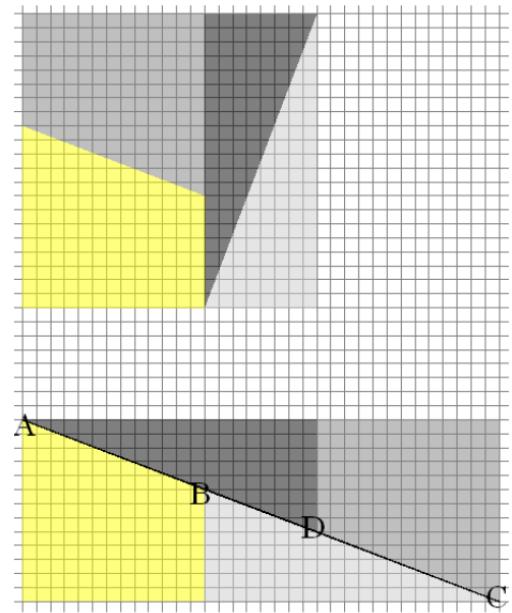


Рис. 2. $f(8)^2$ и $f(7) \times f(9)$

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. 3).



Рис. 3. Карта России

В § 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 легкоразрешимыми.

1. Парадокс «Лжец». Его открытие приписывают древнегреческому софисту Евбулиду (IV в. до н.э.). Вся проблема заключается в интерпретации фразы: «Высказывание, которое я сейчас произношу, ложно». 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 в.):
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 них не является общепризнанным.

2. Апория Зенона²²: **Ахиллес и черепаха.** Вот основная мысль его рассуждений: движение невозможно, ибо самый быстрый бегун, скажем Ахиллес (один из самых сильных и храбрых героев, осаждавших древнюю Трою), никогда не сможет догнать самого медленного, скажем, черепаху. Действительно, если Ахиллес в начале движения находится на некотором расстоянии от черепахи, то он, чтобы догнать черепаху, должен сначала достичь точки, в которой черепаха находилась в начале движения. Расстояние между ними, разумеется, будет убывать. Но оно никогда не исчерпается полностью.

Апории Зенона, из которых до нас дошло только девять, имеют глубокий смысл, направлены на вскрытие понятия бесконечности и так или иначе упираются в проблему континуума, которая приобрела особую актуальность в связи с теорией множеств Г. Кантора (см. главу 3) и квантовой механикой XX в.

3. Парадокс крокодила. В древней «диллеме крокодила» крокодил украл ребенка. Крокодил обещал отцу вернуть ребенка, если отец угадает, вернет ему крокодил ребенка или нет. Что должен сделать крокодил, если отец скажет, что крокодил не вернет ребенка [64. С. 42].

Отец мог рассуждать так: если крокодил не вернет ребенка, то отец будет прав и, в силу обещания крокодила, крокодил должен вернуть ребенка.

Но крокодил может возразить: если я верну ребенка, то отец будет не прав, и поэтому я не должен ребенка возвращать.

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

4. Парадокс Берри [Там же. С. 41]. Впервые парадокс опубликовал Берtrand Расселл, приписав его авторство Дж.Дж. Берри (1867–1928), библиотекарю библиотеки в Оксфорде.

Рассмотрим выражение:

«Наименьшее натуральное число, которое нельзя назвать посредством меньше чем тридцати трех слов».

Поскольку словов конечное число, то существуют конечное множество предложений из менее чем тридцати трех слов и, следовательно, конечное подмножество натуральных чисел, определяемых фразой из тридцати трех слов. Однако множество натуральных чисел бесконечно, следовательно, существуют числа, которые нельзя определить фразой из менее чем тридцати трех слов. Среди них, очевидно, существует наименьшее натуральное число, не описываемое менее чем тридцати тремя словами. Но именно это число определяется приведенной выше фразой, и в ней менее тридцати трех слов. Возникает парадокс: число, описанное данной фразой, существует тогда и только тогда, когда оно не существует.

²² Зенон (ок. 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».

5. Парадокс Греллинга [113. С. 21–22] назван в честь открывшего его немецкого логика и философа Курта Греллинга (1886–1942).

Некоторые русские прилагательные, например «русское», «многосложное», обладают тем самым свойством, которое они называют. Громадное большинство прилагательных, таких как «красное», «французское», «односложное», не обладают называемым каждым из них свойством. Назовем прилагательные второго рода «гетерологические». Нетрудно сразу обнаружить, что прилагательное «гетерологическое» является гетерологическим тогда и только тогда, когда оно не гетерологическое.

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 (см. гл. 3).

7. Парадокс неожиданной казни [48. С. 95–109].

Судья заявил осужденному, что он будет повешен в один из семи дней на следующей неделе в полдень. Судья также добавил, что осужденный узнает о том, в какой именно день это должно произойти, только утром в день казни. Судья славился тем, что всегда держал свое слово.

Осужденный стал размышлять. В последний день недели, в воскресенье его повесить не могут, так как в этом случае он знал бы о времени казни уже в субботу. Если воскресенье исключается, то суббота остается последним днем, когда его могут повесить. И если осужденный будет жив в пятницу днем, то тогда он будет знать, что его повесят в субботу. Следовательно, если его в пятницу не повесили, то и в субботу казнь не состоится. Поэтому суббота также исключается. Продолжая эти рассуждения, осужденный последовательно исключил из дней недели пятницу, четверг, среду и вторник. Во все эти дни казнь не может состояться, поскольку это будет нарушением обещания судьи. Остается понедельник, но и в понедельник узника не могут казнить, поскольку это не будет неожиданно для него. Следовательно, приговор судьи нельзя привести в исполнение.

У осужденного было прекрасное настроение, но в среду состоялась казнь, и она была неожиданной для осужденного. Судья сдержал свое слово.

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 (глава 7).

Парадоксы лжеца, крокодила, Берри, Греллинга и брадобрея относятся к парадоксам автореференции (самоссылочности). Автореференция – 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.

В книге [113] первая глава полностью посвящена парадоксам в математике и логике.

§ 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 привело к математической логике. Математическая логика выросла из философских вопросов относительно оснований математики, но в настоящее время переросли свои философские корни и стала неотъемлемой частью математики в целом.

Математическая логика – логика по предмету, математика по методу.

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.

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

Задачи, решаемые математической логикой:

1. Создание формальных языков и методов в логике, более точных и эффективных, чем использовавшиеся 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 – преобразовать 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 Смаллиан²³ (рис. 4) писал о том, что многие люди спрашивают его, 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 он может сказать: сделать точным понятие *доказательства*.

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 про-

²³ Рэймонд Меррил Смаллиан (англ. Raymond Merrill Smullyan; р. 1919) – американский математик, логик, писатель, даосский философ, астроном-любитель и фокусник-престижитатор. 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.

тиворечий. 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.

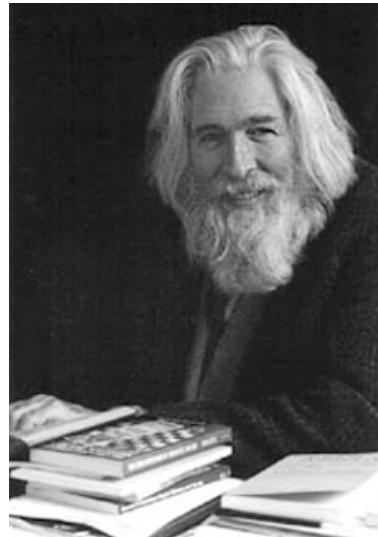


Рис. 4. Рэймонд Смалиан

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. Смалианом [98].

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, чтобы в одну из них положить свой портрет. На крышках шкатулок она приказала сделать надписи:

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 шкатулки, 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 заблагорассудятся? 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 (проводите рассуждение самостоятельно). На этом Р. Смаллиан заканчивает обсуждение своей задачи.

Об отношении математической логики к реальному миру говорит следующая цитата из книги Ю.И. Манина²⁴ [78]:

«Предметом логики не является внешний мир, но лишь системы его осмысливания. 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 § 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.

²⁴ Юрий Иванович Манин (р. 1937) – российский математик, один из основоположников некоммутативной алгебраической геометрии и квантовой информатики.

Если коротко сказать об отношении математики и логики к реальному миру, то спра- ведлив следующий тезис Р. Смаллиана [97. С. 59]:

«Математика и логика изучают все воображаемые миры, а естественные науки только реальный мир».

Задачи

Задача 1. Как дополнить посылки в силлогизме, приведенном Амброзом Бирсом при определении логики, чтобы вывод не вызывал сомнения в правильности?

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

Задача 3. Найдите ошибку в софизме «карта России».

Задача 4. Найдите математические ошибки в софизме с тождественными преобразованиями, использующие операции со степенями и мнимой единицей.

Задача 5. Найдите математическую ошибку в софизме «квадратное уравнение имеет три корня».

Чтобы понять какую-либо науку,
необходимо знать историю этой науки.

Огюст Конт, французский философ

Глава 2. Краткая история логики

В данной главе говорится о том, как зародилась логика в античном мире и как неторопливое развитие логики в течение двух тысячелетий сменилось появлением в XIX в. и активным развитием в XX в. математической логики. И сейчас математическая логика предстает перед нами во всем своем блеске и великолепии. Рассматриваются только основные действующие лица этой истории – философы, логики, математики – и их идеи.

§ 1. Становление логики

Многие науки зародились в античной Греции, и логика не была исключением. Например, Фалес (ок. 625–547 гг. до н.э.; рис. 1) и Пифагор (570–490 гг. до н.э.; рис. 2) использовали логические рассуждения в математике.

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 равен 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 взгляды пифагорейцев на число, поскольку они не знали других чисел, кроме натуральных, или отношений натуральных чисел.

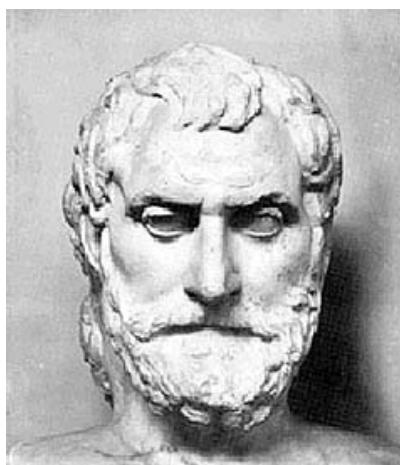


Рис. 1. Фалес

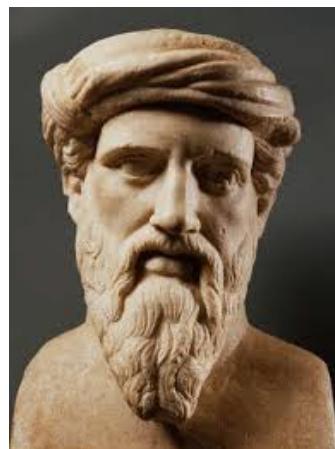


Рис. 2. Пифагор. Бюст.
Рим, Капитолийский музей

Сократ (ок. 469–399 гг. до н.э.; рис. 3) и Платон (ок. 427–347 гг. до н.э.; рис. 4) применяли рассуждения математического типа в философских вопросах.

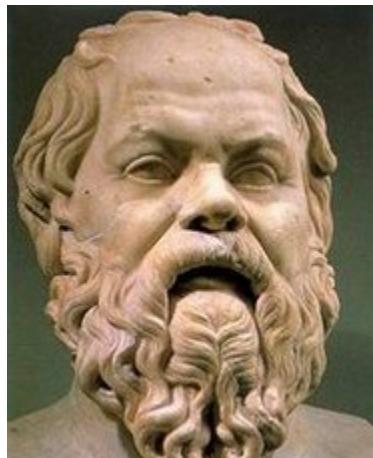


Рис. 3. Сократ. Бюст работы Лисиппа, хранящийся в Лувре

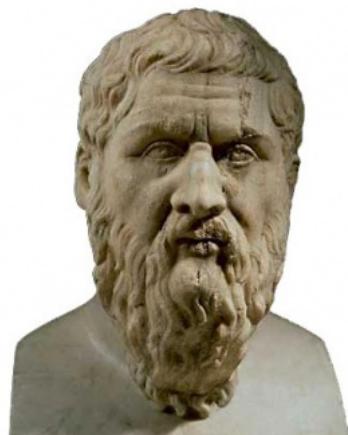


Рис. 4. Платон. Мраморный бюст работы неизвестного скульптора, римская копия. Рим, Капитолийский музей

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».

«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».

Философский метод исследования Сократа получил название **сократовский диалог**. Позиция Сократа – противопоставление внешнего софистического знания и внутреннего философского, которому научить нельзя, но можно открыть в себе самом. Помощником в этом и является Сократ, ремесло которого – не учительство (ибо сам он «ничего не знает»), а нечто вроде повивального («от меня они ничему не могут научиться, просто сами в себе они открывают много прекрасного, если, конечно, имели, и производят его на свет»). Отличие от повивальной бабки лишь в том, что Сократ помогает не рождению ребенка, а рождению мысли, и делает это в диалоге с учеником с помощью вопросов и ответов. Он подвергал предложенные ответы тщательному анализу, в частности путем осмыслиения противоположных доводов.

Платон был учеником Сократа, и основная часть его сочинений – это «Диалоги», участником которых является Сократ, беседующий с историческими, а иногда и вымышленными персонажами. Непревзойденным по силе и влиянию является учение Платона об идеях. Для Платона идеи представляют собой неизменные и вечные объекты мысли, к которым обращаются при объяснении того, как возникают понятия, насколько возможно познание, какие значения имеют слова. Согласно Платону окружающий нас мир мы познаем чувствами и он является производным от мира идей, он – «тень» мира идей. Идея неизменна, постоянна и вечна, а вещи материального мира возникают и гибнут постоянно.

Платон – родоначальник европейской философии. Он был основателем **реализма** (другими словами, математический платонизм) – философского направления в математике, последователи которого считают, что математические объекты (сущности) существуют независимо от математиков. Большинство современных математиков, поддерживают эту позицию.

Однако настоящим основателем классической логики был Аристотель (384–322 гг. до н.э.; рис. 5), ученик Платона.



Рис. 5. Аристотель. Мраморный бюст работы неизвестного скульптора, римская копия. Рим, Национальный римский музей

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 необходимо должны принять заключение (должны также считать его истинным).

Вот классический пример наиболее известного силлогизма:

Все люди – смертны, Сократ – человек, следовательно, Сократ смертен.

Другой пример этого же силлогизма был приведен в гл. 1 – рассуждение, в котором заключение – «у Геракла – деревянные ноги».

Знаменитый математик древности Евклид (ок. 325–265 гг. до н.э.; рис. 6), строго говоря, не был логиком, но его вклад в логику неоспорим.

Главная работа Евклида «Начала» (в латинизированной форме – «Элементы») содержит изложение планиметрии, стереометрии и ряда вопросов теории чисел; в ней он подвел итог предшествующему развитию греческой математики и создал фундамент дальнейшего развития математики. До сих пор классическая геометрия называется в его честь евклидовой. Его величайшим достижением стала 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 неочевидные.

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.

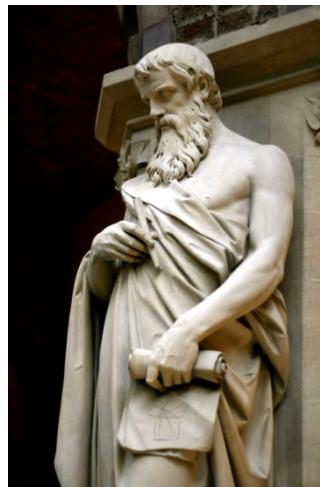


Рис. 6. Статуя Евклида.
Оксфордский университет, Музей естественной истории

В то время, когда последователи Аристотеля продолжали его труд, связанный с логикой силлогизмов, другая греческая школа философов, стоики, исследовали иной 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.

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 Аристотеля и стоиков, поэтому спустя столетие после независимого развития эти подходы слились **в рамках одной дисциплины**.

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

В античной Греции математика получила статус дедуктивной науки, благодаря «Началам» Евклида и отношению к математике великих философов Платона и Аристотеля. Был создан аксиоматический метод и применялись такие виды дедуктивных рассуждений, как **закон противоречия** (никакое высказывание не может быть одновременно истинным и ложным) и **закон исключенного третьего** (высказывание может быть только истинным и ложным). По сути, дедуктивная логика зародилась в математике. Ученые стали считать, что правила дедукции гарантируют получение из исходных посылок заключения, которое по надежности не уступает надежности посылок.

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; рис. 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 Бэко-

на, является бесполезной для открытия новых истин; в лучшем случае она может служить лишь для оправдания и обоснования их.



Рис. 7. Фрэнсис Бэкон

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

Довольно рано возникла идея о том, что, записав все исходные допущения на языке специальных знаков, похожих на математические, можно заменять рассуждение вычислением. Точно сформулированные правила таких логических вычислений можно перевести на язык вычислительной машины, которая 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), дав ей, впрочем, лишь совершенно фантастическое применение.

Более определенный и близкий к реально осуществленному впоследствии замысел универсального логического исчисления развивал Готфрид Лейбниц (1646–1716) – немецкий философ, логик, математик. Лейбниц считал, подобно Аристотелю, что логика может стать независимым орудием для научного познания мира. Он был первым, после Аристотеля, кто продвинул логику вперед. 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) он 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 г. было издано философское эссе Готфрида Лейбница «Рассуждения о метафизике» (*Discours de métaphysique*), в котором поставлен вопрос: как отличить факты, которые можно описать неким законом, от фактов, никаким законам не подчиняющихся? В четвертом разделе своего эссе он высказал очень простую и глубокую мысль: теория должна быть проще данных, которые она объясняет, иначе она не объясняет ничего. Если единственный закон, объясняющий какие-то данные, оказывается слишком сложным, то рассматриваемые данные на самом деле не подчиняются никакому закону.



Рис. 8. Готфрид Вильгельм Лейбниц

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

§ 2. Начало математической логики

К началу XIX столетия, несмотря на свое грандиозное развитие, математика потеряла эталон логической строгости. Можно сказать, что развитие математики за более чем двухтысячелетний период после Евклида и Аристотеля преимущественно шло *ширь*, а не *вглубь*. Все это время дедуктивная логика, применяемая математиками, мало развивалась. Одна из причин – интенсивное применение математики для решения практических задач, когда идеализации и абстрактные понятия возникали из опыта. Морис Клайн в своей книге [63. С. 178, 151] пишет:

«К началу XIX в. математика оказалась в весьма парадоксальной ситуации. Ее успехи в описании и предсказании физических явлений превзошли самые смелые ожидания. Но при этом многие математики еще в XVIII в. отмечали, что все огромное здание математической науки было лишено логического фундамента и держалось на столь шатких основаниях, что не было уверенности в “правильности” этой науки. Подобная ситуация сохранялась и в течение всей первой половины XIX в. Многие математики с головой ушли в новые области физики и добились там значительных успехов, а об основаниях математики никто попросту не задумывался».

«Математический анализ, ядро которого составляет дифференциальное и интегральное исчисление – самая тонкая область всей математики, – был построен на совсем не существующих логических основаниях арифметики и алгебры и на не вполне ясных основах евклидовой геометрии».

Некоторые математики отказывались от доказательства своих утверждений под предлогом отсутствия времени или считали, что доказательство не требуется²⁵.

Как было обнаружено в начале XIX в., евклидова геометрия, которая служила образцом для математиков в качестве аксиоматической системы, имела серьезные изъяны. Исправление этих недостатков было закончено только перед XX в. и привело к новому пониманию аксиоматического метода. Подробно это будет рассмотрено в § 4 главы 6.

²⁵ «Даже в конце XIX в. Карл Густав Якоб Якоби (1804–1854), в работах которого по теории эллиптических функций осталось множество неразрешенных вопросов, говорил: “На гауссовскую строгость у нас нет времени, господа”. Многие математики действовали так, будто то, что им не удавалось доказать, попросту не нуждалось в доказательстве» [63. С. 192–193].

Обоснование математического анализа оказалось невозможным без точного определения понятия вещественного числа [115. С. 170–171]:

«В 1821 г. Коши²⁶ вводит новые требования к строгости в своем знаменитом «Курсе анализа». Он ставит следующие вопросы и отвечает на них.

- Что такое производная? Ответ: предел.
 - Что такое интеграл? Ответ: предел.
 - Что такое бесконечный ряд $a_1 + a_2 + a_3 + \dots$? Ответ: предел.
- Отсюда следует вопрос:
- Что такое предел? Ответ: число.
- И, наконец, последний вопрос:
- Что такое число?»

В 70-х гг. XIX в. немецкий математик Карл Вейерштрасс (1815–1897) и его соратники ответили на этот вопрос. Но понятие иррационального числа объяснялось через рациональные числа. Аксиоматическая теория рациональных чисел было предложена немецким математиком Юлиусом Дедекиндом (1831–1916) и математиком Джузеппе Пеано²⁷ только в 1889 г. Пеано и Дедекинд предложили также и аксиоматику натуральных чисел (1888 г.), с которой мы познакомимся в главе 6.

Обоснование математического анализа, алгебры, геометрии, создание основной системы логических понятий современной математики потребовало от математиков громадного напряжения сил и способностей и было закончено только в XX в. Чтобы логика помогла математике, математики стали применять в логике математические методы.

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; рис. 9) – английский математик и логик, Георг Кантор (1845–1918; рис. 10) – немецкий математик, и Готлоб Фреге (1848–1925) – немецкий логик, математик и философ.

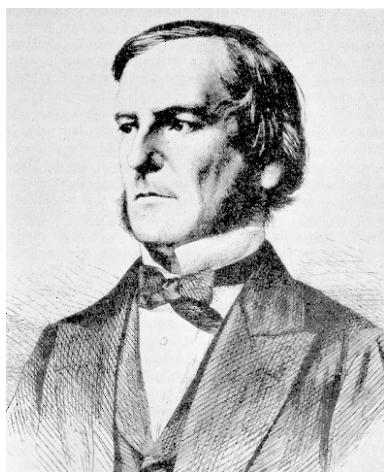


Рис. 9. Джордж Буль

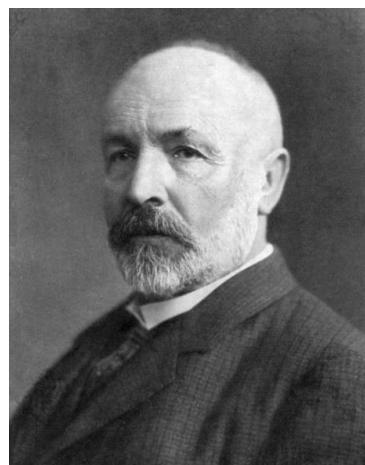


Рис. 10. Георг Кантор

Названная так по имени ее открывателя, **булевая алгебра** была первой разработанной системой, которая рассматривала логику как исчисление. Поэтому булеву алгебру можно считать предшественницей математической логики. Булева алгебра подобна стандартной

²⁶ Огюстен Луи Коши (1789–1857) – французский математик. Работал и в действительном, и в комплексном анализе. Считается, что он сумел облечь анализ Ньютона в строгую форму.

²⁷ Джузеппе Пеано (1858–1932) – итальянский математик. Внёс вклад в математическую логику и философию математики.

арифметике: два значения – 0 и 1 (ложь 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.

Рассмотрим примеры. 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:

$$A = 1 \text{ и } B = 0.$$

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.

В § 5 главы 4 будет рассмотрена аксиоматическая теория булевой алгебры.

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.

Пять примеров множеств:

- $\{2, 3, 5, 7, 11, 13, 17, 19, \dots\}$ – бесконечное множество, содержащее все простые числа;
- {пешка, конь, слон, ладья, ферзь, король};
- {Земля, Луна}, {Юпитер и еще не менее 67 его спутников}, {Марс, Фобос, Деймос} – 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. Рассмотрим утверждение:

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

Это утверждение можно проверить, определив два множества: 1) множество всех штатов, названия которых содержат букву «z»; 2) множество штатов, названия которых начинаются с буквы «A»:

Множество 1: {Arizona}.

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

Как видим, 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.

Кантор открыл, что множества, содержащие бесконечное число элементов, могут различаться по «мощности» (**мощность** – обобщение понятия количества элементов). Операции, которые естественно определить для конечных множеств, он стал применять и для бесконечных множеств, рассматривая последние как уже реализованные, созданные (так называемые актуально бесконечные). 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 учеными того времени. Основными оппонентами в то время были немецкие математики Герман Шварц (1843–1921) и, в наибольшей степени, Леопольд Кронекер (1823–1891), 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 все прочее – дело рук человеческих»).

Тем не менее к концу XIX в. теория множеств стала общепризнанной после успешного использования теории множеств в анализе, особенно после широкого применения Давидом Гильбертом²⁸ теоретико-множественного инструментария.

Теория множеств подробно изложены в главе 3.

Немецкий логик, математик и философ Готлоб Фреге (рис. 11) ввел первые реальные системы формальной логики: логику высказываний и объемлющую ее логику предикатов.



Рис. 11. Готлоб Фреге

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». Например, 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

$$A \& B,$$

$$\neg A \rightarrow B.$$

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

Например, 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 $\neg A \rightarrow B$, в логике предикатов запишут теперь как

²⁸ Давид Гильберт (нем. David Hilbert; 1862–1943) – немецкий математик-универсал.

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

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

$$\begin{aligned} &\text{«Все люди едут в трамвае»,} \\ &\text{«Некоторые люди находятся дома»} \end{aligned}$$

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) – описана в главе 5.

В конце XIX в., 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 Берtrand Рассел (рис. 12) не обнаружил парадокс, названный впоследствии его именем (см. главу 3). Фреге не нашел, как освободиться от этого противоречия.

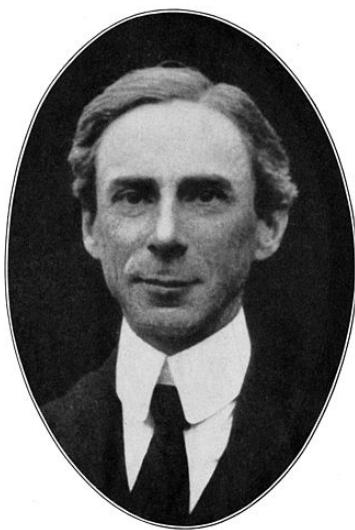


Рис. 12. Берtrand Рассел



Рис. 13. Альфред Уайтхед

Однако Рассел сумел избавиться от подобных парадоксов в теории множеств. В 1910–1913 гг. Берtrand Рассел и Альфред Уайтхед²⁹ (рис. 13) написали фундаментальный труд в трех томах «Principia Mathematica» [104], в котором, используя идеи Фреге, обосновали математику на аксиомах теории множеств и логики.

§ 3. Математическая логика в своем блеске и великолепии

Геттингенская программа

В 20-х гг. XX в. с программой обоснования математики на базе математической логики выступил Давид Гильберт (рис. 14).

²⁹ Альфред Норт Уайтхед (Alfred North Whitehead; 1861–1947) – британский математик, логик, философ.



Рис. 14. Давид Гильберт

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 следующее.

1. Математика является **полной**, т.е. существует полная аксиоматическая теория математики, из которой с помощью последовательного использования правил математической логики можно вывести все положения математики.
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 опровергимо.

Фактически программа Гильberта 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 сформулированные им вопросы: по его мнению, математика действительно была полной, непротиворечивой и разрешимой. Оставалось только это доказать. Подробнее о программе Д. Гильберта можно прочесть в [70. С. 4–15].

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 XIX и XX вв. очень важным подспорьем в изучении логических основ математики, поскольку позволял избегать неточности мысли, которая легко проскальзывает при использовании слов обычного языка, смысл которых дается не точным определением, а созданием привычки к принятому словоупотреблению.

Теоремы Геделя

«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 является ли полной. Непроти-

воречивость 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 Гёдель³⁰ (рис. 15) 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. 15. Курт Гёдель

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

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

В сущности, первая теорема Гёделя о неполноте похоронила надежды Лейбница на существование 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 Геделя показали, что Геттингенская программа Гильберта нереализуема. Теоремам Геделя посвящена глава 11.

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 словом «возможно» («вероятно», «нейтрально»). Иначе – отказаться от аксиомы «Закон исключенного третьего». Древние греки считали невыполнение этого закона немыслимым нарушением логических рассуждений, но описание логики просто как аксиоматической системы (теории) сделало это допустимым.

³⁰ Курт Фридрих Гёдель (нем. Kurt Friedrich Gödel; 1896–1978) – австрийский логик, математик и философ математики.

В 1917 г. Ян Лукасевич³¹ (рис. 16) 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*».



Рис. 16. Ян Лукасевич

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**.

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 используются 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 Алонзо Чёрч³² (рис. 17) и Аллан Тьюринг³³ (рис. 18). Алонзо Чёрч прославился разработкой теории ламбда-исчисления, последовавшей за его знаменитой статьёй 1936 г., в которой он показал существование алгоритмически неразрешимых задач. Эта статья предшествовала знаменитому исследованию

³¹ Ян Лукасевич (1878–1956) – польский логик.

³² Алонзо Чёрч (1903–1995) – американский математик и логик.

³³ Аллан Мэтисон Тьюринг (1912–1954) – английский математик и логик.

Алана Тьюринга на тему проблемы остановки, в котором также было продемонстрировано существование задач, неразрешимых механическими способами. Впоследствии Чёрч и Тьюринг показали, что лямбда-исчисление 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.



Рис. 17. Алонзо Чёрч



Рис. 18. Аллан Тьюринг

Алан Тьюринг доказал, что проблема остановки для машины Тьюринга неразрешима: в общем случае невозможно алгоритмически определить, остановится ли когда-нибудь данная машина. Хотя доказательство Тьюринга было обнародовано в скором времени после эквивалентного доказательства Алонзо Чёрча, в котором использовалось ламбда-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, вычислять все, что можно в принципе вычислить, была крайне оригинальной. После работ Чёрча и Тьюринга математики поняли ограничения алгоритмического подхода – значения не всех точно определяемых функций можно вычислить на компьютере, и не все задачи, поддающиеся решению, можно алгоритмически решить.

В главах 9–10 мы более подробно познакомимся с работами Чёрча и Тьюринга.

Бурбаки

Николя Бурбаки (фр. Nicolas Bourbaki) – псевдоним группы молодых математиков, реализовавших проект систематического изложения современной математики на основе аксиоматического метода. Численность и точный состав группы, созданной в 1935 г., не разглашались, но впоследствии стало известно, что ее основателями были французские математики Андре Вейль, Жан Дельсарт, Жан Дьёдонне, Анри Картан, Клод Шевалле и Рене де Пессель. Первоначально ставилась скромная цель – создание современного курса математического анализа. Но в итоге возник многотомный трактат «Начала математики» («*Éléments de Mathématique*»).

В данном трактате, выходящем с 1939 г., развивается формальная аксиоматическая система, которая, по замыслу авторов, должна охватить главнейшие разделы математики. Бурбаки придавали особое значение абстрактному, логико-ориентированному подходу к математике. Основные принципы изложений: единство и полная формализация математики на основе теории множеств; систематичность; догматизм и самодостаточность. Было решено, что Бурбаки никогда не обобщают специальные случаи, а всегда выводят частные случаи из самых общих. Целью Бурбаки было собрать в различных применяемых в математике процессах то, что можно выделить в виде теории, логически связанной, легко излагаемой и легко используемой.

Решение Бурбаки использовать аксиоматический метод всюду без исключения повлекло необходимость новой организации различных математических дисциплин. Оказалось невозможным сохранить классическое деление математики на анализ, геометрию, алгебру, теорию чисел и т.д. Его место заняла ключевая концепция «структура». Структуры определяются посредством аксиом; например, есть алгебраические структуры, структуры порядка и топологические структуры. Все эти три структуры присутствуют в понятии действительных чисел, и, конечно, не независимо, а связаны между собой сложным образом. Это позволило определить понятие изоморфизма и новую нетрадиционную классификацию основных математических дисциплин. В трактате описываются в основном математические теории, практически полностью исчерпанные, по крайней мере, в их основе. Речь идет лишь об основах, а не о деталях, о теориях, приведенных к такому состоянию, при котором они могут быть изложены чрезвычайно рациональным способом.

Бурбаки акцентировали внимание на использовании обозначений там, где это только возможно, любым способом сводя использование потенциально неточного текста к минимуму³⁴. В частности, были впервые введены символ для пустого множества \emptyset ; символы $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ и \mathbb{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:



Крайняя абстракция, используемая в трактате, приводит к тому, что определение обыкновенного натурального числа 1 в «Теории множеств» можно формально выразить в следующем виде [45. С. 188]:

$$\begin{aligned} \tau_z((\exists u)(\exists U)(u = (U, \{\emptyset\}, Z) \& U \subset \{\emptyset\} \times Z \\ \& (\forall x)((x \in \{\emptyset\}) \Rightarrow (\exists y)((x, y) \in U)) \\ \& (\forall x)(\forall y)(\forall y')(((x, y) \in U \& (x, x') \in U) \Rightarrow (y = y')) \\ \& (\forall y)((y \in Z) \Rightarrow (\exists x)((x, y) \in U)) \\ \& (\forall x)(\forall x')(\forall y)((x, y) \in U \& (x', y) \in U) \Rightarrow (x = x')))). \end{aligned}$$

Причем, учитывая, что в этой записи уже сделаны сокращения, например, пустое множество \emptyset определяется в языке теории множеств Бурбаки как

$$\boxed{\boxed{\tau_{\neg\neg}\in\tau_{\neg\neg}\in\emptyset\emptyset}},$$

мы получаем, что полная запись обычной единицы состоит из 4 523 659 424 929 символов (!) [17].

Однако не надо думать, что Бурбаки оперируют такими громоздкими выражениями. Сами авторы во введении к «Теории множеств» пишут: «...уже начиная с Книги I настоящего Трактата возникает настоятельная необходимость сокращать формализованный текст введением новых слов (называемых “сокращающими символами”) и дополнительных правил синтаксиса (называемых “дедуктивными критериями”) в довольно значительном количестве.

³⁴ Математик, физик и программист, Стивен Вольфрам пишет о математических обозначениях до Бурбаки: «Математическая нотация развивалась в результате непродуманных случайных исторических процессов. Было несколько людей, таких как Лейбниц и Пеано, которые пытались подойти к этому вопросу более системно. Но в основном обозначения появлялись по ходу решения каких-то конкретных задач – подобно тому, как это происходит в обычных разговорных языках» [35].

Поступая так, мы получаем языки, гораздо более удобные, чем формализованный язык в собственном смысле и относительно которых любой мало-мальски опытный математик будет убежден, что их можно рассматривать как стенографические транскрипции формализованного языка».

Деятельность этого коллектива³⁵ дала единый язык для таких областей математики, как алгебра, топология, топологическая алгебра, теория алгебраических чисел, функциональный анализ и др., и способствовала их существенному развитию. Это еще раз подтвердило, что математика едина. Во Франции написано более 40 книг этого трактата. В 1959–1987 гг. были переведены на русский язык более 20 томов.

Через 20 лет после начала работы над трактатом первые изданные книги в какой-то мере частично устарели, так как математика – это живой развивающийся организм. Кроме того, куда двигаться дальше? Какие еще не рассмотренные в трактате общие теории уже можно считать близкими к окончательному виду? На эти вопросы стало невозможно ответить. В 1968 г. Бурбаки объявил о прекращении своей деятельности. Задуманный трактат остался незаконченным.

Математика XX в. восприняла влияние формалистских взглядов Н. Бурбаки [100]:

«...стиль практических 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».

Ю.И. Манин говорит:

«...после Кантора и Бурбаков в мозгах, что бы там ни говорили, сидит теоретико-множественная математика. Когда я про что-то впервые начинаю говорить, я объясняю это в терминах бурбакистских структур: топологическое пространство, линейное пространство, поле вещественных чисел, алгебраическое расширение конечной степени, фундаментальная группа... Я иначе не могу. Если там что-то совсем новое, я говорю, что это множество с такой-то структурой; раньше была похожая, ее называли так-то; другую похожую называли так-то; а я накладываю немного другие аксиомы и буду называть так-то. Начинаешь говорить – начинаешь с этого. То есть исходным образом было это канторовское дискретное множество, на котором потом намечалось что-то дополнительное по Бурбакам» [75].

Трактат «Начала математики» – это не энциклопедия, поскольку содержит полные доказательства; скорее это полезный и удобный рабочий инструмент, которым следует пользоваться математикам, приступающим к исследованиям в новой для них области.

Конечно, это и не учебник, ибо 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...» [119].

Теория вычислительной сложности

В конце XX в. математики перешли к анализу сложности алгоритмов и задач. Если какая-то задача алгоритмически разрешима, то она может иметь несколько алгоритмов для решения. Например, очевидным образом имея алгоритм решения, можно создать бесконечно много других алгоритмов, ухудшая первый. Необходимо уметь сравнивать алгоритмы, предназначенные для решения проблем, по эффективности (по времени выполнения, по используемой памяти). Математики выработали понятие **сложность алгоритма** для оценивания эффективности алгоритма независимо от компьютера, на котором данный алгоритм выпол-

³⁵ О некоторых сторонах деятельности Бурбаки можно прочесть в [55].

няется. Вопросы теории вычислительной сложности не входят в содержание данной книги, поэтому просто скажем, что существуют «быстрые» алгоритмы и «медленные» алгоритмы (точные понятия см. в [67]). Для многих проблем существующие алгоритмы можно упорядочить по их эффективности и естественно использовать быстрые алгоритмы. Если определен лучший по эффективности алгоритм для решения проблемы, то сложность этого алгоритма оценивает **сложность самой проблемы**. Если мы имеем быстрый алгоритм для решения какой-то проблемы, то проблему можно отнести к легкой. Если мы докажем, что быстрого алгоритма не существует, то проблема имеет большую вычислительную сложность, и в этом случае говорят, что проблема труднорешаемая.

Исследование того, какие задачи легкие, а какие труднорешаемые, входит в круг задач теории вычислительной сложности. Первый важный результат этой теории – теорема Кука–Левина – получен независимо в 1971 г. Стивеном Куком (р. 1939) и советским математиком Леонидом Левином (р. 1948). Одна из нерешенных проблем экстраординарной трудности, поставленная в рамках теории вычислительной сложности, (кратко называемая «проблема $P = NP?$ »), объявлена в 2000 г., наряду с другими шестью задачами, проблемой тысячелетия.

На этом рассказ об истории классической логики заканчивается. Дальнейшие главы книги содержат также в основном классические разделы математической логики. Для дополнительного чтения рекомендуются труды [41, 42], в которых дается общая картина, панорама математической логики, центральные конструкции, освобожденные от деталей. Тем, кто захочет узнать о современных логических проблемах, о неклассических логиках, рекомендуем для первоначального изучения книги [86, 97].

Никто не изгонит нас из Рая, который основал Кантор.
Давид Гильберт о теории множеств

Глава 3. Основы теории множеств

В главе рассматривается теоретико-множественный инструмент математики.

§ 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 собой 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 воронов 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**. 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 $A(x)$.

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

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

где «или» является **неразделительным**³⁶. 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.

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.

³⁶ 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*.

Пример 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. $x \in A$.

Как мы обнаружили, различные характеристические свойства могут определять одно и то же множество.

Пример 2. Рассмотрим множества $X = \{2, 3, 5, 7\}$, $Y = \{n \mid n - \text{простое число, меньшее } 10\}$ и $Z = \{n \mid n^4 - 17n^3 + 101n^2 - 247n + 210 = 0\}$. Нетрудно проверить, что $X = Y = Z$.

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.

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 $\{1, 2, 3, 4\}$.

Заметим, что имеют место утверждения для произвольных множеств:

- $X \subseteq X$;
- если $X \subseteq Y$, $Y \subseteq Z$, то $X \subseteq Z$;
- 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. В математике широко используются следующие множества чисел (с соответствующими обозначениями):

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

Для этих множеств выполнены строгие включения $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Очевидно, для произвольных множеств, если $X \subset Y$ и $Y \subset Z$, 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, $1 \notin \{\{1\}\}$, так как единственным элементом множества $\{\{1\}\}$ является $\{1\}$. Еще один пример: для любого x выполнено $x \in \{x\}$ и $\{x\} \in \{\{x\}\}$, но оба соотношения $x \subseteq \{x\}$ и $\{x\} \subseteq \{\{x\}\}$ не верны.

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

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 вещественных корней уравнения $x^2 + 1 = 0$.

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

Пример 4. Если $A = \{1, 2, 3\}$, то $P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\}$.

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

Расплывчатость, недостаточность канторового определения понятия множества стала понятной, когда в 1897 г. итальянский логик Чезаре Бурали-Форти, а в 1901 г. Берtrand Рассел открыли парадоксы, связанные с понятием множества.

В интуитивной («наивной») теории множеств 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.

Парадокс Рассела. 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 элемента». Примером множества, обладающего свойством A , служит, например, любое конечное множество. Если обозначить через U универсум – множество всех множеств, то тогда можно определить множество $Y = \{x \mid x \in U \text{ и } A(x)\} = \{x \mid x \in U \text{ и } x \notin x\}$. Спрашивается, выполняется ли $Y \in Y$ или $Y \notin Y$? Любое из этих двух предположений влечет противоположное утверждение.

Популярная форма этого парадокса известна как парадокс брадобрея (см. глава 1, § 3). Парадокс Рассела и другие трудности, связанные с неограниченным использованием абстрактных понятий в математике, свидетельствовали о кризисе математики на рубеже XIX и XX вв. В частности, о том, что широко используемая теория множеств в ее интуитивном, «наивном» изложении является противоречивой. Требовались радикальные изменения оснований математики. В первой половине XX в. возникли несколько направлений в этой деятельности: логицизм (Б. Рассел и А. Уайтхед), различные аксиоматизации теории множеств (в том числе и метаматематика с программой Гильберта), интуиционизм (Л. Брауэр³⁷) [64, 113]. В главе 6, § 7 описывается одна из аксиоматических теорий для множеств.

§ 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 :

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

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 :

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

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

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

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

³⁷ Лёйтцен Эгберт Ян Брауэр (1881–1966) – голландский философ и математик.

Операцию абсолютного дополнения, как правило, вводят лишь тогда, когда фиксирован универсум 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 \bar{A} всех тех элементов x , которые не принадлежат множеству A :

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

Заметим, что $\bar{A} = U \setminus A$. Часто вместо \bar{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 (1888 г.).

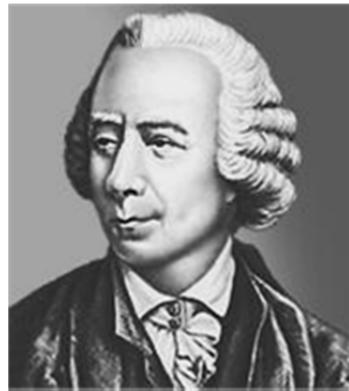


Рис. 1. Леонардо Эйлер

При решении целого ряда задач Эйлер³⁸ (рис. 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 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. 2).

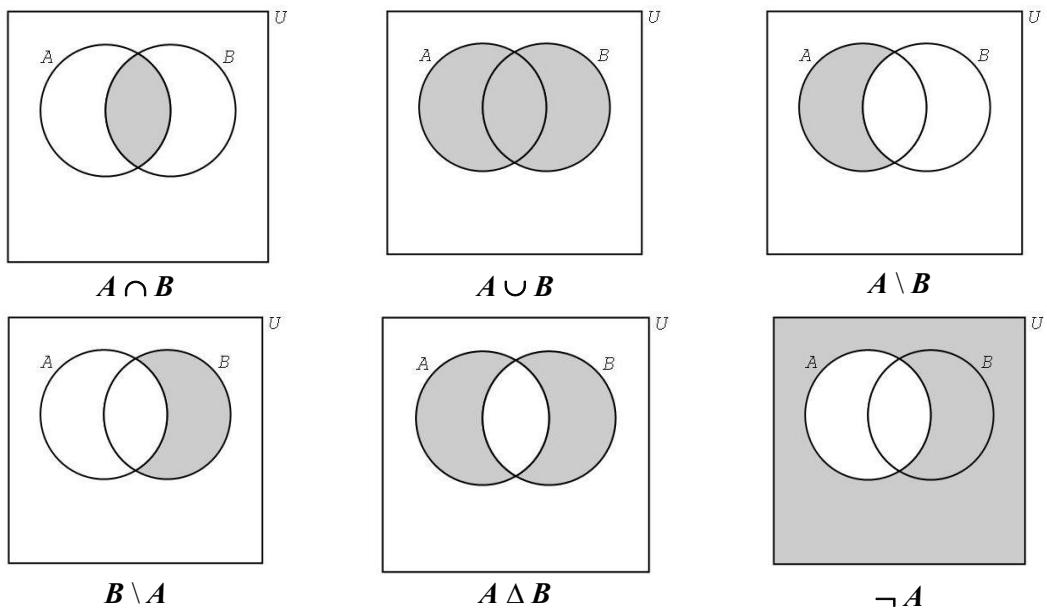


Рис. 2. Операции над множествами

³⁸ Леонард Эйлер (1707 г., Швейцария – 1783 г., Санкт-Петербург) – швейцарский, немецкий и российский математик и механик, внёсший фундаментальный вклад в развитие этих наук. Почти полжизни провёл в России.

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 **булевыми³⁹ 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**.

Теорема 1. Для любых подмножеств A , B и C универсума U выполняются следующие основные булевые 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. $A \cup \emptyset = A$.
- 4'. $A \cap U = A$.
5. $A \cup \neg A = U$.
- 5'. $A \cap \neg A = \emptyset$.
6. $A \cup A = A$ (идемпотентность \cup).
- 6'. $A \cap A = A$ (идемпотентность \cap).
7. $A \cup U = U$.
- 7'. $A \cap \emptyset = \emptyset$.
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 Моргана⁴⁰, а тождества 9 и 9' – законами поглощения.

Докажем тождество 3. Сначала покажем, что $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$. 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, $x \in (A \cup B) \cap (A \cup C)$. 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 $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. 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 $x \in U$ 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, $x \in \neg A \cap \neg B$. 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, $x \in U$ и $x \notin A$ и $x \notin B$. Значит, $x \notin A \cup B$, 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.

³⁹ Причины этого становятся понятными в § 5 главы 4.

⁴⁰ Огастес де Морган (1806–1871) – шотландский математик и логик; к своим идеям в алгебре логики пришёл независимо от Дж. Буля.

Для этого используется частный случай кругов Эйлера – диаграммы Венна⁴¹. При n , равном 2 и 3, диаграммы Венна обычно изображаются в виде кругов. Пусть даны множества $A_1, A_2, \dots, A_n, n > 1$. Начертим диаграмму Венна, изображающую эти множества таким образом, чтобы все подмножества вида $Y_1 \cap Y_2 \cap \dots \cap Y_n$, где Y_k обозначает либо A_k , либо $\neg A_k$, были не пусты. В этом случае всевозможные комбинации $Y_1 \cap Y_2 \cap \dots \cap Y_n$ называются составляющими системы множеств $\{A_1, A_2, \dots, A_n\}$.

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

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

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

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

На рис. 3 и 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.

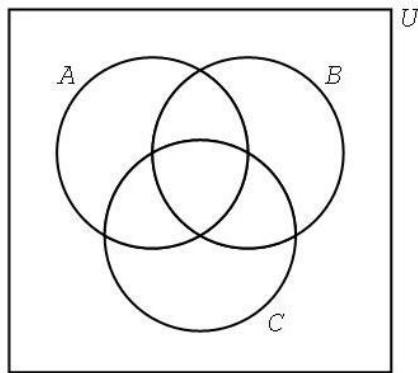


Рис. 3. Диаграмма Венна для трех множеств

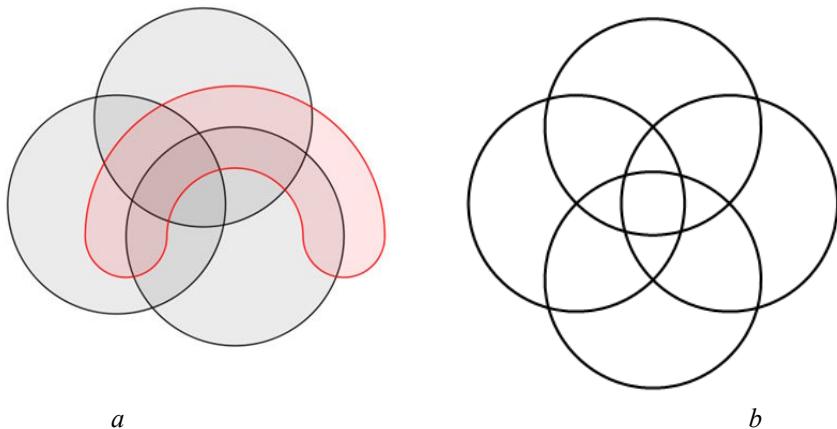


Рис. 4. Правильная (a) и неправильная (b) диаграммы Венна для четырех множеств

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

Доказательство [86. С. 79]. Прежде всего отметим, что любая составляющая S системы $\{X_1, \dots, X_n\}$ однозначно определяет значения всех формул вида $c \in X_i$. Это легко устанавливается по индукции. Отсюда следует, что две составляющие либо совпадают, либо не пере-

⁴¹ Этот вид диаграмм предложил и детально разработал Джон Венн (1834–1923) – английский логик и философ.

секаются. Далее, если Y – булева комбинация $\{X_1, \dots, X_n\}$, S – составляющая этой системы, то S либо подмножество Y , либо не пересекается с Y . Это вытекает из того, что значение характеристического свойства Y полностью определяется значениями всех $c \in X_i$. И наконец, составляющая независимой системы является подмножеством Y тогда и только тогда, когда соответствующее значение в таблице истинности формулы (см. главу 4), определяющей Y , есть **И**. Значит, в независимой системе любая булева комбинация однозначно разлагается на составляющие (т.е. представляется как объединение составляющих), и это разложение сохраняется и для других систем множеств (конечно, для зависимых систем могут появиться и другие разложения). Поэтому если в независимой системе две булевы комбинации имеют одни и те же составляющие, они будут иметь одинаковые значения и в любой другой системе.

Итак, булево равенство достаточно проверить на одной, но хорошо подобранный системе множеств. Следовательно, правильно нарисованная диаграмма Венна полностью обосновывает тождество. ■

Пример 5. Таким образом, диаграмма Венна (рис. 5) для всех множеств A , B и C доказывает равенство $A \cap (B \cup C) = (A \cup B) \cap (A \cup C)$.

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 $A \cap B = A$, 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 $A \cup B = B$.

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

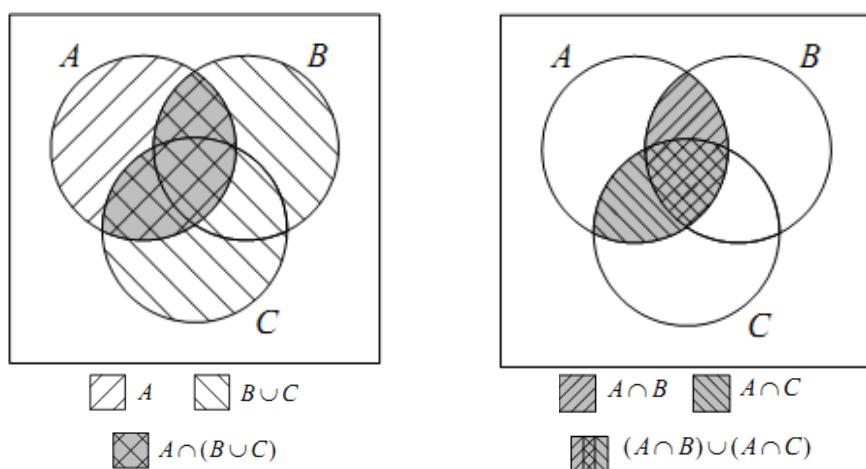


Рис. 5. $A \cap (B \cup C) = (A \cup B) \cap (A \cup C)$

Индексированные семейства множеств

Мы уже видели, что элементы множеств могут быть сами множествами. Примерами являются множество-степень или системы множеств из теоремы Венна. Выражение «множество множеств» звучит несколько неуклюже, и часто в таких ситуациях используют термин *семейство множеств*.

Определение. Пусть Λ^{42} – непустое множество, и положим, что для каждого $\alpha \in \Lambda$ существует соответствующее множество A_α . Семейство множеств $\{A_\alpha \mid \alpha \in \Lambda\}$ называется **индексированным семейством множеств** с индексами из множества Λ . Каждое $\alpha \in \Lambda$ называется **индексом**, а Λ – **индексирующим множеством**.

Определение. Пусть Λ – непустое индексирующее множество и $A = \{A_\alpha \mid \alpha \in \Lambda\}$ – индексированное семейство множеств. **Объединением семейства** множеств A называется множество

$$\bigcup_{\alpha \in \Lambda} A_\alpha = \{x \mid \text{существуют } \alpha \in \Lambda \text{ и } x \in A_\alpha\}.$$

Пересечением семейства множеств A называется множество

$$\bigcap_{\alpha \in \Lambda} A_\alpha = \{x \mid \text{для всех } \alpha \in \Lambda \text{ имеем } x \in A_\alpha\}.$$

Теорема 4. Пусть Λ – непустое индексирующее множество и $A = \{A_\alpha \mid \alpha \in \Lambda\}$ – индексированное семейство множеств. Тогда:

- 1) для каждого $\beta \in \Lambda$ имеем $\bigcap_{\alpha \in \Lambda} A_\alpha \subseteq A_\beta$;
- 2) для каждого $\beta \in \Lambda$ имеем $A_\beta \subseteq \bigcup_{\alpha \in \Lambda} A_\alpha$;
- 3) $\overline{\bigcap_{\alpha \in \Lambda} A_\alpha} = \bigcup_{\alpha \in \Lambda} \overline{A_\alpha}$;
- 4) $\overline{\bigcup_{\alpha \in \Lambda} A_\alpha} = \bigcap_{\alpha \in \Lambda} \overline{A_\alpha}$;

Доказательство. Мы будем доказывать утверждения 1 и 3. Доказательства утверждений 2 и 4 включены в задачу 6.

Для доказательства утверждения 1 положим $\beta \in \Lambda$ и заметим, что если $x \in \bigcap_{\alpha \in \Lambda} A_\alpha$, то $x \in A_\alpha$ для всех $\alpha \in \Lambda$. Поэтому $x \in A_\beta$. Это доказывает утверждение 1.

Чтобы доказать утверждение 3, будем доказывать, что каждое множество есть подмножество другого множества. Положим сначала, что $x \in \overline{\bigcap_{\alpha \in \Lambda} A_\alpha}$. Это означает, что $x \notin \bigcap_{\alpha \in \Lambda} A_\alpha$ и поэтому существует $\beta \in \Lambda$, для которого $x \notin A_\beta$. Следовательно, $x \in \neg A_\beta$, т.е. $x \in \bigcup_{\alpha \in \Lambda} \overline{A_\alpha}$. Поэтому доказано включение

$$\overline{\bigcap_{\alpha \in \Lambda} A_\alpha} \subseteq \bigcup_{\alpha \in \Lambda} \overline{A_\alpha}. \quad (1)$$

Сейчас положим $x \in \bigcup_{\alpha \in \Lambda} \overline{A_\alpha}$. Это означает, что существует такое $\beta \in \Lambda$, что $x \in \neg A_\beta$, т.е. $x \notin A_\beta$. Следовательно, $x \notin \bigcap_{\alpha \in \Lambda} A_\alpha$, т.е. $x \in \overline{\bigcap_{\alpha \in \Lambda} A_\alpha}$. Тем самым доказано включение

$$\bigcup_{\alpha \in \Lambda} \overline{A_\alpha} \subseteq \overline{\bigcap_{\alpha \in \Lambda} A_\alpha}. \quad (2)$$

Противоположные включения (1) и (2) доказывают утверждение 3. ■

⁴² Λ – прописная греческая буква «ламбда».

Многие другие тождества с множествами справедливы и для индексированных семейств множеств. Например, справедливы дистрибутивные законы для пересечения и обединения:

Теорема 5. Пусть Λ – непустое индексирующее множество, $A = \{A_\alpha \mid \alpha \in \Lambda\}$ – индексированное семейство множеств и пусть B – множество. Тогда:

1. $B \cap (\bigcup_{\alpha \in \Lambda} A_\alpha) = \bigcup_{\alpha \in \Lambda} (B \cap A_\alpha);$
2. $B \cup (\bigcap_{\alpha \in \Lambda} A_\alpha) = \bigcap_{\alpha \in \Lambda} (B \cup A_\alpha).$

§ 3. Отношения

Упорядоченная пара $\langle x, y \rangle$ интуитивно определяется как совокупность, состоящая из двух элементов x и y , расположенных в определенном порядке. Элементы x и y называют соответственно первой и второй компонентами упорядоченной пары. Две пары $\langle x, y \rangle$ и $\langle u, v \rangle$ 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. Одно из возможных определений принадлежит К. Куратовскому⁴³: упорядоченная пара $\langle x, y \rangle$ есть множество $\{\{x\}, \{x, y\}\}$. Таким образом достигается асимметрия между x и y .

Аналогично определяется $\langle x_1, x_2, \dots, x_n \rangle$ – **кортеж из n элементов** x_1, x_2, \dots, x_n , $n > 1$, (его называют еще «упорядоченная n -ка»). Используется также следующее соглашение: $\langle x_1, x_2, \dots, x_n \rangle$ совпадает по смыслу с парами $\langle \langle x_1, x_2, \dots, x_{n-1} \rangle, x_n \rangle$ и $\langle x_1, \langle x_2, \dots, x_{n-1}, x_n \rangle \rangle$.

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

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

Пример 6.

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

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 $(1, 2)$ (рис. 6).

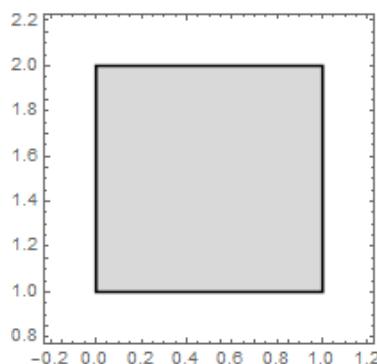


Рис. 6. $[0, 1] \times [1, 2]$

⁴³ Казимеж Куратовский (1896–1980) – польский математик.

Отношением ρ множеств X и Y называется произвольное подмножество $X \times Y$. Если $\langle x, y \rangle \in \rho$, это записывается как $x\text{р}y$; 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 **множеством 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 7.

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

$$A \times B = \{\langle 1, r \rangle, \langle 2, r \rangle, \langle 3, r \rangle, \langle 1, s \rangle, \langle 2, s \rangle, \langle 3, s \rangle\},$$

тогда $\rho = \{\langle 1, r \rangle, \langle 1, s \rangle, \langle 3, s \rangle\}$ есть отношение множеств A и B . Можно также записать $3\rho s$, поскольку $\langle 3, s \rangle \in \rho$. Область определения отношения ρ есть множество $\{1, 3\}$, а множество значений – множество B . Множество $A \times B$ содержит шесть элементов, поэтому имеется $2^6 = 64$ подмножества множества $A \times B$. Следовательно, существует 64 различных отношения на $A \times B$.

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

3. Отношение равенства на множестве \mathbb{R} есть множество $\{\langle x, x \rangle \mid x \in \mathbb{R}\}$. Для этого отношения существует специальное обозначение « $=$ ». Область определения $D_=\$ совпадает с множеством значений $R_=\$ и является множеством \mathbb{R} .

4. Отношение «меньше чем» на множестве \mathbb{Z} есть множество $\{\langle x, y \rangle \mid$ 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 множеством значений $R_<$ и является множеством \mathbb{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 $\rho = \{\langle 1, 1 \rangle, \langle 1, 2 \rangle, \langle 1, 3 \rangle, \langle 1, 4 \rangle, \langle 1, 5 \rangle, \langle 1, 6 \rangle, \langle 2, 2 \rangle, \langle 2, 4 \rangle, \langle 2, 6 \rangle, \langle 3, 3 \rangle, \langle 3, 6 \rangle, \langle 4, 4 \rangle, \langle 5, 5 \rangle, \langle 6, 6 \rangle\}$. Имеем $D_\rho = R_\rho = A$.

6. Отношение $\{\langle x, y \rangle \in \mathbb{R}^2 \mid x^2 + y^2 = 4\}$ есть бинарное отношение на \mathbb{R} . Область определения и множество значений равны и совпадают с множеством $\{t \mid -2 \leq t \leq 2\}$.

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

8. Пусть A – множество женщин, а B – множество мужчин, тогда $\{\langle x, y \rangle \mid y$ 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 булевые операции.

Пример 8. Пусть X, A, B – отрезки, изображенные на рис. 7. Этот рисунок иллюстрирует равенство $(A \cap B) \times X = (A \times X) \cap (B \times X)$.

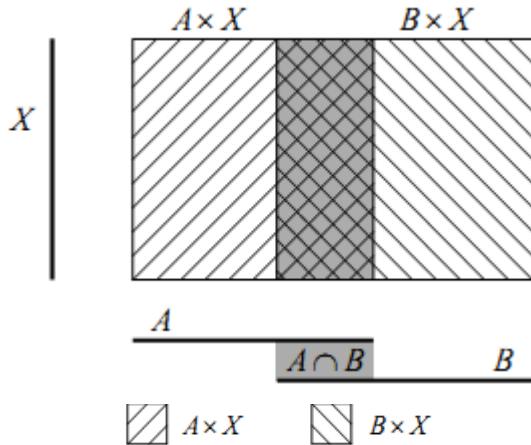


Рис. 7. $(A \cap B) \times X = (A \times X) \cap (B \times X)$

Одной наглядности, конечно, недостаточно для доказательства.

Теорема 6. Пусть A, B и C – множества. Тогда выполнено:

- 1) $A \times (B \cap C) = (A \times B) \cap (A \times C)$;
- 2) $A \times (B \cup C) = (A \times B) \cup (A \times C)$;
- 3) $(A \cap B) \times C = (A \times C) \cap (B \times C)$;
- 4) $(A \cup B) \times C = (A \times C) \cup (B \times C)$;
- 5) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$;
- 6) $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$;
- 7) если $T \subseteq A$, то $T \times B \subseteq A \times B$;
- 8) если $Y \subseteq B$, то $A \times Y \subseteq A \times B$.

Доказательство. Докажем свойства 1, 4, 5 и 7. Остальные утверждения оставим в качестве упражнений.

1. Очевидно, имеем⁴⁴

$$\begin{aligned} < x, y > \in A \times (B \cap C) &\Leftrightarrow x \in A \ \& y \in B \cap C \Leftrightarrow x \in A \ \& y \in B \ \& y \in C \Leftrightarrow \\ &\Leftrightarrow < x, y > \in A \times B \ \& < x, y > \in A \times C \Leftrightarrow < x, y > \in (A \times B) \cap (A \times C). \end{aligned}$$

4. Легко видеть, что

$$\begin{aligned} < x, y > \in (A \cup B) \cap C &\Leftrightarrow (x \in A \vee x \in B) \ \& y \in C \Leftrightarrow \\ &\Leftrightarrow (x \in A \ \& y \in B) \vee (x \in A \ \& y \in C) \Leftrightarrow < x, y > \in (A \times B) \cup (A \times C). \end{aligned}$$

5. Имеем

$$\begin{aligned} < x, y > \in A \times B \setminus C &\Leftrightarrow x \in A \ \& y \in B \setminus C \Leftrightarrow x \in A \ \& y \in B \ \& y \notin C \Leftrightarrow \\ &\Leftrightarrow < x, y > \in A \times B \ \& < x, y > \notin A \times C \Leftrightarrow < x, y > \in (A \times B) \setminus (A \times C). \end{aligned}$$

7. Пусть $T \subseteq A$, тогда

$$< x, y > \in T \times B \Rightarrow x \in T \ \& y \in B \Rightarrow x \in A \ \& y \in B \Rightarrow < x, y > \in A \times B. \blacksquare$$

Есть специальные для бинарных отношений операции. С каждым отношением ρ на $X \times Y$ связано отношение ρ^{-1} на $Y \times X$.

⁴⁴ Символ \Leftrightarrow используется как сокращенная запись слов «тогда и только тогда, когда». Символы $\&$ и \vee есть обозначения союзов «и» и «или», соответственно. Смотрите по этому поводу § 1 главы 4.

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:

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

Другими словами, $\langle y, x \rangle \in \rho^{-1}$ тогда и только тогда, когда $\langle x, y \rangle \in \rho$ 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 9.

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

2. Пусть $\rho = \{ \langle x, y \rangle \mid y \text{ является мужем } x \}$, тогда ρ^{-1} – отношение $\{ \langle x, y \rangle \mid y \text{ – жена } x \}$.

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 $\varphi \circ \rho = \{ \langle x, z \rangle \mid x \in X, z \in Z \text{ и существует } y \in Y, \text{ для которого } \langle x, y \rangle \in \rho \text{ и } \langle y, z \rangle \in \varphi \}$.

Пример 10.

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 7. Для любых отношений выполняются следующие свойства:

$$(\rho^{-1})^{-1} = \rho;$$

$$(\varphi \circ \rho)^{-1} = \rho^{-1} \circ \varphi^{-1}.$$

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

Теорема 8. 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, $\langle a, d \rangle \in (\gamma \circ \varphi) \circ \rho \Leftrightarrow \langle a, b \rangle \in \rho$ 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 $c \in C \Leftrightarrow \langle a, d \rangle \in \gamma \circ (\varphi \circ \rho)$. ■

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 существуют 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 существуют 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 главе 5, § 1.

Пример 11.

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

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 $y \rho_2 z$.

Пример 11а. Отношения, состоящие из конечного числа пар, удобно представлять в виде ориентированных графов, где каждая упорядоченная пара изображается дугой.

1. Как мы видим, отношение « x делится на y », заданное на множестве $\{2, 3, 4, 5, 6, 7, 8, 12\}$, является рефлексивным и транзитивным (рис. 8).

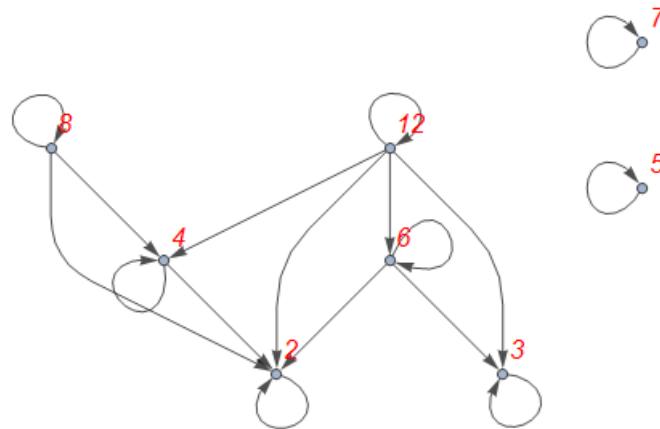


Рис. 8. Отношение « x делится на y »

2. Отношение « x делится на y и частное x/y – простое число», заданное на множестве $\{2, 3, 4, 6, 8, 12\}$, – не транзитивно, не симметрично и не рефлексивно (рис. 9).

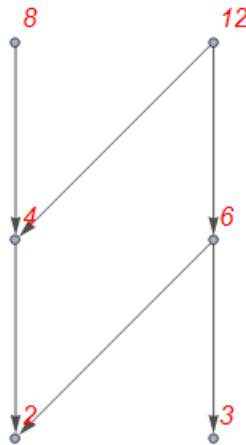


Рис. 9. Отношение « x делится на y
и частное x/y – простое число»

3. Если отношение симметрично, то можно использовать неориентированный граф. На рис. 10 изображено отношение «числа x и y взаимно просты», заданное на множестве $\{1, 2, 3, 4, 5, 6, 7, 8\}$. Это отношение только симметрично.

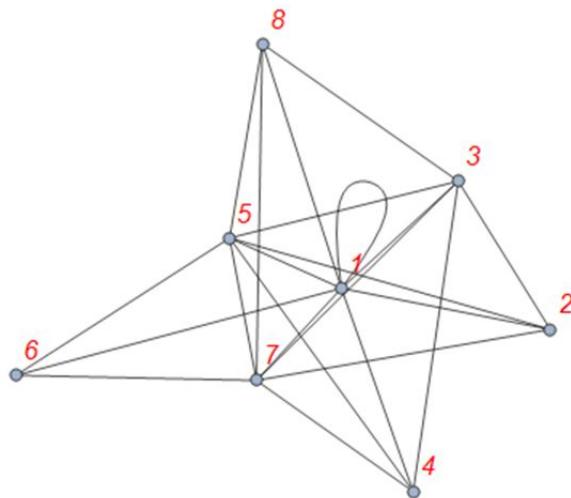


Рис. 10. Отношение «числа x и y взаимно просты»

§ 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 12.

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

2. Пусть $A = \mathbb{R}^2 \setminus \{(0,0)\}$ – множество точек на плоскости за исключением начала координат. Отношение ρ на A определим так: $\langle a, b \rangle \rho \langle c, d \rangle$ тогда и только тогда, когда точки $\langle a, b \rangle$ и $\langle c, d \rangle$ лежат на одной прямой, проходящей через начало координат. Легко показать, что отношение ρ является отношением эквивалентности.

3. Отношение сравнимости по модулю натурального числа n на множестве целых чисел $\mathbb{Z}: x \equiv y \pmod{n}$ выполнено тогда и только тогда, когда $x - y$ делится на n . Это отношение

рефлексивно на \mathbb{Z} , так как для любого $x \in \mathbb{Z}$ имеем $x - x = 0$, 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. $x \equiv z \pmod{n}$.

4. Рассмотрим отношение ρ , определенное на множестве \mathbb{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.

5. Пусть $A = \{1, 2, 3, 4, 5, 6\}$ и отношение ρ_1 на A определено как $\rho_1 = \{\langle 1, 1 \rangle, \langle 2, 2 \rangle, \langle 3, 3 \rangle, \langle 4, 4 \rangle, \langle 5, 5 \rangle, \langle 6, 6 \rangle, \langle 1, 2 \rangle, \langle 1, 4 \rangle, \langle 2, 1 \rangle, \langle 2, 4 \rangle, \langle 3, 5 \rangle, \langle 5, 3 \rangle, \langle 4, 1 \rangle, \langle 4, 2 \rangle\}$. 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 13.

1. Отношение равенства на множестве целых чисел порождает следующие классы эквивалентности: для любого элемента $x \in \mathbb{Z}$ имеем $[x] = \{x\}$, т.е. каждый класс эквивалентности состоит только из одного элемента – числа x .

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

3. Отношение $\rho_1 = \{\langle 1, 1 \rangle, \langle 2, 2 \rangle, \langle 3, 3 \rangle, \langle 4, 4 \rangle, \langle 5, 5 \rangle, \langle 6, 6 \rangle, \langle 1, 2 \rangle, \langle 1, 4 \rangle, \langle 2, 1 \rangle, \langle 2, 4 \rangle, \langle 3, 5 \rangle, \langle 5, 3 \rangle, \langle 4, 1 \rangle, \langle 4, 2 \rangle\}$ 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 9. 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 из 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 14.

1. $X = \{1, 2, 3, 4, 5\}$. Тогда $\{\{1, 2\}, \{3, 5\}, \{4\}\}$ – разбиение множества X .

2. Пусть X – множество студентов университета. Тогда разбиением этого множества является, например, совокупность студенческих групп.

Теорема 10. 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 $x\rho z$. 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 11. 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 9 $x \in [x]$, 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 15.

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 $\{\{1, 2, 4\}, \{5, 3\}, \{6\}\}$.

2. На множестве $\mathbb{N} \times (\mathbb{N} \setminus \{0\})$ определим отношение ρ : $<x, y> \rho <u, v> \Leftrightarrow xv = uy$. Это отношение рефлексивно: $<x, y> \rho <x, y>$, так как $xy = ux$; симметрично: если $<x, y> \rho <u, v>$, то $<u, v> \rho <x, y>$, так как из $xv = uy$ и $v = u/x$ следует, что и $u = v/x$; 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 $xv = uy$ и $uz = vw$, после сокращения получаем $xz = yw$.

Класс эквивалентности, порожденной парой $<x, y>$, для этого отношения ρ определяется соотношением $[<x, y>] = \{<u, v> | x/y = u/v\}$. Каждый класс эквивалентности в этом случае определяет одно положительное рациональное число. Таким образом, фактор-множество $\mathbb{N} \times (\mathbb{N} \setminus \{0\})/\rho$ 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 отношением **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 16.

1. Отношение $x \leq y$ на каждом из множеств $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ и \mathbb{R} есть отношение частичного порядка, причем это линейный порядок (рис. 11).

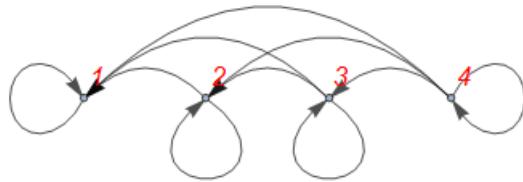


Рис. 11. Линейный порядок $x \leq y$ на множестве $\{1, 2, 3, 4\}$

2. Отношение $x < y$ на каждом из множеств $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ и \mathbb{R} не является отношением частичного порядка, поскольку не рефлексивно.

3. На множестве-степени $P(A)$ отношение $X \subseteq Y$ есть отношение частичного порядка, но оно не является отношением линейного порядка в общем случае. На рис. 12 в случае множества $A = \{x, y, z\}$ линейный порядок отсутствует.

4. Рассмотрим бесконечное множество X , элементы которого сами являются множествами $X = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \dots\}$. Бесконечный список элементов X строится по следующему правилу: \emptyset – первый элемент, и каждый следующий элемент Y в этом списке есть $\alpha \cup \{\alpha\}$, где α – объединение всех предыдущих до Y элементов списка. Отношение \subseteq задает на X линейный порядок. Элементы множеств X участвуют в построении универсума фон-Неймана при аксиоматическом задании теории множеств Цермело–Френкеля (см. главу 6, § 7).

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

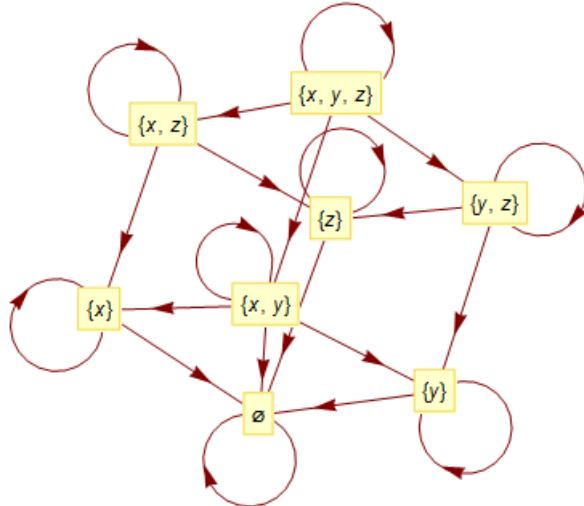


Рис. 12. Частичный порядок $X \subseteq Y$ на множестве $P(\{x, y, z\})$

6. Отношение на множестве слов, определенное как «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**).

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

$$\begin{aligned} 3 &\leq 5 \leq 7 \leq 9 \leq \dots \\ &\leq 2 \times 3 \leq 2 \times 5 \leq 2 \times 7 \leq 2 \times 9 \leq \dots \end{aligned}$$

$$\begin{aligned}
 &\leq 2^2 \times 3 \leq 2^2 \times 5 \leq 2^2 \times 7 \leq 2^2 \times 9 \leq \dots \\
 &\leq 2^3 \times 3 \leq 2^3 \times 5 \leq 2^3 \times 7 \leq 2^3 \times 9 \leq \dots \\
 &\dots \\
 &\dots \\
 &\dots \\
 &\dots \leq 2^n \leq \dots \leq 2^3 \leq 2^2 \leq 2 \leq 1.
 \end{aligned}$$

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 [69. С. 164–169].

§ 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 $\langle x, y \rangle$ и $\langle x, z \rangle$ принадлежат отношению, то $y = z$.

Такое определение понятия «функции» ввел П. Дирихле⁴⁵ (рис. 13). По сути дела, при таком определении мы отождествляем функцию с ее графиком. Это одно из возможных определений. Другое определение, когда функция рассматривается как закон вычисления некоторого значения, используется в главах 8–10.



Рис. 13. Петер Дирихле

Дадим более формальное определение функции.

Отношение f на $X \times Y$ называется **функцией** (или **отображением**) из X в Y и обозначается через $f: X \rightarrow Y$, 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 и говорят, что элемент x отображается в элемент y .

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

⁴⁵ Петер Дирихле (1805–1859) – немецкий математик, внёсший существенный вклад в математический анализ, теорию функций и теорию чисел.

Если $A \subseteq X$, то множество $f(A) = \{f(x) \mid x \in A\}$ называется **образом** множества A при отображении f . Образ $f(X)$ всего множества X называется **областью значений** функции f и иногда обозначается как $\text{Range}(f)$. Если $B \subseteq Y$, то множество $f^{-1}(B) = \{x \mid f(x) \in B\}$ называется **прообразом множества B** .

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 $f: X^n \rightarrow Y$. Тогда пишем $y = f(x_1, \dots, x_n)$ и говорим, что y – значение функции при значениях аргументов x_1, \dots, x_n .

Пример 17.

1. Пусть $X = \{-2, -1, 0, 1, 2\}$, а $Y = \{0, 1, 2, 3, 4, 5\}$. Определим отношение $f \subseteq X \times Y$ как $f = \{<-2, 5>, <-1, 2>, <0, 1>, <1, 2>, <2, 5>\}$. Отношение f – функция из X в Y , так как $f \subseteq X \times Y$ и каждый из элементов X присутствует в качестве первой компоненты упорядоченной пары из f ровно один раз.

2. Пусть $X = \{-2, -1, 0, 1, 2\}$ и $Y = \{0, 1, 2, 3, 4, 5\}$. Функция $f: X \rightarrow Y$ определена соотношением $f(x) = x^2 + 1$. Если $A = \{1, 2\}$, то $f(A) = \{f(x) \mid x \in A\} = \{2, 5\}$ 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 $-1 \in f^{-1}(B)$, так как $f(-1) = 2$, $1 \in f^{-1}(B)$, так как $f(1) = 2$, $-2 \in f^{-1}(B)$, так как $f(-2) = 5$, $2 \in f^{-1}(B)$, так как $f(2) = 5$. 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 есть $f(X) = \{1, 2, 5\}$. 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. 14).

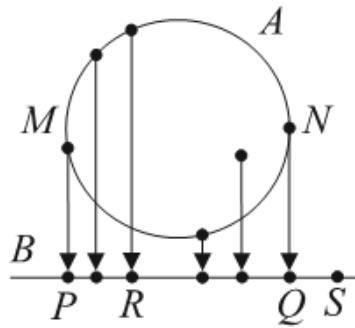


Рис. 14. Ортогональная проекция

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 $f: X \rightarrow Y$. Подчеркнем еще раз три особенности нашего определения функции (рис. 15):

- 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 значений $f(x)$).

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

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

- a) $y \in f(A)$ тогда и только тогда, когда существует такой $x \in A$, что $y = f(x)$;
- b) $x \in f^{-1}(B)$ тогда и только тогда, когда $f(x) \in B$;
- c) из $x \in A$ следует $f(x) \in f(A)$.

Утверждение, обратное c, в общем случае не выполняется. Действительно, возьмем $f(x) = x^2$ и $A = [0, 1]$. Тогда при $x = -0,5$ имеем $f(-0,5) = 0,25 \in [0, 1] = f(A)$. Но $-0,5 \notin A$.

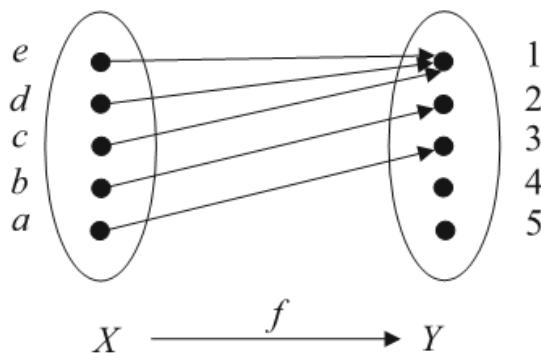


Рис. 15. $f: \{a, b, c, d, e\} \rightarrow \{1, 2, 3, 4, 5\}$

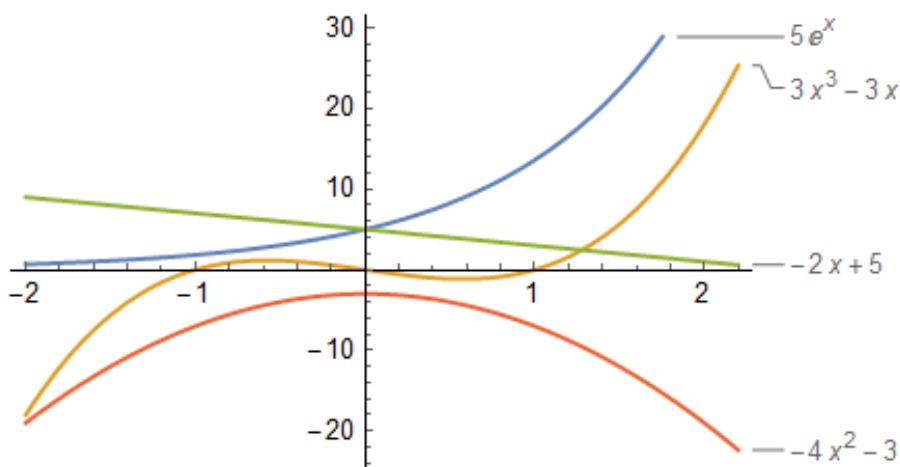


Рис. 16. Четыре функции

Функция $f: X \rightarrow Y$ 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 .

Функция (отображение) $f: X \rightarrow Y$ 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 $\langle x_1, y \rangle \in f$ и $\langle x_2, y \rangle \in f$ 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).

Функция (отображение) $f: X \rightarrow Y$ 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).

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

Пример 18. Рассмотрим четыре функции, отображающие множество действительных чисел во множество действительных чисел $f_i: \mathbb{R} \rightarrow \mathbb{R}$, $i = 1, 2, 3, 4$ (см. рис. 16):

- 1) функция $f_1(x) = 5e^x$ инъективна, но не сюръективна;
- 2) функция $f_2(x) = 3x^3 - 3x$ сюръективна, но не инъективна;
- 3) функция $f_3(x) = -2x + 5$ биективна;
- 4) функция $f_4(x) = -x^2 - 3$ не является ни инъективной, ни сюръективной.

Рассмотрим три множества A , B , C , и пусть даны некоторые отображения $f: A \rightarrow B$ и $g: B \rightarrow C$. Их можем записать в виде цепочки

$$A \xrightarrow{f} B \xrightarrow{g} C.$$

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

Композиция двух функций f и g есть отношение $g \circ f = \{(a, c) \mid \text{существует такое } b, \text{ что } b = f(a) \text{ и } c = g(b)\}$.

Теорема 12. Композиция двух функций есть функция. При этом, если $f: A \rightarrow B$, $g: B \rightarrow C$, то $g \circ f: A \rightarrow C$.

Доказательство. Действительно, если $\langle a, c_1 \rangle \in g \circ f$ и $\langle a, c_2 \rangle \in g \circ f$, то существует такое b_1 , что $b_1 = f(a)$, $c_1 = g(b_1)$, и существует такое b_2 , что $b_2 = f(a)$, $c_2 = g(b_2)$. Поскольку f – функция, то $b_1 = b_2$; поскольку g – функция, то $c_1 = c_2$ и, следовательно, $g \circ f$ – функция. Вторая часть утверждения очевидна. ■

Таким образом, для любого $a \in A$ имеем $(g \circ f)(a) = g(f(a))$ (рис. 17).

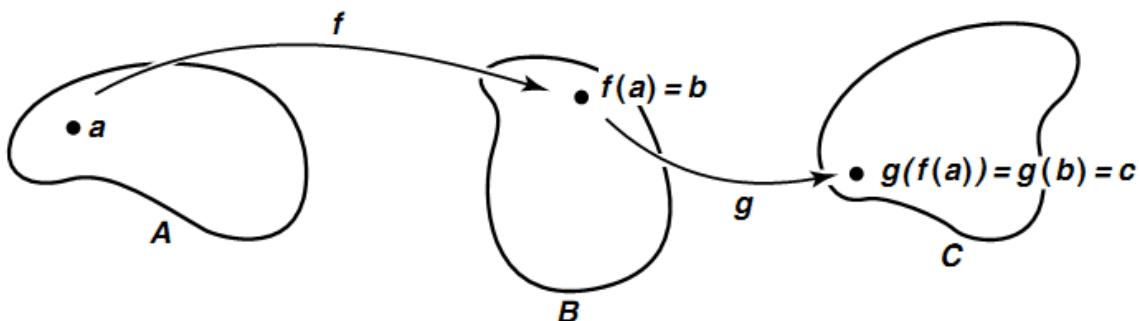


Рис. 17. Композиция функций

Верно также и следующее утверждение.

Теорема 13.

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

Тождественным отображением множества X в себя называется отображение $e_X: X \rightarrow X$ такое, что для любого $x \in X$ имеем $e_X(x) = x$. Тогда, если $f: X \rightarrow Y$, 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 14. Отображение $f: X \rightarrow Y$ имеет обратное отображение $f^{-1}: Y \rightarrow X$ 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 $f: X \rightarrow Y$. Заметим, что для того, чтобы обратное отношение f^{-1} было функцией на $f(X)$, достаточно инъективности функции f . Поэтому функция $f(x) = x^2: \mathbb{R} \rightarrow \mathbb{R}$, 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 $f: X \rightarrow Y$ – биекция, то $f^{-1} \circ f = e_X$ и $f \circ f^{-1} = e_Y$.

§ 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.

Прежде чем рассматривать отношение равнomoщности 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 нем 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. Портъе, 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 – в номер 3 и т.д. Каждый из постояльцев 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 ($n = 1, 2, 3, \dots$) 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 занятим полностью. Но, к сожалению, второй отель скоро сгорел, хотя, к счастью, все его постояльцы не пострадали. Портъе 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 нем, но при этом освободилось бесконечно много номеров (все те, «адреса» которых нечетны), в которых находчивый портвье расселил новых гостей.

Теперь изучим понятие равномощности более строго. Во-первых, мы обнаружили парадоксальный вывод, что «бесконечная часть может иметь столько же элементов, что и целое бесконечное множество», например, множество четных чисел равномочно множеству целых чисел. Точно так же отрезки $[0, 1]$ и $[0, 2]$ равномочны, поскольку отображение $x \rightarrow 2x$ является биекцией.

Отношение равномощности, очевидно, является отношением эквивалентности на множестве всех множеств (транзитивность следует из теоремы 13 (пункт 3)). Для эквивалентных бесконечных множеств мы говорим, что у них одинаковая **мощность**.

Пример 19.

1. Два отрезка AB и CD имеют одинаковую мощность (рис. 18).

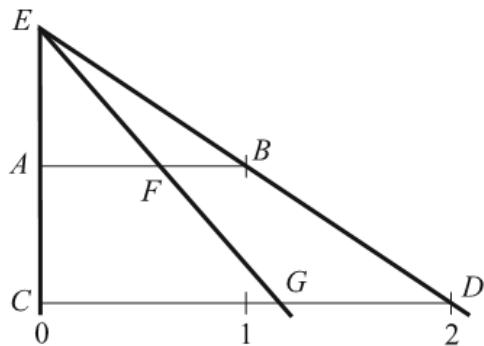


Рис. 18. Биекция между двумя отрезками

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

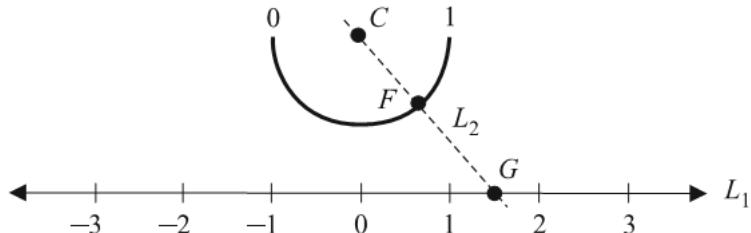


Рис. 19. Полуокружность равномочна всей прямой

3. Любой открытый отрезок равномщен множеству вещественных чисел \mathbb{R} . Для этого замечаем, что любые два отрезка равномочны. Полуокружность радиуса 1 равномощна отрезку $(-1, 1)$ (используем ортогональную биекцию полуокружности на отрезок). Полуокружность равномощна также всей прямой (рис. 19).

4. Полуинтервалы $[0, 1]$ и $(0, 1]$ имеют одинаковую мощность (в силу биекции $x \rightarrow 1 - x$).

5. Множество бесконечных последовательностей нулей и единиц равномочно 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 равномочно 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 и поэтому равномощно каждому из них (см. теорему 15).

Теорема 15 (Кантора–Шрёдера–Бернштейна)⁴⁶. Если множество A равномощно некоторому подмножеству множества B , а множество B равномощно некоторому подмножеству множества A , то A и B равномощны.

Доказательство. Имеем существование двух инъекций $f: A \rightarrow B$ и $g: B \rightarrow A$. Конечно, если хотя бы одно из отображений f и g есть биекция, то доказывать нечего. В общем случае отображения не являются биекциями и мы должны использовать f и g каким-то способом для построения взаимно-однозначного соответствия h между A и B .

Во-первых, определим подмножества $A_n \subseteq A$ для всех $n \in \mathbb{N}$ рекурсивно:

$$a) A_0 = A \setminus g(B);$$

b) определим множество A_1 как образ множества A_0 под действием суперпозиции отображений $f \circ g$, множество A_2 – как образ множества A_1 при отображении $f \circ g$ и т.д. То есть $A_{n+1} = g(f(A_n))$ для всех $n \in \mathbb{N}$.

Во-вторых, определим $B_n \subseteq B$ для всех $n \in \mathbb{N}$ как $B_n = f(A_n)$. Из определения сразу получаем $A_{n+1} = g(B_n)$. Заметим, что если $a \notin A_0$, то $a \in \text{Range}(g)$, так что $a = g(b)$ для некоторого $b \in B$. Так как g – инъекция, то такое $b \in B$ – единственное, и в этом случае можно написать $b = g^{-1}(a)$. Здесь через g^{-1} обозначено «обратное» отображение, определенное на $\text{Range}(g)$, точнее, $g^{-1} = \{\langle a, b \rangle \mid \langle b, a \rangle \in g\}$.

Теперь мы можем определить функцию $h: A \rightarrow B$:

$$h(a) = \begin{cases} f(a), & \text{если } a \in A_n \text{ для некоторого } n \in \mathbb{N}, \\ g^{-1}(a) & \text{иначе.} \end{cases}$$

Это определение дает значение $h(a)$ для всех $a \in A$, потому что если a не принадлежит никакому множеству A_n , то, в частности, $a \notin A_0$ и, следовательно, $g^{-1}(a)$.

Для доказательства биективности h необходимо доказать инъективность и сюръективность. Начнем с доказательства инъективности. Возьмем такие $a, a' \in A$, что $h(a) = h(a')$, и покажем $a = a'$. Если оба элемента a и a' принадлежат $\bigcup\{A_n \mid n \in \mathbb{N}\}$, мы имеем $h(a) = f(a)$ и $h(a') = f(a')$: так как f инъективно, то получаем $a = a'$. Подобным образом, если ни a , ни a' не принадлежит $\bigcup\{A_n \mid n \in \mathbb{N}\}$, то из инъективности g^{-1} следует $a = a'$.

Рассмотрим случай, когда один из двух элементов a, a' , скажем a , принадлежит $\bigcup\{A_n \mid n \in \mathbb{N}\}$, и другой, a' – не принадлежит. Положим, что $a \in A_n$. Тогда $h(a) = f(a) \in B_n$, в то время как $h(a') = g^{-1}(a')$. Имеем $a \neq a'$. Может ли $f(a) = g^{-1}(a')$? Если равенство имеет место, то $a' = g(g^{-1}(a')) = g(f(a))$ (поскольку мы допускаем, что $g^{-1}(a') = f(a) \in A_{n+1}$). Последнее противоречит тому, что $a' \notin \bigcup\{A_n \mid n \in \mathbb{N}\}$. Поэтому в этом случае $h(a) \neq h(a')$. На этом доказательство инъективности заканчивается.

Для доказательства сюръективности покажем, что для каждого $b \in B$ существует $a \in A$, для которого $h(a) = b$. Нет проблем, если $b \in \bigcup\{B_n \mid n \in \mathbb{N}\}$, так как тогда $b = f(a)$ для какого-

⁴⁶ На доказательство этой теоремы претендовали несколько математиков. Эрнст Шрёдер (1841–1902) и Феликс Бернштейн (1878–1956) – немецкие математики. Кантор в своем доказательстве в 1896 использовал вспомогательное утверждение, эквивалентное аксиоме выбора (об аксиоме выбора см. в главе 6, § 7). Доказательство Шрёдера, данное примерно в то же время, содержало ошибку, которая в конечном счете была исправлена. Доказательство Бернштейна, опубликованное в 1896 г., было первым корректным доказательством без использования аксиомы выбора.

то a в некотором A_n . Рассмотрим случай, когда $b \notin \bigcup\{B_n \mid n \in \mathbb{N}\}$, Принадлежит ли $g(b)$ некоторому A_n ? Если $g(b) \in A_0$, то это противоречит тому, что $A_0 = A \setminus g(B)$. Так что $g(b)$ не принадлежит A_0 . Если b не принадлежит B_n для некоторого n , то из-за инъективности g не может быть $g(b) \in g(B_n)$, т.е $g(b)$ не принадлежит A_{n+1} . Поэтому $g(b)$ не принадлежит A_n для всех $n \in \mathbb{N}$. Из определения h получаем $h(g(b)) = g^{-1}(g(b))$ (так как $g(b) \notin \bigcup\{A_n \mid n \in \mathbb{N}\} = b$, что дает $b \in \text{Range}(h)$).

Поэтому h – сюръективное отображение и, следовательно, h есть биекция и теорема доказана. ■

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

Конечные и бесконечные множества отличаются по следующему важному признаку – определению Рассела.

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

Пример 20. Множество натуральных чисел $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ можно поставить во взаимно-однозначное соответствие со множеством неотрицательных четных чисел с помощью биекции $n \rightarrow 2n$. Поскольку неотрицательные четные числа составляют собственное подмножество множества \mathbb{N} , то по признаку Рассела \mathbb{N} является бесконечным множеством (что мы и подозревали до этого!).

Счетное множество – множество, равномошное множеству натуральных чисел \mathbb{N} , т.е. если его можно представить в виде $\{x_0, x_1, x_2, \dots\}$ (здесь x_i – элемент, соответствующий числу i ; соответствие взаимно однозначно, так что x_i все различны).

Например, множество целых чисел \mathbb{Z} счетно, так как целые числа можно расположить в последовательность $0, 1, -1, 2, -2, 3, -3, \dots$. Мощность счетных множеств обозначается, согласно Кантору, символом \aleph_0 (читается *алеф-нуль*, \aleph – «алеф» – первая буква в древнееврейском алфавите).

Теорема 16.

1. Подмножество счетного множества конечно или счетно.
2. Всякое бесконечное множество содержит счетное подмножество.
3. Объединение конечного или счетного числа конечных или счетных множеств конечно или счетно.

Доказательство.

1. Пусть B – подмножество счетного множества

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

Выбросим из последовательности x_0, x_1, x_2, \dots 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 счетно).

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, \dots ; построение не прервется ни на каком шаге, поскольку A бесконечно. Теперь множество $B = \{b_0, b_1, \dots\}$ и будет искомым подмножеством. (Заметим, что B не обязано совпадать с A , даже если A счетно.)

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

a_{00}	a_{01}	a_{02}	a_{03}	...
a_{10}	a_{11}	a_{12}	a_{13}	...
a_{20}	a_{21}	a_{22}	a_{23}	...
a_{30}	a_{31}	a_{32}	a_{33}	...
...

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

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

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 счетное множество. ■

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

Пример 21 (счетные множества).

1. Множество \mathbb{Q} рациональных чисел счетно. В самом деле, рациональные числа представляются несократимыми дробями с целыми числителем и знаменателем. Множество дробей с данным знаменателем счетно, поэтому \mathbb{Q} представимо в виде объединения счетного числа счетных множеств. На рис. 20 показано, каким образом можно задать перечисление всех положительных рациональных чисел.

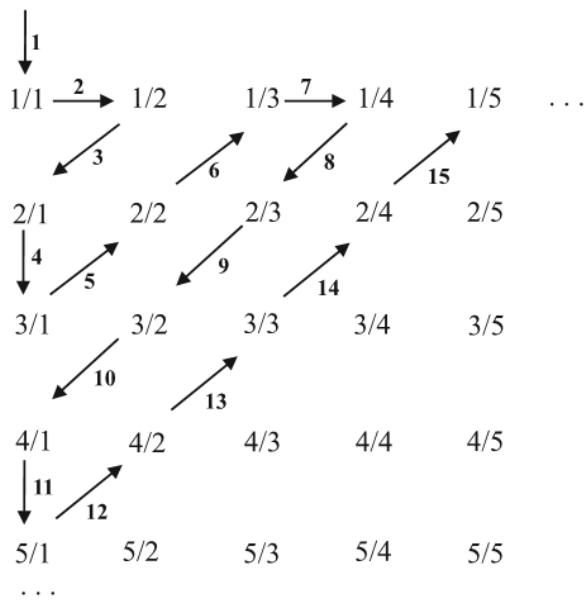


Рис. 20. Множество \mathbb{Q} счетно

2. Множество \mathbb{N}^k , элементами которого являются наборы из k натуральных чисел, счетно.

3. Множество всех конечных последовательностей натуральных чисел счетно. В самом деле, множество всех последовательностей данной длины счетно (предыдущий пример), так что интересующее нас множество разбивается на счетное число счетных множеств.

4. В предыдущем примере не обязательно говорить о натуральных числах – можно взять любое счетное (или конечное) множество. Например, множество всех текстов, использующих русский алфавит (текст можно считать конечной последовательностью букв, пробелов, знаков препинания и т.п.), счетно; то же самое можно сказать о множестве (всех мыслимых) компьютерных программ и т.д.

Теорема 17. Если множество A бесконечно, а множество B конечно или счетно, 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 счетно). 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 счетны, 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 счетными? Классический пример не равномощных бесконечных множеств дает «диагональная конструкция Кантора».

Теорема 18 (Кантор). Множество бесконечных последовательностей нулей и единиц несчетно.

Доказательство. Предположим, что оно счетно. Тогда все последовательности нулей и единиц можно перенумеровать: $\alpha_0, \alpha_1, \dots$. Составим бесконечную вниз последовательность, строками которой будут наши последовательности:

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

(через α_{ij} мы обозначаем j -й член i -й последовательности). Теперь рассмотрим последовательность, образованную стоящими на диагонали членами $\alpha_{00}, \alpha_{11}, \alpha_{22}, \dots$; ее i -й член есть α_{ii} и совпадает с i -м членом i -й 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 все последовательности – противоречие. ■

Множество-степень $P(\mathbb{N})$ – множество подмножеств натурального ряда – равномощно множеству бесконечных последовательностей нулей и единиц. Действительно, сопоставим каждому подмножеству $A \subseteq \mathbb{N}$ бесконечную последовательность $\alpha_0, \alpha_1, \alpha_2, \dots$, 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 18: множество \mathbb{N} не равномощно $P(\mathbb{N})$.

Теорема 19. Отрезок $[0,1]$ равномщен 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 попадет x , и т.д.

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

$$x_0/2 + x_1/4 + x_2/8 + \dots$$

Описанное соответствие не вполне взаимно однозначно: двоично-рациональные числа (вида $m/2^n$) имеют два представления. Например, $3/8 = 0,1100\dots = 0,010111\dots$ Соответствие станет взаимно однозначным, если отбросить дроби с единицей в периоде. Но таких дробей счетное 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 обозначается символом **C** (читается «континуум»).

Докажем следующий удивительный факт.

Теорема 20. 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 19). Осталось заметить, что паре последовательностей нулей и единиц $(x_0 x_1 x_2 \dots, y_0 y_1 y_2 \dots)$ можно поставить в соответствие последовательность-смесь $x_0 y_0 x_1 y_1 x_2 y_2 \dots$ и что это соответствие будет взаимно однозначным. ■

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

Кантор доказал и обобщение теоремы 18.

Теорема 21. Никакое множество X не равномощно множеству $P(X)$ всех своих подмножеств.

Доказательство. Очевидно, не существует взаимно однозначного соответствия между пустым множеством \emptyset и его множеством-степенью $P(\emptyset) = \{\emptyset\}$, содержащим один элемент. Теперь предположим, что X – не пусто и существует биекция f между X и $P(\emptyset)$. 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

$$\begin{aligned} f(1) &= \{2, 5, 7, 9, 10\}, \\ f(2) &= \{2, 4, 6, 8, \dots\}, \\ f(3) &= \emptyset, \\ f(4) &= \{1, 2, 3, 4, 5, 6, 7, \dots\}, \\ f(5) &= \{1, 2\}, \\ &\dots \end{aligned}$$

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 $W = \{x \mid x \in X \text{ и } x \notin f(x)\}$. 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 $P(X)$ неверно. ■

Пример 22.

Пусть $X = \{1, 2, 3, 4\}$ и

$$\begin{aligned} f(1) &= \{2, 4\}, \\ f(2) &= \{1, 2, 3, 4\}, \\ f(3) &= \{1, 3\}, \\ f(4) &= \emptyset. \end{aligned}$$

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

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

Что означает ноль в обозначении \aleph_0 ? Что такое, скажем, \aleph_1 ? Обычно \aleph_1 обозначает наименьшую несчетную мощность. Сравнение мощностей имеет точный смысл. Дело в том, что различные мощности линейно упорядочиваются [46]. В работе Кантора 1878 года была сформулирована **континуум-гипотеза**: всякое подмножество отрезка либо конечно, либо счетно, либо равномощно всему отрезку. Другими словами, $\aleph_1 = \mathbf{c}$. О дальнейшей судьбе этой гипотезы см. в главе 6, § 7, где кратко рассматривается аксиоматизация теории множеств.

Задачи

Задача 1. Несколько множеств называются *непересекающимися*, если все они попарно не пересекаются. Постройте пример, показывающий, что утверждение «множества A , B и C не пересекаются» означает больше, чем $A \cap B \cap C = \emptyset$.

Задача 2. Постройте пример, показывающий, что для операции разность множеств не выполняется ассоциативность.

Задача 3. Когда возможны равенства: a) $A \cup B = \neg A$; b) $A \cap B = \neg A$; c) $A \cup B = A \cap B$?

Задача 4. Определить операции \cup и \setminus (каждую по отдельности) через операции Δ и \cap .

Задача 5. Введите операцию над множествами, на основе которой могут быть определены все операции, введенные в § 2.

Задача 6. Докажите утверждения 2 и 4 теоремы 4.

Задача 7. Докажите теорему 5.

Задача 8. Докажите, что если множество A состоит из n элементов, то множество-степень $P(A)$ состоит из 2^n элементов.

Задача 9. Пусть упорядоченная пара определена по Куратовскому: $\langle x, y \rangle$ есть множество $\{\{x\}, \{x, y\}\}$. Докажите, что $\langle x, y \rangle = \langle u, v \rangle \Leftrightarrow x = u$ и $y = v$. Сравните ваше доказательство с доказательством в [46. С. 36].

Задача 10. Опишите геометрический образ произведения отрезка на окружность.

Задача 11. Каков будет геометрический образ произведения двух окружностей?

Задача 12. Военный оркестр демонстрировал свое искусство на площади. Сначала музыканты построились в виде квадрата, а затем перестроились в прямоугольник, причем число шеренг увеличилось на 3. Сколько музыкантов в оркестре? Сколько фигур «ладья» можно поставить на шахматной доске так, чтобы они не били друг друга?

Задача 13. Докажите утверждения 2, 3, 6 и 8 из теоремы 6.

Задача 14. Опишите множество точек координатной плоскости, координаты которых удовлетворяют соотношению $|x| + |y| = 1$.

Задача 15. Какое отношение выполняется для координат $\langle x, y \rangle$ точек, составляющих отрезки прямых, лежащих внутри квадрата $\langle 0, 10 \rangle \times \langle 0, 10 \rangle$ на рис. 21?

Задача 16. Является ли отношение « x делится на y » отношением частичного (линейного) порядка на множестве \mathbb{N} ? А на множестве \mathbb{Z} ?

Задача 17. Являются ли отображениями следующие отношения на множестве живущих людей?

- A. Каждому человеку ставится в соответствие его дочь.
 B. Каждому человеку ставится в соответствие его мать.
 C. Каждому человеку ставится в соответствие его год рождения.

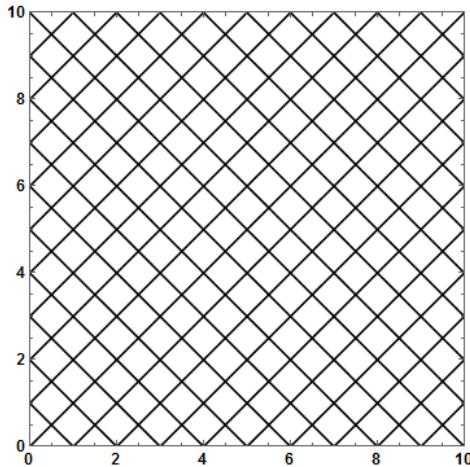


Рис. 21. Определите отношение

Задача 18. Участникам математической олимпиады было предложено пять задач. Является ли функцией соответствие, сопоставляющее каждому участнику:

- a) номера решенных им задач;
 b) сумму номеров решенных им задач?

Задача 19. Найдите область определения функции $y = \sqrt{3 - \sqrt{x^2 - 16}}$.

Задача 20. Будут ли наложениями или вложениями отображения:

- a) каждому человеку ставится в соответствие его мать;
 b) каждому человеку ставится в соответствие его год рождения.

Задача 21. Для функции $y = \sqrt{3 - \sqrt{x^2 - 16}}$ найдите прообраз отрезка $[1, 2]$.

Задача 22. Пусть $f: X \rightarrow Y$ и $A \subseteq X$. Для каких отображений выполнено утверждение: элемент $x \in A$ тогда и только тогда, когда $f(x) \in f(A)$ (см. замечание 3, с).

Задача 23. Докажите теорему 13.

Задача 24. Пусть $f: A \rightarrow B$ и $A_0 \subseteq A$ и $B_0 \subseteq B$.

- a) Докажите, что $A_0 \subseteq f^{-1}(f(A_0))$ и равенство имеет место, если f инъективно.
 b) Докажите, что $f(f^{-1}(B_0)) \subseteq B_0$ и равенство имеет место, если f суръективно.

Задача 25. Проверьте булевы тождества:

- a) $(A \setminus B) \cup (B \setminus C) \cup (C \setminus D) \cup (D \setminus A) = (A \cup B \cup C \cup D) \setminus (A \cap B \cap C \cap D)$;
 b) $(A \Delta B) \Delta (C \Delta D) = (A \Delta D) \Delta (C \Delta B)$;
 c) $(A \setminus B \setminus C) \cup (B \setminus C \setminus D) \cup (C \setminus D \setminus A) \cup (D \setminus A \setminus B) = A \cap B \cup (A \cap C) \cup (A \cap D) \cup (B \cap C) \cup (B \cap D) \cup (C \cap D)$.

В задачах 26 и 27 символ \Rightarrow заменяет слово «следует».

Задача 26. Пусть $f: A \rightarrow B$ и $A_i \subseteq A$ для $i = 0$ и $i = 1$. Докажите, что f сохраняет только включения и объединения множеств:

- a) $A_0 \subseteq A_1 \Rightarrow f(A_0) \subseteq f(A_1)$;
 b) $f(A_0 \cup A_1) = f(A_0) \cup f(A_1)$;
 c) $f(A_0 \cap A_1) \subseteq f(A_0) \cap f(A_1)$ и равенство имеет место, если f инъективно;
 d) $f(A_0 \setminus A_1) \supseteq f(A_0) \setminus f(A_1)$ и равенство имеет место, если f инъективно.

Задача 27. Пусть $f: A \rightarrow B$ и $g: B \rightarrow C$.

- Докажите, что $C_0 \subseteq C \Rightarrow (g \circ f)^{-1}(C_0) = f^{-1}(g^{-1}(C_0))$.
- Докажите, что если f и g инъективны, то $g \circ f$ инъективно.
- Докажите, что если f и g сюръективны, то $g \circ f$ сюръективно.

Задача 28. Пусть M – непустое множество и $\varphi = M^2$. Является ли φ отношением эквивалентности? Отношением частичного порядка?

Задача 29. Докажите ассоциативность симметрической разности $A \Delta (B \Delta C) = (A \Delta B) \Delta C$.

Задача 30. Решить систему уравнений:

$$\begin{cases} A \cap X = B, \\ A \cup X = C, \end{cases}$$

где A, B, C – данные множества, удовлетворяющие условию $B \subseteq A \subseteq C$.

Задача 31. Пусть $A = \{a_1, a_2, \dots, a_n\}$ – конечное множество. Определим отображение

$$f: P(A) \rightarrow \{0,1\}^n$$

следующим образом: если $B \subseteq A$, то $f(B) = \langle \alpha_1, \alpha_2, \dots, \alpha_n \rangle$, где $\alpha_i = 0$ при $a_i \notin B$ и $\alpha_i = 1$ при $a_i \in B$. Как найти $f(B \cap C), f(B \cup C), f(A \setminus B)$, если известны $f(B)$ и $f(C)$?

Задача 32. Перечислите всевозможные линейные порядки на множестве $\{1, 2\}$, на множестве $\{1, 2, 3\}$. (Линейный порядок – это множество упорядоченных пар определенного вида. Значит всевозможные линейные порядки на каком-то множестве – это множество множеств упорядоченных пар.) Выскажите предположение о числе линейных порядков на множестве из n элементов.

Задача 33. Пусть M – некоторое множество, на $P(M)$ определено бинарное отношение $X \rho Y \Leftrightarrow \langle X \Delta Y \text{ – конечное множество} \rangle$. Доказать, что ρ – отношение эквивалентности и найти классы эквивалентности.

Задача 34. На множестве вещественных чисел \mathbb{R} задано бинарное отношение $a \rho b \Leftrightarrow a^2 + a = b^2 + b$. Докажите, что ρ – отношение эквивалентности. Сколько элементов в классе эквивалентности?

Задача 35. Докажите, что $B = (\neg A \cap B) \cup (\neg B \cap A) \Rightarrow A = \emptyset$.

Задача 36. Являются ли отношениями эквивалентности объединение и пересечение двух отношений эквивалентностей?

Задача 37. Является ли транзитивным отношение, обратное для транзитивного отношения? Докажите или опровергните.

Задача 38. Является ли объединение двух транзитивных отношений транзитивным? Докажите или опровергните.

Задача 39. Приведите пример транзитивного отношения ρ , для которого $\rho \circ \rho \neq \rho$.

Задача 40. Пусть $f: A \rightarrow B$ и $g: B \rightarrow C$.

- Если $g \circ f$ инъективно, то что вы можете сказать об инъективности f и g ?
- Если $g \circ f$ сюръективно, то что вы можете сказать об сюръективности f и g ?

Сформулируйте ваши ответы на а и б в виде теорем и докажите их.

Задача 41. Доказать, что если отображение f удовлетворяет условию $f(A \cap B) = f(A) \cap f(B)$ для любых A и B , то f – инъективное отображение.

Задача 42. Рассмотрим множество всех многочленов от одной переменной x , коэффициенты которых – натуральные числа. Упорядочим его так: многочлен P больше многочлена Q , если $P(x) > Q(x)$ для всех достаточно больших x . Покажите, что это определение задает линейный порядок.

Задача 43. Проверить, что $A \Delta B = C \Leftrightarrow B \Delta C = A \Leftrightarrow C \Delta A = B$ (напоминаем, что символ \Leftrightarrow есть замена выражения «тогда и только тогда, когда»).

Задача 44. Пусть ρ – отношение на множестве X . Докажите (символ \Rightarrow заменяет слово «следует»):

- а) ρ симметрично $\Leftrightarrow \rho^{-1} = \rho$;
- б) ρ транзитивно $\Leftrightarrow \rho \circ \rho \subseteq \rho$;
- в) ρ рефлексивно $\Rightarrow \rho \subseteq \rho \circ \rho$;
- г) ρ рефлексивно и транзитивно $\Rightarrow \rho = \rho \circ \rho$.

Одна из главных целей теоретического исследования – найти точку зрения, с которой предмет представляется наиболее простым.

Джозайя Уиллард Гибс (1839–1903), американский физик

Глава 4. Пропозициональная логика

Математическая логика начинается с «логики высказываний» или пропозициональной логики» (лат. *propositio* – высказывание).

§ 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 1. Простые высказывания:

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 какое-нибудь натуральное число, то можно утверждать о его истинности или ложности. Утверждение 10 субъективно, поэтому нельзя говорить о 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”».

Такие предложения, как 10 и 12, принципиально не могут иметь четкой и однозначной интерпретации. Н.Н. Непейвода называет эти предложения **квазивысказываниями** [86. 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 есте-

ственном языке субъективна. Человек является лгуном, если он сознательно говорит ложь. Р. Смаллиан в книге [98] 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**. Когда синтаксическому выражению, содержащему свободные переменные, нужно придать какую-то семантику, то требуется выбрать объекты универсума, чтобы интерпретировать эти переменные.

Пример 2.

1. Переменные x , y и z являются свободными в выражении $x^2 + y^2 = z^2$. Логическое значение этого выражения определяется интерпретацией переменных x , y и z .

2. Переменная x в выражении $x + \sin(1/x)$ является свободной. Числовое значение этого выражение **зависит от x** , т.е. определяется значением (интерпретацией) x .

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

Пример 3.

$$a) \lim_{x \rightarrow 0} \frac{\sin x}{x} = 1, b) \sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}, c) \int_0^1 x^2 + 1 \, dx.$$

В случаях а и с переменная x принимает численные значения из множества вещественных чисел, а в случае б переменная k – натуральное. Но, очевидно, подстановки чисел в эти выражения вместо x и k бессмысленны (говорят, что данные выражения *не зависят от переменных*).

В том случае, когда по смыслу выражения, содержащего переменную, подстановка вместо нее 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 связанный.

В одном выражении одна и та же переменная может употребляться и как свободная и как связанная. Например, в выражении

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

самое левое вхождение переменной x является свободным, а все остальные вхождения переменной – связанными. Точно так же из трех вхождений переменной x в интеграле

$$\int_0^x \sin x \, dx$$

только вхождение переменной x в качестве верхнего предела интегрирования является свободным. 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 ненулевым 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 $A(x_1, x_2, \dots, x_n)$, явно указывая все ее параметры. Тогда если c_1, c_2, \dots, c_n – имена каких-либо объектов из универсума возможных значений переменных x_1, x_2, \dots, x_n соответственно, то через $A(c_1, c_2, \dots, c_n)$ обозначается высказывание, полученное из $A(x_1, x_2, \dots, x_n)$ подстановкой c_1 вместо x_1 , c_2 вместо x_2, \dots, c_n вместо x_n .

Пример 4. 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*⁴⁷.

• **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, для высказываний выполняются следующие два **соглашения**:

1. Имеются исходные неопределяемые понятия **истина** и **ложь** (обозначения: **1** и **0** или **И** и **Л**), которые являются **истинностными (логическими) значениями** высказываний.

⁴⁷ 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).

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

$$\text{«Солнце вращается вокруг Земли»}. \quad (1)$$

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

$$\text{«Неверно, что Солнце вращается вокруг Земли»}. \quad (2)$$

которое, очевидно, снова будет высказыванием (истинным). Обозначим высказывание (1) буквой A , тогда высказывание (2) традиционно обозначается $\neg A$ и называется **отрицанием высказывания A** . Символ \neg называется **операцией (связкой) отрицания**.

Заметим, что мы могли бы поступить по-другому для образования отрицания A , а именно мы могли бы просто изменить сказуемое в выражении (1):

$$\text{«Солнце не вращается вокруг Земли»}. \quad (3)$$

С грамматической точки зрения (2) и (3) – это разные предложения. Но поскольку в дальнейшем мы будем интересоваться лишь истинностными значениями выражений, то высказывания, подобные (2) и (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 имеются два высказывания: A и B . Мы можем образовать новое выражение, соединив два данных выражения союзом «и»: « A и B ». Такое выражение A и B естественно считать истинным только в случае, когда высказывания оба истинны. Например, мы можем построить сложное выражение из выражений (1) и (2), используя союз «и»:

$$\text{«Солнце вращается вокруг Земли и неверно, что Солнце вращается вокруг Земли»}.$$

Выражение « A и B » называется **конъюнкцией** выражений 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 $A \& B$ выражения A и B равноправны, но даже для этой простой связки ее математический смысл не всегда совпадает с содержательным.

Пример 5 [86]. В самом деле, математически $A \& B$ и $B \& A$ означают 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 6. 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 конъюнкцию⁴⁸ 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.

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 $2 \times 2 = 5$ ».

Импликация

Сложное высказывание «Из A следует B » символически записывается $A \supset B$ или $A \rightarrow B$. Знак « \supset » (и \rightarrow) 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.

⁴⁸ Операция конъюнкции двуместная, поэтому мы должны использовать скобки и писать, например, так: $(A \& B) \& C$, но в силу ассоциативности конъюнкции (§ 3, теорема 3) скобки можно опустить.

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 10, то n делится на 5».

Общепризнано, что это утверждение является верным. Поэтому будут истинными и высказывания $A(10)$, $A(8)$ и $A(5)$:

«Если 10 делится на 10, то 10 делится на 5».

«Если 8 делится на 10, то 8 делится на 5».

«Если 5 делится на 10, то 5 делится на 5».

Но, пользуясь соглашением 2 и заменяя утверждения о делимости на 10 (и на 5) на их конкретные логические значения, получаем, что тогда должно быть

$$(I \supset I) = I,$$

$$(L \supset L) = I,$$

$$(L \supset I) = I.$$

Другими словами, должны быть истинны утверждения:

«Из истины следует истина», (4)

«Из лжи следует ложь», (5)

«Из лжи следует истина». (6)

Истинность $A(10)$, $A(8)$ и $A(5)$ мы должны принять, если желаем обеспечить возможность подстановки в доказанные теоремы конкретных значений переменных. А по соглашению 2 нам приходится принять и (4)–(6).

Определение $(L \supset I) = I$ и соответствующее ему утверждение (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 все вороны белые».

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 $A \leftrightarrow B$. Знак \leftrightarrow 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 $A \leftrightarrow B$ истинно тогда и только тогда, когда истинностные значения A и B совпадают, и ложно в противном случае.

Очевидно, можно считать, что формула $A \leftrightarrow B$ 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.

A	B	$\neg A$	$A \& B$	$A \vee B$	$A \supset B$	$A \leftrightarrow B$
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 7.

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».

A : «У людей на руке пять пальцев» – истина;

B : «В этом предложении пять слов» – истина;

$A \& B$: «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.

§ 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»), \leftrightarrow («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 прописными латинскими буквами, возможно, с индексами – натуральными числами, например $Q, R, X, Y, Z, P, P_1, P_2, \dots, P_n, \dots$

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:

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 $(A \wedge B)$, $(A \vee B)$, $(A \supset B)$, $(A \leftrightarrow B)$ – также формулы.

Для любых формул A и B будем называть формулу $\neg A$ *отрицанием* формулы A и, соответственно, формулы $(A \wedge B)$, $(A \vee B)$, $(A \supset B)$, $(A \leftrightarrow B)$ 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 обозначать формулы строчными латинскими буквами⁴⁹, иногда с нижними индексами. Примеры формул: $A, C \leftrightarrow \neg C, \neg(C \supset (X_1 \wedge (B \vee X_2)))$.

Таким образом, мы определили **язык логики высказываний**: это упорядоченная пара $\langle A, F \rangle$, где A – алфавит логики высказываний, F – формулы логики высказываний.

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

$$\neg(C \supset (X_1 \wedge (B \vee X_2))), \quad (1)$$

то предполагаем, что C, X_1, X_2, B – произвольные формулы, 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 (1) 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 (тиографски тождественны). Если какая-то формула не является частью другой формулы, то 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.

⁴⁹ Используя шрифт Verdana.

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

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

можно переписать в виде

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

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

Единственность декомпозиции

Может быть доказано [64. С. 103; 118], 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 $B_1 = B_2$.

Подформулы формул

Определение подформулы, как и определение формулы, рекурсивно:

1. Подформулой пропозициональной переменной является только она сама.
2. Подформулой формулы $\neg A$ являются сама формула $\neg A$, формула A и любая подформула формулы A .
3. Подформулой формулы $A \square B$ (\square – любая бинарная логическая связка) являются 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 8. Множество подформул формулы $\neg(C \supset X_1 \& (B \vee X_2))$ есть

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

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

Введем понятие интерпретации языка логики высказываний. Интерпретировать язык логики высказываний – 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 : $P \rightarrow \{\text{И}, \text{Л}\}$, где P – счетное множество всех пропозициональных переменных, $\{\text{И}, \text{Л}\}$ – множество, состоящее из двух истинностных значений.

Любую интерпретацию ϕ можно продолжить до отображения $\phi : F \rightarrow \{\text{И}, \text{Л}\}$, заданного на множестве всех формул рекурсивным определением.

Для определения $\phi(A)$ частично упорядочим все подформулы формулы A относительно порядка «быть подформулой». И далее для любой подформулы B используем следующие правила:

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

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

Пусть A – произвольная формула и $X_1, X_2, \dots, X_n, n > 0$, – все переменные, входящие в A . Присвоим каждой переменной X_i ($i = 1, 2, \dots, n$) 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, \dots, 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, \dots, X_n .

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

Пример 9. Пусть

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

и $\{\text{Л}, \text{И}\}$ – набор истинностных значений переменных X и Y соответственно. Пусть определена интерпретация φ , для которой $\varphi(X) = \text{Л}$, $\varphi(Y) = \text{И}$ ⁵⁰. Тогда по правилам вычисления $\varphi(A)$ получаем истинностное значение

$$\begin{aligned} \varphi(A) &= \neg \varphi((X \vee (\neg Y \supset X)) \supset \neg Y) = \neg(\varphi(X \vee (\neg Y \supset X)) \supset \varphi(\neg Y)) = \\ &= \neg((\varphi(X) \vee \varphi(\neg Y \supset X)) \supset \neg \varphi(Y)) = \neg((\text{Л} \vee (\varphi(\neg Y) \supset \varphi(X))) \supset \neg \text{И}) = \\ &= \neg((\text{Л} \vee (\neg \varphi(Y) \supset \text{Л})) \supset \text{Л}) = \neg((\text{Л} \vee (\neg \text{И} \supset \text{Л})) \supset \text{Л}) = \neg((\text{Л} \vee (\text{Л} \supset \text{Л})) \supset \text{Л}) = \\ &= \neg((\text{Л} \vee \text{И}) \supset \text{Л}) = \neg(\text{И} \supset \text{Л}) = \neg \text{Л} = \text{И}. \end{aligned}$$

Таким образом, формула A является истинной на наборе $\{X = \text{Л}, Y = \text{И}\}$. И на этом же наборе формула $(X \vee (\neg Y \supset X)) \supset \neg Y$ 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	$\neg Y$	$\neg Y \supset X$	$X \vee (\neg Y \supset X)$	$(X \vee (\neg Y \supset X)) \supset \neg Y$	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 формуле имеется n переменных, то ее таблица истинности содержит 2^n строк. Столбцы соответствуют под-

⁵⁰ Через φ обозначается произвольная интерпретация с указанными значениями на переменных X и Y .

формулам 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).

«Криминальные» задачи

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 неопровергнутое 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 $A \vee B = \text{И}$. Далее, если $A = \text{И}$, то по формуле 3 $C = \text{Л}$. Получили противоречие с исходным предположением. Следовательно, $B = \text{И}$.

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

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	И	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.

Задача 2. Мистер Макгрегор, владелец лавки из Лондона, сообщил по телефону в Скотланд-Ярд о том, что его ограбили. Трех преступников-рецидивистов A , B и C , подозреваемых в ограблении, вызвали на допрос.

Установлено следующее:

1. Каждый из тройки подозреваемых A , B и C в день ограбления побывал в лавке, и никто больше в тот день в лавку не заходил.

2. Если A виновен, то у него был ровно один сообщник.

3. Если B не виновен, то C также не виновен.

4. Если виновны ровно двое подозреваемых, то A – один из них.

5. Если C не виновен, то B также не виновен.

Против кого надо выдвинуть обвинение?

Так же как в предыдущей задаче, будем считать, что истинность переменной означает, что соответствующая персона – преступник. Имеем истинные формулы:

1. $A \vee B \vee C$.

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

3. $\neg B \supset \neg C$.

4. $(A \& B) \vee (A \& C) \vee (B \& C) \supset A$.

5. $\neg C \supset \neg B$.

Рассуждаем на основе формул. Прежде всего заметим, что из формул 3 и 5 следует, что B и C могут быть виновны только одновременно.

Пусть B и C виновны. Тогда из формулы 2 следует, что $A = \text{Л}$, но это противоречит истинности формулы 4.

Следовательно, B и C не виновны. Тогда по формуле 1 $A = \text{И}$, но это противоречит истинности формулы 2.

Мы получили, что не существует варианта, когда все пять исходных формул ложны. Следовательно, преступником является мистер Макгрегор.

Задачи о рыцарях и лжецах

Логик Раймонд Смаллиан в нескольких своих книгах (например, [98]) 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.

Задача 3. В этот раз α говорит о себе и β следующее: «Мы оба или рыцари, или лжецы». Кто они?

Решение. Если α – рыцарь, то β – рыцарь. Если же α – лжец, то он лжет, и β – рыцарь. В любом случае β – рыцарь, а α может быть и рыцарем, и лжецом.

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 также неизвестно, высказывание P – истина или ложь. Но, несомненно, если α – рыцарь, то P истинно, и наоборот, если P истинно, то α – рыцарь. Следовательно, формула $A \leftrightarrow P$ должна всегда быть истинной. И точно так же для любого другого жителя β , говорящего какое-то высказывание Q , должна быть истинна формула $B \leftrightarrow Q$, где B обозначает высказывание « β – рыцарь». Решением задачи является интерпретация языка логики высказываний, в которой все таким образом составленные формулы являются истинными.

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

A	B	$\neg A \ \& \ \neg B$	$A \leftrightarrow \neg A \ \& \ \neg B$
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 $A \leftrightarrow \neg(A \ \& \ B)$, полученной из условия задачи.

A	B	$\neg(A \ \& \ B)$	$A \leftrightarrow \neg(A \ \& \ B)$
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.

Решение задачи 3. Построим таблицу истинности для формулы $A \leftrightarrow (A \leftrightarrow B)$, полученной из условия задачи.

A	B	$A \leftrightarrow B$	$A \leftrightarrow (A \leftrightarrow B)$
И	И	И	И
И	Л	Л	Л
Л	И	Л	И
Л	Л	И	Л

По таблице получаем два решения, в которых единственным образом определено: β – рыцарь.

Задача 4. Перед нами три островитянина α , β и γ . Двое из них высказывают следующие утверждения:

- α сказал: «Мы все лжецы»;
- β сказал: «Один из нас рыцарь».

Кто из них рыцарь, а кто лжец?

Решение. Пусть C обозначает высказывание « γ – рыцарь». Из условия задачи получаем две формулы

$$F = A \leftrightarrow \neg A \ \& \ \neg B \ \& \ \neg C,$$

$$Q = B \leftrightarrow ((A \ \& \ \neg C \ \& \ \neg B) \vee (B \ \& \ \neg C \ \& \ \neg A) \vee (C \ \& \ \neg A \ \& \ \neg B)).$$

Строим таблицу истинности, где E обозначает формулу

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

A	B	C	$\neg A \& \neg B \& \neg C$	F	E	Q
И	И	И	Л	Л	Л	Л
И	И	Л	Л	Л	Л	Л
И	Л	И	Л	Л	Л	И
И	Л	Л	Л	Л	И	Л
Л	И	И	Л	И	Л	Л
Л	И	Л	Л	И	И	И
Л	Л	И	Л	И	И	Л
Л	Л	Л	И	Л	Л	И

Мы видим, что формулы F и Q истинны одновременно, только когда $A = \text{Л}$, $B = \text{И}$, $C = \text{Л}$. Поэтому α и γ – лжецы, а β – рыцарь.

В следующих задачах рыцари и лжецы говорят импликации.

Задача 5. «Так как я рыцарь, то $2 \times 2 = 4$ ».

Задача 6. «Так как я рыцарь, то $2 \times 2 = 5$ ».

Задача 7. «Так как я лжец, то $2 \times 2 = 4$ ».

Задача 8. «Так как я лжец, то $2 \times 2 = 5$ ».

Решения. Нетрудно установить (проделайте это сами), что говорящий в задачах 5 и 7 есть рыцарь; в задаче 8 говорящий может быть кем угодно; в задаче 6, наоборот, говорящий не может быть ни рыцарем, ни лжецом.

Вернемся к автореференции, о которой шла речь в конце первого параграфа.

Крайняя опасность автореференции обыграна в парадоксе Карри⁵¹.

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 9. В этот раз β говорит о себе и α следующее: «Если я рыцарь, то α – рыцарь». Кто они?

Решение. Имеем, формула $B \leftrightarrow (B \supset A)$ есть истина. Построим таблицу истинности

A	B	$B \supset A$	$B \leftrightarrow (B \supset A)$
И	И	И	И
И	Л	И	Л
Л	И	Л	Л
Л	Л	И	Л

Так как $B \leftrightarrow (B \supset A)$ – истина, то $B = \text{И}$, $A = \text{И}$, следовательно, β и α – рыцари.

Таким образом, парадокс Карри возникает, когда мы предполагаем, что формула $B \leftrightarrow (B \supset A)$ есть истина.

⁵¹ Хаскелл Брукс Карри (1900–1982) – американский математик и логик.

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 Wolfram Mathematica [33].

§ 3. Тавтологии и равносильности

Определим несколько важных видов формул.

Формула называется **выполнимой**, если существует интерпретация, в которой эта формула истинна.

Формула называется **опровергимой**, если существует интерпретация, в которой эта формула ложна.

Формула A называется **тавтологией** (или **тождественно истинной**), если она истинна во всех интерпретациях (в этом случае мы будем использовать обозначение $\models A$).

Формула называется **противоречием** (или **тождественно ложной**), если она 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 опровергимой;
- 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, \dots, X_n , а B – формула, полученная из A одновременной подстановкой формул C_1, C_2, \dots, C_n вместо X_1, X_2, \dots, 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, \dots, Y_k , содержащихся в формулах C_1, C_2, \dots, C_n . Если A – тавтология, то докажем, что B – тавтология. От противного. Пусть Y_1, Y_2, \dots, Y_k – все переменные, содержащиеся в формулах C_1, C_2, \dots, C_n . Только эти переменные являются пропозициональными переменными, присутствующими в формуле B . Рассмотрим интерпретацию ϕ , определенную для всех переменных Y_1, Y_2, \dots, Y_k , и предположим, что формула B ложна в этой интерпретации. Тогда $\phi(C_1), \phi(C_2), \dots, \phi(C_n)$ – некоторый набор истинностных значений для переменных X_1, X_2, \dots, X_n соответственно, при которых формула A – ложна (так как формула B построена из подформул C_1, C_2, \dots, C_n таким же образом, как A построена из X_1, X_2, \dots, X_n). Получили противоречие. Случай, когда формула A является противоречием, 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 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. $\models (A \supset B) \supset ((B \supset C) \supset (A \supset C))$ (**цепное рассуждение**).
5. $\models (A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$.
6. $\models (A \& B) \supset A; (A \& B) \supset B$.
7. $\models A \supset (B \supset (A \& B))$.
8. $\models A \supset (A \vee B); B \supset (A \vee B)$.
9. $\models (\neg B \supset \neg A) \supset ((\neg B \supset A) \supset B)$.
10. $\models ((A \supset B) \supset A) \supset A$ (**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, опровергаемой, 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 рассматривающих формулах, но тоже до некоторого предела.

Тавтологичность формул некоторого вида можно установить с помощью доказательства от противного. Подробно метод доказательства от противного описан в главе 7, § 3.

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 10. Является ли формула $((P \supset Q) \& P) \supset Q$ тавтологией?

Решение. Предположим, что $((P \supset Q) \& P) \supset Q$ ложна при некоторых значениях пропозициональных переменных P и Q . Представим наши рассуждения в виде таблицы. Каждая следующая строка таблицы есть логическое следствие предыдущей.

$((P \supset Q) \& P) \supset Q = \text{Л}$	
$(P \supset Q) \& P = \text{И}$	$Q = \text{Л}$
$P \supset Q = \text{И}, P = \text{И}$	
$\text{И} \supset Q = \text{И}$ (подставили в формулу И вместо P)	
$Q = \text{И}$	

Получили противоречие ($Q = \text{И}$ и $Q = \text{Л}$ одновременно), следовательно, исходное предположение о ложности $((P \supset Q) \& P) \supset Q$ неверно, и получаем $\models ((P \supset Q) \& P) \supset Q$.

Задача 11. Является ли тавтологией формула

$$((P \supset Q) \& (\neg R \supset \neg Q) \& (T \supset \neg R)) \supset (P \supset \neg T)?$$

Решение. Предположим, что формула ложна при некоторых значениях пропозициональных переменных P , Q , R и T .

$((P \supset Q) \& (\neg R \supset \neg Q) \& (T \supset \neg R)) \supset (P \supset \neg T) = \text{Л}$	
$(P \supset Q) \& (\neg R \supset \neg Q) \& (T \supset \neg R) = \text{И}$	$P \supset \neg T = \text{Л}$
$P \supset Q = \text{И}, \neg R \supset \neg Q = \text{И}, T \supset \neg R = \text{И}$	$P = \text{И}, \neg T = \text{Л}$
$\text{И} \supset Q = \text{И}, \neg R \supset \neg Q = \text{И}, \text{И} \supset \neg R = \text{И}$ (подставили в формулы И вместо P и T)	
$Q = \text{И}, \neg R = \text{И}, \neg R \supset \neg Q = \text{И}$	
$\text{И} \supset \neg \text{И} = \text{И}$ (подставили в формулы И вместо Q и $\neg R$)	
$\text{И} \supset \text{Л} = \text{И}$. Но это невозможно!	

Пришли к противоречию, следовательно, исходная формула – тавтология.

Задача 12. Является ли формула $((P \supset Q) \& P) \supset (Q \supset \neg P)$ тавтологией?

Решение. Предположим, что формула $((P \supset Q) \& P) \supset (Q \supset \neg P)$ ложна при некоторых значениях пропозициональных переменных P и Q .

$((P \supset Q) \& P) \supset (Q \supset \neg P) = \text{Л}$	
$(P \supset Q) \& P = \text{И}$	$Q \supset \neg P = \text{Л}$
$P \supset Q = \text{И}, P = \text{И}$	$Q = \text{И}, \neg P = \text{Л}$
$\text{И} \supset Q = \text{И}$ (подставили в формулу И вместо P)	
$Q = \text{И}$	

Получили значения переменных ($Q = \text{И}$ и $P = \text{И}$), при которых формула ложна:

$$((P \supset Q) \& P) \supset (Q \supset \neg P) = \text{Л},$$

следовательно, эта формула не является тавтологией.

На множестве пропозициональных формул определим отношение эквивалентности.

Формулы A и B называются **равносильными**⁵², если они принимают одинаковые истинностные значения в любой интерпретации. Равносильность формул обозначается как $A \sim B$.

Установить, равносильные формулы или нет, мы можем с помощью таблицы истинности, построенной сразу для двух формул.

Пример 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 $\neg X \vee \neg Y \sim \neg(X \& Y)$.

Замечание 1. Из определений тавтологии и равносильности сразу следует, что $A \sim B$ тогда и только тогда, когда $\models A \leftrightarrow B$.

Теорема 2. Пусть формулы A и B равносильны, причем X_1, X_2, \dots, 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, \dots, C_n вместо X_1, X_2, \dots, X_n соответственно. Тогда $D \sim E$.

Доказательство следует из предыдущего замечания и теоремы 1.

Теорема 3 (основные равносильности). Для любых формул A, B, C справедливы следующие равносильности:

1. $A \& B \sim B \& A$ (коммутативность $\&$).

⁵² Используют также термин «эквивалентные формулы».

2. $A \& A \sim A$ (идемпотентность $\&$).
3. $A \& (B \& C) \sim (A \& B) \& C$ (ассоциативность $\&$).
4. $A \vee B \sim B \vee A$ (коммутативность \vee).
5. $A \vee A \sim A$ (идемпотентность \vee).
6. $A \vee (B \vee C) \sim (A \vee B) \vee C$ (ассоциативность \vee).
7. $A \vee (B \& C) \sim (A \vee B) \& (A \vee C)$ (дистрибутивность \vee относительно $\&$).
8. $A \& (B \vee C) \sim (A \& B) \vee (A \& C)$ (дистрибутивность $\&$ относительно \vee).
9. $A \& (A \vee B) \sim A$ (первый закон поглощения).
10. $A \vee (A \& B) \sim A$ (второй закон поглощения).
11. $\neg\neg A \sim A$ (снятия двойного отрицания).
12. $\neg(A \& B) \sim \neg A \vee \neg B$ (первый закон де Моргана).
13. $\neg(A \vee B) \sim \neg A \& \neg B$ (второй закон де Моргана).
14. $A \sim (A \& B) \vee (A \& \neg B)$ (первый закон расщепления).
15. $A \sim (A \vee B) \& (A \vee \neg B)$ (второй закон расщепления).
16. $A \leftrightarrow B \sim (A \supset B) \& (B \supset A) \sim (A \& B) \vee (\neg A \& \neg B)$.
17. $A \supset B \sim \neg A \vee B \sim \neg(A \& \neg B)$.
18. $A \vee B \sim \neg A \supset B \sim \neg(\neg A \& \neg B)$.
19. $A \& B \sim \neg(A \supset \neg B) \sim \neg(\neg A \vee \neg B)$.
20. $A \supset B \sim \neg B \supset \neg A$ (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.

Пример 12. Пусть символ \oplus обозначает бинарную операцию «исключающее или», которая выдаёт истину только в случае, когда один из операндов имеет значение истины. Тогда $A \oplus B \sim (A \& \neg B) \vee (B \& \neg A)$, 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 $A \sim B$, то $C_A \sim C_B$.

Для доказательства нам потребуется две леммы.

Лемма 1. Пусть $A \sim B$ и C – произвольная формула. Тогда $\neg A \sim \neg B$, $A \& C \sim B \& C$, $C \& A \sim C \& B$, $A \vee C \sim B \vee C$, $C \vee A \sim C \vee B$, $A \supset C \sim B \supset C$, $C \supset A \sim C \supset B$, $A \leftrightarrow C \sim B \leftrightarrow C$, $C \leftrightarrow A \sim C \leftrightarrow B$.

Доказательство. Докажем, например, равносильность $A \supset C \sim B \supset C$. 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 $A \sim B$ 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 $C_A \sim C_B$.

Доказательство будет проведено в §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, $C_A \sim C_B$. ■

Замечание 2. 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, $A \& B \& C \& D$, можно вообще не использовать скобки. Так как n -кратная дизъюнкция также ассоциативна, то мы можем использовать n -кратную дизъюнкцию также без скобок.

Замечание 3. Для каждой формулы можно указать равносильную ей формулу, не содержащую логических символов « \supset » и « \leftrightarrow ». В самом деле, опираясь на правило равносильных преобразований, можно в исходной формуле каждую подформулу вида $A \leftrightarrow B$ 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 из теоремы 3).

§ 4. Логическое следование

Дадим основные определения этого параграфа.

Непустое множество формул Γ будем называть **выполнимым**⁵³, если существует интерпретация φ , что все формулы из Γ в интерпретации φ истинны. При этом интерпретация φ называется **моделью** множества формул Γ .

Пустое множество выполнимо, и его модель есть любая интерпретация.

Заметим, что если множество Γ конечно и состоит, например, из формул A_1, A_2, \dots, A_n , то невыполнимость множества Γ равносильна противоречивости формулы

$$A_1 \& A_2 \& \dots \& A_n.$$

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 ».

⁵³ Используется также терминология: логически непротиворечивое, непротиворечивое или семантически непротиворечивое множество формул, сравните с логикой первого порядка (глава 5).

Если $\Gamma = \{A_1, A_2, \dots, A_n\}$, то пишут $A_1, A_2, \dots, A_n \models A$. Для $\Gamma = \emptyset$ пишут $\models A$, что согласуется с ранее введенным обозначением для тавтологий, поскольку тождественно истинная формула истинна в любой интерпретации.

Замечание 4. 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 обще, при $n \geq 1$: $A_1, A_2, \dots, A_{n-1}, A_n \models B$ тогда и только тогда, когда $A_1, A_2, \dots, A_{n-1} \models A_n \supset B$.

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 \perp , ибо в них формула $A \supset B$ всегда принимает значение **И** (по правилу импликации). Рассмотрим прочие строки, т.е. такие, 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 $n \geq 2$. Возьмем таблицы истинности для $A_1, A_2, \dots, A_n, B, A_n \supset B$. Рассуждаем, как и выше, но на этот раз в качестве A фигурирует A_n : мы ограничиваемся рассмотрением тех строк, где A_1, A_2, \dots, A_{n-1} дают **И**.

Следствие. При $n \geq 1$ $A_1, A_2, \dots, A_{n-1}, A_n \models B$ тогда и только тогда, когда

$$\models A_1 \supset (\dots (A_{n-1} \supset (A_n \supset B)) \dots).$$

Доказательство проводится n -кратным применением теоремы.

Таким образом, задача установления того, какие формулы являются логическими следствиями данных формул $A_1, A_2, \dots, A_{n-1}, A_n$ сводится к задаче выяснения, какие формулы есть тавтологии. В этом, в частности, и заключается важная роль тавтологий.

Пример 13. 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 $P = \perp$, а $Q = \top$, то $(P \supset Q) \supset (Q \supset P) = \perp$. Противоречие говорит о том, что $Q \supset P$ не является логическим следствием $P \supset Q$.

Чистая математика была открыта
Булем в работе, которая называлась
«Законы мышления».

Берtrand Рассел

§ 5. Булевы алгебры

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.

Определение булевых алгебр и их интерпретации

Рассмотрим первый пример в данной работе аксиоматической теории – теорию булевых алгебр. В главе 6 будет точно определено, что такая аксиоматическая теория, и изучены

различные формальные и неформальные теории. Множество элементов B с заданными на нем двуместными операциями \wedge и \vee (конъюнкцией и дизъюнкцией) и одноместной операцией \neg (отрицанием) называется **булевой алгеброй**, если выполнены следующие аксиомы (f, g, h – произвольные элементы множества):

$$\begin{aligned} f \wedge g &= g \wedge f, f \vee g = g \vee f \text{ (законы коммутативности);} \\ (f \wedge g) \wedge h &= f \wedge (g \wedge h), (f \vee g) \vee h = f \vee (g \vee h) \text{ (законы ассоциативности);} \\ f \wedge f &= f, f \vee f = f \text{ (законы идемпотентности);} \\ f \wedge (g \vee f) &= f, f \vee (g \wedge f) = f \text{ (законы поглощения);} \\ f \wedge (g \vee h) &= (f \wedge g) \vee (f \wedge h), f \vee (g \wedge h) = (f \vee g) \wedge (f \vee h) \text{ (законы дистрибутивности);} \\ \neg(\neg f) &= f \text{ (закон инволюции);} \\ \neg(f \wedge g) &= \neg f \vee \neg g, \neg(f \vee g) = \neg f \wedge \neg g \text{ (законы де Моргана);} \\ f \wedge (g \vee \neg g) &= f, f \vee (g \wedge \neg g) = f \text{ (законы нейтральности).} \end{aligned}$$

Для произвольных элементов f, g справедливы равенства $f \wedge \neg f = g \wedge \neg g$ и $f \vee \neg f = g \vee \neg g$. Действительно, в силу законов нейтральности и коммутативности имеем

$$\begin{aligned} f \wedge \neg f &= (f \wedge \neg f) \vee (g \wedge \neg g) = (g \wedge \neg g) \vee (f \wedge \neg f) = g \wedge \neg g \\ f \vee \neg f &= (f \vee \neg f) \wedge (g \vee \neg g) = (g \vee \neg g) \wedge (f \vee \neg f) = g \vee \neg g. \end{aligned}$$

Если обозначить элемент $f \wedge \neg f$ через **O** и элемент $f \vee \neg f$ через **L**, то для произвольного элемента f получим равенства

$$\begin{aligned} \neg L &= O, \neg O = L, \\ f \wedge L &= f, f \wedge O = O, \\ f \vee L &= L, f \vee O = f. \end{aligned}$$

Булева алгебра называется **вырожденной**, если **O** = **L**; в таком случае в силу равенств $f = f \wedge L = f \wedge O = O$ она не содержит никаких других элементов и поэтому состоит ровно из одного элемента. Мы будем рассматривать только невырожденные алгебры, в которых всегда присутствуют **нейтральные элементы**: **O** (**нулевой элемент**) и **L** (**единичный элемент**).

Выполняется свойство *неразложимости нейтрального элемента L*: из $f \wedge g = L$ следует $f = g = L$. В самом деле, $f = f \vee (g \wedge f) = f \vee L = L$.

А существуют ли вообще булевы алгебры? Может быть, определение противоречиво, и нельзя ввести ни для какого множества булевы операции, так чтобы выполнялись аксиомы булевой алгебры.

Невырожденные булевы алгебры существуют. Укажем некоторые модели (интерпретации) булевых алгебр – конкретные примеры.

Двоичная интерпретация

В реализации вычислений на компьютере очень важна булева алгебра, содержащая только два элемента: нулевой (1) и единичный (0). Определим требуемые операции с помощью таблиц.

\wedge	1	0
1	1	0
0	0	0

\vee	1	0
1	1	1
0	1	0

	1	0
\neg	0	1

Логика высказываний

Положим B – множество высказываний с обычными логическими операциями конъюнкции, дизъюнкции и отрицания. Равенство высказываний интерпретируется как отношение равносильности.

В этом случае аксиомы булевой алгебры являются основными равносильностями логики высказываний и, следовательно, выполнены. Класс эквивалентности относительно равносильности, содержащий все тавтологии, обозначим через **И**. Через **Л** обозначим класс эквивалентности, содержащий все противоречия. Легко убедиться, что **И** и **Л** являются нейтральными элементами (**Л** и **О** соответственно).

Теоретико-множественная интерпретация

Возьмем произвольное непустое множество A и положим $B = \{X \mid X \subseteq A\}$ – множество степени множества A . Определим конъюнкцию элементов B как пересечение множеств, дизъюнкцию сопоставим объединение множеств. Под отрицанием $\neg X$ будем подразумевать разность $A \setminus X$. Таким образом, введенные операции удовлетворяют всем аксиомам булевой алгебры, если под единичным элементом считать множество A , а нулевым элементом является пустое множество \emptyset .

Две последние интерпретации булевой алгебры подсказывают, что многие задачи о формулах высказываний мы можем переводить на язык множеств и использовать диаграммы Венна, а при доказательстве теоретико-множественных тождеств можно использовать таблицы истинности.

Осталось только перевести полностью все операции логики высказываний на язык теории множеств (это сделано в следующем пункте).

Булевые функции

Пусть M – произвольная булева алгебра с определенными операциями \wedge , \vee и \neg . Для натурального $n > 1$ рассмотрим множество B функций $f: M^n \rightarrow M$. Таким образом, имеем $f: \langle x_1, x_2, \dots, x_n \rangle \rightarrow f(x_1, x_2, \dots, x_n)$. На множестве B определим булевые операции следующим образом:

$$\begin{aligned}f_1 \wedge f_2: \langle x_1, x_2, \dots, x_n \rangle &\rightarrow f_1(x_1, x_2, \dots, x_n) \wedge f_2(x_1, x_2, \dots, x_n), \\f_1 \vee f_2: \langle x_1, x_2, \dots, x_n \rangle &\rightarrow f_1(x_1, x_2, \dots, x_n) \vee f_2(x_1, x_2, \dots, x_n), \\\neg f: \langle x_1, x_2, \dots, x_n \rangle &\rightarrow \neg f(x_1, x_2, \dots, x_n).\end{aligned}$$

Введем две постоянные функции

$$\begin{aligned}0: \langle x_1, x_2, \dots, x_n \rangle &\rightarrow \mathbf{O}, \\1: \langle x_1, x_2, \dots, x_n \rangle &\rightarrow \mathbf{L}.\end{aligned}$$

Легко проверить, что множество B с так определенными операциями является булевой алгеброй, где 0 и 1 – нулевой и единичный нейтральный элемент. В этом случае элементы B называются **булевыми функциями**.

Рассмотрим еще одну модель булевой алгебры.

Если булева алгебра M двухэлементна (т.е. содержит только **О** и **Л**), то булевые функции называются **двоичными функциями**.

Если в двухэлементной булевой алгебре элементы **Л** и **О** интерпретировать как «включено» и «выключено», то двоичные функции называются **переключательными функциями**. При такой интерпретации элементы **Л** и **О** в M обозначаются соответственно через 1 и 0.

Если $M = \{\mathbf{И}, \mathbf{Л}\}$ – булева алгебра значений истинности, то булевые функции являются функциями истинности или функциями логики высказываний.

Переключательные функции одной переменной имеют вид $f: \{0, 1\} \rightarrow \{0, 1\}$, и может быть только четыре различных одноместных переключательных функций:

- $0: x \rightarrow 0;$
 $1: x \rightarrow 1;$
 $id: x \rightarrow x$, тождественная функция;
 $neg: x \rightarrow \neg x$, функция отрицания.

Всякую переключательную функцию от n переменных можно задать таблицей из 2^n строк, в которой в каждой строке записывают одну из оценок списка переменных, принимающих значение 0 или 1.

Пример 14. Для $n = 3$ переключательную функцию можно задать таблицей:

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
1	1	1	$f(1, 1, 1)$
1	1	0	$f(1, 1, 0)$
1	0	1	$f(1, 0, 1)$
1	0	0	$f(1, 0, 0)$
0	1	1	$f(0, 1, 1)$
0	1	0	$f(0, 1, 0)$
0	0	1	$f(0, 0, 1)$
0	0	0	$f(0, 0, 0)$

Поскольку длина каждого столбца равна 2^n , а различных столбцов из 0 и 1 длины 2^n имеется 2^{2^n} , то существует точно 2^{2^n} переключательных функций от n переменных. В частности, при $n = 2$ имеем 16 различных переключательных функций.

Вопрос: можно ли свести все переключательные функции к какому-нибудь меньшему числу «базисных» переключательных функций?

Ответ: это возможно. Например, можно все переключательные функции представить как композицию только трех функций: двуместная конъюнкция $x_1 \wedge x_2$, двуместная дизъюнкция $x_1 \vee x_2$, одноместная функция отрицания $\neg x$.

Лемма 3. Для всякой n -местной переключательной функции f выполняется соотношение: для любого i , $1 \leq i \leq n$, имеем

$$\begin{aligned} f(x_1, x_2, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n) = \\ = (x_i \wedge f(x_1, x_2, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n)) \vee (\neg x_i \wedge f(x_1, x_2, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n)). \end{aligned}$$

Доказательство. Первый случай: $x_i = 1$. Тогда $\neg x_i = 0$ и правая часть доказываемого соотношения равна $(1 \wedge f(x_1, x_2, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n)) \vee (0 \wedge f(x_1, x_2, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n))$. Первый член в дизъюнкции равен $f(x_1, x_2, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n)$, а второй 0. Следовательно, правая часть равна $f(x_1, x_2, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_n)$, но точно такое же значение имеет левая часть.

Второй случай: $x_i = 0$. Аналогично, как и в первом случае, получаем, что правая часть равна $f(x_1, x_2, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n)$. ■

Теорема 6 (о булевой нормальной форме). Каждую переключательную функцию можно однозначно представить в следующей (дизъюнктивной) нормальной форме:

$$\begin{aligned} f(x_1, x_2, \dots, x_n) = \\ = (x_1 \wedge x_2 \wedge \dots \wedge x_{n-1} \wedge x_n \wedge f(1, 1, \dots, 1, 1)) \vee \\ \vee (\neg x_1 \wedge x_2 \wedge \dots \wedge x_{n-1} \wedge x_n \wedge f(0, 1, \dots, 1, 1)) \vee \\ \vee (x_1 \wedge \neg x_2 \wedge \dots \wedge x_{n-1} \wedge x_n \wedge f(1, 0, \dots, 1, 1)) \\ \dots \\ \vee (\neg x_1 \wedge \neg x_2 \wedge \dots \wedge \neg x_{n-1} \wedge x_n \wedge f(0, 0, \dots, 0, 1)) \vee \\ \vee (\neg x_1 \wedge \neg x_2 \wedge \dots \wedge \neg x_{n-1} \wedge \neg x_n \wedge f(0, 0, \dots, 0, 0)). \end{aligned}$$

Доказательство. Лемма 3 позволяет «выносить» переменную x_i за знак переключательной функции. Последовательным применением леммы к x_1, x_2, \dots, x_n получаем доказательство. ■

Если в правой части равенства какой-то вызов функции $f(\dots) = 0$, то соответствующий член, разумеется, выпадает из представления. Таким образом, всякая переключательная функция представима в виде дизъюнкции k , $0 \leq k \leq 2^n$, членов – так называемых **совершенных конъюнкций**. Каждая совершенная конъюнкция – это n -местная конъюнкция, у которой все аргументы – либо сами переменные, либо их отрицания.

Пример 15. Пусть переключательная функция задана таблицей.

x_1	x_2	x_3	$f(x_1, x_2, x_3)$
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	1
0	0	0	0

Тогда $f(x_1, x_2, x_3) = (x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3) \vee (\neg x_1 \wedge \neg x_2 \wedge x_3)$.

Всего имеется 16 двуместных переключательных функций. Они распадаются на следующие группы:

- функция без совершенных конъюнкций: $f(x_1, x_2) = 0$;
- функция со всеми четырьмя совершенными конъюнкциями

$$(x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2) = 1.$$

Четыре функции по одной совершенной конъюнкции:

– $x_1 \wedge x_2$ – стандартная конъюнкция;

– $\neg x_1 \wedge \neg x_2$ – функция Пирса⁵⁴ (используется обозначение $x_1 \downarrow x_2$);

– $x_1 \wedge \neg x_2$ – разность x_1 и x_2 (используется обозначение $x_1 \setminus x_2$ в теоретико-множественной интерпретации);

– $\neg x_1 \wedge x_2 = x_2 \setminus x_1$.

Четыре функции по три совершенных конъюнкций:

– $(x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2) = x_1 \vee x_2$ – дизъюнкция;

– $(x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2)$ – штрих Шеффера⁵⁵ (используется обозначение $x_1 | x_2$);

– $(x_1 \wedge x_2) \vee (\neg x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2)$ – если x_1 , то x_2 (используется обозначение $x_1 \supset x_2$ в интерпретации логики высказываний);

– $(x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge \neg x_2) = x_2 \supset x_1$.

Шесть функций по две совершенных конъюнкций:

– $(x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2)$ – эквиваленция (используется обозначение $x_1 \leftrightarrow x_2$ в интерпретации логики высказываний);

– $(x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge x_2)$ – симметрическая разность (используется обозначение $x_1 \Delta x_2$ в теоретико-множественной интерпретации);

– $(x_1 \wedge x_2) \vee (x_1 \wedge \neg x_2)$;

– $(\neg x_1 \wedge x_2) \vee (\neg x_1 \wedge \neg x_2)$;

– $(x_1 \wedge x_2) \vee (\neg x_1 \wedge x_2)$;

– $(x_1 \wedge \neg x_2) \vee (\neg x_1 \wedge \neg x_2)$.

⁵⁴ Чарльз Сандерс Пирс (1839–1914) – американский философ, логик, математик.

⁵⁵ Генри Морис Шеффер (1882–1964) – американский логик.

Вопрос о тождественности двух переключательных функций можно решить, приведя их к совершенной дизъюнктивной нормальной форме или преобразуя булевы выражения по законам булевой алгебры.

Полные системы булевых функций

Система функций $\{f_1, f_2, \dots, f_n\}$ называется **полной**, если любая булева функция может быть выражена через функции f_1, f_2, \dots, f_n с помощью композиции.

Теорема 7. Следующие системы булевых функций полны: $\{\wedge, \vee, \neg\}$; $\{\vee, \neg\}$; $\{\wedge, \neg\}$; $\{\supset, \neg\}$; $\{\Delta, \wedge, 1\}$; $\{\downarrow\}$; $\{\mid\}$.

То, что система функций $\{\wedge, \vee, \neg\}$ является полной, доказано в теореме 6. Полноту остальных систем булевых функций предлагаем доказать читателю.

Рассмотрим систему $\{\Delta, \wedge, 1\}$. Будем вместо символа Δ писать знак сложения «+», а вместо \wedge – знак умножения «» или вообще его опускать, т.е. вместо $x \wedge y$ писать xy . Как введенные операции сложения и умножения действуют, показано в таблице.

x	y	$x + y$	xy
1	1	0	1
1	0	1	0
0	1	1	0
0	0	0	0

Легко проверить, что выполняются свойства, аналогичные обычным свойствам арифметики сложения и умножения: коммутативность, ассоциативность, дистрибутивность умножения относительно сложения. Элементы 1 и 0 ведут себя как обычные числовые единица и нуль, за исключением правила $1 + 1 = 0$.

Поскольку система $\{+, \cdot, 1\}$ полная, то любую переключательную функцию можно представить в виде многочлена с единичными коэффициентами и с переменными, входящими только в первой степени. Такие многочлены называются **многочленами Жегалкина**⁵⁶.

Задачи

Задача 1. Обосновать метод доказательства «разбором случаев»: для того, чтобы доказать формулу $(A_1 \vee A_2 \vee \dots \vee A_n) \supset B$, необходимо и достаточно доказать формулу

$$(A_1 \supset B) \& (A_2 \supset B) \& \dots \& (A_n \supset B).$$

«Криминальные» задачи

Задача 2. На этот раз на допрос были вызваны четверо подозреваемых в ограблении: A, B, C и D . Неопровергнутыми уликами доказано, что, по крайней мере, один из них виновен и что никто, кроме A, B, C и D , в ограблении не участвовал. Кроме того, удалось установить следующее:

1. A , безусловно, не виновен.
2. Если B виновен, то у него был ровно один соучастник.
3. Если C виновен, то у него было ровно два соучастника.

Особенно важно узнать, виновен или не виновен D , так как D был опасным преступником. К счастью, приведенных выше фактов достаточно, чтобы установить виновность или невиновность подозреваемого D . Итак, виновен или не виновен D ?

Задача 3. По обвинению в ограблении перед судом предстали A, B и C . Установлено следующее:

1. Если A не виновен или B виновен, то C виновен.

⁵⁶ Иван Иванович Жегалкин (1869–1947) – российский и советский математик и логик.

2. Если A не виновен, то C не виновен.

Можно ли на основании этих данных установить виновность каждого из трех подсудимых?

Задача 4. По обвинению в ограблении перед судом предстали A , B и C . Установлено следующее:

1. По крайней мере, один из трех подсудимых виновен.

2. Если A виновен и B не виновен, то C виновен.

Этих данных недостаточно, чтобы доказать виновность каждого из трех подсудимых в отдельности, но эти же данные позволяют отобрать двух подсудимых, о которых известно, что один из них заведомо виновен. О каких двух подсудимых идет речь?

Задача 5. Подсудимых четверо: A , B , C и D . Установлено следующее:

1. Если A и B оба виновны, то C был соучастником.

2. Если A виновен, то, по крайней мере, один из обвиняемых B или C был соучастником.

3. Если C виновен, то D был соучастником.

4. Если A не виновен, то D виновен.

Кто из четырех подсудимых виновен вне всякого сомнения и чья вина остается под сомнением?

Задача 6. Подсудимых четверо: A , B , C и D . Установлено следующее:

1. Если A виновен, то B был соучастником.

2. Если B виновен, то либо C был соучастником, либо A не виновен.

3. Если D не виновен, то A виновен и C не виновен.

4. Если D виновен, то A виновен.

Кто из подсудимых виновен и кто не виновен?

Задачи с рыцарями и лжецами (7–19)

Задача 7. Путешественник встретил двух островитян α и β . Островитянин α сказал: «Или я лжец, или β – рыцарь». Кто на самом деле α и кто β ?

Задача 8. Путешественник встретил двух островитян α и β . Островитянин α сказал: «Если β – рыцарь, то я – лжец». Кто на самом деле α и кто β ?

Задача 9. Путешественник встретил трех островитян α , β и γ . Островитянин α сказал: «Мы все лжецы». Островитянин β сказал: «Двое из нас рыцари». Кто на самом деле α и γ ?

Задача 10. Путешественник встретил трех островитян α , β и γ . Путешественник разговаривает с ними по отдельности и начинает с α : «Ты – рыцарь или лжец?» Островитянин сказал так тихо, что путешественник не понял его ответ. «Что сказал α ?» – спросил путешественник у β . Островитянин β ответил: « α сказал, что он лжец». «Не верьте β , он лжет», – вмешивается в разговор γ . «А как насчет α ?» – спрашивает путешественник у γ . «Он сказала правду», – отвечает γ . Кто на самом деле α , β и γ ?

Задача 11. На острове живет ровно сто человек. Путешественник спрашивает первого встречного, сколько из них лжецов. «Один», – отвечает он. На этот же вопрос путешественника следующий островитянин отвечает: «Два». И так продолжается дальше, пока последний островитянин на этот вопрос не ответит: «Сто». Сколько лжецов на острове?

Задача 12. Та же ситуация, что в предыдущей задаче, но первый на этот вопрос отвечает «минимум один», второй – «минимум два», а последний – «минимум сто». Сколько лжецов на острове?

Задача 13. Та же ситуация, что и в задаче 11, но первый на этот вопрос отвечает «максимум один», второй – «максимум два», а последний – «максимум сто». Сколько лжецов на острове?

Задача 14. Однажды на острове встретились четыре местных жителя и между ними произошел такой разговор:

A: D – рыцарь тогда и только тогда, когда B – лжец.

B: D – рыцарь и C – рыцарь.

C: A – лжец или D – рыцарь.

Задача 15. Однажды на острове встретились четыре местных жителя, и между ними произошел такой разговор:

- A: C – рыцарь и D – лжец.*
- B: C – рыцарь или D – рыцарь.*
- C: B – лжец и A – лжец.*

Задача 16. Однажды на острове встретились пять местных жителя, и между ними произошел такой разговор:

- A: C – рыцарь и B – лжец.*
- B: C – лжец тогда и только тогда, когда A – лжец.*
- C: B – лжец тогда и только тогда, когда E – рыцарь.*
- D: A – лжец и B – рыцарь.*

Задача 17. Однажды в одной комнате находилось несколько жителей острова. Трое из них сказали по два высказывания:

- «Нас тут не больше трех человек. Все мы лжецы».
- «Нас тут не больше четырех человек. Не все мы лжецы».
- «Нас тут пятеро. Трое из них – лжецы».

Сколько в комнате человек и сколько среди них лжецов?

Задача 18. Однажды на острове встретились четыре местных жителя и между ними произошел такой разговор:

- «По меньшей мере один из нас лжец».
- «По меньшей мере двое из нас лжецы».
- «По меньшей мере трое из нас лжецы».
- «Среди нас нет лжецов».

Кем является каждый из четырех – рыцарем или лжецом?

Задача 19. Четыре разных человека говорят о себе следующее.

- А. «Так как я рыцарь, то $2 \times 2 = 4$ ».
- Б. «Так как я рыцарь, то $2 \times 2 = 5$ ».
- В. «Так как я лжец, то $2 \times 2 = 4$ ».
- Г. «Так как я лжец, то $2 \times 2 = 5$ ».

Кто они? (Замечание. Вообще говоря, возможны четыре ситуации: 1) человек – рыцарь; 2) человек – лжец; 3) фразу могли сказать и рыцарь, и лжец; 4) если фразу не могут сказать ни рыцарь, ни лжец, то мы считаем, что этот человек не является жителем острова рыцарей и лжецов.)

Задача 20. Проверьте решения задач 5–8 о рыцарях и лжецах из § 2.

Задача 21. Проверьте, что множество B булевых функций, определенное в § 5 (пункт «Булевые функции»), действительно является булевой алгеброй.

Задача 22. Докажите, что каждая из следующих систем булевых функций $\{\wedge, \vee, \neg\}$, $\{\vee, \neg\}$, $\{\wedge, \neg\}$, $\{\supset, \neg\}$, $\{\Delta, \wedge, 1\}$, $\{\downarrow\}$, $\{\}\}$ является полной.

Задача 23. Докажите, что переключательная функция $x \vee y \vee z$ представима в виде многочлена Жегалкина $xyz + xy + xz + yz + x + y + z$.

Задача 24. Докажите, что переключательную функцию

$$(x_1 \wedge x_2 \wedge x_3) \vee (\neg x_1 \wedge \neg x_2 \wedge x_3) \vee (\neg x_1 \wedge x_2 \wedge \neg x_3) \vee (x_1 \wedge \neg x_2 \wedge \neg x_3)$$

можно представить в виде многочлена Жегалкина $x_1x_2 + x_1x_3 + x_1 + x_2 + x_3$.

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.

§ 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 всяkim 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 придет к следующему определению: *k*-местным **предикатом** на универсуме D называется произвольная функция

$$P: D^k \rightarrow \{\text{И}, \text{Л}\}.$$

Пример 1.

1.1. Пусть универсум – множество натуральных чисел \mathbb{N} . Определим одноместный предикат $P: \mathbb{N} \rightarrow \{\text{И}, \text{Л}\}$, так что $P(n) = \text{И}$ тогда и только тогда, когда n есть простое число.

1.2. Пусть универсум есть произвольное множество D , элементы которого сами являются множествами. Определим двуместный предикат $A: D^2 \rightarrow \{\text{И}, \text{Л}\}$, так что $A(X, Y) = \text{И}$ 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 $\pi \in \mathbb{R}$, где \mathbb{R} обозначает множество действительных чисел. Но в логике для единобразия мы пользуемся предикатной записью $P(t_1, \dots, t_n)$, чтобы обозначить высказывание, образованное применением n -местного отношения P к предметам t_1, \dots, 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 \ll в формуле $a \gg b$).

Вообще, всякий раз, когда речь идет о «свойствах» объектов (пример 1.1) или «отношениях» между ними (пример 1.2), то 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.

Правило для квантора всеобщности. 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, то 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.

Переход от формулы $A(x)$ к формуле $\forall x A(x)$ называется **операцией связывания переменной квантором всеобщности**.

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.

Правило для квантора существования. 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.

Переход от формулы $A(x)$ к формуле $\exists x A(x)$ называется **операцией связывания переменной квантором существования**.

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 $A(x_1, x_2, \dots, x_n)$, $n > 1$, применение квантора общности или существования по любой переменной связывает эту переменную и создает предикат с числом параметром, меньшим на единицу. Например, рассмотрим высказывательную форму $x \geq 0 \supset x = y^2$, 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 семь 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, операции над множествами можно точно определить следующим образом:

- пересечение: $A \cap B = \{x \mid (x \in A) \& (x \in B)\}$;
- объединение: $A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$;
- разность: $A \setminus B = \{x \mid (x \in A) \& (x \notin B)\}$;
- симметрическая разность: $A \Delta B = \{x \mid ((x \in A) \& (x \notin B)) \vee ((x \in B) \& (x \notin A))\}$.

Понятия «включение» и «множество-степень» определяются $A \subseteq B \Leftrightarrow \forall x (x \in A \rightarrow x \in B)$ и $P(A) = \{X \mid X \subseteq A\}$, соответственно.

Далее для доказательства основных тождеств алгебры множеств (глава 3, теорема 1) можно использовать логические равносильности.

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \text{ (дистрибутивность } \cup \text{ относительно } \cap\text{).}$$

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) $\{x \mid x \in U \& \neg(x \in A) \& \neg(x \in B)\} =$ (определение дополнения) $\{x \mid x \in \neg A \& x \in \neg B\} = \neg A \cap \neg B.$

Следующие замечания были приведены в главе 3, но без обоснования:

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.

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.

Теперь мы можем воспользоваться свойствами импликации для обоснования. Транзитивность описывается формулой

$$\forall x \forall y \forall z (\langle x, y \rangle \in \rho \& \langle y, z \rangle \in \rho \supset \langle x, z \rangle \in \rho).$$

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

Антисимметричность описывается формулой

$$\forall x \forall y (\langle x, y \rangle \in \rho \& \langle y, x \rangle \in \rho \supset x = y).$$

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, § 7).

§ 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, относящихся 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 предикатах⁵⁷. 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 $\Omega = \langle \text{Cnst}, \text{Fn}, \text{Pr} \rangle$, 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.

Определение **терма** носит индуктивный характер и содержит три пункта. Первые два пункта являются базисом индукции и указывают, какие объекты языка следует непосред-

⁵⁷ Из-за этих ограничений язык называется языком **первого** порядка.

ственno 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, \dots, t_k – термы, то выражение $f(t_1, t_2, \dots, t_k)$ есть терм.

Пример 2. Пусть сигнатура содержит целые числа в качестве констант, двуместные функциональные символы $+$ и \times , и пусть x и y – переменные. Тогда выражения

$$-7 + x, y, ((1 + 2) + (3 + 4)) \times (x + 10)$$

суть термы. Заметим, что функциональные символы « $+$ » и « \times » в данном случае пишутся в инфиксной форме (между аргументами).

Атомарные (или **элементарные**) формулы определяются как выражения вида $P(t_1, t_2, \dots, t_k)$, где P есть k -местный предикатный символ ($k \geq 1$), а t_1, t_2, \dots, t_k – термы. Всякий 0-местный предикатный символ также считается атомной формулой. Кроме того, имеется предикатный символ « $=$ », обозначающий предикат «равенство» и используемый в инфиксном виде. Таким образом, к числу атомарных формул относятся выражения вида $t_1 = t_2$, где t_1, t_2 – термы.

Формулы определяются индуктивно с помощью следующих четырех пунктов, причем первый пункт представляет собой 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 $(A \& B)$, $(A \vee B)$, $(A \supset B)$, $(A \leftrightarrow B)$ суть формулы.
4. Если A – формула, x – переменная, то выражения $\forall x A$ и $\exists x A$ 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, $\{\&, \vee, \supset, \leftrightarrow, \neg, \forall, \exists\}$ – 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 21(4)).

Пример 3. 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

$$\text{‘Григорий Чхартишвили’} = \text{‘Борис Акунин’}.$$

Пример 4. Пусть сигнатура содержит константы, функциональные символы и переменные такие же, как в примере 2. А среди предикатных символов присутствуют двуместный символ F и одноместный символ G . Тогда следующие выражения являются формулами:

$$G(-7), \forall x \exists y F(x, y \times (x + 10)), \exists y ((y = 1 + 2) \supset G(y + 2)), \neg F(3 + 4, x \times x).$$

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 (см. главу 4).

В формулах вида $\forall x A$ и $\exists x A$ 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 (см. главу 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).

Примеры 5.

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 выполняет приказ человека y ».

Предикат $C(x) \Leftrightarrow$ «человек x виноват».

Формула: $(A(\text{Я}, \text{Генерал}) \& \neg B(\text{Генерал}, \text{Я})) \supset (C(\text{Я}) \& \neg C(\text{Генерал}))$.

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 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: $\forall x((A(x) \& \neg B(x)) \supset C(x)) \& ((\neg A(x) \& B(x)) \supset D(x))$.

3. 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.

Решение.

Логика высказываний:

A : «Тело движется равномерно и прямолинейно»

B : «На тело не действуют силы».

C : «Равнодействующая действующих на тело сил равна нулю»

Формула: $A \leftrightarrow (B \vee C)$

Логика предикатов:

Универсум: физические тела.

Предикат $A_1(x) \Leftrightarrow$ «тело x движется равномерно».

Предикат $A_2(x) \Leftrightarrow$ «тело x движется прямолинейно».

Предикат $B(x) \Leftrightarrow$ «на тело x не действуют силы».

Предикат $C(x) \Leftrightarrow$ «на тело x действуют силы, равнодействующая которых равна нулю».

Формула: $\forall x((A_1(x) \& A_2(x)) \leftrightarrow (B(x) \vee C(x)))$.

4. Квадрат гипотенузы равен сумме квадратов катетов.

Решение.

Логика высказываний:

A : «Квадрат гипотенузы равен сумме квадратов катетов»

Формула: A .

Логика предикатов:

Три универсума: множество прямоугольных треугольников, множество отрезков прямых, множество положительных действительных чисел.

Предикат $A(t, x, y, z) \Leftrightarrow$ «отрезки x и y – катеты, а z – гипотенуза прямоугольного треугольника t ».

Функция $d(x)$ вычисляет длину отрезка x .

Формула: $\forall t, x, y, z(A(t, x, y, z) \supset d(x)^2 + d(y)^2 = d(z)^2)$.

Приведем два языка первого порядка, играющие наиболее важную роль в математике и логике.

Язык формальной арифметики предназначен для записи утверждений о натуральных числах. Сигнатура языка содержит единственную константу **0** и три функциональных символа: одноместный S и двуместные « $+$ » и « \times ». 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 \emptyset (см. пример 8 в следующем параграфе).

§ 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 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**⁵⁸), 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.

⁵⁸ Если интерпретация известна, то носитель интерпретации называют также **универсумом**.

Для пропозициональной формулы, задав интерпретацию переменных, мы получаем интерпретацию всей формулы. Точно так же 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 $\Omega = \langle \text{Cnst}, \text{Fn}, \text{Pr} \rangle$, нужно:

1) фиксировать некоторое непустое множество D – носитель интерпретации (также называют универсумом);

2) с каждой константой $c \in \text{Cnts}$ сопоставить элемент $\bar{c} \in D$;

3) с каждым k -местным функциональным символом $f \in \text{Fn}$ сопоставить некоторую k -местную функцию $\bar{f} : D^k \rightarrow D$;

4) с каждым k -местным предикатным символом $P \in \text{Pr}$ сопоставить k -местный предикат $\bar{P} : D^k \rightarrow \{\text{И}, \text{Л}\}$.

Если P есть 0-местный предикатный символ, то с ним сопоставляется одно из двух истинностных значений **И** или **Л**.

Будем называть $\bar{c}, \bar{f}, \bar{P}$ интерпретациями соответственно константы c , функционального символа f и предикатного символа P .

Интерпретация предикатного символа « $=$ » понимается всегда как отношения равенства элементов D .

Универсум D является областью возможных значений для каждой переменной.

Пример 6. Пусть $\Omega = \langle \{0\}, \{S, +, \times\}, \{=\} \rangle$ – сигнатура языка формальной арифметики. Рассмотрим следующую интерпретацию.

Носитель интерпретации – множество натуральных чисел \mathbb{N} ; константа **0** интерпретируется как число 0. Функциональный символ S интерпретируется как $\bar{S}(x) = x + 1$, с привычной точки зрения $S(x)$ – это следующее за x натуральное число. Поэтому термы, имеющие вид $S(0), S(S(0)), S(S(S(0)))$ и т.д., есть имена натуральных чисел 1, 2, 3 и т.д. Функциональные символы « $+$ » и « \times » интерпретируются как операции сложения и умножения соответственно. Язык формальной 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 $S(\dots S(0)\dots)$, где символ S повторяется k раз, кратко будем обозначать k . Таким образом, натуральное число k именуется термом 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 $((xxx)+((2\times x)\times y))+y\times y$ представляет полином $x^2+2xy+y^2$.

Средствами языка формальной арифметики легко записываются простейшие утверждения о свойствах натуральных чисел, например:

- 1) « x – четное число» соответствует $\exists y(x = y + y)$;
- 2) « x – простое число» соответствует « $1 < x$ & $\neg \exists y \exists z(y < x \& z < x \& x = y \times z)$ », где утверждения со знаком « $\&$ » должны быть заменены соответствующими подформулами;
- 3) «существует бесконечно много простых чисел» соответствует $\forall x \exists y(x < y \& y – \text{простое число})$ с уже введенными обозначениями для подформул.

Эта интерпретация называется **стандартной интерпретацией языка формальной арифметики**.

Пример 7. Сигнатуре $\Omega = \langle \{0\}, \{S, +, \times\}, \{=\} \rangle$ 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 $S(\dots S(\mathbf{0})\dots)$, где символ S повторяется k раз, кратко будем обозначать \mathbf{k} . В этом случае термы **1, 2, 3, 4, ...** именуют подряд идущие простые числа 3, 5, 7, 11,

Функциональные символы «+» и « \times » 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 8. Пусть $\Omega = <\{\emptyset\}, \emptyset, \{=, \in\}>$ – сигнатура языка теории множеств. Считаем, что носитель интерпретации есть $\mathbb{R} \cup P(\mathbb{R})^{59}$, где \mathbb{R} – множество вещественных чисел, а $P(\mathbb{R})$ – множество-степень \mathbb{R} .

Константа \emptyset интерпретируется как пустое множество, функциональные символы отсутствуют, и предикатный символ \in интерпретируется как отношение принадлежности вещественного числа 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 $A = \emptyset$.
- 4) $\forall x (x \in A \& x \in B \leftrightarrow x \in C)$ 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 присвоить 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 присвоены определенные значения из носителя интерпретации, говорить о каком-либо истинностном значении данной формулы не имеет смысла.

Пример 9. Рассмотрим три различных интерпретации сигнатуры $\Omega = < M, \emptyset, \{=, \leq\}>$ языка частично упорядоченного множества.

1. Пусть носителем интерпретации будет множество \mathbb{Z} , предикатный символ « $=$ » обозначает совпадение элементов в \mathbb{Z} , а символу « \leq » поставлен в соответствие двуместный предикат $P: \mathbb{Z}^2 \rightarrow \{\text{И}, \text{Л}\}$, такой что $P(m, n) = \text{И}$ тогда и только тогда, когда $m \leq n$.

2. Интерпретацию определим точно так же, но носитель есть \mathbb{Q} вместо \mathbb{Z} .

3. Пусть носителем будет множество \mathbb{R} ; предикатный символ « $=$ » определяется таким образом: $P(x, y) = \text{И}$ тогда и только тогда, когда $|x - y| = 10$; предикатный символ \leq определяется таким образом: $Q(x, y) = \text{И}$ тогда и только тогда, когда $x^2 + y^2 = 1$.

⁵⁹ На самом деле мы здесь используем два носителя и, следовательно, имеются предметные переменные двух типов. Строчными буквами именуются числа из универсума \mathbb{R} , а прописными – множества из универсума $P(\mathbb{R})$. Правильное задание универсума см. в главе 6, § 7.

Рассмотрим формулу в сигнатуре частично упорядоченного множества:

$$\forall x \ y ((x \leq y) \& \neg(x = y)) \supset \exists z (x \leq z) \& (z \leq y) \& \neg(z = x) \& \neg(z = y). \quad (1)$$

Формула (1) истинна в интерпретации 2, но ложна в интерпретациях 1 и 3.

Чтобы придать вышесказанному точный смысл, мы вводим понятие оценки.

Пусть D – носитель интерпретации. **Оценкой** в этой интерпретации называется любое отображение $v: X \rightarrow D$, 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 формальной арифметики и оценке $v(x) = 4$, $v(y) = 2$ терм $((x \times x) + ((2 \times x) \times y)) + (y \times y)$ имеет в качестве значения натуральное число 36.

Перейдем теперь к определению значения формулы при фиксированной интерпретации произвольного языка первого порядка и заданной оценке v переменных. Будем для любого терма t обозначать через $v(t)$ значение терма, порожденное оценкой v переменных. Также через $v(A)$ обозначим значение формулы A ; значением будет **И** или **Л**. Определение $v(A)$ индуктивно.

1. В случае атомарной формулы $A(t_1, t_2, \dots, t_k)$ значением этой формулы будет $\bar{A}(v(t_1), v(t_2), \dots, v(t_k))$, где \bar{A} – k -местный предикат на носителе интерпретации, соответствующий предикатному символу A .

2. Значение формулы $t_1 = t_2$ равно значению равенства $v(t_1) = v(t_2)$.

3. Значение $v(\neg A)$ определяется как $\neg v(A)$, т.е. как логическое отрицание значения $v(A)$.

4. Пусть \square обозначает любую бинарную операцию: конъюнкцию, дизъюнкцию, импликацию или эквиваленцию. Тогда значение $v(A \square B)$ определяется как $v(A) \square v(B)$, где символ « \square » в последнем выражении обозначает соответствующую бинарную операцию (конъюнкцию, дизъюнкцию, импликацию или эквиваленцию) над значениями $v(A)$ и $v(B)$.

5. Значение $v(\forall x A) = \text{И}$ тогда и только тогда, когда $v'(\forall x A) = \text{И}$ для любой оценки v' , отличающейся от v только значением переменной x . Причем значение $v'(x)$ может быть каким угодно.

6. Значение $v(\exists x A) = \text{И}$ тогда и только тогда, когда $v'(\exists x A) = \text{И}$ хотя бы для одной оценки v' , отличающейся от v только значением переменной x . Причем значение $v'(x)$ может быть каким угодно.

Как видим, при определении значений $v(\forall x A)$ и $v(\exists x A)$ значение $v(x)$ также может быть произвольным. Поэтому, используя индукцию по построению формулы A , можно доказать, что истинность формулы A определяется только значениями ее свободных переменных.

Замечание 1. Если переменная x не содержится свободно в формуле A языка первого порядка и задана некоторая интерпретация сигнатуры языка, то истинностные значения формул $\forall x A$, $\exists x A$ и A совпадают.

Имеет место следующее утверждение (см., например, [66]).

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** .

Пример 10. Рассмотрим истинностные значения формул в стандартной интерпретации языка формальной арифметики.

1. $\exists y (\mathbf{0} = y \times 2)$. При оценке $v(y) = 1$ формула $\mathbf{0} = y \times 2$ является ложной. При оценке $v(y) = 0$ формула $\mathbf{0} = y \times 2$ является истинной, и поэтому $\exists y (\mathbf{0} = y \times 2)$ 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 $\exists y (x = y + y)$ для всех y имеет ложное значение, откуда должна следовать ложность исходной формулы $\forall x \exists y (x = y + y)$. Но эта гипотеза требует доказательства.

§ 4. Формулы общезначимые, выполнимые и логически эквивалентные

Введем некоторые термины, которые часто будем использовать в дальнейшем.

Одна и та же замкнутая формула может быть истинной в одной интерпретации и ложной в другой. Формула называется **общезначимой** (или **тождественно истинной**), если она истинна в любой интерпретации при любой ее оценке. Оказывается, общезначимые формулы существуют.

Пример 11.

1. 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.

2. 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 $A(v(x))$ 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 $\exists x A(x)$ будут истинными и импликация дает **И**. В случае б формула $\forall x A(x)$ имеет значение **Л** и импликация снова дает **И**.

3. Формула $\forall x, y (F(x) \supset F(x) \vee F(y))$ является общезначимой для произвольной формулы $F(x)$ 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 $F(a) \supset F(a) \vee F(b)$ по свойствам импликации будет истинна для любых истинностных значений $F(a)$ и $F(b)$.

4. **Принцип пьяницы.** Рэймонд Смаллиан в своей книге [98. 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?

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

$$\exists x(P(x) \supset \forall y P(y)).$$

Эта формула истинна в данной интерпретации при любом распределении пьющих людей в универсуме.

Действительно, любая оценка переменных означает соответствующее распределение пьющих людей. Возможны 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, $\exists x(P(x) \supset \forall y P(y))$ 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 $\exists x(P(x) \supset \forall y P(y))$ имеет значение **И**.

В примере с пьяницей мы нигде не использовали специфику интерпретации, поэтому произвольная формула $A(x)$, выражающая некоторое свойство элементов носителя интерпретации, дает общезначимую формулу

$$\exists x (A(x) \supset \forall y A(y)).$$

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-тавтологию вместо всех пропозициональных переменных подставить какие-нибудь формулы языка первого порядка, то, очевидно, получим формулу языка первого порядка. Будем называть такую формулу также **тавтологией**. Рассмотренный выше пример 1 демонстрирует одну из таких тавтологий $-A \vee \neg A$.

Теорема 1. Любая тавтология общезначима.

Доказательство. Пусть $B(X_1, X_2, \dots, X_n)$ – пропозициональная формула с переменными X_1, X_2, \dots, X_n , а A_1, A_2, \dots, A_n – произвольные формулы языка первого порядка. Обозначим через $B(A_1, A_2, \dots, A_n)$ формулу, полученную подстановкой в $B(X_1, X_2, \dots, X_n)$ формул A_1, A_2, \dots, A_n вместо X_1, X_2, \dots, X_n соответственно. Выберем произвольную интерпретацию и оценку языка первого порядка, тогда каждая формула A_1, A_2, \dots, A_n будет иметь некоторое истинностное значение. Следовательно, мы можем получить истинностное значение формулы $B(A_1, A_2, \dots, A_n)$ такое же, как значение формулы $B(X_1, X_2, \dots, X_n)$, где истинностные значения переменных X_1, X_2, \dots, X_n совпадают с истинностными значениями формул A_1, A_2, \dots, A_n соответственно. Но формула $B(X_1, X_2, \dots, X_n)$ имеет значение **И**, следовательно, значение формулы $B(A_1, A_2, \dots, A_n)$ также **И**. ■

Рассмотренные формулы из примера 11 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 $\phi \models A$.

Пример 12. 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 $A \leftrightarrow B$ общезначима. Если A и B логически эквивалентны, то будем писать $A \sim B$.

Теорема 2. Пусть даны пропозициональные формулы B и C с переменными X_1, X_2, \dots, X_n и A_1, A_2, \dots, A_n – формулы языка первого порядка. Обозначим через $B(A_1, A_2, \dots, A_n)$ и $C(A_1, A_2, \dots, A_n)$ формулы, полученные подстановкой в B и C формул A_1, A_2, \dots, A_n вместо X_1, X_2, \dots, X_n соответственно. Тогда, если $B \equiv C$, то $B(A_1, A_2, \dots, A_n) \sim C(A_1, A_2, \dots, A_n)$.

Доказательство. Так как $B \sim C$ в логике высказываний, то $B \leftrightarrow C$ – пропозициональная тавтология, следовательно, по теореме 1 формула $B(A_1, A_2, \dots, A_n) \sim C(A_1, A_2, \dots, A_n)$ является общезначимой, что и требовалось доказать. ■

Теорема 3. Какие бы ни были формулы A и B , справедливы следующие утверждения о логической эквивалентности:

1. $\forall x(A(x) \& B(x)) \sim \forall x A(x) \& \forall x B(x)$.
2. $\exists x(A(x) \vee B(x)) \sim \exists x A(x) \vee \exists x B(x)$.
3. Если B не содержит свободных вхождений переменной x , то:
 - a) $\exists x(A(x) \& B) \sim \exists x A(x) \& B$;
 - b) $\forall x(A(x) \vee B) \sim \forall x A(x) \vee B$.
4. $\neg \exists x A(x) \sim \forall x \neg A(x)$.
5. $\neg \forall x A(x) \sim \exists x \neg A(x)$.
6. Если $A(x)$ не содержит y , то:
 - a) $\forall x A(x) \sim \forall y A(y)$;
 - b) $\exists x A(x) \sim \exists y A(y)$.

Доказательство. Утверждение 1 говорит, что универсальный квантор всегда можно выносить и распределять относительно $\&$. Утверждение 2 говорит, что квантор существования всегда можно выносить и распределять относительно \vee .

Докажем утверждение 1 теоремы: $\forall x(A(x) \& B(x)) \sim \forall x A(x) \& \forall x B(x)$. Пусть D – носитель интерпретации, при которой левая формула имеет значение И. Тогда при любом значении x формулы $A(x)$ и $B(x)$ истинны и, следовательно, правая часть в 1 также истинна. Наоборот, если правая часть истинна, то при любом значении $c \in D$ формулы $A(c)$ и $B(c)$ истинны, и, следовательно, истинна и левая часть при любом значении $x = c$.

Утверждения За теоремы говорят о том, что квантор существования можно распределять и выносить относительно $\&$, если один из членов конъюнкции не содержит свободных вхождений переменной, которая связывается квантором.

Утверждения 3б теоремы говорят о том, что квантор общности можно распределять и выносить относительно \vee , если один из членов дизъюнкции не содержит свободных вхождений переменной, которая связывается квантором.

Докажем 3а: $\exists x(A(x) \& B) \sim \exists x A(x) \& B$. Пусть D – носитель интерпретации, при которой левая формула имеет значение И. Существует такое $c \in D$, что в данной интерпретации истинна формула $A(c) \& B$, т.е. формула $A(c)$ истинна, а B истинна независимо от значений x . Тогда в этой интерпретации истинны формулы $\exists x A(x)$ и B . То, что из истинности правой части в 3а следует истинность левой части, доказывается аналогично.

Все остальные утверждения в теореме 3 доказываются подобным образом. ■

Из утверждений 4 и 5 следует, что кванторы \forall и \exists взаимозаменяемы.

Доказательство следующих теорем смотрите в [109. С. 40–41].

Теорема 4. Пусть A произвольная формула, а $B \sim C$. Тогда:

- | | |
|-------------------------------------|---|
| 1) $A \& B \sim A \& C$; | 5) $A \leftrightarrow B \sim A \leftrightarrow C$; |
| 2) $A \vee B \sim A \vee C$; | 6) $\neg B \sim \neg C$; |
| 3) $A \supset B \sim A \supset C$; | 7) $\exists x B \sim \exists x C$; |
| 4) $B \supset A \sim C \supset A$; | 8) $\forall x B \sim \forall x C$. |

Теорема 5. Пусть A – произвольная формула, а $B \sim C$. Пусть A_1 получена из A заменой некоторых вхождений формулы B на C . Тогда $A \sim A_1$.

В языках первого порядка по определению существует предикат равенство « $=$ ». Причем общепринято предполагать, что этот предикат обладает следующим свойством⁶⁰. Если A – произвольная формула языка первого порядка, то формула

$$\forall x \forall y (x = y \supset (A(x) \supset A(y)))$$

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, говорящие 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:

$$\forall x \forall y \forall z (x = y \& y = z \supset x = z);$$

$$\forall x \forall y (x = y \supset y = x);$$

$$\forall x \forall y \forall z (x = y \& x = z \supset y = z).$$

Докажем для образца первое из этих равенств: если первый предмет равен второму, а второй – третьему, то первый предмет равен третьему. В самом деле, пусть при конкретных произвольных x, y, z выполнено $x = y$ и $y = z$. Тогда по основному свойству равенства в $x = y$ можно у заменить на z и получим $x = z$, что и требовалось доказать.

Выразимость

Пусть $A(x_1, x_2, \dots, x_n)$ – формула сигнатуры Ω со свободными переменными x_1, x_2, \dots, 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 $R(a_1, a_2, \dots, a_n) = \text{И}$ тогда и только тогда, когда $\varphi \models A(a_1, a_2, \dots, a_n)$ для любых значений a_1, a_2, \dots, a_n из D переменных x_1, x_2, \dots, 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 $P(b) = \text{И}$.

Пример 13. Возьмем стандартную интерпретацию языка формальной арифметики $\langle \{0\}, \{S, +, \times\}, \{=\} \rangle$. Формула $\exists y (x = S(y + y))$ выражает предикат « x – нечетно». Формула $\exists z (y = x + z)$ выражает предикат « $x \leq y$ ». Предикат $x = 0$ можно выразить двумя разными формулами $x = 0$ и $x + x = x$.

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 $B \subset D$ выражимы, то $A \cap B$ выражимо.
2. Если $A \subset D$ и $B \subset D$ выражимы, то $A \cup B$ выражимо.
3. Если $A \subset D$ выражимо, то $D \setminus A$ выражимо.

⁶⁰ Отношение равенства с перечисленными здесь свойствами используется не только в языках первого порядка – оно повсеместно встречается в математике.

Доказательство. Действительно, если формулы P и Q со свободными переменными u и z выражают множества A и B соответственно, то формула $P \& Q$, в которой все свободные вхождения u 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 14. Множество формул $\{\forall xy (x = y), \exists zy (P(z) \& \neg P(y))\}$ 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 $\emptyset \models A$ выполнено тогда и только тогда, когда A – общезначимая формула. Обычно для общезначимых формул пишут просто $\models A$.

Теорема 7. Пусть Γ – некоторое множество замкнутых формул сигнатуры Ω , A и B – замкнутые формулы сигнатуры Ω . Тогда:

- $\Gamma \models A$ и $\Gamma \models B$ тогда и только тогда, когда $\Gamma \models A \& B$;
- $\Gamma \cup \{A\} \models B$ тогда и только тогда, когда $\Gamma \models A \supset B$;
- $\Gamma \models A$ тогда и только тогда, когда множество $\Gamma \cup \{\neg A\}$ несовместно.

Доказательство [109. С. 58–59]. Утверждение (а) очевидно.

Докажем (б). Пусть $\Gamma \cup \{A\} \models B$ и ϕ – произвольная модель множества Γ . Если A не выполнима в ϕ , то по определению истинности $\phi \models A \supset B$. Если же $\phi \models A$, то ϕ является моделью множества $\Gamma \cup \{A\}$, и по условию $\phi \models B$. Значит, и в этом случае $\phi \models A \supset B$. Таким образом, формула истинна в любой модели множества Γ , т.е. $\Gamma \models A \supset B$.

Обратно, если $\Gamma \models A \supset B$ и ϕ – произвольная модель множества $\Gamma \cup \{A\}$, то имеем $\phi \models A \supset B$ и $\phi \models A$. Отсюда немедленно следует, что $\phi \models B$. Значит, B истинна в любой модели множества $\Gamma \cup \{A\}$, т.е. $\Gamma \cup \{A\} \models B$.

Теперь докажем (в). Пусть $\Gamma \models A$. Допустим, что множество $\Gamma \cup \{\neg A\}$ совместно, т.е. существует его модель ϕ . Тогда $\phi \models \neg A$ и ϕ является также моделью для Γ . По условию в этом случае $\Gamma \models A$. Значит, $\phi \models A$ и $\phi \models \neg A$. Но это невозможно, полученное противоречие показывает, что множество $\Gamma \cup \{\neg A\}$ на самом деле несовместно.

Пусть множество $\Gamma \cup \{\neg A\}$ несовместно, т.е. не имеет модели, и пусть ϕ – произвольная модель множества Γ . Тогда $\phi \models A$, так как иначе $\phi \models \neg A$ и ϕ была бы моделью множества $\Gamma \cup \{\neg A\}$. Значит, A истинно в любой модели множества Γ , т.е. $\Gamma \models A$. Теорема доказана. ■

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 15. Пусть сигнатура не содержит никаких констант, функциональных и предикатных символов (равенство присутствует). Рассмотрим одноэлементное множество $\Gamma = \{\forall xy (x = y)\}$ формул этой сигнатуры. Это множество семантически полно, поскольку все его модели – одноэлементные множества, и любая замкнутая формула в этой модели либо истинна, либо ложна.

Математики как французы: все, что вы им говорите, они переводят на свой язык, и это тотчас же становится чем-то совершенно иным.

Иоганн Вольфганг Гёте (1749–1832), немецкий поэт

§ 5. Перевод с естественного языка на логический и обратно

Рассмотрим рекомендации и примеры перевода высказываний на русском языке на язык логики предикатов. Исходные высказывания по большей части 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.⁶¹ 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.

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 минимизировать⁶², 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

⁶¹ Тем более что во многих случаях это было бы сделать затруднительно или невозможно.

⁶² «Не следует создавать сущностей больше необходимого числа» – принцип «бритва Оккама». Оккам Уильям (ок. 1285–1349), английский философ-схоласт, логик.

зывание вида «Все объекты x из U , обладающие свойством A , обладают свойством B ». На языке множеств мы имеем $X_1 \subseteq X_2$, что можно представить на языке первого порядка формулой $\forall x (A(x) \supset B(x))$.

При прежних обозначениях пусть имеется высказывание вида «Есть объект x из U , обладающий свойствами A и B ». На языке множеств имеем $X_1 \cap X_2 \neq \emptyset$ и пишем на языке первого порядка формулу $\exists x (A(x) \& B(x))$.

Таким образом, имеем простые правила:

«Если A , то B » – пишем $\forall x (A(x) \supset B(x))$;

«Некоторые A есть B » – пишем $\exists x (A(x) \& B(x))$.

Пример 16.

1. *Все, что сделано из золота, драгоценно.*

Универсум: изделия. Предикаты: $Z(x)$ – « x сделано из золота», $D(x)$ – « x – драгоценное изделие».

Формула: $\forall x (Z(x) \supset D(x))$.

2. *Некоторые свиньи не умеют летать.*

Универсум: животные. Предикаты: $S(x)$ – « x – свинья», $E(x)$ – « x умеет летать».

Формула: $\exists x (S(x) \& \neg E(x))$.

3. *Ни один ребенок не любит прилежно заниматься.*

Универсум: люди. Предикаты: $B(x)$ – « x – ребенок», $L(x)$ – « x любит прилежно заниматься».

Формула: $\forall x (B(x) \supset \neg L(x))$.

4. *Чтобы не быть собакой, достаточно быть кошкой.*

Универсум: животные. Предикаты: $D(x)$ – « x – собака», $C(x)$ – « x – кошка».

Формула: $\forall x (C(x) \supset \neg D(x))$.

5. *Чтобы не быть собакой, достаточно и необходимо быть кошкой.*

Универсум: животные. Предикаты: $D(x)$ – « x – собака», $C(x)$ – « x – кошка».

Формула: $\forall x (C(x) \leftrightarrow \neg D(x))$.

6. *Гамлет и Клавдий ненавидят друг друга.*

Универсум: люди. Гамлет и Клавдий – константы. Предикат: $A(x, y)$ – « x ненавидит y ».

Формула: $A(\text{Клавдий}, \text{Гамлет}) \& A(\text{Гамлет}, \text{Клавдий})$.

7. *Не все студенты отличники или спортсмены.*

Универсум: $D = \{\text{люди}\}$. Предикаты: $T(x)$ – « x – студент», $O(x)$ – « x – отличник», $S(x)$ – « x – спортсмен».

Формула: $\exists x T(x) \& \neg O(x) \& \neg S(x)$

8. *Логика часто ставит меня в тупик.*

Универсумы: науки и люди. Предикат: $A(x, y)$ – «наука x часто ставит в тупик человека y ». «Логика» и «я» – константы из соответствующих универсумов.

Формула: $A(\text{Логика}, \text{я})$.

9. *Число делится на 25 в том и только в том случае, когда оно делится на 50 либо дает при делении на 50 остаток 25.*

Универсум: \mathbb{N} – натуральные числа. Предикат: $O(x, y, z)$ – « x при делении на y дает остаток z ⁶³».

Формула: $\forall x (O(x, 25, 0) \leftrightarrow (O(x, 50, 0) \vee O(x, 50, 25)))$.

10. *Молодо – зелено.*

Универсум: люди. Предикаты: $B(x)$ – « x – молодой», $G(x)$ – « x – малоопытный».

Формула: $\forall x (B(x) \supset G(x))$.

⁶³ Совершенно излишне для записи этого высказывания заводить три различных предиката: « x делится на 25», « x делится на 50», « x при делении на 50 дает в остатке 25».

11. Все лекарства имеют отвратительный вкус.

Универсум: средства, которые принимаются внутрь. Предикаты: $L(x)$ – « x – лекарство», $B(x)$ – « x имеет отвратительный вкус».

Формула: $\forall x (L(x) \supset B(x))$.

12. Ни у одной ящерицы нет волос.

Универсум: животные. Предикаты: $B(x)$ – « x – ящерица», $G(x)$ – « x имеет волосы».

Формула: $\forall x (B(x) \supset \neg G(x))$.

13. Некоторые лекции невозможно понять.

Универсум: публичные выступления. Предикаты: $B(x)$ – « x – лекция», $G(x)$ – « x – понимаемое выступление».

Формула: $\exists x (B(x) \& \neg G(x))$.

«Многоэтажные» кванторы. Дополнительные ограничения

Рассмотрим утверждение «*Все бешеные собаки смертельно опасны*». Здесь говорится, что если данное животное x – собака, и причем бешеная, то x – смертельно опасное. Следовательно, если предикат $D(x)$ означает «животное x – собака», предикат $M(x)$ – «животное x – бешеное», а предикат $Z(x)$ – « x – смертельно опасное», то формальная запись этого утверждение имеет вид

$$\forall x(D(x) \& M(x) \supset Z(x)).$$

Аналогично утверждение «*Некоторые старательные студенты получают стипендию*» можно записать в виде

$$\exists x(P(x) \& S(x) \& O(x)).$$

$P(x)$ означает « x – студент»; $S(x)$ – « 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 варианта⁶⁴:

$$\forall x(x < 0 \supset \forall y(y > 0 \supset x \times y < 0)),$$

$$\forall x \forall y(x < 0 \& y > 0 \supset x \times y < 0).$$

Хотя эти две формы и эквивалентны, но вторая, пожалуй, несколько выразительнее и яснее подчеркивает равноправие двух чисел. Для последней формулы можно использовать сокращение

$$\forall xy(x < 0 \& y > 0 \supset x \times y < 0),$$

т.е. несколько однородных кванторов соединяются в один. Заметим, что в исходном высказывании не присутствуют явно слова («все», «любые» и т.п.), которые 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:

⁶⁴ Какие еще варианты возможны?

$$\forall x (x \in \mathbb{Z} \supset \exists y (y \in \mathbb{Z} \ \& \ y < x)). \quad (2)$$

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 (2), конечно же, истинно, то утверждение

$$\exists y (y \in \mathbb{Z} \ \& \ \forall x (x \in \mathbb{Z} \supset y < x))$$

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 неопределенно, но, переходя к началу формулы, мы видим, что y должно быть предварительно выбрано. Но какое бы целое число y мы не 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 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

$$\exists z (z \in \mathbb{R} \ \& \ x < z \ \& \ z < y)$$

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

$$\forall x \exists y, z (x \in \mathbb{Z} \supset y \in \mathbb{Z} \ \& \ y > x \ \& \ z \in \mathbb{Z} \ \& \ z < x),$$

но лучше всего перевод:

$$\forall x (x \in \mathbb{Z} \supset \exists y (y \in \mathbb{Z} \ \& \ y > x) \ \& \ \exists z (z \in \mathbb{Z} \ \& \ z < x)),$$

где каждый квантор относится лишь к тем утверждениям, которые он связывает.

Резюме

- Если предложение достаточно сложное, его перевод на формальный язык лучше всего писать изнутри, начиная с 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 прочтите ее начерно, а затем – начисто, изгоняя явное упоминание кванторов и связанных переменных.
- Свободные переменные должны входить в окончательную словесную формулировку утверждений.

Пример 17 [83].

1. Либо каждый любит кого-нибудь, либо не один не любит всех либо некто любит всех, и кто-то не любит никого.

Универсум: люди; предикат $A(x, y)$ выражает отношение « x любит y ». Выразим сначала подформулы:

«каждый любит кого-нибудь» – $\forall x \exists y A(x, y)$;

«некто любит всех» – $\exists x \forall y A(x, y)$;

«не один не любит всех» – $\neg \exists x \forall y A(x, y)$;

«кто-то не любит никого» – $\exists x \forall y \neg A(x, y)$.

Окончательная формула: $\forall x \exists y A(x, y) \vee \neg \exists x \forall y A(x, y) \vee (\exists x \forall y A(x, y) \& \exists x \forall y \neg A(x, y))$.

2. Ты можешь обманывать кого-то все время, ты можешь обманывать всех некоторое время, но ты не можешь обманывать всех все время.

Универсум: люди; предикаты: $A(x, y)$ выражает отношение « x обманывает y некоторое время», $B(x, y)$ выражает отношение « x обманывает y все время». В этой фразе речь идет не о конкретном человеке (константа «ты»), а любом, кто занимается обманом. Создадим сначала подформулы:

«ты можешь обманывать кого-то все время» – $\exists y B(x, y)$;

«ты можешь обманывать всех некоторое время» – $\forall y A(x, y)$;

«ты не можешь обманывать всех все время» – $\neg \forall y B(x, y)$.

Окончательная формула: $\forall x ((\exists y B(x, y) \vee \forall y A(x, y)) \supset \neg \forall y B(x, y))$.

3. Если всякий разумный философ – циник и только женщины являются разумными философами, то тогда если существуют разумные философы, некоторые из женщин – циники.

Универсум: люди; предикаты: $F(x)$ – « x – разумный философ», $W(x)$ – « x – женщина», $C(x)$ – « x – циник». Определим подформулы:

«всякий разумный философ – циник» – $\forall x (F(x) \supset C(x))$;

«только женщины являются разумными философами» – $\forall x (F(x) \supset W(x))$.

Предложению «если существуют разумные философы, некоторые из женщин – циники» соответствует формула $\exists x F(x) \supset \exists x (F(x) \& W(x))$.

Окончательная формула:

$(\forall x (F(x) \supset C(x)) \& \forall x (F(x) \supset W(x))) \supset (\exists x F(x) \supset \exists x (F(x) \& W(x)))$

4. Гипотеза Гольдбаха: любое четное число, начиная с 4, можно представить в виде суммы двух простых чисел⁶⁵.

Универсум – \mathbb{N} . Будем использовать предикаты $P(x)$ – « x – простое число», $x|y$ – « x – делитель y », константу – число 2, функциональный символ «+». Тогда гипотезу можно записать в виде

$$\forall n (2|n) \& \neg(n = 2) \supset \exists k m (P(k) \& P(m) \& (n = m + k))$$

Единственность и неединственность

При изложении этого пункта следуем [86]. 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:

$$\forall xy (A(x) \& A(y) \supset x = y).$$

⁶⁵ Кристиан Гольдбах (1690–1764), немецкий математик, предложил эту задачу Эйлеру в письме. Одна из самых старых нерешенных математических проблем.

Заметим, что утверждение « x , удовлетворяющее A , единственno», 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

$$\exists x A(x) \& \forall xy(A(x) \& A(y) \supset x = y).$$

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 речь идет о количестве каких-то объектов, следует использовать предикат равенства.

Общий способ получить утверждение «существует не более n таких x , что $A(x)$ »:

$$\exists x_1 \dots x_n (\forall y (A(y) \sim x_1 = y \vee \dots \vee x_n = y)).$$

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:

$$\exists xy (x \neq y \& A(x) \& A(y)).$$

Так же просто сказать и то, что их ровно два:

$$\exists xy (x \neq y \& \forall z (A(z) \sim z = x \vee z = y)).$$

А вот как записывается, что решений не более двух:

$$\forall xyz (x \neq y \& x \neq z \& y \neq z \supset \neg(A(x) \& A(y) \& A(z)))$$

Подобным образом можно написать формулы и для большего числа решений.

Задачи

Задача 1. Используя язык предикатов, запишите определение инъективности и сюръективности.

Задача 2. Истинна ли формула $x = x$ в интерпретации $\langle \mathbf{Z}, \emptyset, = \rangle$?

Задача 3. Пусть P – двуместный предикатный символ. Какие из следующих формул являются общезначимыми:

- a) $\forall x \exists y P(x, y) \supset \exists y \forall x P(x, y);$
- b) $\exists x \forall y P(x, y) \supset \forall y \exists x P(x, y)?$

Задача 4. Для каждой интерпретации приведите пример формулы, которая будет истинной или ложной в зависимости от носителя интерпретации:

a) носитель интерпретации – \mathbf{N} или \mathbf{Z} ; предикатный символ « \ll » интерпретируется как строгое неравенство чисел;

b) носитель интерпретации – \mathbf{Q} или \mathbf{Z} ; предикатный символ « \ll » интерпретируется как строгое неравенство чисел.

Задача 5. Вернитесь к примеру 9 из § 3. Проверьте истинность формулы (1) в указанных интерпретациях.

Задача 6. Докажите утверждения 2, 4, 5 и 6 из теоремы 3.

Задача 7. То, что последовательность вещественных чисел a_n , $n = 1, 2, 3, \dots$, не ограничена, можно записать на языке первого порядка в виде формулы

$$\neg \exists M (\forall n (|a_n| \leq |M|)).$$

Докажите, используя теорему 3 и транзитивность отношения логической эквивалентности, что эта формула равносильно следующей:

$$\forall M (\exists n (|a_n| > |M|)).$$

Задача 8. Задачи на обратный перевод. Пусть $f(x)$ – произвольная фиксированная функция, заданная на отрезке $[a, b]$.

а. Рассмотрим интерпретацию: носитель – множество действительных чисел, $P(x, \delta)$ обозначает $|x - x_0| < \delta$, $Q(x, \varepsilon) = |f(x) - A| < \varepsilon$, $R(\varepsilon) - \varepsilon > 0$. Здесь x_0 – фиксированный элемент отрезка $[a, b]$; A – некоторое фиксированное действительное число. Какое утверждение выражает формула

$$\forall \varepsilon \exists \delta \forall x ((R(\varepsilon) \& P(x, \delta)) \supset Q(x, \varepsilon))?$$

б. Рассмотрим интерпретацию: носитель – множество действительных чисел, $P(x, \delta)$ обозначает $|x - x_0| < \delta$, $S(x, \varepsilon) = |f(x) - f(x_0)| < \varepsilon$, $R(\varepsilon) - \varepsilon > 0$. Здесь x_0 – фиксированный элемент отрезка $[a, b]$. Какое утверждение выражает формула

$$\forall \varepsilon \exists \delta \forall x ((R(\varepsilon) \& P(x, \delta)) \supset S(x, \varepsilon))?$$

с. Рассмотрим интерпретацию: носитель – множество действительных чисел, $P(x, x_1, \delta)$ обозначает $|x - x_1| < \delta$, $S(x, x_1, \varepsilon) = |f(x) - f(x_1)| < \varepsilon$, $R(\varepsilon) - \varepsilon > 0$, $D(x) = x \in [a, b]$. Какое утверждение выражает формула

$$\forall x_1 \forall \varepsilon \exists \delta \forall x ((D(x_1) \& R(\varepsilon) \& P(x, x_1, \delta)) \supset S(x, x_1, \varepsilon))?$$

Задача 9. Пусть $f: \mathbb{R} \rightarrow \mathbb{R}$. Определите, для каких функций f выполнено свойство

$$\exists \delta \forall a \forall \varepsilon \forall x ((\delta > 0) \& (a \in \mathbb{R}) \& (\varepsilon > 0) \& (x \in \mathbb{R}) \& (|x - a| \leq \delta) \rightarrow (|f(x) - f(a)| \leq \varepsilon))?$$

Задача 10. Пусть $f: \mathbb{R} \rightarrow \mathbb{R}$. Как записать, что функция f равномерно непрерывна?

Условия следующих задач принадлежат Раймонду Смаллиану [27].

Некий путешественник однажды посетил целый архипелаг островов, на которых жили только рыцари и лжецы (рыцари всегда говорят правду, лжецы всегда лгут). Он заинтересовался количеством рыцарей и лжецов на отдельных островах. Кроме того, он хотел выяснить, есть ли какая-нибудь связь между курильщиками и лжецами. Будем говорить, что два аборигена (жители острова) являются людьми одного типа, если они оба лжецы или оба рыцари. Это соглашение распространяется на любое количество людей.

Задача 11. На первом острове, который он посетил, все жители сказали одно и то же: «Все мы здесь принадлежим одному типу». Какой можно сделать вывод о жителях этого острова?

Задача 12. На следующем острове путешественник в какой-то день опросил всех жителей, за исключением одного, который спал. Они сказали: «Все мы лжецы». На следующий день путешественник встретил жителя, спавшего за день до этого, и спросил его: «Правда ли, что все жители этой острова являются лжецами?» Житель ответил («да» или «нет»). Какой ответ он дал?

Задача 13. На следующем острове путешественник был особенно заинтересован в курении аборигенов. Они все сказали то же самое: «Все рыцари на этом острове курят». Какой можно сделать вывод о распределении рыцарей и лжецов на острове и их отношении к курению?

Задача 14. На очередном острове все жители сказали: «Некоторые из нас – рыцари и некоторые – лжецы». Каков состав этого острова?

Задача 15. На следующем острове каждый житель сказал: «Некоторые лжецы на этом острове курят». Что можно узнать из этого?

Задача 16. На следующем острове все жители были одного типа и каждый из них сказал: «Если я курю, то все жители этого острова курят». Что можно узнать из этого?

Задача 17. На следующем острове все жители были одного типа и каждый из них сказал: «Если любой житель этого острова курит, то и я курю». Что можно узнать из этого?

Задача 18. На следующем острове также все были одного и того же типа и каждый сказал: «Некоторые из нас курят, но я нет». Что отсюда следует?

Задача 19. Предположим, что на том же острове вместо ответа в задаче 13 каждый житель сделал следующие два утверждения: «Некоторые из нас курят» и «Я не курю». Что бы вы заключили из этого?

Задача 20. Следующий остров населяли два племени – племя *A* и племя *B*. Каждый человек из племени *A* сказал: «Все жители этого острова – рыцари» и «Все мы курим». Каждый человек племени *B* сказал: «Некоторые из жителей этого острова есть лжецы» и «Никто на этом острове не курит». Что отсюда следует?

Задача 21. Рассмотрим в качестве универсума множество всех людей и введем константы Холмс (Шерлок Холмс) и Мориарти. Пусть предикат $A(x, y)$ истинен только тогда, когда «человек x может победить человека y ». Переведите на язык логики предикатов утверждения, связанные с борьбой Холмса против преступников.

- a. Холмс может победить любого, кто может победить Мориарти.
- b. Холмс может победить любого, кого может победить Мориарти.
- c. Если Мориарти может быть побежден, то Холмс сможет победить Мориарти.
- d. Если каждый человек может победить Мориарти, то и Холмс сможет.
- e. Любой победитель Холмса может победить Мориарти.
- f. Ни один человек не сможет победить Холмса, пока он не сможет победить Мориарти.
- g. Каждый может победить кого-то, кто не может победить Мориарти.
- h. Каждый может победить любого, кто не может победить Мориарти.
- i. Любой человек, победивший Холмса, может победить и человека, которого может победить и Холмс.

Задача 22. Как представить на языке логики предикатов следующие утверждения, где предикат на множестве людей $K(x, y)$ означает «человек x знает человека y »?

- a. Каждый знает кого-нибудь.
- b. Кто-то знает каждого.
- c. О некоторых знает каждый.
- d. Каждый знает кого-то, кто его не знает.
- e. Есть кто-то, знающий каждого, кто его знает.

... эмпирические системы утрачивают свою актуальность, математические же никогда. Их бессмертие в их «пустоте».

Станислав Лем. *Сумма технологии*

Глава 6. Аксиоматические теории

§ 1. Предварительные понятия и простые примеры

Человеческому мышлению свойственны мыслительные процессы двух видов: осознанные и неосознанные. Осознанные рассуждения в большинстве случаев можно передать 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.

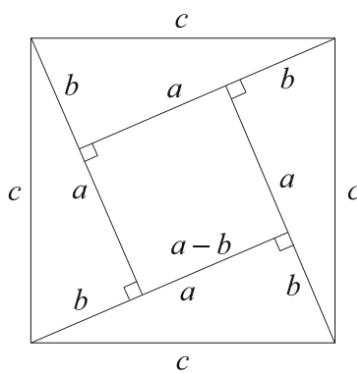


Рис. 1. Доказательство Бхаскары

В Древней Индии для доказательства нередко использовались математические рисунки. Доказательство теоремы, которую мы сейчас называем теоремой Пифагора, сводилось у индийского математика Бхаскары (1114–1185) к рисунку с пояснением в одно слово «Смотри!»⁶⁶ (рис. 1).

⁶⁶ Историки-математики считают, что Бхаскара выражал площадь квадрата, построенного на гипотенузе, как сумму площадей треугольников ($4ab/2$) и площадь квадрата $(a - b)^2$. Следовательно, $c^2 = 4ab/2 + (a - b)^2$, потом $c^2 = 2ab + a^2 - 2ab + b^2$ и, наконец, $c^2 = a^2 + b^2$.

Современные доказательства опираются на аксиоматический метод⁶⁷. 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 в. 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 реальности⁶⁸.

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 psychology в нем не меньше, чем математики.

Неформальное (содержательное, психологическое) доказательство – это рассуждение, которое настолько убеждает 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 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 т.д.

Пример 1 [110. С. 383]. Доказательство от противного. 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*.

⁶⁷ Кроме аксиоматического метода используется также генетический подход [90]. В этом случае пытаются моделировать интуицию средствами другой теории (которая сама может также быть интуитивной).

⁶⁸ Смотрите в данной главе неевклидову геометрию (§ 4), континuum-гипотезу и аксиому выбора (§ 7).

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.

Однако 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, или просто дедуктика, 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 – серьезный и несерьезный [117].

Пример 2 (несерьезный). Рассмотрим 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!)

Пример 3 (теория L). 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 $aabb$; вывод (доказательство) для нее есть

$$a, ab, aaba, aabab, aabb.$$

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.

§ 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 $\{R_1, R_2, \dots, R_m\}$ отношений между формулами, называемых **правилами вывода**. Каждое правило вывода позволяет получать из некоторого конечного множества формул новую формулу.

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 пра-

вил порождения конкретных аксиом из схемы аксиом⁶⁹. 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.

Выводимость

Опишем более точно дедуктивную систему для формальной аксиоматической теории. Пусть A_1, A_2, \dots, A_n, A – формулы теории T . Если существует такое правило вывода R , что $\langle A_1, A_2, \dots, A_n, A \rangle \in R$, то говорят, что формула A **непосредственно выводима** из формул A_1, A_2, \dots, A_n по правилу вывода R . Обычно этот факт записывают следующим образом:

$$\frac{A_1, A_2, \dots, A_n}{A} R,$$

где формулы A_1, A_2, \dots, 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, \dots, 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}, \dots, F_{j_n} ($j_1, \dots, j_n < i$). Если в теории T существует вывод формулы A из множества формул Γ , то это записывается следующим образом:

$$\Gamma \vdash_T A,$$

где формулы из Γ называются **гипотезами** вывода, а формула A – **выводимой** из множества Γ . Если теория T подразумевается, то ее обозначение обычно опускают.

Если множество Γ конечно: $\Gamma = \{B_1, B_2, \dots, B_n\}$, то вместо

$$\{B_1, B_2, \dots, B_n\} \vdash - A$$

пишут $B_1, B_2, \dots, B_n \vdash - A$. Если Γ есть пустое множество \emptyset , то A называют **теоремой** (или **доказуемой** формулой) и в этом случае используют сокращенную запись $\vdash - A$ (« A есть теорема»).

Отметим, что в соотношении $\{\text{теоремы}\} \subset \{\text{формулы}\} \subset \{\text{выражения}\}$ включение множеств является строгим.

Обычно дедуктивная система удовлетворяет требованиям, сформулированным в замечании 1 (§ 1 данной главы).

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 T можно считать формальной, если построен алгоритм⁷⁰ для проверки правильности рассужде-

⁶⁹ Каждая аксиома получается из схемы заменой переменных в схеме, как правило, на произвольные формулы.

⁷⁰ Пока мы можем довольствоваться интуитивным пониманием алгоритмов. Точное определение понятия алгоритма смотрите в главах 9–10.

ний с точки зрения принципов теории T . Это значит, что если некто предлагает математический текст, являющийся, по его мнению, доказательством некоторой теоремы в теории T , то, применяя алгоритм, мы можем проверить, действительно ли предложенный текст соответствует стандартам правильности, принятым в T . Таким образом, стандарт правильности рассуждений для теории 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 $\models P$).
- 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.

При рассмотрении аксиоматических теорий в общем виде любое множество замкнутых формул данного языка может быть принято в качестве системы аксиом. Пусть Γ – произвольное множество замкнутых формул языка.

- Интерпретация называется **моделью множества формул Γ** , если все формулы этого множества истинны в данной интерпретации. Множество Γ 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 дедуктика **корректна** относительно семантики.
- **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 Γ , если P выполняется (т.е. истинна) в любой модели Γ (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: $A \sim B$), 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 formalизуется, 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*** (пример 2) 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*** (пример 3). Можно доказать, например, следующее утверждение, относящееся ко всем теоремам ***L***: если X – теорема, то aaX – тоже теорема (см. главу 7, § 2, пример 14).

Формальная теория с языком первого порядка называется **семантически непротиворечивой**, если никакое ложное утверждение не обладает доказательством⁷¹, иначе теория называется **семантически противоречивой**.

Формальная теория ***T*** с языком первого порядка называется **синтаксически противоречивой**, если существует формула A , доказуемая вместе со своим отрицанием $\neg A$. Теория называется **синтаксически непротиворечивой**, если она не является синтаксически противоречивой.

В дальнейшем если речь идет просто о непротиворечивости теории, то подразумевается, что теория непротиворечива и синтаксически, и семантически.

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) семантической 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 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.

Для первоначального знакомства с аксиоматическими теориями познакомимся с простыми учебными примерами, взятыми из книги Дугласа Хоффстадтера⁷² (рис. 2) «Гёдель, Эшер, Бах: эта бесконечная гирлянда» [117].

⁷¹ Семантическая непротиворечивость равносильна тому, что дедуктика корректна относительно семантики.

⁷² Дуглас Роберт Хоффстадтер (р. 1945) – американский физик и информатик. Получил всемирную известность благодаря книге «Гёдель, Эшер, Бах: эта бесконечная гирлянда», опубликованной в 1979 г. и в 1980 г. получившей Пулитцеровскую премию в категории «Нехудожественная литература».



Рис. 2. Дуглас Хоффстадтер

Пример 4. Формальная теория MIU.

Алфавит: M, I, U .

Формулы = $\{M, I, U\}^*$.

Определим дедуктивную систему:

Аксиома: MI .

Правила вывода:

- 1) $xI \rightarrow xIU$ (продукция);
- 2) $Mx \rightarrow Mxx$ (продукция);
- 3) $III \rightarrow U$ (правило переписывания);
- 4) $UU \rightarrow \emptyset$ (правило переписывания, \emptyset 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
$MIII$	Правило 2
MUI	Правило 3
$MUIU$	Правило 1
$MUIUUIU$	Правило 2
$MUIIU$	Правило 4

Пример 5. Формальная теория 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 теории PR используются только удлиняющие правила, т.е. количество символов в формуле в результате применения правила вывода увеличивается.

Определим семантическую структуру. Выберем следующую интерпретацию теории PR (одну из возможных).

- Универсум – множество целых положительных чисел.

- Стока, 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 теории PR .

Теперь мы можем использовать 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» приложимо 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 теорией PR и сложением натуральных чисел.

Пример 6. Формальная теория 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 теории UR .

- Универсум — множество целых положительных чисел.
- Стока, состоящая из n тире, интерпретируется как число n .
- P интерпретируется как символ « \times ».
- 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 .

Пример 7. Формальная теория $PR1$.

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 теории PR1.

1. Выберем интерпретацию теории PR1 такую же, как для PR.

- Универсум – множество целых положительных чисел.
- Стока, 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 теории 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

$$\langle x + y = z + 1 \vee x + y = z \rangle,$$

и поэтому данная интерпретация является моделью теории PR1. Более того, любое истинное утверждение

$$\langle x + y = z + 1 \vee x + y = z \rangle$$

описывается в виде теоремы $xPyRz$ теории PR1, т.е. теория с данной интерпретацией является полной.

3. В последней интерпретации символ R понимается снова по-другому.

- R интерпретируется как символ « \geq ».

Указанная интерпретация теореме $xPyRz$ ставит в соответствие истинное утверждение о целых положительных числах « $x + y \geq z$ », и поэтому данная интерпретация является моделью теории PR1. Но мы сейчас имеем существенное отличие от предыдущей интерпретации: не все истинные утверждения вида $x + y \geq z$ являются теоремами в PR1. Так, например, формула $\neg P - R -$ имеет истинную интерпретацию $2 + 1 \geq 1$, но это не теорема.

§ 3. Исчисление высказываний

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

$$A_1) A \supset (B \supset A);$$

$$A_2) (A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C));$$

$$A_3) (\neg B \supset \neg A) \supset ((\neg B \supset A) \supset B)$$

и правилом вывода MP (*Modus Ponens* обычно переводится как **правило отделения**):

$$\frac{A, A \supset B}{B} \text{ MP}.$$

Здесь A , B и C – любые пропозициональные формулы⁷³. Таким образом, множество аксиом исчисления высказываний бесконечно, хотя задано тремя схемами аксиом. Множество правил вывода также бесконечно, хотя задано только одной схемой.

⁷³ До конца данного параграфа под словом «формула» мы будем понимать только пропозициональные формулы.

Пример 8. Для любой формулы A построим вывод формулы $A \supset A$, т.е. $A \supset A$ – теорема.

Подставляя в схему аксиом A_2 вместо B формулу $A \supset A$ и вместо C формулу A , получаем аксиому

$$(A \supset ((A \supset A) \supset A)) \supset ((A \supset (A \supset A)) \supset (A \supset A)). \quad (1)$$

Подставляя в A_1 вместо формулы B формулу $A \supset A$, получаем аксиому

$$A \supset ((A \supset A) \supset A). \quad (2)$$

Из формул (1) и (2) по правилу MP получаем

$$(A \supset (A \supset A)) \supset (A \supset A). \quad (3)$$

Подставляя в A_1 вместо формулы B формулу A , получаем аксиому

$$A \supset (A \supset A). \quad (4)$$

Из формул (3) и (4) по правилу MP получаем $A \supset A$.

Теорема 1. Пусть Γ – произвольное множество гипотез. Если $\Gamma \vdash A \supset B$ и $\Gamma \vdash A$, то $\Gamma \vdash B$.

Доказательство. Пусть A_1, A_2, \dots, A_n – вывод формулы A из Γ , где A_n совпадает с A . Пусть B_1, B_2, \dots, B_m – вывод формулы $A \supset B$ из Γ , где B_n совпадает с $A \supset B$. Тогда $A_1, A_2, \dots, A_n, B_1, B_2, \dots, B_m, B$ – вывод формулы B из Γ . 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 2 (о дедукции для исчисления высказываний)⁷⁴. Пусть Γ – множество формул. Имеем $\Gamma \cup \{A\} \vdash B$ тогда и только тогда, когда $\Gamma \vdash A \supset B$.

Доказательство. Необходимость. Пусть $\Gamma \vdash A \supset B$, тогда и $\Gamma, A \vdash A \supset B$. (Для краткости опускаем фигурные скобки и заменяем знак объединения запятой.) По определению $\Gamma, A \vdash A$, откуда по MP следует $\Gamma, A \vdash B$.

Достаточность. Пусть B_1, B_2, \dots, B_n есть вывод $\Gamma, A \vdash B$, где $B_n = B$. Индукцией по i ($1 \leq i \leq n$) докажем, что $\Gamma \vdash A \supset B$.

Базис индукции. B_1 должно быть элементом Γ , либо быть аксиомой, либо совпадать с A . По схеме аксиом A_1 формула $B_1 \supset (A \supset B_1)$ является аксиомой. Поэтому в первых двух случаях $\Gamma \vdash A \supset B$ по MP . В третьем случае, когда B_1 совпадает с A , мы имеем $\vdash A \supset B_1$ (см. пример 8) и, следовательно, $\Gamma \vdash A \supset B_1$.

Индуктивный переход. Допустим теперь, что $\Gamma \vdash A \supset B_k$ для любого $k < i$. Для B_i имеем четыре возможности:

- 1) B_i есть аксиома;
- 2) $B_i \in \Gamma$;
- 3) B_i совпадает с A ;
- 4) B_i следует по MP из некоторых B_k и B_m , где $k < i$ и $m < i$ и B_m имеет вид $B_k \supset B_i$.

В первых трех случаях $\Gamma \vdash A \supset B$ доказывается также, как при $i = 1$. В последнем случае применим индуктивное предположение, согласно которому $\Gamma \vdash A \supset B_k$ и $\Gamma \vdash A \supset (B_k \supset B_i)$. По схеме аксиом A_2 , $\vdash (A \supset (B_k \supset B_i)) \supset ((A \supset B_k) \supset (A \supset B_i))$. Следовательно, по MP , $\Gamma \vdash (A \supset B_k) \supset (A \supset B_i)$ и, снова по MP , $\Gamma \vdash A \supset B_i$. ■

Следствие:

1. $A \supset B, B \supset C \vdash A \supset C$.
2. $A \supset (B \supset C), B \vdash A \supset C$.

⁷⁴ Жак Эрбран (1908–1931) – французский математик и логик, доказал теорему в 1930 г.

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 $A \supset (B \supset C), B \vdash A \supset C$. ■

Полнота, разрешимость и непротиворечивость исчисления высказываний

В исчислении высказываний есть два понятия, касающиеся формул, – теорема и тавтология. Аксиомы и правило вывода придуманы так, что эти два понятия совпадают.

Наша цель – показать, что формула исчисления высказываний является тавтологией тогда и только тогда, когда она есть теорема. В одну сторону это совсем просто.

Теорема 3.

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 формул A и $A \supset B$ являются тавтологиями. Тогда формула A истинна и, по свойствам импликации, B истинно. Следовательно, B – тавтология. ■

Для доказательства обратного утверждения нам потребуется несколько лемм.

Лемма 1 [83. С. 41–43]. Для любых формул A, B следующие формулы являются теоремами:

- a) $\neg\neg B \supset B$;
- b) $B \supset \neg\neg B$;
- c) $\neg A \supset (A \supset B)$;
- d) $(\neg B \supset \neg A) \supset (A \supset B)$;
- e) $(A \supset B) \supset (\neg B \supset \neg A)$;
- f) $A \supset (\neg B \supset \neg(A \supset B))$;
- g) $(A \supset B) \supset ((\neg A \supset B) \supset B)$.

Лемма 2. Если $\Gamma, A \vdash B$ и $\Gamma, \neg A \vdash B$, то $\Gamma \vdash B$.

Доказательство. По лемме 1(g) формула $(A \supset B) \supset ((\neg A \supset B) \supset B)$ является теоремой. Таким образом, $\Gamma \vdash (A \supset B) \supset ((\neg A \supset B) \supset B)$. Кроме того, по теореме о дедукции $\Gamma \vdash A \supset B$ и $\Gamma \vdash \neg A \supset B$. Теперь дважды воспользуемся теоремой 1. ■

Лемма 3 [83. С. 43]. Пусть A содержит пропозициональные переменные X_1, X_2, \dots, X_m и пусть задано некоторое распределение истинностных значений для X_1, X_2, \dots, X_m . Пусть тогда X'_i есть X_i , если X_i принимает значение **И**, и $\neg X_i$, если X_i принимает значение **Л**, и пусть, наконец, A' есть A , если при этом распределении A принимает значение **И**, и $\neg A$, если A принимает значение **Л**. Тогда $X'_1, X'_2, \dots, X'_m \vdash A'$.

Если, например, A обозначает $\neg(\neg X_1 \supset X_2)$, то для каждой строки истинностной таблицы

X_1	X_2	$\neg(\neg X_1 \supset X_2)$
И	И	Л
Л	И	Л
И	Л	Л
Л	Л	И

лемма 3 утверждает факт соответствующей выводимости. Так, в частности, третьей строке соответствует утверждение $X_1, \neg X_2 \vdash \neg(\neg X_1 \supset X_2)$, а четвертой строке – утверждение $\neg X_1, \neg X_2 \vdash \neg(\neg X_1 \supset X_2)$.

Доказательство. Проведем доказательство с помощью математической индукции по числу n вхождений в A логических связок.

Базис индукции. Если $n = 0$, то A представляет собой просто пропозициональную переменную X_1 , и утверждение леммы сводится к $X_1 \vdash X_1$ и $\neg X_1 \vdash \neg X_1$.

Индуктивный переход. Допустим теперь, что лемма верна при любом $j < n$.

Случай 1. A имеет вид отрицания: $\neg B$. Число вхождений логических связок в B , очевидно, меньше n .

Случай 1а. Пусть при заданном распределении истинностных значений B принимает значение **И**. Тогда A принимает значение **Л**. Таким образом, B' есть B , а A' есть $\neg A$. По индуктивному предположению, примененному к B , мы имеем $X'_1, X'_2, \dots, X'_m \vdash B$. Следовательно, по лемме 1б и PM , $X'_1, X'_2, \dots, X'_m \vdash \neg\neg B$. Но $\neg\neg B$ есть A' .

Случай 1б. Пусть B принимает значение **Л**; тогда B' есть $\neg B$, а A' совпадает с A . По индуктивному предположению $X'_1, X'_2, \dots, X'_m \vdash \neg B$, что и требовалось получить, ибо $\neg B$ есть A' .

Случай 2. Формула A имеет вид $B \supset C$. Тогда число вхождений логических связок в B и C меньше, чем в A . Поэтому, в силу индуктивного предположения, $X'_1, X'_2, \dots, X'_m \vdash B'$ и $X'_1, X'_2, \dots, X'_m \vdash C$.

Случай 2а. Формула B принимает значение **Л**. Тогда A принимает значение **И** и B' есть $\neg B$, а A' есть A . Таким образом, $X'_1, X'_2, \dots, X'_m \vdash \neg B$, и по лемме 1(с) следует, что $X'_1, X'_2, \dots, X'_m \vdash B \supset C$, но $B \supset C$ есть A .

Случай 2б. Формула C принимает значение **И**. Следовательно, A принимает значение **И** и C есть C , а A' есть A . Имеем $X'_1, X'_2, \dots, X'_m \vdash C$, и тогда по схеме аксиом A_1 имеем $X'_1, X'_2, \dots, X'_m \vdash B \supset C$, где $B \supset C$ совпадает с A .

Случай 2с. Формула B принимает значение **И** и C принимает значение **Л**. Тогда A' есть $\neg A$, ибо A принимает значение **Л**, B' есть B и C есть $\neg C$. Имеем $X'_1, X'_2, \dots, X'_m \vdash B$ и $X'_1, X'_2, \dots, X'_m \vdash \neg C$. Отсюда по лемме 1(ж) получаем $X'_1, X'_2, \dots, X'_m \vdash \neg(B \supset C)$, где $\neg(B \supset C)$ есть A' . ■

Теорема 4 (Пост⁷⁵, 1921). Формула A в исчислении высказываний является теоремой тогда и только тогда, когда A – тавтология.

Доказательство. Нам осталось доказать только половину теоремы, другая половина доказана в теореме 3. Итак, пусть A есть тавтология, докажем, что она доказуема. Предположим, что X_1, X_2, \dots, X_m – все пропозициональные переменные, содержащиеся в A . При каждом распределении истинностных значений для переменных X_1, X_2, \dots, X_m мы имеем, в силу леммы 3, $X'_1, X'_2, \dots, X'_m \vdash A$ (A' совпадает с A , так как A есть тавтология). Поэтому в случае, когда X_m принимает значение **И**, мы, применив лемму 3, получаем $X'_1, X'_2, \dots, X'_m \vdash A$; когда же X_m принимает значение **Л**, то по той же лемме получаем $X'_1, X'_2, \dots, \neg X'_m \vdash A$. Отсюда по лемме 2 $X'_1, X'_2, \dots, X'_{m-1} \vdash A$. Точно таким же образом, рассмотрев два случая, когда X_{m-1} принимает значение **И** и **Л**, и снова применив леммы 3 и 2, мы исключим X_{m-1} и так далее; после m таких шагов мы придем к $\vdash A$. ■

⁷⁵ Эмиль Леон Пост (1897–1954) – американский математик и логик.

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 опровергнутая формула не может быть доказана.

Другие аксиоматизации исчисления высказываний

Теория, определенная для пропозициональной логики, не является единственной возможной аксиоматизацией исчисления высказываний. Ее 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 [83. С. 48–51]. В классической логике все аксиоматизации приводят к одному множеству выводимых формул.

Например, оставив МР как единственное правило вывода, можно объявить схемами аксиом следующие формулы:

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

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 в. большое количество споров. Математики-интуиционисты отказались признавать закон исключенного третьего [64. С. 113].

Пример 9 («теодиция наоборот»).

Любую тавтологию логики высказываний можно включить в логический вывод на любом шаге, так как все тавтологии доказуемы в исчислении высказываний. Кроме того, все тавтологии вида $X \leftrightarrow Y$ можно использовать как правило вывода следующим образом. Если формула X получена на каком-то шаге вывода, то далее мы можем использовать в выводе формулу Y .

Рассмотрим соответствующий пример логического вывода, взятый из [54. С. 36–38] в немножко измененном виде.

Пусть дано множество Γ , состоящее из гипотез:

1. $(L \wedge W) \supset V$.
2. $\neg L \supset \neg U$.
3. $\neg W \supset \neg B$.
4. $\neg V$.
5. $E \supset (U \wedge B)$.

Докажем, что $\Gamma \vdash \neg E$.

Перечислим тавтологии, которые будем использовать:

- $\alpha: (A \supset B) \leftrightarrow (B \vee \neg A),$
- $\beta: (A \supset B) \leftrightarrow (\neg B \supset \neg A),$
- $\gamma: \neg(B \vee A) \leftrightarrow (\neg B \wedge \neg A),$
- $\delta: \neg(B \wedge A) \leftrightarrow (\neg B \vee \neg A),$
- $\varepsilon: ((A \supset B) \wedge (B \supset C)) \supset (A \supset C).$
- $\zeta: ((A \supset B) \wedge \neg B) \supset \neg A.$
- $\eta: A \leftrightarrow \neg \neg A.$

Выход $\neg E$ из Γ состоит из следующего списка выводимых формул:

- | | |
|---------------------------|--|
| 1. $\neg(L \wedge W)$ | гипотезы 1 и 4 и тавтология ζ |
| 2. $\neg L \vee \neg W$ | формула 1 и тавтология δ |
| 3. $U \rightarrow L$ | гипотеза 2 и тавтология β |
| 4. $L \rightarrow \neg W$ | формула 2 и тавтология α |
| 5. $U \rightarrow \neg W$ | формула 3, 4 и тавтология ε |
| 6. $U \rightarrow \neg B$ | формула 5, гипотеза 3 и тавтология ε |
| 7. $\neg U \vee \neg B$ | формула 6 и тавтология α |
| 8. $\neg(U \wedge B)$ | формула 7 и тавтология δ |
| 9. $\neg E$ | формула 8, гипотеза 5 и тавтология ζ |

Этот пример интересен возможной интерпретацией высказываний L, W, U, B, V, E , которые означают следующее:

L : Бог может предотвратить зло.

W : Бог хочет предотвратить зло.

U : Бог всемогущ.

B : Бог не злой.

V : Бог предотвращает зло.

E : Бог существует.

Исходные гипотезы-посылки тогда интерпретируются как высказывания:

$(L \wedge W) \supset V$: Если Бог может и хочет предотвратить зло, то он предотвращает.

$\neg L \supset \neg U$: Если Бог не может предотвратить зло, то он не всемогущ.

$\neg W \supset \neg B$: Если Бог не хочет предотвратить зло, то он злой.

$\neg V$: Бог не предотвращает зло.

$E \supset (U \wedge B)$: Если Бог существует, то он всемогущ и не злой.

Таким образом, полученный вывод $\Gamma \vdash \neg E$, приводящий к утверждению, что «Бог не существует», является «теодицеей наоборот»⁷⁶. Но заметим, что в § 5 говорится о доказательстве К. Геделя о существовании Бога.

§ 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 все это не определения, а пояснения понятий. При современном изложении геометрии данные понятия не определяются. Евклид дает 19 аксиом [108], 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

⁷⁶ Теодицей – богооправдание – совокупность религиозно-философских доктрин, призванных оправдать управление Вселенной добрым Богом, несмотря на наличие зла в мире. Термин введен Лейбницием в 1710 г.

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. На современном языке пятый постулат Евклида можно сформулировать так [106. С. 304]:

При пересечении двух прямых третьей, секущей, образуются четыре внутренних угла. Если сумма двух из них, расположенных по одну сторону от секущей, меньше 180° , то эти две прямые пересекаются, и притом по ту же сторону от секущей.

В современном и более простом, но математически равносильном виде⁷⁷ аксиома о параллельности гласит:

Дана прямая и точка вне ее; не существует двух различных прямых, проходящих через данную точку и параллельных данной прямой.

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 удается доказать без использования того же пятого постулата.

Глубокое исследование аксиомы о параллельных, основанное на совершенно оригинальном принципе, провел в 1733 г. 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 [60. С. 215–217]. Но ему не удалось получить противоречие.

В первой половине XIX в. по пути, проложенному Саккери, пошли немецкий математик Карл Гаусс (1777–1855), венгерский математик Янош Бойяи (1802–1860 гг.) и российский математик Николай Лобачевский (1792–1856). Но цель у них была уже иная – не разработать неевклидову геометрию как невозможную, а, наоборот, построить альтернативную геометрию и выяснить ее возможную роль в реальном мире. На тот момент это была совершенно еретическая идея; никто из ученых 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 г. и публикации 1829 г.; Бойяи – в письме 1831 г. и публикации 1832 г.), 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 гео-

⁷⁷ Сформулировал аксиому в данном виде Джон Плейфэр (1748–1819) – шотландский математик.

метрии, 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 m , n и l , попарно параллельные друг другу в различных направлениях (рис. 3).

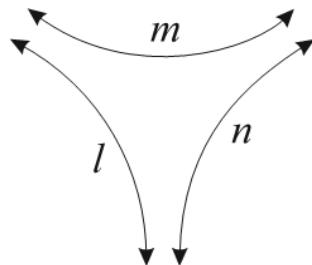


Рис. 3. Треугольник из параллельных прямых

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 свое 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.

История на Лобачевском закончиться не могла, поскольку два вопроса еще требовали ответа. Во-первых, нужна была модель, оправдывающая логические построения. Человечество воспринимало геометрию Евклида как мировую данность. Сколько бы ни говорилось об абстрактном описании точек, линий и плоскостей, их толкование явно и неявно было физическим. Хотелось подобного для геометрии Лобачевского, поскольку без реализующей модели логические фокусы остаются приведениями.

Во-вторых, существовала проблема непротиворечивости, которая, вообще говоря, не разрешима, но здесь ситуация была особая. Непротиворечивость геометрии Евклида тоже неясна, но там в пользу определенного благополучия служат наличие реальной модели, интуиция и многовековой опыт. Для новой геометрии – никакой опоры.

Только спустя 40 лет появились модель Феликса Клейна и модель Пуанкаре, реализующие аксиоматику геометрии Лобачевского на базе евклидовой геометрии. В модели Клейна (рис. 4) плоскость – внутренность круга k , прямые – хорды. Через точку P проходит целый пучок хорд, не пересекающих прямую a .

Поскольку модель строится как подсистема обычной геометрии, то геометрия Лобачевского непротиворечива, если непротиворечивой является евклидова геометрия.

Первая последовательная и полная аксиоматическая теория для евклидовой геометрии была создана Д. Гильбертом в самом конце XIX в., после того как немецкий математик Мориц Пац (1843–1930) и Гильберт обнаружили все утверждения, которые Евклид не сформулировал в виде аксиом, но использовал при доказательствах [50].

Дадим представление об аксиоматике Гильberta в неформальном виде. Полное описание аксиом и понятий и примеры доказательств геометрических теорем представлены в [108]. Восемь понятий считаются неопределенными: «точка», «прямая», «плоскость», отношение «точка лежит на прямой», отношение «точка лежит на плоскости», отношение «точка

В 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.

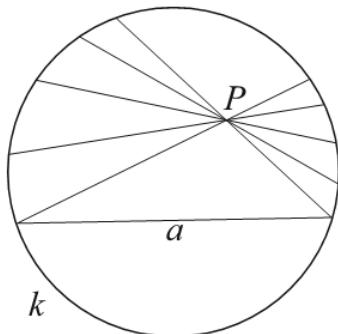


Рис. 4. Модель Клейна

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 из этой группы приведем аксиому Паша (Мориц Паш открыл ее 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 r , проходит не более одной прямой, параллельной прямой r .

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 Дедекином) сводится к непротиворечивости рациональных чисел, что, в свою очередь, сводится к непротиворечивости теории элементарной арифметики **PA** (см. § 6 данной главы).

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. Но в доступных нашему наблюдению областях пространства евклидова геометрия соблюдается с высокой степенью точности.

§ 5. Теории первого порядка

Языки первого порядка используются в формальных теориях первого порядка.

Синтаксические свойства истинности теорий с языками первого порядка

Пусть дана некоторая формальная теория T с языком первого порядка Ω и задана интерпретация φ этого языка. Обозначим через F_φ множество всех формул теории T , истинных в данной интерпретации. Множество F_φ обладает определенными свойствами, которые отражают заложенную в языки первого порядка логику, не зависящую от конкретных особенностей интерпретации.

Предварительно надо обсудить условие безопасной подстановки в формулу терма вместо переменной. Если терм t подставляется (без предосторожностей) вместо свободных вхождений переменной y в выражение $A(y)$, то некоторые переменные в t могут стать связанными. Пусть $A(y)$ – истинная формула

$$\int_0^1 (x^2 + y) \, dx = y + \frac{1}{3}$$

и $t \equiv x$, тогда $A(x)$ – ложная формула

$$\int_0^1 (x^2 + x) \, dx = x + \frac{1}{3}.$$

Это явление называется **коллизией переменных**.

Говорят, что **подстановка терма t вместо y в A корректна**, если никакая свободная переменная терма t не становится связанный после подстановки t вместо (свободных вхождений) переменной y в A . Именно некорректная подстановка вызвала только что упомянутую коллизию переменных. Переименовывая связанные переменные в A , мы всегда можем избежать коллизии переменных. Например, подстановка $t \equiv x$ вместо y в формулу

$$\int_0^1 (u^2 + y) \, du = y + \frac{1}{3}$$

является корректной.

Для языка первого порядка понятие корректной подстановки уточняется. 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 10.

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 F_Φ .

1. Для любой замкнутой формулы P либо $P \in F_\Phi$, либо $\neg P \in F_\Phi$.

2. Множество F_Φ не содержит противоречия, т.е. ни для какой формулы P не может быть, чтобы одновременно выполнялись $P \in F_\Phi$ и $\neg P \in F_\Phi$.

3. Множество F_Φ содержит все тавтологии языка Ω (см. глава 5, § 4).

4. Множество F_Φ содержит следующие общезначимые формулы:

a) $\forall x A(x) \supset A(t)$,

где $A(t)$ есть формула теории T и t есть терм теории T , свободный для x в $A(x)$. Условие, чтобы t был свободен для x , – гигиеническое правило при изменении обозначений;

b) $\forall x (A \supset B(x)) \supset (A \supset \forall x B(x))$,

где A не содержит свободных вхождений переменной x ;

c) $(\forall x \neg A(x)) \leftrightarrow (\neg \exists x A(x))$.

5. Множество F_Φ замкнуто относительно правил вывода modus ponens и обобщения. По определению это означает, что если $A \in F_\Phi$ и $A \supset B \in F_\Phi$, то также $B \in F_\Phi$; если $A \in F_\Phi$, то $\forall x A \in F_\Phi$ 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 T разбиваются на два класса: логические (вместе с аксиомами равенства) и собственные (или нелогические).

Логические аксиомы: каковы бы ни были формулы A , B и C теории T , следующие формулы являются логическими аксиомами теории T :

$A_1. A \supset (B \supset A)$.

$A_2. (A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$.

$A_3. (\neg B \supset \neg A) \supset ((\neg B \supset A) \supset B)$.

$A_4. \forall x A(x) \supset A(t)$, где $A(t)$ есть формула теории T и t есть терм теории T , свободный для x в $A(x)$ ⁷⁸. Заметим, что t может совпадать с x , и тогда мы получаем более простую аксиому $\forall x A(x) \supset A(x)$.

$A_5. \forall x (A \supset B(x)) \supset (A \supset \forall x B(x))$, где формула A не содержит свободных вхождений переменной x .

Аксиомы равенства:

$A_6. t_1 = t_1$.

$A_7. t_1 = t_2 \supset t_2 = t_1$.

⁷⁸ Что происходит, если данное ограничение на терм t не выполнено, смотрите в § 6, пример 11.

A₈. $t_1 = t_2 \& t_2 = t_3 \supset t_1 = t_3.$

A₉. $t_1 = s_1 \& \dots \& t_n = s_n \supset f(t_1, \dots, t_n) = f(s_1, \dots, s_n).$

A₁₀. $t_1 = s_1 \& \dots \& t_n = s_n \supset P(t_1, \dots, t_n) \equiv P(s_1, \dots, s_n).$

В этих аксиомах $t_1, \dots, t_n, s_1, \dots, s_n$ – 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:

$$1. \quad \text{Modus ponens: } \frac{A, A \supset B}{B} \quad MP.$$

$$2. \quad \text{Правило обобщения: } \frac{A(x)}{\forall x A(x)} \quad Gen.$$

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 $\forall a, b, \forall$ (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 A_1 – A_3 являются также аксиомами исчисления высказываний, поэтому с помощью правила modus ponens выводимы все тавтологии языка Ω . Аксиомы A_4 – A_5 называются «логическими аксиомами с кванторами». Аксиома 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.

Теории первого порядка с собственными аксиомами широко распространены в математике. Некоторые из них применяются в логическом программировании [43, 73]. 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 1960-е гг., 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 гг., а в 1965 г. Дж. Робинсон⁷⁹ предложил метод резолюций [21], который и по сей день лежит в основе большинства систем поиска логического вывода.

Наиболее распространен язык логического программирования Prolog. Составляя программу на языке Prolog, программист тем самым создает прикладную теорию первого порядка – записывает собственные аксиомы теории и ничего больше. Причем эти аксиомы пишут-

⁷⁹ Джон Алан Робинсон (англ. John Alan Robinson; р. 1930) – английский философ и логик.

ся в таком виде, что программировать может даже человек, не знающий математической логики. Интерпретатор с языка Prolog содержит все остальные (логические) аксиомы и пытается доказать формулы, предлагаемые программистом.

Так же как для исчисления высказываний, в теориях первого порядка импликация тесно связана с выводимостью.

Теорема 5 (теорема о дедукции для теории первого порядка). Если $\Gamma \cup \{A\} \vdash B$, то $\Gamma \vdash A \supset B$.

Доказательство см., например, в [109. С. 70].

Важные свойства теорий первого порядка описываются в метатеоремах 6–11.

Теорема 6. Если теория первого порядка синтаксически 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. Ее 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.

Формальная теория пригодна для описания тех предметных областей, которые являются ею моделями. Справедлива:

Теорема 7. Если теория первого порядка имеет модель, то она синтаксически непротиворечива.

Доказательство см., например, в [109. С. 73].

Теорема 8 (о корректности исчисления предикатов) [109. С. 64]. Любая выводимая формула исчисления предикатов общезначима.

Теорема 9 (теорема 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 в том случае, когда либо S противоречива, 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 [78. С. 64–69; 109. 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 [109. 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 (Алонзо Чёрч). Исчисление предикатов неразрешимо.

Доказательство см. в [65. Р. 312–318].

Логическое программирование основано на расширении исчисления предикатов собственными аксиомами программиста (программа и является записью таких аксиом). Таким образом, каждая программа на языке Prolog является формальной теорией, созданной ad hoc. В силу теоремы Чёрча такая теория не может быть разрешимой – она является полуразрешимой (см. § 2 данной главы).

§ 6. Аксиоматика Пеано

Теория формальной арифметики **PA** явилась началом использования в математике формальных аксиоматических теорий первого порядка. Язык формальной арифметики – язык первого порядка, имеет сигнатуру, состоящую из одной константы 0, одноместного функционального символа S и двух двуместных функциональных символов + и \times . Как обычно для языка первого порядка, используется предикатный символ $=$. Стандартная интерпретация этого языка (см. главу 5, пример 6) имеет своим носителем множество натуральных чисел \mathbb{N} , константу 0, функциональные символы интерпретируются как сложение и умножение, а $S(x)$ обозначает $x + 1$.

Собственные аксиомы **PA** суть формулы следующих видов:

$$P_1. (P(\mathbf{0}) \& \forall x(P(x) \supset P(S(x)))) \supset \forall z P(z)$$

(принцип математической индукции, P – произвольная формула).

$$P_2. S(t_1) = S(t_2) \supset t_1 = t_2.$$

$$P_3. \neg(S(t) = \mathbf{0}).$$

$$P_4. t + \mathbf{0} = t.$$

$$P_5. t_1 + S(t_2) = S(t_1 + t_2).$$

$$P_6. \mathbf{0} \times t = \mathbf{0}.$$

$$P_7. S(t_1) \times t_2 = t_1 \times t_2 + t_2.$$

Аксиомы **P₂** и **P₃** обеспечивают существование нуля и операции «непосредственно следующий». Аксиомы **P₄–P₇** представляют собой рекурсивные равенства, служащие определениями операций сложения и умножения.

С помощью правила *MP* из схемы аксиом **P₁** мы можем получить следующее правило индукции: из $P(\mathbf{0})$ и $\forall x(P(x) \supset P(S(x)))$ выводится $\forall x P(x)$.

Аксиомы **P₁–P₃** ввел Пеано (в 1891 г.) для аксиоматизации натурального ряда.

Пример 11. Среди логических аксиом для теории первого порядка (см. § 5 данной главы) присутствует аксиома

$$A_4. \forall x A(x) \supset A(t),$$

где $A(t)$ есть формула теории **T** и t есть терм теории **T**, свободный для x в $A(x)$.

Сейчас удобно на примере системы **PA** пояснить, почему необходимо в **A₄** требование, чтобы терм t был свободным для x в $A(x)$. Пусть $A(x)$ есть формула $\exists b(b = x + 1)$. Тогда $\forall x A(x)$, обозначающая формулу $\forall x \exists b(b = x + 1)$, является истинной формулой при стандартной интерпретации **PA**. Терм $t \equiv b$ не является свободным для x в $A(x)$, так как результат его подстановки в $A(x)$ вместо x дает $\exists b(b = b + 1)$ – ложную формулу при стандартной интерпретации **PA**. Следовательно, тогда частный случай аксиомы **A₄** является ложной формулой $\forall x \exists b(b = x + 1) \supset \exists b(b = b + 1)$.

Основным средством вывода теорем в теории **PA** 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 $A(x) \supset A(S(x))$. 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 $A(S(x))$ (транзитивность равенства).

По теореме 5 (о дедукции) отсюда следует $\vdash A(x) \supset A(S(x))$, а затем получаем $\vdash \forall x(A(x) \supset A(S(x)))$. Так как $A(\mathbf{0})$ уже доказано, то по схеме индукции получаем $\vdash \forall xA(x)$ или $\vdash \mathbf{0} + x = x$.

Аналогично доказываются другие простые теоремы **PA**. 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 **PA** 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 **PA**.

Вопросы, связанные с полнотой и непротиворечивостью теории **PA**, рассматриваются в гл. 11.

§ 7. Аксиоматика Цермело–Френкеля

Понять – значит привыкнуть и научиться использовать.

Richard Feynman (1918–1988),
американский физик

Теория множеств, созданная Г. Кантором, в связи со своей универсальностью оказалась очень удобной для построения многих областей математики. Но наличие парадоксов, подобных парадоксу Рассела, в этом фундаменте математики привело исследователей к различным философским переосмыслениям и в самой теории множеств.

Ясно, что можно двигаться следующими путями: либо строить новую, гораздо более разветвленную теорию совокупностей, которые могут быть сложнее, чем множества, либо вводить какие-то разумные ограничения при образовании множеств из элементов.

Рассел считал, что причина парадоксов лежит в использовании порочного круга в определениях. Он провозгласил принцип порочного круга: *никакая совокупность не может содержать элементов, определимых только в терминах этой совокупности, а также элементов, включающих в себя или предполагающих эту совокупность*.

Б. Рассел и А. Уайтхед пошли первым путем – они строили так называемую *теорию типов*, где в иерархии подобных типов элементы, множества элементов, множества множеств элементов и т.д. занимают различные сложностные слои. В такой теории известные парадоксы теории множеств просто не могут возникнуть.

Более современная точка зрения предлагает все же вводить различные ограничения при собирании элементов в множества с тем, чтобы избежать ситуаций, подобных парадоксу Рассела. Цермело в 1908 г. предложил ограничиться рассмотрением множеств, предусмотренных некоторым списком аксиом. Эти аксиомы сформулированы так, что не видно, как можно было бы вывести из них известные парадоксы. В то же время аксиомы эти достаточны для вывода из них обычного запаса предложений классической математики, в том числе и абстрактной теории множеств, но без парадоксов.

Наибольшую известность в этом отношении получила **аксиоматика Цермело–Френкеля**⁸⁰, которая обычно называется системой **ZF** или **ZFC**, где **C** подчеркивает присут-

⁸⁰ Абрахам Френкель (1891–1965) – израильский математик, рожденный в Германии.

ствие в системе аксиомы выбора. Сигнатура языка первого порядка Цермело–Френкеля содержит единственную константу \emptyset (имя пустого множества при интерпретации), и два предикатных символа: « $=$ » (равенство) и символ принадлежности « \in ».

Прежде чем начать описывать аксиомы, сразу укажем, что является стандартной интерпретацией языка. В качестве носителя интерпретации определяется **универсум фон Неймана**⁸¹. Это ограниченный класс множеств, в отличие от канторовского универсума. 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 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 V множеством не является. Поэтому точно формулируются те операции, которые не выводят за пределы V . Символы переменных языка являются только именами множеств. Полное описание универсума V [78. 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 P : «множество всех подмножеств». Таким образом, первые множества следующие:

$$\begin{aligned} V_0 &= \emptyset, \\ V_1 &= P(V_0) = \{\emptyset\}, \\ V_2 &= P(V_1) = \{\emptyset, \{\emptyset\}\}, \\ &\dots\dots \\ V_{n+1} &= P(V_n), \\ &\dots\dots \end{aligned}$$

²

Имеем $V_n \subset V_{n+1}$. Множество V_n состоит из 2^{2^n} ($n-1$ двоек) конечных множеств, элементами которых, в свою очередь являются конечные множества, 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 P .

Перечислим аксиомы **ZFC**, которые являются истинными в стандартной интерпретации с носителем V .

1. Аксиома пустого множества

$$\forall x \neg(x \in \emptyset).$$

2. Аксиома пары

$$\forall x, y \exists X \forall z (z \in X \leftrightarrow z = x \vee z = y).$$

3. Аксиома объединения множества множеств

$$\forall X \exists Y \forall y (y \in Y \leftrightarrow \exists x (x \in X \& y \in x)).$$

Множество Y обозначается просто $\cup X$.

4. Аксиома множества всех подмножеств

$$\forall X \exists Y \forall Z (Z \in Y \leftrightarrow \forall x (x \in Z \supset x \in X)).$$

Множество Y есть множество всех подмножеств множества X .

⁸¹ Джон фон Нейман (1903–1957) – американский математик (венгр по происхождению). Сделал значительный вклад в функциональный анализ, логику и другие области математики.

5. Аксиома объемности

$$\forall X, Y (\forall z (z \in X \leftrightarrow z \in Y) \supset X = Y).$$

Если множества имеют одни и те же элементы, то они равны.

6. Аксиома регулярности

$$\forall X \exists x (x \in X \& \neg \exists y (y \in x \& y \in X)).$$

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.

$$\exists X \exists f \left(\begin{array}{l} f : X \rightarrow X \quad \& \\ \forall x, y (x \in X \& y \in X \supset f(x) = f(y) \supset x = y) \quad \& \\ \exists y (y \in X \& \forall x (x \in X \supset f(x) \neq y)) \end{array} \right).$$

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 дополнительно имеем $\forall x (x \in X \supset \exists 1 y A(x, y))$, тогда $\{y \mid \exists x (x \in X \& A(x, y))\}$, 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**

$$\forall X \left(\begin{array}{l} \forall Y (Y \in X \supset \exists y (y \in Y)) \supset \\ \exists f (f : X \rightarrow \bigcup X \& \forall Y (Y \in X \supset f(Y) \in Y)) \end{array} \right)$$

утверждает, что для каждого множества X существует функция выбора на X , т.е. функция f , сопоставляющая всякому подмножеству $Y \in X$ элемент $f(Y) \in Y$.

Вольно говоря, согласно аксиомам **ZFC** множеством называется то, что **либо** состоит из конечного числа объектов, **либо** является множеством всех натуральных чисел, **либо** получается применением к уже имеющемуся множеству уже имеющейся функции (или, что почти то же самое, получается взятием подмножества уже имеющегося множества), **либо** является объединением уже имеющегося множества уже имеющихся множеств, **либо**, наконец, является множеством всех подмножеств уже имеющегося множества. Для совокупности объектов не существует никаких других причин быть множеством, кроме перечисленных выше и аксиомы выбора. То есть если какое-то множество не получается при помощи перечисленных выше конструкций, то единственной причиной, по которой оно может существовать, во всех случаях является аксиома выбора.

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, п. 2):

Всякое бесконечное множество содержит счетное подмножество.

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, \dots ; построение не прервется ни на каком шаге, поскольку A бесконечно. Теперь множество $B = \{b_0, b_1, \dots\}$ и будет искомым подмножеством.

Очевидно, каждый акт выбора элемента b_i возможен только при использовании аксиомы выбора. 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» следствиями⁸².

Теорема 12 (Банаха–Тарского). Шар $B \subset \mathbb{R}^3$ допускает разбиение на конечное число непересекающихся множеств B_1, B_2, \dots, 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 [51]. Хотя теорема и 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 Гедель доказал (1940 г.), что аксиома выбора не противоречит системе аксиом **ZF**. Точнее, если **ZF** непротиворечива, то и **ZFC** непротиворечива. Пол Коэн⁸³ в свою очередь доказал (1963 г.), что если **ZF** непротиворечива, то и **ZF** плюс отрицание **AC** также непротиворечиво.

В теорию множеств **ZF** можно добавлять и другие аксиомы, лишь бы они не противоречили существующим. В связи с этим рассмотрим гипотезу континуума. Доказав, что мощность отрезка $[0, 1]$ превосходит мощность множества натуральных чисел \mathbb{N} , 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 (рис. 5), 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

$$\frac{1}{3}\left(1 + \frac{2}{3} + \left(\frac{2}{3}\right)^2 + \dots\right) = 1,$$

т.е. «вся длина» выбрасывается, но, тем не менее, C оказывается равномощно континууму.



Рис. 5. Множество Кантора

В результате многих безуспешных попыток Кантор пришел к убеждению справедливости следующего утверждения.

Гипотеза континуума (ГК). Не существует множества, промежуточного по мощности, между \mathbb{N} и $[0, 1]$, т.е. вслед за счетным множеством сразу идет континуум.

Эту гипотезу не могли доказать в течение 80 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 ее можно

⁸² Берtrand Рассел так отзывался 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».

⁸³ Пол Джозеф Коэн (1934–2007) – американский математик.

добавить как аксиому. И снова Коэн доказал (1963 г.), что если теория ZF непротиворечива, то ΓK 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 нее, с аксиомой выбора или без нее), и все они в одинаковой степени непротиворечивы.

А как же обстоит дело с непротиворечивостью аксиоматики 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, если оно и произойдет, послужит лишь прояснению, уточнению и, возможно, перестройке наших представлений, но не их крушению, как это многократно случалось в прошлом» [78].

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 P_1 (см. § 6 данной главы) является частным случаем трансфинитной индукции, каковая в ZFC не постулируется, а доказывается [41. С. 66–67].

Еще одно замечание о непротиворечивости аксиоматики ZF см. в главе 11 после теоремы 10.

Подведя итог рассмотрению аксиоматизации геометрии и теории множеств, мы видим, что у математиков есть выбор – считать следующие утверждения аксиомами или к таковым отнести их отрицания: аксиома о параллельных, аксиома выбора и гипотеза континуума. Тем самым правомочно утверждать о существовании различных математических реальностей.

Задачи

Задача 1. В § 5 главы 4 рассматривалась аксиоматическая теория – булева алгебра. Используя понятия, введенные в данной главе, изучите, какими свойствами обладает теория булевых алгебр.

Задача 2. Для формальной теории MU (пример 4) найдите вывод MU или докажите, что он невозможен.

Задача 3. Докажите, что формальная теория, имеющая только удлиняющие правила вывода, обладает разрешающим алгоритмом (см. пример 5), и напишите разрешающий алгоритм на псевдокоде.

Задача 4. Выразите в стандартной интерпретации элементарной арифметики свойства и отношения натуральных чисел:

- a) свойство: $n = 1$;
- b) отношение: a делит b ;
- c) свойство: $n = 7$;
- d) свойство: n представимо в виде суммы трех квадратов;
- e) отношение: $x > y$;
- f) отношение: a и b – взаимно просты;
- g) отношение: q есть частное при делении a на b ;
- h) отношение: r есть остаток при делении a на b ;
- i) свойство: x – простое число;
- j) свойство: коммутативность сложения;
- k) свойство: n – степень двойки. Подсказка: степени двойки характеризуются тем, что все их неединичные делители четны.

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

Глава 7. Математическое доказательство

В данной главе доказательство в математике исследуется с разных сторон. Уточняются данные ранее определения различных видов математических доказательств. Рассматриваются и другие методы доказательств.

§ 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 необходимо также догадаться, как привести 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 главе 1 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 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.

а. Каждое следующее число на 3 больше, чем предыдущее, поэтому мы предсказываем, что после 15 должно следовать 18.

б. 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 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 третью разности для последовательности a_n :

$$\begin{array}{cccc} 12 & 18 & 24 & 30 \\ & 6 & 6 & 6 \end{array}$$

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 1 и 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 установили 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 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 Ферма⁸⁴, Эйлер, Лангранж⁸⁵, Гаусс и др. 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. 1).



Рис. 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 слагаемых n -угольных чисел. Гипотезу Ферма доказал Коши только в 1815 г. [52. С. 62–65].

Треугольное число – это число кружков, которые могут быть расположены в форме правильного треугольника. На рис. 2 изображены первые пять треугольных чисел S_n , $n = 1, 2, 3, 4, 5$.

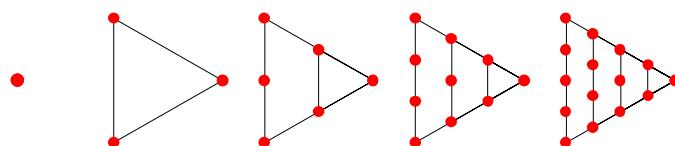


Рис. 2. $S_1 = 1, S_2 = 3, S_3 = 6, S_4 = 10, S_5 = 15$

Очевидно, с чисто арифметической точки зрения n -е треугольное число – это сумма n первых натуральных чисел. Поэтому получаем $S_n = n(n + 1)/2$.

Заключение, основанное на индуктивном рассуждении, может быть некорректно.

⁸⁴ Пьер де Ферма (1601–1665) – французский величайший математик-любитель всех времен. Видный специалист в теории чисел, автор Великой теоремы Ферма.

⁸⁵ Жозеф Луи Лагранж (1736–1813) – французский математик, астроном и механик.

Пример 4 (Amer. Math. Monthly. 1977. V. 84, № 6). Известна задача 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. 3).

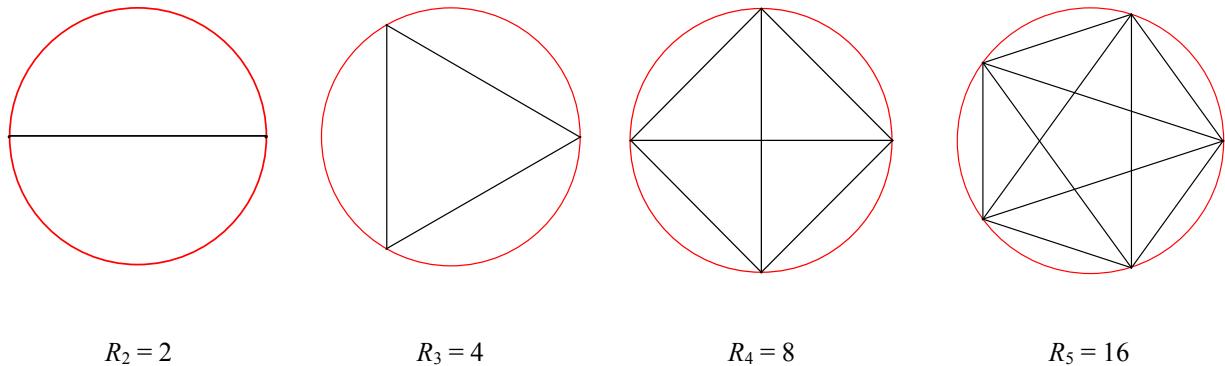


Рис. 3. Хорды в круге

Результаты при $n = 2, 3, 4$ и 5 наводят на мысль, что $R_n = 2^{n-1}$, но $R_6 = 31$ (рис. 4).

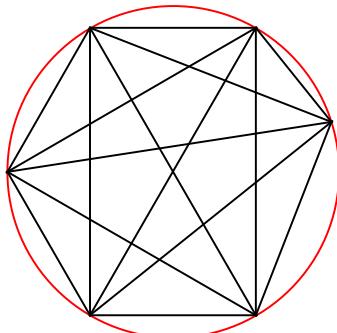


Рис. 4. Контрпример: $R_6 = 31$

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

$$R_n = 1 + \frac{n(n-1)}{2} + \frac{n(n-1)(n-2)(n-3)}{24}. \quad (1)$$

Парадокс Гемпеля⁸⁶. В науке широко используется *принцип индукции*, который утверждает: «Наблюдение явления X , которое соответствует теории T , дополнительно подтверждает теорию T ».

Предположим, биолог ищет доказательства своей гипотезы «Все вороны черные». Но для этого ему нет необходимости отправляться в экспедиции. Ибо в силу закона контрапозиции $A \supset B \sim \neg B \supset \neg A$ дополнительным свидетельством гипотезы является всякий нечерный предмет, найденный биологом дома (конечно, если он не окажется вороном).

Логика бессильна формализовать индукцию (но см. [92. Т. 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...

⁸⁶ Карл Густав Гемпель (1905–1997) – немецкий и американский философ.

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 неожиданные тропинки в широкую магистраль, по которой может проехать любой.

§ 2. Математическая индукция

Математическая индукция является приемом доказательства, часто полезным для подтверждения математических предположений, к которому мы пришли с помощью некоторого процесса индукции.

В книге [92] Д. Пойа⁸⁷ (рис. 5) рассказывает, как с помощью индукции можно найти формулу для суммы n первых квадратов

$$1 + 4 + 9 + 16 + \dots + n^2.$$

Он сравнивает эту сумму с суммой первых n натуральных чисел с известной формулой

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}.$$



Рис. 5. Дьёрдь Пойа

Пойа 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	...
$1 + 2 + 3 + \dots + n$	1	3	6	10	15	21	...
$1 + 4 + 9 + 16 + \dots + n^2$	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	...
$1^2 + 2^2 + \dots + n^2$	1	5	7	3	11	13	...
$1 + 2 + \dots + n$		$\frac{1}{3}$	$\frac{1}{3}$		$\frac{1}{3}$	$\frac{1}{3}$	

⁸⁷ Дьёрдь Пойа (англ. George Polya – Джордж Поля; 1887–1985) – 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:

$$\frac{3}{3} \quad \frac{5}{3} \quad \frac{7}{3} \quad \frac{9}{3} \quad \frac{11}{3} \quad \frac{13}{3},$$

его почти невозможно не заметить. Едва ли мы сможем удержаться и не сформулировать предположение, что

$$\frac{1^2 + 2^2 + \dots + n^2}{1+2+\dots+n} = \frac{2n+1}{3}.$$

Пользуясь значением знаменателя в левой части, которое мы считаем известным, можем высказать наше предположение в форме

$$1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

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, проводит следующее доказательство.

«Предположительно верно, что

$$1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Неоспоримо верно, что

$$(n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{3} - \frac{n(n+1)(2n+1)}{6}.$$

Следовательно, верно, что

$$1^2 + 2^2 + 3^2 + \dots + n^2 + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}$$

(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» [22].

Далее Д. Пойя 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 к рассмотрению разнообразных вариантов математической индукции. Современное развитие принципа математической индукции началось с аксиомой Пеано для теории формальной арифметики ЕА. Аксиома математической индукции (см. главу 6, § 6) в стандартной интерпретации ЕА выражается формулой

$$(P(0) \& \forall x(P(x) \supset P(x+1)) \supset \forall n P(n)) \tag{2}$$

Из аксиомы (2) следует теорема.

Теорема 1 (Принцип математической индукции). Пусть $P(n)$ – свойство натуральных чисел, выражимых в теории ЕА.

Если:

- 1) выполнено $P(0)$ и
- 2) для каждого $k \geq 0$ из $P(k)$ следует $P(k+1)$,

то для каждого $n \geq 0$ справедливо $P(n)$.

Доказательство. Из истинности формул $P(0)$ и $\forall x(P(x) \supset P(x + 1))$ в силу аксиомы (2) следует $\forall nP(n)$. ■

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 5. Приведем с помощью математической индукции доказательство справедливости формулы для суммы квадратов

$$1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}. \quad (3)$$

Пусть $P(n)$ обозначает равенство (3). Очевидно, базис индукции выполнен, $0^2 = 0 \times 1 \times 1 / 6 = 0$. Докажем индуктивный переход от $P(n)$ к $P(n+1)$: добавим к обеим частям равенства (3) слагаемое $(n+1)^2$. Тогда слева будет сумма первых $n+1$ квадратов, а справа получаем

$$\frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6},$$

что и требовалось доказать. ■

Пример 6. Пусть дана последовательность $1, 1, 2, 3, 5, 8, \dots$ чисел Фибоначчи $f(n)$ (см. главу 1, § 3). Докажите формулу Кассини⁸⁸ $f(n+1)f(n-1) - f(n)^2 = (-1)^n$ при $n > 1$.

Доказательство. Определим $P(n)$ как $f(n+1)f(n-1) - f(n)^2 = (-1)^n$ при $n > 1$.

Базис индукции выполняется для $n = 2$: $f(3)f(1) - f(2)^2 = (-1)^2$.

Шаг индукции. Пусть для $k \geq 2$ выполнено $P(k)$: $f(k+1)f(k-1) - f(k)^2 = (-1)^k$. Докажем $P(k+1)$. Имеем

$$\begin{aligned} f(k+2)f(k) &= (f(k+1) + f(k))f(k) = \\ &= f(k+1)f(k) + f(k)^2 = f(k+1)f(k) + f(k+1)f(k-1) - (-1)^k \text{ (в силу } P(k) \text{)} = \\ &= f(k+1)(f(k) + f(k-1)) - (-1)^k = f(k+1)f(k+1) - (-1)^k = f(k+1)^2 - (-1)^k. \end{aligned}$$

Отсюда получаем $f(k+2)f(k) = f(k+1)^2 + (-1)^{k+1}$, т.е. $f(k+2)f(k) - f(k+1)^2 = (-1)^{k+1}$.

По принципу математической индукции имеем $f(n+1)f(n-1) - f(n)^2 = (-1)^n$ при $n > 1$. ■

Формула Кассини объясняет софизм с числами Фибоначчи, рассмотренный в главе 1, § 3.

Выполнение базиса индукции необходимо для индуктивного доказательства.

Пример 7. 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 8. Для любого натурального n число $n^2 + 5n + 1$ – четное. Хотя легко доказать, что индуктивный шаг из четности $n^2 + 5n + 1$ выводит четность $(n+1)^2 + 5(n+1) + 1$, но верности одного индуктивного перехода недостаточно.

Базис в математической индукции может быть любым натуральным числом.

⁸⁸ Джованни Доменико Кассини (1625–1712) – итальянский и французский астроном.

Теорема 2 (принцип математической индукции с базисом, большим 0). Пусть $P(n)$ – свойство натуральных чисел, выражимых в теории ЕА.

Если:

- 1) для некоторого $k \geq 0$ выполнено $P(k)$ и
- 2) для каждого $m \geq k$ из $P(m)$ следует $P(m + 1)$,

то для каждого $n \geq k$ справедливо $P(n)$.

Доказательство. Положим $T(n) = P(n + k)$. Тогда имеем:

1a) выполнено $T(0)$ и

2a) для каждого $m \geq 0$ из $T(m)$ следует $T(m + 1)$, и теорема 1 дает для каждого $n \geq 0$ истинность $T(n)$, что влечет справедливость $P(n)$ для всех $n \geq k$. ■

Теорема 3. Принцип математической индукции эквивалентен существованию наименьшего элемента в любом непустом подмножестве \mathbb{N} .

Доказательство.

1. Пусть в любом непустом подмножестве \mathbb{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 $k \geq 0$ из $P(k)$ следует $P(k+1)$.

Будем рассуждать от противного: множество $B = \{n \mid \neg P(n)\}$ непусто. Тогда существует наименьший элемент $m \in B$. Так как $P(0)$ по базису индукции – истина, то $m > 0$. Следовательно, $m - 1 \in \mathbb{N}$ 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 $n \geq 0$ справедливо $P(n)$.

2. Пусть справедлив принцип математической индукции и B – непустое подмножество \mathbb{N} . Докажем, что в B существует наименьший элемент. От противного: пусть в B нет наименьшего элемента. Определим предикат

$$P(n) = \langle\langle \forall m (m \leq n \supset m \notin B) \rangle\rangle.$$

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 $m \leq k$ 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 $m \leq k + 1$ 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 $n \geq 0$ справедливо $P(n)$. Последнее означает, что $B = \emptyset$. 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 переходит 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

$$\forall x (x < 0 \supset P(x)),$$

а отсюда по индуктивному переходу имеем $P(0)$.

Теорема 4 (возвратная индукция). Пусть $P(n)$ – свойство натуральных чисел, выражимых в теории ЕА.

Если для всех x утверждение $\forall y (y < x \supset P(y))$ влечет $P(x)$, то для каждого $n \geq 0$ справедливо $P(n)$.

Еще одна переформулировка метода математической индукции:

Теорема 5 (принцип бесконечного спуска). Пусть $P(n)$ – свойство натуральных чисел, выражимых в теории ЕА.

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

$$\forall n (P(n) \supset \exists m (m < n \& P(m))) \supset \forall n \neg P(n).$$

Теорема 6. Следующие пять свойств множества \mathbb{N} натуральных чисел эквивалентны:

- a) принцип математической индукции (теорема 1);
- b) любое непустое подмножество \mathbb{N} имеет наименьший элемент;
- c) всякая строго убывающая последовательность натуральных чисел конечна;
- d) возвратная индукция (теорема 4);
- e) принцип бесконечного спуска (теорема 5).

Доказательство. $(a) \Leftrightarrow (b)$: эквивалентность (a) и (b) доказана в теореме 3.

$(b) \Leftrightarrow (c)$: если $x_0 > x_1 > x_2 > \dots$ – 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

$$\langle\!\langle \text{Для всех } x \text{ утверждение } \forall y (y < x \supset P(y)) \text{ влечет } P(x)\rangle\!\rangle. \quad (4)$$

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 (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 был бы 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.

Пример 9. Пусть k – натуральное число и \sqrt{k} – не целое. Докажите, что \sqrt{k} – иррациональное число.

Доказательство. 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} – 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 7 (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 $m \geq 2$ и допустим, что для каждого k , удовлетворяющего неравенству $2 \leq k < m$, утверждение $P(k)$ истинно. Если m – простое число, то $P(m)$ – истина. Если m – составное число, то существуют r и s , для которых выполнено $2 \leq r < m$, $2 \leq s < m$ и $r \cdot s = m$. Так как $P(r)$ и $P(s)$ выполнены, то r и s – произведения простых чисел. Поэтому $r \cdot s$ есть произведение простых чисел. В силу возвратной индукции получаем, что любое n разложимо в произведение простых чисел.

2. Покажем единственность разложения, следуя [57. С. 17–18]. Пусть $S(n)$ утверждает, что n имеет единственное представление (с точностью до порядка сомножителей) в виде произведения простых чисел. Возьмем некоторое $m \geq 2$ и допустим, что для каждого k , удовлетворяющего неравенству $2 \leq k < m$, 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,

$$m = pqr \dots = p'q'r'\dots,$$

где p, q, r, \dots и p', q', r', \dots – простые. Одно и то же простое число не может встретиться в двух разложениях, так как в этом случае мы сократили бы на это простое и получили 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 $m \geq p^2$. Аналогично $m \geq p'^2$. 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

$$m - pp' = pp'QR\dots,$$

где Q, R, \dots – простые числа. Отсюда следует, что число pp' делит m . Но $m = pqr\dots$, поэтому (после сокращения на p) получается, что p' делит $qr\dots$. Ввиду вспомогательного утверждения, приведенного выше в скобках, это невозможно, ибо $qr\dots$ – число, меньшее m , и p' не является одним из простых q, r, \dots , входящих в его разложение. Это противоречие доказывает, что для m выполнено $S(m)$. В силу возвратной индукции 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 $n \geq 0$ из $P(n)$ следует $P(n + 2)$,
то для всех $n \geq 0$ справедливо $P(n)$.

В действительности, два отдельных индуктивных доказательства комбинируются в одно (одно для четных и другое для нечетных чисел). Приведем пример, где три индуктивных доказательства свернуты в одно.

Пример 10. Докажите, что если натуральное $n > 13$, то существуют такие натуральные числа a и b , что $n = 3a + 8b$.

Доказательство. 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 ($P(k) \supset P(k + 3)$). 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 $14, 17, 20, \dots$; второе – для последовательности $15, 18, 21, \dots$ и третье – для последовательности $16, 19, 22, \dots$. ■

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 $k \geq m$. Тогда в результате для всех $n \geq m$ справедливо $P(n)$.

Пример 11. Докажите, что для любого $n \geq 1$ выполнено неравенство $f(n) \leq \left(\frac{5}{3}\right)^{n-1}$.

Доказательство. Пусть $P(n)$ есть утверждение $f(n) \leq \left(\frac{5}{3}\right)^{n-1}$ для $n \geq 1$.

Базис индукции. Имеем $P(1): 1 \leq 1$ – истина и $P(2): 1 \leq 5/3$ – истина.

Индуктивный шаг. Пусть $k \geq 1$ и $P(k) \& P(k+1)$ – истина. Тогда

$$\begin{aligned} f(k + 2) &= f(k) + f(k + 1) \leq \\ &\leq \left(\frac{5}{3}\right)^{k-1} + \left(\frac{5}{3}\right)^k \quad (\text{в силу } P(k) \text{ и } P(k+1)) = \end{aligned}$$

$$\begin{aligned}
&= \left(\frac{5}{3}\right)^{k-1} \left(1 + \frac{5}{3}\right) = \left(\frac{5}{3}\right)^{k-1} \left(\frac{8}{3}\right) < \\
&< \left(\frac{5}{3}\right)^{k-1} \left(\frac{25}{9}\right) = \left(\frac{5}{3}\right)^{k+1}.
\end{aligned}$$

Мы доказали $P(k+2)$. Поэтому $P(n)$ справедливо для $n \geq 1$. ■

Парадоксы и софизм при математической индукции

1. Парадокс неожиданной казни. Мы встретились с этим парадоксом в главе 1, § 3. Кажется, до сих пор не существует удовлетворительного разрешения этого парадокса, однако см. книгу Р. Смаллиана [97. С. 16–20].

2. Парадокс Ришара. Рассмотрим этот парадокс в иной форме по сравнению с оригинальным описанием в [64. С. 41].

Пример 12. 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 $k \geq 0$ фиксировано и допустим, что имеет место $P(0), P(1), \dots, P(k - 1)$, 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 главе 1, § 3.

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 с 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 $n + 1$ также должны быть одинаковой масти. Таким образом, все $n + 1$ 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 $n \geq 1$. Но это невозможно, поскольку пересечение двух множеств $\{1, 2, \dots, n\}$ и $\{2, 3, \dots, n + 1\}$ пусто при $n = 1$.

4. Парадокс изобретателя. Попробуем доказать методом математической индукции неравенство⁸⁹

$$\frac{1 \cdot 3 \cdot \dots \cdot (2n-1)}{2 \cdot 4 \cdot \dots \cdot 2n} < \frac{1}{\sqrt{n}}, \quad n \geq 1.$$

⁸⁹ В изложении следуем [122. С. 568].

Базис индукции

$$\frac{1}{2} < \frac{1}{\sqrt{1}}.$$

По предположению индукции

$$\frac{1 \cdot 3 \cdots (2k-1) \cdot (2k+1)}{2 \cdot 4 \cdots 2k \cdot (2k+2)} = \frac{1 \cdot 3 \cdots (2k-1)}{2 \cdot 4 \cdots 2k} \cdot \frac{2k+1}{2k+2} < \frac{1}{\sqrt{k}} \cdot \frac{2k+1}{2k+2},$$

и нам остается доказать, что

$$\frac{2k+1}{2k+2} \leq \frac{1}{\sqrt{k+1}}. \quad (5)$$

Возводя обе части неравенства в квадрат и избавляясь от знаменателей, приходим к эквивалентному неравенству

$$(k+1)(2k+1)^2 \leq k(2k+2)^2 \quad (6)$$

и далее, раскрывая скобки, – к неравенству

$$4k^3 + 8k^2 + 5k + 1 \leq 4k^3 + 8k^2 + 4k.$$

Это неравенство неверно! Следовательно, неверны и неравенства (6) и (5). Можно считать, что неверно исходное неравенство? Нет нельзя. Неудача говорит лишь о том, что конкретный метод доказательства – индукция – не годится. Попробуем теперь доказать неравенство

$$\frac{1 \cdot 3 \cdots (2n-1)}{2 \cdot 4 \cdots 2n} < \frac{1}{\sqrt{n+1}}, n \geq 1. \quad (7)$$

Неравенство (7) сильнее нашего исходного неравенства, и, казалось бы, доказывать его тем же методом – индукцией – дело безнадежное. Все же попробуем.

Базис индукции

$$\frac{1}{2} < \frac{1}{\sqrt{1+1}}.$$

По предположению индукции

$$\frac{1 \cdot 3 \cdots (2k-1) \cdot (2k+1)}{2 \cdot 4 \cdots 2k \cdot (2k+2)} = \frac{1 \cdot 3 \cdots (2k-1)}{2 \cdot 4 \cdots 2k} \cdot \frac{2k+1}{2k+2} < \frac{1}{\sqrt{k+1}} \cdot \frac{2k+1}{2k+2},$$

и нам надо доказать, что

$$\frac{1}{\sqrt{k+1}} \frac{2k+1}{2k+2} \leq \frac{1}{\sqrt{k+2}}.$$

Снова возводя обе части неравенства в квадрат, избавляясь от знаменателей и раскрывая скобки, приходим к эквивалентному неравенству

$$4k^3 + 12k^2 + 9k + 2 \leq 4k^3 + 12k^2 + 12k + 4.$$

Это неравенство верно.

Следовательно, мы доказали (методом математической индукции) неравенство (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 [91. С. 138]. Он использовал наблюдение, что при доказательстве по математической индукции часто необходимо усиливать доказываемое предложение, и индуктивное утверждение становится намного сложнее конечно-го 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 устраниć 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 [86. С. 323–325; 87. С. 868–869] пишет, что даже в принципе в математических доказательствах внешне простых предложений нельзя обойтись без сложных лемм. Парадокс изобретателя показывает полную методологическую несостоятельность редукционизма и эмпиризма⁹⁰. 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 типа B .

Индуктивный переход. Если мы имеем выражения A_1, \dots, A_n типа B , то C , построенное из них, также есть выражение типа B .

С 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, \dots, 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 словами, 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 13. Примерами индуктивного определения по построению являются определение пропозициональной формулы (глава 4, § 2), определение термов и формул языка первого порядка (глава 5, § 2).

Доказательство леммы 2 для теоремы 4 из главы 4, § 3 было отложено. Сейчас мы проведем доказательство этой леммы с помощью математической индукции по построению.

⁹⁰ 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.

Лемма 2 (из главы 4). Пусть $A \sim B$ 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 $C_A \sim C_B$.

Доказательство. Для доказательства 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 , $C_A \sim C_B$ – не что иное, как $A \sim B$.

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 $D \leftrightarrow E$, 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 $D_A \sim D_B$. Применим теперь лемму 1 (для теоремы 4 из главы 4, § 3) в случае $A \supset C \sim B \supset C$, где в роли A выступает D_A и в роли B – D_B , в роли C – E . В результате получаем $C_A \sim C_B$. Другие случаи рассматриваются аналогично. ■

Пример 14. В главе 6 была определена теория L . Формулами в теории L являются все возможные строки, составленные из букв a , b . Единственной аксиомой L является строка a , наконец, в L имеется два правила вывода:

$$\frac{X}{Xb} \quad \text{и} \quad \frac{X}{aXa}.$$

В главе 6, § 2 была сформулирована метатеорема: если X – теорема, то aaX – тоже теорема.

Докажем ее, 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. ■

Что имеет значение?

Фантазия в первую очередь.

И еще дар к абстрактному мышлению.

Александр Александрович Алехин (1892–1946),
4-й чемпион мира по шахматам

§ 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 «естественней» 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 $\langle\Gamma|-P\rangle$ или $\langle\neg\Gamma|-P\rangle$ для разных теорий первого порядка, множеств Γ и разных (классов) формул P .

Результат $\langle\Gamma|-P\rangle$ 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 $\langle\Gamma|-P\rangle$ может вообще не сопровождаться предъявлением вывода P из Γ , хотя бы и неполного. В этом случае мы $\langle\neg\Gamma|-P\rangle$, а доказываем, что существует доказательство P .

Результат $\langle\neg\Gamma|-P\rangle$ 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 есть «настоящие» математические доказательства или что математики на самом деле работают в рамках определенных формальных систем.

По словам Ю.И. Манина [78. С. 54], «*в качестве средства общения, открытия, фиксации материала никакой формальный язык не способен конкурировать со смесью национального математического языка и формул, привычной для каждого работающего математика*». Кроме того, неформальное доказательство говорит нам об идее, заложенной в доказательство (см. цитату из Манина в качестве эпиграфа к данной главе).

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, а также и некоторые неформальные доказательства. Например, использование диаграмм Венна для обоснования тождеств алгебры множеств (глава 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 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. глава 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. Используя системы компьютерной алгебры, проверка может быть проделана для очень больших чисел. Например, самая старая открытая проблема со времен Античности: существуют ли нечетные совершенные⁹¹ числа? На конец 2014 г. проверены все нечетные числа, меньшие 10^{300} . Нечетное совершенное число не обнаружено.

3. Использование теоремы о дедукции. Теорема о дедукции справедлива для исчисления высказываний (глава 6, теорема 2) и для теорий первого порядка (глава 6, теорема 5). 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 .

Пример 15. Докажите, что для каждого целого n , если n – четное, то n^2 – тоже четное.

Доказательство. Так как n четное, 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.

⁹¹ Натуральное число n называется совершенным, если сумма всех его делителей равна $2n$.

Пример 16. На основе контрапозиции докажите, что если m и n – произвольные положительные целые числа, такие что $m \times n \leq 100$, то либо $m \leq 10$, либо $n \leq 10$.

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 совершают компьютер с помощью специальных программных систем доказательства теорем (например, с помощью языка программирования Prolog).

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:

$$\begin{aligned} A \supset B &\sim \neg(A \supset B) \supset (C \& \neg C) \sim (A \& \neg B) \supset (C \& \neg C), \\ A \supset B &\sim (A \& \neg B) \supset \neg A, \\ A \supset B &\sim (A \& \neg B) \supset B. \end{aligned}$$

Используя вторую из приведенных равносильностей для доказательства $A \supset B$, мы допускаем одновременно A и $\neg B$, т.е. предполагаем, что заключение ложно:

$$\neg(A \supset B) \sim \neg(\neg A \vee B) \sim A \& \neg B.$$

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 жертвує *партию*» [116. С. 61].

Мы уже применяли в главе 4, § 3 метод от противного при доказательстве тавтологичности некоторых импликаций. Следующие примеры знамениты.

Теорема 8 (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

$$\sqrt{2} = \frac{p}{q} \text{».}$$

В самом деле, тогда приходим к равенству $p^2 = 2q^2$. Можно 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

$$4r^2 = 2q^2, \text{ или } 2r^2 = q^2.$$

Так как с левой стороны теперь имеется 2 в качестве множителя, значит q^2 , а следовательно, и q – четное. Таким образом, 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 9 (Евклид). Доказать, что простых чисел бесконечно много.

Доказательство. Предположим, что существует конечное множество простых чисел и p есть наибольшее из них: $2, 3, 5, 7, 11, \dots, p$. Определим число $N = p! + 1$. Число N при делении на любое из чисел, меньших 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

$$k \cdot k = k^2 > k \cdot 1 = k.$$

Последнее 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

$$\forall x (A(x) \supset B(x)),$$

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, т.е. 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 контрпример, для которого гипотеза невыполнима.

Знаменитых контрпримеров множество⁹². Перечислим некоторые из них.

Пример 17. Ферма предполагал, что все числа вида

$$p_k = 2^{2^k} + 1$$

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

⁹² Д. Пойа: «Математика состоит из двух вещей – теорем и контрпримеров».

все остальные числа, которые удалось проверить на простоту, оказались составными. Число p_5 было разложено на множители Эйлером.

Пример 18. 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 решений в целых числах. В 1966 г. был найден для $n = 5$ контрпример

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5.$$

Для $n = 4$ контрпример был найден в 1986 г.:

$$2682440^4 + 15365639^4 + 1879760^4 = 206156734^4.$$

Пример 19. В 1806 г. А.-М. Ампер⁹³ предпринял попытку доказать, что всякая «произвольная» функция дифференцируема всюду за исключением «исключительных и изолированных» значений аргумента. Один из контрпримеров был найден в 1930 г. Б. ван дер Варденом⁹⁴ – 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 общенациональный 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.

Отметим, что математическая индукция очень часто используется для доказательства гипотез, полученных с помощью индукции.

8. Интуиционистская логика и конструктивные доказательства.

Голландский математик Лейтзен Брауэр (1881–1966) создал целую школу в области основания математики – **математический интуионизм**. Брауэр в 1908 г. в статье «Недостоверность логических принципов» заявил, что традиционная классическая логика была абстрагирована от математики конечных множеств и, забыв об этом, математики стали ошибочно применять ее без какого-либо оправдания к математике бесконечных множеств. Он считал, что парадоксы возникли потому, что математики стали рассуждать об очень абстрактных объектах без всякой осторожности. А эти объекты, возможно, существуют только в противоречивой фантазии математиков.

Неинтуиционистская математика и интуиционистская математика Брауэра существенно различаются в их точке зрения на бесконечность. В классической математике бесконечность рассматривается как **актуальная**, или завершенная. Бесконечное множество рассматривается как существующее в виде завершенной совокупности до и независимо от всякого процесса порождения или построения его человеком, как если бы оно полностью лежало перед нами для нашего обозрения. В интуиционистской математике бесконечность рассматривается только как **потенциальная**, или становящаяся, или конструктивная [49].

⁹³ Андре-Мари Ампер (1775–1836) – знаменитый французский физик и математик.

⁹⁴ Бартель ван дер Варден (1903–1996) – голландский математик.

Брауэр заявлял, что возникшие противоречия в математике являются лишь симптомами болезни, а надо устраниить ее причину. Причину он видел в том, что математические рассуждения и понятия утратили интуитивный смысл, и нужно вернуться к основам и пересмотреть даже логические законы. Формальные правила интуиционистской логики высказываний были разработаны Арендом Гейтингом (1898–1980 гг.), учеником Брауэра.

Принципом классической логики, который является истинным при рассуждениях о конечных множествах, но который интуиционисты не принимают для бесконечных множеств, является закон исключенного третьего ($A \vee \neg A$ – тавтология).

Конечно, сразу же возникают естественные вопросы: почему именно эта аксиома вызывает сомнения? Вообще-то аксиом много, и можно было бы исключить любую и смотреть, что получится без нее, но ясно, что, скорее всего, получится что-то странное. Как понять, какие формулы останутся теоремами без закона исключенного третьего? Раньше у исчисления высказываний была «сверхзадача» – вывести все тавтологии и только их, а теперь?

Интуиционистское исчисление высказываний возникло как попытка формализовать (пусть частично) методы рассуждений, практикуемые в интуиционистской математике. Интуиционизм отвергает идею о том, что все высказывания делятся на истинные и ложные (пусть неизвестным нам образом). С этой точки зрения закон исключенного третьего совершенно безоснователен: $A \vee \neg A$ означает, что для произвольного утверждения A мы можем установить либо A , либо его отрицание (т.е. объяснить, почему A в принципе не может быть установлено) – а почему, собственно?

Пусть A есть утверждение «существует натуральное число n , для которого истинно $P(n)$ ». Интуиционистское доказательство предложения A должно быть **конструктивным** в следующем (узком) смысле: это доказательство действительно предоставляет пример такого n , что $P(n)$, или, по крайней мере, указывает метод, позволяющий в принципе найти такой пример.

В классической математике встречаются **неконструктивные** или **косвенные** доказательства существования, которые не принимают интуиционисты. Например, чтобы доказать предложение «существует n такое, что $P(n)$ », классически настроенный математик может вывести противоречие из допущения, что истинно $\forall n \neg P(n)$. Согласно обеим логикам – классической и интуиционистской – это в силу доказательства от противного дает истинность предложения $\neg \forall n \neg P(n)$, но (вообще говоря) этого не позволяет сделать логика интуиционистская. Такое классическое, доказательство существования не приближает нас к обладанию примером числа n , такого, что $P(n)$ (хотя иногда мы все же можем получить такой пример другим способом). Интуиционисты отказываются принять такое доказательство существования, потому что его заключение «существует натуральное число n , для которого истинно $P(n)$ », они могут воспринимать только как ссылку на пример числа n , такого что $P(n)$, а такого примера получено не было. Классическое понимание, обозначающее, что где-то в завершенной бесконечной (актуальной) совокупности всех натуральных чисел встречается такое n , что $P(n)$, для них не годится.

Обычно, говоря об интуиционизме, приводят следующий пример рассуждения, неприемлемого с точки зрения интуиционизма. Докажем, что существуют иррациональные числа α и β , для которых α^β рационально. В самом деле, рассмотрим два случая. Если $\sqrt{2}^{\sqrt{2}}$ рационально, то положим $\alpha = \beta = \sqrt{2}$. Если же $\sqrt{2}^{\sqrt{2}}$ иррационально, то положим $\alpha = \sqrt{2}^{\sqrt{2}}$ и $\beta = \sqrt{2}$; легко проверить, что $\alpha^\beta = 2$. Интуиционист скажет, что это рассуждение некорректно: доказать существование чего-то означает построить этот объект, а мы так и не построили чисел α и β , поскольку не установили, какой из двух случаев имеет место.

Ярким примером чистой теоремы существования является теорема о неподвижной точке: любое непрерывное отображение замкнутого шара в себя в конечномерном евклидовом пространстве \mathbb{R}^n имеет неподвижную точку.

Ирония судьбы заключается в том, что теорема первоначально была доказана для случая $n = 2$ самим Брауэром до того, как он стал интуиционистом. Но самое важное у Брауэра было то, что он полностью видоизменил приоритеты математики. Если традиционная математика занимается поиском и доказательством теорем, то он начал ее рассматривать как источник построений. Мало доказать теорему, нужно, чтобы обоснование дало нам построение объекта, существование которого утверждается в теореме. А использование доказательств в качестве источника построений – именно то, что нужно от математики информатику.

Развитие математики в XX в. показало, что интуиционистская логика связана с важнейшими математическими понятиями. Дальнейшее развитие интуионизма привело к возникновению современной **конструктивной математики** [79. С. 4].

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.: [110. 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.

Мнение Ю.И. Манина [78. С. 54–55].

1. *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 оспаривается закон исключенного третьего. С этих крайне критических позиций наши «доказательства» в лучшем случае выводят бесмыслицу 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.

2. *Уровни доказательности.* Каждое предложенное доказательство апробируется на приемлемость математиками, иногда нескольких поколений. При этом подлежат уточнению и само доказательство, и его результат. Чаще всего доказательство является более или менее краткой схемы 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».

3. *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.

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 общим ожиданиям, 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.

Доказательство Гёделя существования Бога

Используя язык логики предикатов, можно доказывать значительно более сильные утверждения, чем только применяя исчисление высказываний. В качестве математического курьеза приведем высказывание Юрия Манина из книги [77. С. 87]:

«Гёделевское отнологическое доказательство. В третьем томе собрания сочинений Гёделя, недавно выпущенном издательством Oxford University Press, содержится заметка, датированная 1970 годом. Она представляет собой формальное рассуждение, призванное доказать существование Бога как воплощение всех положительных свойств...»

И заканчивает, без обсуждения, следующими словами:

«Само по себе доказательство представляет собой страницу формул на языке модальной логики (с использованием, наряду с привычной символикой, кванторов необходимости и возможности). Оно подразделяется на пять аксиом и две теоремы. Для удобства читателей доказательство представлено на отдельной странице».

Читатель может познакомиться с доказательством в книге Манина.

Лучший способ в чем-то разобраться до конца –
это попробовать научить этому компьютер.

Дональд Кнут

§ 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 Леонардо Эйлер был непревзойденным 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 сумму делителей натуральных чисел [91. С. 39–43, 11–122].

В XIX в. очень много вычислений было проделано в астрономии. Например, французский математик Урбен Леверье (1811–1877) проводил громоздкие расчеты орбиты Нептуна, основанные на аналитических вычислениях возмущенной орбиты Урана (что и позволило открыть Нептун).

Впечатляющие вычисления с помощью карандаша и бумаги проделал французский астроном Шарль-Эжен Делоне (1816–1872) для определения орбиты Луны. Он вывел около 40 тыс. формул. На их вывод потребовалось 10 лет и еще 10 ушло на проверку формул. Окончательная формула занимала 128 страниц его книги с результатами работы. Проверка его аналитических преобразований была проведена двумя американскими математиками с помощью компьютера в 70-е гг. XX в. Компьютеру потребовалось двое суток работы.

Большие усилия тратили математики на определение числа π , вручную вычисляя большое количество цифр. Так, наилучший результат к концу XIX в. был получен английским математиком-любителем Вильямом Шенксом (1812–1882). Он потратил 15 лет на то, чтобы вычислить 707 цифр, хотя из-за ошибки только первые 527 были верными. Он использовал формулу Мэчина (John Machin; 1680–1751)

$$\frac{\pi}{4} = 4 \operatorname{arctg} \frac{1}{5} - \operatorname{arctg} \frac{1}{239}.$$

Ошибка Шенкса в 1944 г. обнаружил Фергюсон (D.E. Ferguson); он считал по формуле, подобной формуле Мэчина:

$$\frac{\pi}{4} = 3 \operatorname{arctg} \frac{1}{4} + \operatorname{arctg} \frac{1}{20} + \operatorname{arctg} \frac{1}{1985}$$

на настольном механическом калькуляторе.

В начале 50-х гг. стали появляться первые программы, производящие частично аналитические вычисления. В 1951 г. с помощью компьютера EDSAC 1 было открыто наибольшее известное простое число $180(2^{127} - 1)^2 + 1$ с 79 десятичными цифрами. В 1952 г. математики Эмиль Артин (1898–1962) и Джон фон Нейман проделали большие вычисления, связанные с эллиптическими кривыми, на компьютере MANIAC. В 1953 г. было показано, как алгоритмы в теории групп могут быть реализованы на компьютере.

В 60-х гг. ХХ в. 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 11-я версия – 2016 г. [33].

Применение Mathematica позволяет эффективно вычислять математические объекты, что проливает свет на используемые математические понятия. Причем использование Mathematica не требует глубоких знаний программирования.

Пример 20. В § 1, пример 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 $n = 1, 2, \dots, 6$ – это числа 1, 2, 4, 8, 16, 31. Mathematica может определить закономерность этой последовательности:

```
FindSequenceFunction[{1, 2, 4, 8, 16, 31}, n]
```

$$\frac{1}{24}(24 - 18n + 23n^2 - 6n^3 + n^4).$$

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 [92, 93] и И. Лакатос⁹⁵ [71], убежденные сторонники эвристических методов и квазиэмпирической природы математики.

⁹⁵ Имре Лакатос (1922–1974) – английский философ венгерского происхождения.

Экспериментальной математике посвящены книги [3, 5]. Методы экспериментальной математики в естественно-научных дисциплинах, в первую очередь в физике, применяются и обосновываются в книге Стивена Вольфрама «Новый вид науки» [34].

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 эффективно, 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 является неразрешимым, т.е. для таких теорий не существует алгоритма, который нашел бы доказательство для теоремы. Что может компьютер – так это постепенно, в результате процесса вычисления порождать все новые утверждения, выводимые в данной формальной системе, и этот процесс потенциально никогда не заканчивается. Так как мы не можем заранее знать, встретится ли 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 то, как это сделать, представляет 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 возможным всерьез надеяться на создание систем, которые действительно могли бы помочь работе математика при построении и проверке математических доказательств, т.е. фактически взять на себя часть его интеллектуальной работы. На данный момент эта область очень быстро развивается, и существует более десятка различных систем, предназначенных для автоматического и полуавтоматического, т.е. интерактивного, доказательства теорем. Для этих систем появилось специфическое название «theorem prover» (система поиска вывода, «прувер») [31].

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 21. Теорема Жордана⁹⁶ о кривой: если J – простая замкнутая кривая в \mathbf{R}^2 , то $\mathbf{R}^2 \setminus J$ имеет две компоненты («внутренняя» и «внешняя») с J в качестве общей границы [56].

В 2005 г. были независимо созданы два формальных доказательства этой теоремы с помощью пруверов HOL Light и Mizar [12].

Пример 22. Теорема Гёделя о неполноте (см. главу 11). Формализованные доказательства этой теоремы были созданы в 1986 г. с помощью системы Nqthm [23] и в 2003 г. с помощью системы Coq [18].

Пример 23. Теорема о распределении простых чисел (с историей доказательств этой теоремы можно познакомиться в [53. С. 191–192, 159]). Было формализовано два известных

⁹⁶ Мари Энмон Камиль Жордан (1838–1922) – французский математик. Теорема Жордана знаменита простой формулировкой и чрезвычайно сложным доказательством.

доказательства этой теоремы: в 2005 г. с помощью прувера Isabelle и в 2009 г. с помощью прувера HOL Light [13].

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» – означает, что разные страны на этой карте, если они имеют общий участок границы, должны быть окрашены 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 математик-любитель по фамилии Гутри⁹⁷ в 1852 г. Первые доказательства были предложены А.В. Кемпе⁹⁸ в 1879 г. и П.Г. Тэйт⁹⁹ 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 К. Аппелем¹⁰⁰ и Т.В. Хакеном¹⁰¹ в 1976 г. [2]

Аппель и Хакен свели доказательство этого результата к перебору более 1 476 различных графов и проверке 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 1 000 часов машинного времени.

Как математическое сообщество отнеслось к такому доказательству? Согласно традиционным представлениям, прочно утвердившимся в XX в., 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.

⁹⁷ Francis Guthrie (1831–1899) – математик и ботаник из Южно-Африканского Союза.

⁹⁸ Alfred Bray Kempe (1849–1922) – английский математик.

⁹⁹ Peter Guthrie Tait (1831–1901) – шотландский ученый в области математической физики.

¹⁰⁰ Кеннет Аппель (1932–2013) – американский математик.

¹⁰¹ Вольфганг Хакен (р. 1928) – немецкий и американский математик.

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 касались не компьютерной части, а в человеческой. В доказательстве были найдены недочеты. В начале 1980-х гг. Ульрих Шмидт (Рейнско-Вестфальский технический университет, Ахена) исследовал доказательство Аппеля и Хакена и обнаружил пропуски в математической части доказательства.

В 1989 г. Аппель и Хакен напечатали дополненное и исправленное доказательство теоремы [1]. Все обнаруженные Шмидтом пропуски вариантов были устранины, были исправлены и прочие ошибки, найденные другими математики. К доказательству был приложен полный текст программы.

Вслед за этим известные специалисты по теории графов Н. Робертсон, Д.П. Сандерс, П.Д. Сеймур и Р. 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 [20]. 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 было сделать только с помощью компьютера.

В 2004 г. группа французских ученых под руководством Жоржа Гонтье полностью формализовала с помощью системы интерактивного поиска вывода Соq компьютерную часть на основе доказательства Робертсона и его соавторов. Работа включает как верификацию содежательного сведения, так и компьютерного перебора. Фактически была написана верифицированная в Соq программа перебора (и не нужно было вводить 633 случая от руки) [10].

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, доказательства 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 содержится 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 обычный человек может сделать ошибку. Значит, и вы можете сделать ту же самую ошибку, читая это место и соответственно ее не заметив.

И с этой задачей – 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. Беклемишев¹⁰² 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 гарантиру-

¹⁰² Лев Дмитриевич Беклемишев (р. 1967) – российский математик, доктор физико-математических наук. Работы в области математической логики.

ет ни один прувер. Несмотря на это, в целом компьютерные доказательства намного надежнее 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 удовлетворяют 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 верифицировал как содержательную часть доказательства, сведение к перебору, так и формально доказал 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 [32].

Существуют две интересные книги, переведенные на русский язык, посвященные математическим доказательствам. Первая книга [36] – о лучших доказательствах со времен Евклида до наших дней, и вторая книга [68] – о том, как развивалось с течением времени понятие математического доказательства, и рассмотрен вклад в историю доказательств многих знаменитых математиков, в частности Сринивасы Рамануджана и Пола Эрдёша.

Решая математическую задачу, я не думаю о красоте, –
я думаю только о том, как решить задачу. Но если
найденное некрасиво, значит, оно и неверно.

Бакминстер Фаллер (1885–1983), американский инженер

Задачи

Задача 1. В §3 приведен софизм «Единица – наибольшее число». По каким причинам доказательство софизма неверно?

Задача 2. Докажите с помощью математической индукции, что $n^{n+1} > (n+1)^n$ при целом $n > 2$.

Задача 3. Докажите, что если $x + 1/x$ – целое, то $x^k + 1/x^k$ – целое при любом k . Используйте математическую индукцию.

Задача 4. Докажите с помощью математической индукции неравенство Бернулли: если $x > -1$ и n – натуральное число, то

$$(1+x)^n \geq 1 + nx.$$

Задача 5. В некоторой стране каждые два города соединены напрямую автомобильной либо железной дорогой. Докажите, что из любого города в любой другой можно добраться на автомобиле, или из любого города в любой другой можно добраться на поезде. Используйте математическую индукцию.

Задача 6. Функция Аккермана (см. главу 9). Определим последовательность одноместных функций $F_n: \mathbb{N} \rightarrow \mathbb{N}$, $n \in \mathbb{N}$, следующим образом:

$$\begin{aligned} F_0(x) &= x + 1; \\ F_{n+1}(x) &= F_n(F_n(\dots F_n(1)\dots)), \end{aligned}$$

где справа функция F_n применяется $x + 1$ раз.

Докажите:

- a) $F_1(x + 1) = F_0(F_1(x))$;
- b) $F_{n+1}(x + 1) = F_n(F_{n+1}(x))$;
- c) $F_1(x) = x + 2$;
- d) $F_2(x) = 2x + 3$;
- e) $F_3(x) = 2^{x+3} - 3$;
- f) $F_4(x) = \underbrace{2^2}_{x+3 \text{ раза}} - 3$.

Задача 7. Догадайтесь, в соответствии с каким правилом выбираются члены последовательности $2, 7, -3, 2, -8, -3, -13, -8, -18, \dots$.

Задача 8. Догадайтесь, в соответствии с каким правилом выбираются члены последовательности $1, 5, 12, 22, 35, \dots$.

Задача 9. Где ошибка в следующем доказательстве?

Теорема. Пусть a – любое положительное число. Для положительных целых чисел n имеем $a^{n-1} = 1$.

Доказательство. Если $n = 1$, то $a^{n-1} = a^{1-1} = a^0 = 1$. Применяя метод индукции и предполагая, что теорема верна для $1, 2, \dots, n$, имеем

$$a^{(n+1)-1} = a^n = \frac{a^{n-1} \times a^{n-1}}{a^{n-2}} = \frac{1 \times 1}{1} = 1,$$

следовательно, теорема верна также и для $n+1$.

Задача 10. Где ошибка в следующем доказательстве?

Мы утверждаем, что $6n = 0$ для любого $n \in \mathbb{N}$. Очевидно, базис индукции справедлив для $n = 0$.

Возьмем теперь $n > 0$. Пусть $n = a + b$. По индуктивному предположению $6a = 0$ и $6b = 0$. Поэтому $6n = 6(a + b) = 6a + 6b = 0 + 0 = 0$.

Задача 11. Если $x, y \in \{\text{true}, \text{false}\}$, то пусть $x \oplus y$ обозначает операцию «исключающее или» ($x \oplus y$ истинно \Leftrightarrow ровно один из operandов x или y имеет истинное значение). Заметим, что операция «исключающее или» является ассоциативной, т.е. $a \oplus (b \oplus c) = (a \oplus b) \oplus c$. Докажите индукцией по n , что $x_1 \oplus x_2 \oplus x_3 \oplus \dots \oplus x_n$ истинно тогда и только тогда, когда нечетное число operandов $x_1, x_2, x_3, \dots, x_n$ имеют истинное значение.

Задача 12. Определим формулу σ_k рекурсивно следующим образом:

$$\sigma_0 = P \supset Q \text{ и } \sigma_{k+1} = \sigma_k \supset P.$$

Для каких значений k формула σ_k является тавтологией?

Задача 13. Если p – простое число, то \sqrt{p} – иррациональное число. Докажите.

Задача 14. Пусть n – натуральное число, а \sqrt{n} – ненатуральное число, тогда \sqrt{n} – иррациональное число.

Задача 15. Найти натуральные числа x и y , если из четырех утверждений:

- a) $x - y$ делится на 3;
- b) $x + 2y$ – простое число;
- c) $x = 4y - 1$;
- d) $x + 7$ делится на y ,

три истинны, а одно ложно. Найти все решения.

Задача 16. Найдите все такие двузначные числа x , для каждого из которых два из следующих четырех утверждений верны, а два – неверны:

- a) x делится на 5;
- b) x делится на 23;
- c) $x + 7$ есть точный квадрат;
- d) $x - 10$ есть точный квадрат.

Задача 17. Из чашки с кофе в чашку с молоком перелили ложку кофе, затем такую же ложку смеси перелили обратно. Чего больше: молока в чашке с кофе или кофе в чашке с молоком? Исходный объем жидкостей в чашках был одинаковый.

Задача 18. В погребе 8 банок клубничного варенья, 7 малинового и 5 вишневого. Сколько банок можно в темноте вынести из погреба с уверенностью, что там останутся еще хотя бы 4 банки одного сорта варенья и 3 банки другого?

Задача 19. Гениальные математики (математическая индукция). Каждому из двух гениальных математиков сообщили по натуральному числу, причем им известно, что эти числа отличаются на единицу. Они поочередно спрашивают друг друга: «Известно ли тебе мое число?» Докажите, что рано или поздно, кто-то из них ответит «да». Сколько вопросов они зададут друг другу? (Математики предполагаются правдивыми и бессмертными.)

Задача 20. Господин S и господин P . S – первая буква слова «somme» (фр. сумма), P – слова «produit» (фр. произведение).

Выберем два натуральных числа, больших единицы, но меньших ста. Значение их суммы сообщено господину S , значение их произведения – господину P . Господин P звонит по телефону господину S .

P : Я не могу найти эти два числа.

S : Я знаю, что вам это и не удалось бы.

P : Ах, так... Но тогда я их знаю!

S : Ну, тогда и я тоже их знаю!

Найдите эти числа.

Все должно быть изложено так просто,
как только возможно, но не проще.
Альберт Эйнштейн

Глава 8. Неформально о вычислимости

Теория вычислимости, которой посвящены эта глава и две следующих, рассматривает математические вопросы, связанные с понятиями «алгоритм» и «вычислимая функция». По каким причинам изучаются эти понятия?

Во-первых, мы получаем ответ на вопрос, какие задачи могут, и какие не могут решать компьютеры? И ответ не зависит от того, с какими компьютерами мы имеем дело. В точном смысле современные компьютеры математически эквивалентны так называемой «универсальной» машине Тьюринга.

Во-вторых, приходим к теоремам Гёделя о неполноте, возможно, к наиболее философски значимым результатам в истории математики.

Теория вычислимости хотя и является составной частью оснований математики, но, тем не менее, богата многочисленными приложениями в компьютерных науках.

§ 1. Понятие алгоритма и неформальная вычислимость

Под **алгоритмом** понимается способ преобразования представления информации. Слово *algorithm* произошло от имени ал-Хорезми – автора известного арабского учебника по математике¹⁰³. Интуитивно алгоритм – некоторое формальное предписание, выполняя которое, можно получить решение задачи.

Первым примером алгоритма был алгоритм нахождения общей меры длин двух отрезков. Он был описан Евклидом в «Началах» и в современном виде предназначен для нахождения наибольшего общего делителя двух натуральных чисел. Постепенно алгоритмы стали широко использоваться в арифметике, геометрии и алгебре, причем формулировки алгоритмов на естественном языке не вызывали затруднений для их понимания и применения.

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 [95]. Решение некоторых проблем требовало построения алгоритмов. В частности, в 10-й проблеме предлагалось найти универсальный метод для распознавания разрешимости диофантовых уравнений (см. главу 10). Безуспешные поиски алгоритмов решения ряда проблем привели к мысли, что таких алгоритмов не существует. Но для получения математического доказательства невозможности алгоритмизации решения требуется формализация понятия «алгоритм».

В 20-е гг. XX в. лидеры интуиционизма Лейтзен Брауэр и Герман Вейль¹⁰⁴ четко сформулировали роль алгоритмов в конструктивной математике. Они писали в своих работах, что конструктивное доказательство существования объекта с заданными свойствами дает процедуру (алгоритм) построения такого объекта, в отличие от неконструктивного доказательства «чистого существования».

Одним из источников возникновения теории вычислимости была Гётtingенская программа Гильberta. Гильберт надеялся получить «эффективную» или «механическую» процедуру для проверки непротиворечивости любых формальных аксиоматических систем. В середине 30-х гг. XX в. четверо математиков (Алонзо Чёрч, Стивен Клини¹⁰⁵, Эмиль Пост и

¹⁰³ В сочинении «Об индийском числе» ал-Хорезми Мухамед ибн Муса (ок. 783–850) изложил позиционную систему. Латинский перевод этого труда, сделанный в середине XII в., начинался словами: «Dixit Algoritmi» (сказал ал-Хорезми) [37. С. 10].

¹⁰⁴ Герман Клаус Гugo Вейль (1885–1955) – немецкий математик и физик-теоретик.

¹⁰⁵ Стивен Коул Клини (1909–1994) – американский математик и логик.

Алан Тьюринг) независимо друг от друга предложили точные определения эффективной процедуры (в современной терминологии – алгоритма). Хотя эти определения очень отличались друг от друга, впоследствии было доказано, что все они эквивалентны.

Если мы описываем алгоритм решения задачи на интуитивном уровне, то, как правило, все математики соглашаются, что используется именно алгоритм. Современное распространение компьютеров и информатики способствует этому. В данной главе мы рассмотрим понятия *перечислимости* и *разрешимости* и докажем те результаты, для которых достаточно интуитивного понимания алгоритма.

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 элементарным и локальным.

- *Ввод.* Алгоритм имеет некоторое (быть может, равное нулю) число входных данных, т.е. величин, заданных ему до начала работы.

- *Выход.* 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.

Примеры «почти» алгоритмов: медицинский и кулинарный рецепты. Кстати, почему такие рецепты во многих случаях нельзя рассматривать как алгоритмы?

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 \mathbb{N} обозначает множество натуральных чисел $\{0, 1, 2, \dots\}$. Объекты, которые мы будем рассматривать, будут функциями с областью определения $D_f \subseteq \mathbb{N}^k$ (k – целое положительное число) и с областью значений $R_f \subseteq \mathbb{N}$. Такие функции будем называть ***k*-местными частичными**. Слово «частичная» должно напомнить о том, что функция определена на подмножестве \mathbb{N}^k (конечно, в частном случае может быть $D_f = \mathbb{N}^k$, тогда функция называется **всюду определенной**).

Вычислимые функции

Назовем *k*-местную функцию $f: \mathbb{N}^k \rightarrow \mathbb{N}$ **вычислимой**, если существует алгоритм A , ее вычисляющий, т.е. такой алгоритм A , что:

1. Если на вход алгоритма A поступил вектор $x = \langle x_1, x_2, \dots, x_k \rangle$ из D_f , то вычисление должно закончиться после конечного числа шагов и выдать $f(x)$.

2. Если на вход алгоритма A поступил вектор 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 вычислена, в качестве A надо взять программу, которая всегда зацикливается.

2. Можно было бы изменить определение, сказав так: «если $f(x)$ не определено, то либо алгоритм A не останавливается, либо останавливается, но ничего не печатает на выходе». На самом деле от этого ничего бы не изменилось (вместо того чтобы останавливаться, ничего не напечатав, алгоритм может зацикливался).

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 x из области определения.

§ 2. Перечислимые и разрешимые множества

Определим мощность множества k -местных частичных вычислимых функций $f: \mathbb{N}^k \rightarrow \mathbb{N}$. Значения любой такой функции определяются некоторым алгоритмом, запись которого на любом универсальном языке программирования есть программа – конечная последовательность символов в некотором конечном алфавите A :

$$P = a_1 a_2 \dots a_m, \text{ все } a_i \in A. \quad (1)$$

Множество всех таких программ счетно (см. главу 3, пример 21(4)). Остановимся только на частичных вычислимых функциях одного аргумента. Их счетное число и запись программы вычислений в виде (1) позволяют все вычислимые функции перенумеровать:

$$f_1(n), \dots, f_m(n), \dots. \quad (2)$$

Можно использовать лексикографический порядок: сначала перечисляются все программы из одного символа, потом из двух, потом из трех и т.д.

Таким образом, вычислимая функция – это множество эквивалентных алгоритмов, дающих на любом входе n один и тот же результат – определенный или неопределенный. В нумерации (2) каждая функция имеет бесконечное число своих представителей (номеров).

Что касается существования невычислимых функций, то это ясно из того, что различных функций $f(n)$ имеется континuum¹⁰⁶, а вычислимых – только счетное число.

Конкретно указать невычислимую функцию тоже просто. Воспользуемся «диагональной конструкцией» Кантора, используемой им при доказательстве несчетности множества бесконечных последовательностей нулей и единиц. Очевидно, функция

$$h(n) = \begin{cases} f_n(n) + 1, & \text{если значение } f_n(n) \text{ определено,} \\ 0, & \text{если значение } f_n(n) \text{ не определено} \end{cases}$$

невычислена. Для доказательства предположим противное, т.е. $h(p) = f_p(p)$ при некотором p . Но этого не может быть, так как $h(p) \neq f_p(p)$, если значение $f_p(p)$ определено, и $h(p)$ определено, если $f_p(p)$ не определено.

¹⁰⁶ Если функции принимают только значения $0, 1, \dots, 9$, то каждой функции f соответствует вещественное число $0.f(1)f(2)\dots \in [0, 1]$.

Множество натуральных чисел называется **перечислимым**, если оно перечисляется некоторым алгоритмом, т.е. если существует алгоритм, который печатает (в произвольном порядке и с произвольными промежутками времени) все элементы этого множества и только их.

Такой алгоритм не имеет входа; напечатав несколько чисел, он может надолго задуматься и следующее число напечатать после большого перерыва (а может вообще больше никогда ничего не напечатать, тогда множество будет конечным).

Теорема 1. Следующие определения эквивалентны:

1. Множество перечислимо, если оно перечисляется некоторым алгоритмом.
2. Множество перечислимо, если оно есть область определения вычислимой функции.
3. Множество перечислимо, если оно есть область значений вычислимой функции.
4. Множество X перечислимо, если его **полухарактеристическая функция**

$$\varphi(n) = \begin{cases} 0, & \text{если } n \in X, \\ \text{не определено}, & \text{если } n \notin X \end{cases}$$

вычислима.

Доказательство. Чтобы доказать эквивалентность этих определений, воспользуемся возможностью пошагового исполнения алгоритма.

(1) \Rightarrow (4) \Rightarrow (2). Пусть X перечисляется некоторым алгоритмом A . Покажем, что полухарактеристическая функция $\varphi(n)$ множества X вычислима. В самом деле, алгоритм ее вычисления таков: получив на вход число n , пошагово выполнять алгоритм A , ожидая, пока он напечатает число n . Как только он это сделает, выдать на выход 0 и закончить работу. Поэтому $\varphi(n)$ вычислима. Но, очевидно, (4) \Rightarrow (2), так как X – область определения вычислимой функции.

(2) \Rightarrow (1). Пусть X есть область определения (вычислимой) функции f , вычисляемой некоторым алгоритмом B . Тогда X перечисляется следующим алгоритмом A : параллельно запускать B на входах 0, 1, 2, ..., делая все больше шагов работы алгоритма B (сначала один шаг работы на входах 0 и 1; потом по два шага работы на входах 0, 1, 2, потом по три на входах 0, 1, 2, 3 и т.д.). Все аргументы, на которых алгоритм B заканчивает работу, печатать по мере обнаружения.

(1) \Rightarrow (3). Если X – область значений $f(n)$, то как порождать его элементы? Процедура «зависнет» на первом же n , при котором значение $f(n)$ не определено. Пусть $P(n, m)$ обозначает реализацию m шагов работы программы по вычислению значения $f(n)$. Пары чисел (n, m) упорядочиваются стандартным образом (рис. 1; нумеруются вдоль ломаной начиная с (1, 1)).

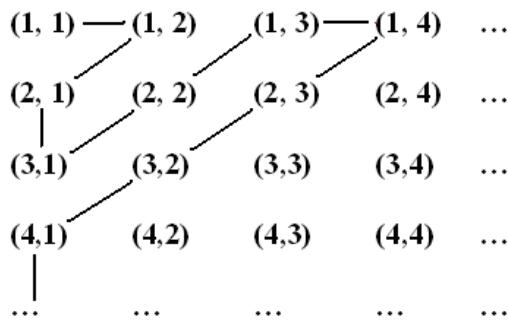


Рис. 1. Порядок выполнения алгоритма

После этого программе дается возможность последовательно работать по m шагов, вычисляя $f(n)$, в избранном порядке. Понятно, все значения $f(n)$ будут рано или поздно перечислены.

(3) \Rightarrow (2). Осталось еще убедиться, что всякое перечислимое множество есть область определения вычислимой функции. Это можно сделать, например, так: пусть X есть область

значений вычислимой функции, вычисляемой некоторым алгоритмом A . Тогда X есть область определения функции

$$g(x) = \begin{cases} x, & \text{если } A \text{ заканчивает свою работу на } x, \\ & \text{не определено в противном случае.} \end{cases}$$

Вычисляющий эту функцию алгоритм действует так же, как и A , но только вместо результата работы алгоритма A выдает копию входа. ■

Теорема 2. Пересечение и объединение перечислимых множеств перечислимы.

Доказательство. Если X и Y перечисляются алгоритмами A и B , то их объединение перечисляется алгоритмом, который параллельно выполняет по шагам A и B и печатает все, что печатают A и B . С пересечением немного сложнее: результаты работы A и B надо накапливать и сверять друг с другом, что появится общего – печатать. ■

Позже увидим, что существует перечислимое множество с неперечислимым дополнением (СМ. следствие из теоремы 13).

Множество натуральных чисел X называется **разрешимым**, если существует алгоритм, который по любому натуральному n определяет, принадлежит ли оно множеству X .

Другими словами, X разрешимо, если его **характеристическая функция**

$$\chi_X(n) = \begin{cases} 1, & \text{если } n \in X, \\ 0, & \text{если } n \notin X \end{cases}$$

вычислима.

Аналогично определяют разрешимость множеств пар натуральных чисел, множеств рациональных чисел и т.п. Очевидно, любое конечное множество разрешимо.

Теорема 3. Свойства разрешимых множеств:

1. Если $A \subseteq \mathbb{N}$ и $B \subseteq \mathbb{N}$ разрешимы, то $A \cap B$ разрешимо.
2. Если $A \subseteq \mathbb{N}$ и $B \subseteq \mathbb{N}$ разрешимы, то $A \cup B$ разрешимо.
3. Если $A \subseteq \mathbb{N}$ разрешимо, то $\mathbb{N} \setminus A$ разрешимо.

Доказательство. Характеристические функции множеств $A \cap B$, $A \cup B$, $\mathbb{N} \setminus A$ вычислимым образом выражаются через характеристические функции множеств A и B :

$$\begin{aligned} \chi_{A \cap B} &= \chi_A \cdot \chi_B, \\ \chi_{A \cup B} &= \chi_A + \chi_B - \chi_A \cdot \chi_B, \\ \chi_{\mathbb{N} \setminus A} &= 1 - \chi_A. \quad \blacksquare \end{aligned}$$

Замечание 1. Теорема 3 показывает, что использование множеств в математике и в практике программирования существенно различается: операции с множествами, которые математик воспринимает как элементарные, для программиста элементарными не являются и требуют алгоритмической реализации.

Теорема 4 (Пост). Всякое разрешимое множество натуральных чисел перечислимо. Если множество A и его дополнение $\mathbb{N} \setminus A$ перечислимы, то A разрешимо.

Доказательство. Если принадлежность числа к множеству A можно проверить некоторым алгоритмом, то A и его дополнение перечислимы: надо по очереди проверять принадлежность чисел $0, 1, 2, \dots$ и печатать те из них, которые принадлежат A (или те, которые не принадлежат A).

В другую сторону: если у нас есть алгоритм, перечисляющий A , а также другой алгоритм, перечисляющий дополнение к A , то для выяснения принадлежности заданного числа n к A надо запустить оба эти алгоритма и ждать, пока один из них напечатает n (мы знаем, что рано или поздно ровно один из них это сделает). Посмотрев, какой алгоритм это сделал, мы узнаем, лежит ли n в A . ■

Теорема говорит, что разрешимые множества – это перечислимые множества с перечислимыми дополнениями. Напротив, перечислимые множества можно определить через разрешимые.

Теорема 5. Множество P натуральных чисел перечислимо тогда и только тогда, когда оно является проекцией некоторого разрешимого множества Q пар натуральных чисел. **Проекция** получается, если от пар оставить их первые компоненты:

$$x \in P \Leftrightarrow \exists y (\langle x, y \rangle \in Q).$$

Доказательство. Проекция любого перечислимого множества перечислима (перечисляющий алгоритм должен лишь удалять вторые члены пар), так что проекция разрешимого множества тем более перечислима.

Напротив, если P – перечислимое множество, перечисляемое алгоритмом A , то оно есть проекция разрешимого множества Q , состоящего из всех таких пар $\langle x, n \rangle$, что x появляется в течении первых n шагов работы алгоритма A . (Это свойство, очевидно, разрешимо.) ■

Теорема 6. Функция f с натуральными аргументами и значениями вычислима тогда и только тогда, когда ее график

$$F = \{\langle x, y \rangle \mid f(x) \text{ определено и равно } y\}$$

является перечислимым множеством пар натуральных чисел.

Доказательство. Пусть f вычислима. Тогда существует алгоритм, перечисляющий ее область определения, т.е. печатающий все x , на которых f определена (теорема 1). Если теперь для каждого из таких x вычислять еще и значение $f(x)$, получим алгоритм, перечисляющий множество F .

Напротив, если имеется алгоритм, перечисляющий F , то функция f вычисляется таким алгоритмом: имея на входе n , ждем появления в F пары, первый член которой равен n ; как только такая пара появилась, печатаем ее второй член и закончим работу. ■

Уточним понятия образа и прообраза множества для частичной функции f с натуральными аргументами и значениями. **Образ** множества A при f определяется как множество всех чисел $f(n)$, для которых $n \in A$ и $f(n)$ определено. **Прообраз** множества A при f определяется как множество всех тех n , при которых $f(n)$ определено и принадлежит A .

Теорема 7. Прообраз и образ перечислимого множества при вычислимой функции перечислимы.

Доказательство. В самом деле, прообраз перечислимого множества A при вычислимой функции f можно получить так: взять график f , пересечь его с перечислимым множеством $\mathbb{N} \times A$ и спроектировать на первую координату. Рассуждение для образов аналогично, только координаты меняются местами. ■

§ 3. Универсальные функции и неразрешимые множества

Сейчас мы построим пример перечислимого множества, не являющегося разрешимым. При этом будет использоваться так называемая универсальная функция. Говорят, что функция U двух натуральных аргументов является **универсальной** для класса вычислимых функций одного аргумента, если для каждого n функция

$$U_n: x \rightarrow U(n, x)$$

(сечение функции U при фиксированном n) является вычислимой и если все вычислимые функции (одного аргумента) встречаются среди U_n . (Напомним, что ни функция U , ни вычислимые функции одного аргумента не обязаны быть всюду определенными.)

Аналогичное определение можно дать и для других классов функций (одного аргумента): например, функция U двух аргументов будет универсальной для класса всех всюду

определенных вычислимых функций одного аргумента, если ее сечения U_n являются всюду определенными вычислимыми функциями одного аргумента и исчерпывают все такие функции. Очевидно, универсальные функции существуют для любых счетных классов (и только для них).

Ключевую роль в этом разделе играет следующая теорема.

Теорема 8. Существует вычислимая функция двух аргументов, являющаяся универсальной функцией для класса вычислимых функций одного аргумента.

Доказательство. Запишем все программы, вычисляющие функции одного аргумента, в вычислимую последовательность p_0, p_1, \dots (например, в порядке возрастания их длины). Положим $U(i, x)$ равным результату работы i -й программы на входе x . Тогда функция U и будет искомой вычислимой универсальной функцией. Сечение U_i будет вычислимой функцией, вычисляемой программой p_i . Алгоритм, вычисляющий саму функцию U , есть по существу *интерпретатор* для используемого языка программирования (он применяет первый аргумент ко второму, если отождествить программу и ее номер). ■

Мы построили универсальную функцию для класса всех вычислимых функций одного аргумента. Можно ли сделать то же самое для класса всюду определенных вычислимых функций? Оказывается, что нет.

Теорема 9. Не существует вычислимой всюду определенной функции двух аргументов, универсальной для класса всех вычислимых всюду определенных функций одного аргумента.

Доказательство. Пусть U – произвольная вычислимая всюду определенная функция двух аргументов. Рассмотрим диагональную функцию $u(n) = U(n, n)$. Очевидно, на аргументе n функция u совпадает с функцией U_n , а функция $g(n) = u(n) + 1$ отличается от U_n . Таким образом, вычислимая всюду определенная функция $g(n)$ отличается от всех сечений U_n , и потому функция U не является универсальной. ■

Почему это рассуждение не проходит для класса всех вычислимых функций (в том числе частичных)? Дело в том, что значение $g(n) = U(n, n) + 1$ теперь не обязано отличаться от значения $U_n(n) = U(n, n)$, так как оба они могут быть не определены.

Теорема 10. Существует вычислимая функция g (с натуральными аргументами и значениями), от которой никакая вычислимая функция f не может всюду отличаться: для любой вычислимой функции f найдется такое число n , что $f(n) = g(n)$ (последнее равенство понимается в том смысле, что либо оба значения $f(n)$ и $g(n)$ не определены, либо оба определены и равны).

Доказательство. Возьмем диагональную функцию $g(n) = U(n, n)$ (здесь U вычислимая функция двух аргументов, универсальная для класса вычислимых функций одного аргумента, построенная в доказательстве теоремы 8). Любая вычислимая функция f есть U_n при некотором n , и потому $f(n) = U_n(n) = U(n, n) = g(n)$. ■

Теорема 11. Существует вычислимая функция, не имеющая всюду определенного вычислимого продолжения.

Доказательство. Такова, например, функция $h(n) = g(n) + 1$, где g – функция из теоремы 10. Считаем, что $h(n)$ неопределенно, если $g(n)$ не определено. Функция h вычислена очевидным образом. Но если бы h имела всюду определенное вычислимое продолжение h' , то h' всюду отличалась бы от функции g , что противоречит теореме 10. В самом деле, h' отличается от g в тех местах, где функция g определена – функция h' на единицу больше g ; там же, где $g(n)$ не определено, $h'(n)$ определено и, следовательно, отличается также от g . ■

Теорема 12. Существует вычислимая функция, принимающая только значения 0 и 1 и не имеющая всюду определенного вычислимого продолжения.

Доказательство. Вместо функции $h(x) = g(x) + 1$ можно рассмотреть функцию

$$p(x) = \begin{cases} 1, & \text{если } g(x) = 0, \\ 0, & \text{если } g(x) > 0, \\ \text{не определено}, & \text{если } g(x) \text{ не определено.} \end{cases}$$

Тогда любое всюду определенное продолжение функции p будет по-прежнему отличаться от g всюду и потому не будет вычислимым. ■

Этот результат можно перевести на язык перечислимых множеств. Говорят, что два не-пересекающихся множества X и Y **отделяются** множеством C , если множество C содержит одно из них и не пересекается с другим.

Теорема 13. Существуют два непересекающихся перечислимых множества X и Y , которые не отделяются никаким разрешимым множеством.

Доказательство. В самом деле, пусть p – вычислимая функция, принимающая только значения 0 и 1 и не имеющая всюду определенного вычислимого продолжения. Пусть $X = \{x \mid p(x) = 1\}$ и $Y = \{x \mid p(x) = 0\}$. Легко видеть, что множества X и Y перечисlimы. Пусть они отделяются разрешимым множеством C ; будем считать, что C содержит X и не пересекается с Y (если, наоборот, перейдем к дополнению). Тогда характеристическая функция множества C (равная 1 внутри C и 0 вне него) продолжает p . ■

Следствие. Существует перечислимое неразрешимое множество. (Переформулировка: существует перечислимое множество с неперечислимым дополнением.)

Для доказательства достаточно заметить, что если два множества не отделимы разрешимыми множествами, то ни одно из них не разрешимо.

Теорема 14 (независимое доказательство от теоремы 13). Существует перечислимое неразрешимое множество.

Доказательство. Рассмотрим вычислимую функцию $f(x)$, не имеющую всюду определенного вычислимого продолжения. Ее область определения F будет искомым множеством. В самом деле, F перечислимо (как область определения вычислимой функции). Если бы F было разрешимо, то функция

$$g(x) = \begin{cases} f(x), & \text{если } x \in F, \\ 0, & \text{если } x \notin F, \end{cases}$$

была бы вычислимым всюду определенным продолжением функции f (при вычислении $g(x)$ мы сначала проверяем, лежит ли x в F , если лежит, то вычисляем $f(x)$). ■

Замечание 2. Введенные понятия и полученные результаты § 2 и 3 данной главы легко переносятся на многомерный случай, когда речь идет о вычислимых функциях нескольких натуральных переменных и о перечислимых и разрешимых множествах в \mathbb{N}^k (см.: [61]).

Замечание 3. Теория вычислимости в настоящее время достаточно обширная. Мы ограничились в изложении только основными понятиями и некоторыми результатами, необходимыми для рассмотрения теоремы Матиясевича (глава 10) и теоремы Геделя о неполноте (глава 11).

Можно объясняться с теми, кто говорит на другом языке, но не с теми, кто в те же слова вкладывает совсем другой смысл.

Жан Ростан (1894–1977),
французский биолог

Глава 9. Формализации вычислимости

Интуитивного понимания алгоритма становится недостаточно для получения отрицательных результатов: в таких случаях надо доказывать отсутствие любых алгоритмов. Поэтому необходимы формальные определения понятий алгоритма и вычислимой функции, которые позволяют изучать алгоритмы и вычислимые функции как математические объекты.

При формализации алгоритма наибольшую трудность вызывает требование элементарности шагов в неформальном определении алгоритма. Что подразумевать под элементарными действиями? Не исключим ли мы при формализации некоторые виды алгоритмов? Но математики – основоположники теории алгоритмов – несмотря на различные подходы к «элементарности», успешно справились с этой проблемой.

Мы приведем три формализации вычислимости, созданные приблизительно в одно время: частично-рекурсивные функции; машины Тьюринга; ламбда-исчисление. Первые две формализации описываются очень кратко, поскольку наша цель – дать начальное представление о частично-рекурсивных функциях и машинах Тьюринга. В дальнейшем они рассматриваться не будут. Интересующийся этими вопросами читатель может обратиться к книгам [47, 83]. Мы же уделим особое внимание ламбда-исчислению.

§ 1. Частично-рекурсивные функции

Определения

Этот подход к формализации понятия алгоритма принадлежит Курту Гёделю и Стивену Клини (1936).

Основная идея состояла в том, чтобы получить все вычислимые функции из существенно ограниченного множества базисных функций с помощью простейших алгоритмических средств.

Множество **базисных** функций таково ($\mathbf{x} = \langle x_1, \dots, x_k \rangle \in \mathbb{N}^k$):

- постоянная функция $0(\mathbf{x}) = 0$;
- одноместная функция следования $s(x) = x + 1$;
- функции проекции pr_i , $1 \leq i \leq k$, $pr_i(\mathbf{x}) = x_i$.

Нетривиальные вычислительные функции можно получать с помощью композиции (суперпозиции) уже имеющихся функций. Этот способ явно алгоритмический.

• **Оператор суперпозиции.** Говорят, что k -местная функция $f(\mathbf{x})$ получена с помощью суперпозиции из m -местной функции $\phi(y_1, y_2, \dots, y_m)$ и k -местных функций $g_1(\mathbf{x}), g_2(\mathbf{x}), \dots, g_m(\mathbf{x})$, если $f(\mathbf{x}) = \phi(g_1(\mathbf{x}), g_2(\mathbf{x}), \dots, g_m(\mathbf{x}))$.

В общем случае, функции ϕ и g_1, g_2, \dots, g_m являются частично определенными. Поэтому если какая-то из функций $g_i(\mathbf{x})$ не определена для \mathbf{x} или функция ϕ не определена для соответствующих y_1, y_2, \dots, y_m , то и функция $f(\mathbf{x})$ не определена для данного значения \mathbf{x} .

Второй (несколько более сложный) способ действует так.

• **Примитивная рекурсия.** При $n \geq 0$ из n -местной функции f и $(n+2)$ -местной функции g строится $(n+1)$ -местная функция h по следующей схеме:

$$\begin{aligned} h(0, \mathbf{x}) &= f(\mathbf{x}), \\ h(y+1, \mathbf{x}) &= g(y, \mathbf{x}, h(y, \mathbf{x})). \end{aligned}$$

При $n = 0$ получаем (a – константа):

$$\begin{aligned} h(0) &= a, \\ h(y+1) &= g(y, h(y)). \end{aligned}$$

Как и в предыдущем случае, значение функции h будет не определено, если хотя бы одно из промежуточных значений не будет вычислено.

Два упомянутых способа позволяют задать только всюду определенные функции. Частично-определенные функции порождаются с помощью третьего гёделева механизма.

• **Оператор минимизации.** Эта операция ставит в соответствие частичной функции $f: \mathbb{N}^{k+1} \rightarrow \mathbb{N}$ частичную функцию $h: \mathbb{N}^k \rightarrow \mathbb{N}$, которая определяется так ($\mathbf{x} = \langle x_1, \dots, x_k \rangle$): область определения $D_h = \{\mathbf{x} \mid \text{существует } x_{k+1} \geq 0, f(\mathbf{x}, x_{k+1}) = 0 \text{ и } \langle \mathbf{x}, y \rangle \in D_f \text{ для всех } y \leq x_{k+1}\}$; $h(\mathbf{x}) = \text{наименьшее значение } y, \text{ при котором } f(\mathbf{x}, y) = 0$.

Оператор минимизации обозначается так: $h(\mathbf{x}) = \mu y [f(\mathbf{x}, y) = 0]$.

Очевидно, что даже если f всюду определено, но нигде не обращается в 0, то $\mu y [f(\mathbf{x}, y) = 0]$ нигде не определено. Естественный путь вычисления $h(\mathbf{x})$ состоит в подсчете значения $f(\mathbf{x}, y)$ последовательно для $y = 0, 1, 2, \dots$ до тех пор, пока не найдется y , обращающее $f(\mathbf{x}, y)$ в 0. Этот алгоритм не остановится, если $f(\mathbf{x}, y)$ 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 $f(\mathbf{x}, y) = 0$, требуется для обеспечения однозначности функции h . Область определения функции h , на первый взгляд, представляется искусственно суженной: если, скажем, $f(\mathbf{x}, 1) = 0$, а $f(\mathbf{x}, 0)$ не определено, мы считаем функцию $h(\mathbf{x})$ 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 [76. 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.

Примеры рекурсивности

Рассмотрим примеры частично-рекурсивных функций. Много других примеров можно найти в [76, 83].

- Сложение двух чисел:

$$\text{sum}: \langle y, x \rangle \rightarrow x + y.$$

Эта функция является общерекурсивной в силу примитивной рекурсии

$$\begin{aligned} \text{sum}(0, x) &= \text{pr}_1(x) = x, \\ \text{sum}(y+1, x) &= s(\text{sum}(y, x)) = \text{sum}(y, x) + 1. \end{aligned}$$

Считая известным частично-рекурсивность функции sum , легко убедиться с помощью примитивной рекурсии и композиции в частично-рекурсивности функции

$$\langle x_1, x_2, \dots, x_n \rangle \rightarrow x_1 + x_2 + \dots + x_n.$$

- Умножение двух чисел:

$$prod: \langle y, x \rangle \rightarrow x \cdot y.$$

Используем примитивную рекурсию:

$$\begin{aligned} prod(0, x) &= 0(x) = 0, \\ prod(y + 1, x) &= sum(prod(y, x), x). \end{aligned}$$

Считая известным частично-рекурсивность функции $prod$, легко убедиться с помощью примитивной рекурсии и композиции в частично-рекурсивности функции

$$\langle x_1, x_2, \dots, x_n \rangle \rightarrow x_1 \cdot x_2 \cdot \dots \cdot x_n.$$

- Возведение в степень

$$power: \langle y, x \rangle \rightarrow x^y.$$

Используем примитивную рекурсию:

$$\begin{aligned} power(0, x) &= s(0(x)) = 1, \\ power(y + 1, x) &= prod(power(y, x), x). \end{aligned}$$

- Усеченное вычитание 1:

$$\begin{aligned} \delta(x) &= x - 1, \text{ если } x > 0, \\ \delta(0) &= 0. \end{aligned}$$

Эта функция примитивно-рекурсивна; действительно,

$$\begin{aligned} \delta(0) &= 0 = 0(x), \\ \delta(y + 1) &= y = pr_2(\langle x, y \rangle). \end{aligned}$$

- Усеченная разность:

$$\begin{aligned} x \div y &= x - y, \text{ если } x \geq y, \\ x \div y &= 0, \text{ если } x < y. \end{aligned}$$

Эта функция примитивно-рекурсивна, действительно,

$$\begin{aligned} x \div 0 &= x, \\ x \div (y + 1) &= \delta(x \div y). \end{aligned}$$

- Модуль разности:

$$\begin{aligned} |x - y| &= x - y, \text{ если } x \geq y, \\ |x - y| &= y - x, \text{ если } x < y. \end{aligned}$$

Эта функция примитивно-рекурсивна в силу суперпозиции

$$|x - y| = (x \div y) + (y \div x).$$

- Факториал.

Действительно,

$$\begin{aligned} 0! &= 1, \\ (y + 1)! &= prod(y!, y + 1). \end{aligned}$$

- $\min(x, y)$ – наименьшее из чисел x и y .

В силу суперпозиции $\min(x, y) = x \div (x \div y)$.

- Знак числа (функция сигнум):

$$\begin{aligned} sg(x) &= 0, \text{ если } x = 0, \\ sg(x) &= 1, \text{ если } x > 1. \end{aligned}$$

В силу рекурсии

$$\begin{aligned} sg(0) &= 0, \\ sg(y + 1) &= 1. \end{aligned}$$

- $rm(y, x)$ – остаток от деления y на x , если $x \neq 0$, и y , если $x = 0$.

В силу рекурсии и суперпозиции

$$\begin{aligned} rm(0, x) &= 0, \\ rm(y + 1, x) &= prod(s(rm(y, x)), sg(|x - s(rm(y, x))|)). \end{aligned}$$

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, [83. С. 135–150]).

Используя минимизацию (μ -оператор), можно получать частично-определенные функции из всюду определенных функций. Например, полагая, что $f(x, y)$ есть частично-рекурсивная функция $|x - y^2|$, мы обнаруживаем, что $g(x) = \mu y[f(x, y) = 0]$ – 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 $F_n: \mathbb{N} \rightarrow \mathbb{N}$, $n \in \mathbb{N}$, следующим образом:

$$\begin{aligned} F_0(x) &= x + 1, \\ F_{n+1}(x) &= F_n(F_n(\dots F_n(1)\dots)) \text{ (функция } F_n \text{ применяется } x + 1 \text{ раз).} \end{aligned}$$

Поэтому $F_1(x) = x + 2$, $F_2(x) = 2x + 3$, $F_3(x) = 2^{x+3} - 3$,

$$F_4(x) = \underbrace{2}_{\vdots}^2 - 3 \text{ (башня из } x+3 \text{ двойки) и т.д.}$$

Имеем следующие свойства:

1) для каждого n функция $x \rightarrow F_n(x)$ является примитивно-рекурсивной;

2) $F_n(x) > 0$;

3) $F_n(x + 1) > F_n(x)$;

4) $F_n(x) > x$;

5) $F_{n+1}(x) \geq F_n(x + 1)$;

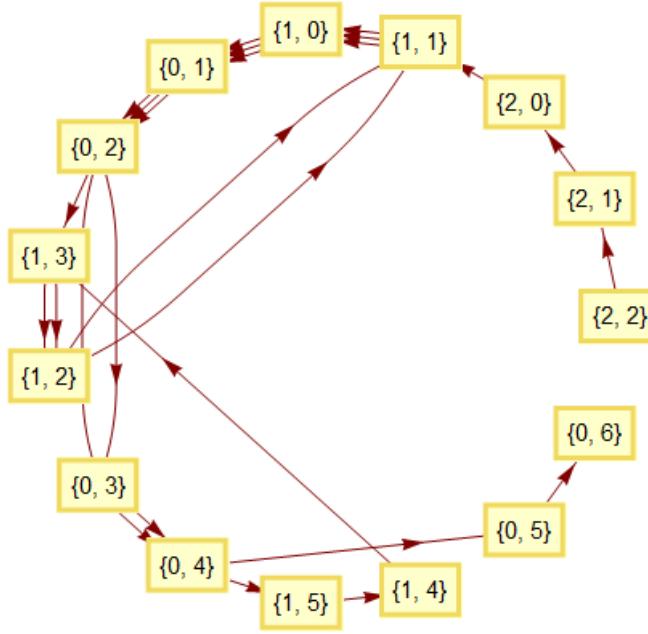
6) для каждой k -местной примитивно-рекурсивной функции $f(x_1, x_2, \dots, x_k)$ существует такое n , что F_n мажорирует f , т.е. $f(x_1, x_2, \dots, x_k) \leq F_n(\max(x_1, x_2, \dots, x_k))$ для всех x_1, x_2, \dots, x_k .

Функция $A(n, x) = F_n(x)$ известна как **функция Аккермана**¹⁰⁷. Ее можно определить и в традиционной записи:

¹⁰⁷ Вильгельм Фридрих Аккерман (1896–1962) – немецкий математик и логик.

$$\begin{aligned}
 f(0, y) &= y + 1, \\
 f(x + 1, 0) &= f(x, 1), \\
 f(x + 1, y + 1) &= f(x, f(x + 1, y)).
 \end{aligned}$$

В отличие от примитивной рекурсии последовательность значений аргументов при вычислении $f(x, y)$ не обнаруживает признаков упорядочивания: прежде чем закончить вычисление функция многократно вызывает себя, причем второй параметр как больше, так и меньше исходного значения (рис.1).



В частности, $f(3, 5) = 1021$, но прежде чем получить это значение, функция вызывает себя 693 964 раза, а различных пар параметров во время вычисления всего 1 539. Можно думать, что при каких-то значениях функция Аккермана уходит в бесконечную рекурсию, но известно [61. С. 53–54], что она всюду определена, не является примитивно-рекурсивной и $f(x, x)$ растет быстрее любой одноместной примитивной функции.

В главе 10 мы приведем доводы в пользу правдоподобности того, что понятие частично-рекурсивной функции есть точный математический эквивалент интуитивной идеи вычислимой функции.

§ 2. Машины Тьюринга

Рассмотрим еще один способ определения вычислимых функций, следуя в изложении [101. С. 12–14]. Формулировка, выраженная в терминах воображаемой вычислительной машины, была дана английским математиком Алланом 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. По сути дела, вычисление значений функций с помощью машин Тьюринга – это абстрагирование ручного вычисления с помощью карандаша и бумаги.

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, \dots, 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 компонента того, что нужно делать. Мы можем формализовать эти идеи, взяв в качестве машины Тьюринга эту функцию перехода.

МашинаТьюринга – это функция M , такая что для некоторого натурального числа n область определения этой функции есть подмножество множества $\{0, 1, \dots, n\} \times \{0, 1\}$, а область значений есть подмножество множества $\{0, 1\} \times \{\text{Л, П}\} \times \{0, 1, \dots, n\}$.

Например, пусть $M(3,1) = <0, \text{Л}, 2>$. 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

$$<n_1> 0 <n_2> 0 \dots 0 <n_k>$$

получено комбинацией k строчек из 1, каждая отделена от другой 0.

Наконец, мы можем определить вычислимость.

Вычислимость по Тьюрингу

Пусть $D_f \subseteq N^k$ – область определения k -местной функции $f: D_f \rightarrow N$. 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

$$<n_1> 0 <n_2> 0 \dots 0 <n_k>,$$

(вся остальная часть ленты пуста), тогда:

- если $f(n_1, n_2, \dots, n_k)$ определено, то M , обязательно остановится, обозревая самый левый символ строки $<f(n_1, n_2, \dots, n_k)>$, при этом часть, находящаяся справа от этой строчки, пустая;
- если $f(n_1, n_2, \dots, n_k)$ 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 1. Построим машину Тьюринга, вычисляющую сумму $n_1 + n_2$. Зададим функцию M следующим образом:

$$\begin{aligned}M(0, 1) &= \langle 1, \Pi, 0 \rangle; \\M(0, 0) &= \langle 1, \Pi, 1 \rangle; \\M(1, 1) &= \langle 1, \Pi, 1 \rangle; \\M(1, 0) &= \langle 0, \Lambda, 2 \rangle; \\M(2, 1) &= \langle 0, \Lambda, 3 \rangle; \\M(3, 1) &= \langle 0, \Lambda, 4 \rangle; \\M(4, 1) &= \langle 1, \Lambda, 4 \rangle; \\M(4, 0) &= \langle 0, \Pi, 5 \rangle.\end{aligned}$$

Посмотрим, как происходит сложение 1+1. В текущей строке символов обозреваемый символ выделен.

Номер инструкции	Текущая строка символов	Комментарий
0	0110110	Прохождение через первое слагаемое
0	0110110	
0	0110110	Заполнение промежутка 1
1	0111110	
1	0111110	Прохождение через второе слагаемое
1	0111110	
2	0111110	Конец второго слагаемого
3	0111110	Стирание 1
3	0111100	Стирание второй 1
4	0111000	Движение назад
4	0111000	
4	0111000	
5	0111000	Остановка

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 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.

Универсальные вычислительные возможности машины Тьюринга установить не трудно. Сначала конструируются машины, выполняющие базовые арифметические и логические операции, затем выясняется возможность работы таких машин в комбинации друг с другом, что порождает более сложные машины. Те в комбинации друг с другом порождают еще более сложные машины. Наконец, мы приходим к идее универсальной машины Тьюринга. Проведем аналогию с современными компьютерами. Операционная система допускает в качестве своих входных данных другую программу. Пусть имеется некоторая машина Тьюринга M , которая получает на входе два натуральных числа. Одно из этих чисел является подходящим кодом машины Тьюринга N , а другое – число x . Машина M служит исполнительной программой, выходом которой будет результат применения N к x . Такую машину можно назвать **универсальной машиной Тьюринга**. О реализации этих идей и построении универсальной машины Тьюринга в самых общих чертах можно прочесть в [101. С. 18–19]. Детальное описание машин Тьюринга было проделано за прошедшее время после их изобретения. Для полноты картины можно воспользоваться книгами [85, 120].

Желтая река течет тысячи миль на север...
Затем поворачивает на восток и течет непрерывно,
Не важно, как она изгибается и поворачивается,
Ее воды выходят из источника на горе Кунь-Лунь.
Железная флейта

§ 3. Ламбда-исчисление

Значение ламбда-исчисления

Ламбда-исчисление представляет класс (частичных) функций (**λ -определенные функции**), который в точности характеризует неформальное понятие эффективной вычислимости. Другими словами, λ -исчисление, наряду с другими подходами, формализует понятие алгоритма. И несмотря на наиболее абстрактный характер по сравнению с другими формализациями вычислимости, в настоящее время ламбда-исчисление является основной формализацией. Одной из причин этого является следующий факт – это единственная формализация, которая, хотя и с некоторыми неудобствами, действительно может быть непосредственно использована для написания программ (т.е. эта формализация наиболее близка к программированию).

Ламбда-исчисление было изобретено Алонзом Чёрчем около 1930 г. Чёрч первоначально строил λ -исчисление как часть общей системы функций, которая должна стать основанием математики. Но из-за найденных парадоксов эта система оказалась противоречивой. Книга Чёрча [7] содержит непротиворечивую подтеорию его первоначальной системы, имеющую дело только с функциональной частью. Эта теория и есть λ -исчисление.

Ламбда-исчисление – это бестиповая теория, рассматривающая функции как *правила*, а не как графики. В противоположность подходу Дирихле (вводившему функции как множество пар, состоящих из аргумента и значения) более старое понятие определяет функцию как процесс перехода от аргумента к значению. С первой точки зрения $x^2 - 4$ и $(x+2)(x-2)$ – разные обозначения одной и той же функции; со второй точки зрения – это разные функции.

Что значит «функция $5x^3 + 2$ »? Если кто-то хочет быть точным, он вводит по этому поводу функциональный символ, например f , и говорит: «функция $f: \mathbb{R} \rightarrow \mathbb{R}$, определенная соотношением $f(x) = 5x^3 + 2$ ». При этом очевидно, что переменную x можно здесь, не меняя смысла, заменить другой переменной y . Ламбда-запись устраняет произвольность в выборе f в качестве функционального символа. Она предлагает вместо f выражение « $\lambda x. 5x^3 + 2$ ».

Кроме того, обычная запись $f(x)$ может обозначать как имя функции f , так и вызов функции с аргументом x . Для более строгого подхода это необходимо различать. В ламбда-обозначениях вызов функции с аргументом x выглядит как $(\lambda x. 5x^3 + 2)x$.

Функции, как правило, рассматриваются в полной общности. Например, мы можем считать, что функции заданы определениями на обычном русском языке и применяются к аргументам, также описанным по-русски. Также мы можем рассматривать функции, заданные программами и применяемые к другим программам. В обоих случаях перед нами *бестиповая структура*, где объекты изучения являются одновременно и функциями, и аргументами. Это отправная точка бестипового λ -исчисления. В частности, функция может применяться к самой себе.

Ламбда-исчисление стало объектом особенно пристального внимания в информатике после того, как выяснилось, что оно представляет собой удобную теоретическую модель современного функционального программирования [112]. Кроме того, большинство конструкций традиционных языков программирования может быть более или менее непосредственно отражено в конструкции ламбда-исчисления.

Функциональные языки являются в основном удобной формой синтаксической записи для конструкций различных вариантов ламбда-исчисления (соответствующие отклонения в

языке от синтаксиса ламбда-выражений называются «синтаксическим сахаром»). Некоторые современные языки (Haskell¹⁰⁸, Clean¹⁰⁹) имеют стопроцентные соответствия своей семантике семантике подразумеваемых конструкций ламбда-исчисления. Причем, λ -выражения используются в качестве промежуточного кода, в который можно транслировать исходную программу.

Функциональные языки «улучшают» нотацию λ -исчисления в прагматическом смысле, но при этом в какой-то мере теряются элегантность и простота последнего.

Изучение и понимание многих сложных ситуаций в программировании, например таких, как автоаппликативность (самоприменимость) или авторепликативность (самовоспроизведение), сильно облегчаются, если уже имеется опыт работы в λ -исчислении, где выделены в чистом виде основные идеи и трудности.

Язык ламбда-исчисления является сейчас одним из важнейших выразительных средств в логике, информатике, математической лингвистике, искусственном интеллекте и когнитивной науке.

Синтаксис и семантика ламбда-исчисления

Ламбда-исчисление есть язык для определения функций. Выражения языка называются **λ -выражениями**, и каждое такое выражение обозначает функцию. Далее мы рассмотрим, как функции могут представлять различные структуры данных: числа, списки и т.д. Для некоторых λ -выражений мы будем использовать имена (или сокращенные обозначения), они будут записываться полужирным шрифтом.

Определение λ -выражений (λ -термов)

Имеется три вида λ -выражений:

- **Переменные:** x, y и т.д.

- **Функциональная аппликация:** если M и N есть произвольные λ -термы, то можно построить новый λ -терм (MN) (обозначающий применение, или **аппликацию**, оператора M к аргументу N). Например, если $(\langle m \rangle, \langle n \rangle)$ обозначает функцию, представляющую пару чисел m и n , и **sum** обозначает функцию сложения в λ -исчислении, то аппликация (**sum** ($\langle m \rangle, \langle n \rangle$)) обозначает $\langle m + n \rangle$ (т.е. ламбда-терм, представляющий число $m + n$).

- **Абстракция:** по любой переменной x и любому λ -терму M можно построить новый λ -терм ($\lambda x. M$) (обозначающий функцию от x , определяемую λ -термом M). Такая конструкция называется **λ -абстракцией**. Например, $\lambda x. \text{sum} (x, \langle 1 \rangle)$ обозначает функцию от x , которая увеличивает аргумент на 1.

Пример 1. а) Например, тождественная функция представляется λ -термом ($\lambda x. x$). Аппликация ($\lambda x. x$) E дает E .

б) Пусть λ -выражения $\langle 0 \rangle, \langle 1 \rangle, \langle 2 \rangle, \dots$ представляют числа 0, 1, 2, ... соответственно и **add** есть λ -выражение, обозначающее функцию, удовлетворяющую правилу

$$((\text{add} \langle m \rangle) \langle n \rangle) = \langle m+n \rangle.$$

Тогда $(\lambda x. ((\text{add} \langle 1 \rangle) x))$ есть λ -выражение, обозначающее функцию, что преобразует $\langle n \rangle$ в $\langle n+1 \rangle$, и $(\lambda x. (\lambda y. ((\text{add} x) y)))$ есть λ -выражение, обозначающее функцию, которая преобразует $\langle m \rangle$ в функцию $(\lambda y. ((\text{add} \langle m \rangle) y))$.

Символ x после λ называется **связанной переменной** абстракции и соответствует понятию формального параметра в традиционной процедуре или функции. Выражение справа от точки называется **телом абстракции**, и, подобно коду традиционной процедуры или функции, оно описывает, что нужно сделать с параметром, поступившим на вход функции. Мы читаем символ λ как «функция от» и точку (.) как «которая возвращает».

¹⁰⁸ Haskell: www.haskell.org

¹⁰⁹ Clean: <http://clean.cs.ru.nl/>

Чтобы уменьшить число применяемых скобок, будем использовать следующие соглашения:

- Операция аппликации левоассоциативна, т.е. $E_1 E_2 \dots E_n$ обозначает $((\dots(E_1 E_2)\dots)E_n)$. Например, $E_1 E_2 E_3$ обозначает $((E_1 E_2) E_3)$.

- $\lambda V. E_1 E_2 \dots E_n$ обозначает $(\lambda V. (E_1 E_2 \dots E_n))$. Область действия λV распространяется направо так далеко, как это возможно, т.е., например, $\lambda x.xu$ обозначает $\lambda x.(xy)$, а не $(\lambda x.x)y$.

- Операция абстракции является правоассоциативной, т.е., например, $\lambda V_1. \lambda V_2. \dots \lambda V_n. E$ обозначает $(\lambda V_1. (\lambda V_2. (\dots (\lambda V_n. E) \dots)))$. Запись $\lambda V_1. \lambda V_2. \dots \lambda V_n. E$ иногда еще более сокращают: $\lambda V_1 V_2 \dots V_n. E$. Так, например, $\lambda x.y.z.E$ обозначает $(\lambda x.(\lambda y.(\lambda z.E)))$.

Ламбда-терм определяется рекурсивно, и его грамматику можно определить в виде следующей формы Бэкуса – Наура:

$$Exp = Var \mid \lambda Var . Exp \mid Exp Exp.$$

В соответствии с этой грамматикой ламбда-термы представляются в виде синтаксических деревьев, а не в виде последовательности символов. Отсюда следует, что соглашения об ассоциативности операции применения функции, эквивалентность выражений вида $\lambda xy.S$ и $\lambda x.\lambda y.S$, неоднозначность в именах переменных происходят только из необходимости представления ламбда-термов в удобном человеку виде и не являются частью формальной системы.

Вычисление ламбда-выражений

Переменная, расположенная не на месте связанной переменной, может быть **связанной** или **свободной**¹¹⁰, что определяется с помощью следующих правил:

1. Переменная x оказывается свободной в выражении x .

2. Все x , имеющиеся в $\lambda x.M$, являются связанными. Если кроме x в $\lambda x.M$ есть переменная y , то последняя будет свободной или связанный в зависимости от того, свободна она или связана в M .

3. Переменная, встречающаяся в термах M или N выражения (MN) , будет связанный или свободной в общем терме в зависимости от того, свободна она или связана в M или N . Свободные (связанные) переменные – это переменные, которые, по крайней мере, один раз появляются в терме в свободном (связанном) виде.

Нам понадобится следующее определение **подстановки** терма в другой терм вместо свободного вхождения переменной. Для любых λ -термов M, N и переменной x через $[N/x]M$ обозначим результат подстановки N вместо каждого свободного вхождения x в M и замены всех λy в M таким образом, чтобы свободные переменные из N не стали связанными в $[N/x]M$. Мы употребляем запись $M \equiv N$ для обозначения того, что термы M и N синтаксически совпадают.

Подстановка:

a) $[N/x]x \equiv N$;

b) $[N/x]y \equiv y$, если переменная y не совпадает с x ;

c) $[N/x](PQ) \equiv ([N/x]P [N/x]Q)$;

d) $[N/x](\lambda x.P) \equiv \lambda x.P$;

e) $[N/x](\lambda y.P) \equiv \lambda y.[N/x]P$, если y не имеет свободных вхождений в N , x имеет свободное вхождение в P ;

f) $[N/x](\lambda y.P) \equiv \lambda z.[N/x]([z/y]P)$, если y имеет свободное вхождение в N , x имеет свободное вхождение в P и z – любая переменная, не имеющая свободных вхождений в N .

Пример 2. Поясним суть определения. Пусть $M \equiv \lambda y.yx$.

Если $N \equiv vx$, то $[(vx)/x](\lambda y.yx) \equiv \lambda y. [(vx)/x](yx)$ (согласно (e)) $\equiv \lambda y. y(vx)$ (согласно (a)).

¹¹⁰ Использования свободных и связанных переменных в λ -исчислении являются частным случаем применения свободных и связанных переменных в именных и высказывательных формах (см. главу 4).

Если $N \equiv yx$, то $[(yx)/x](\lambda y.yx) \equiv \lambda z. [(yx)/x](zx)$ (согласно (f)) $\equiv \lambda z.z(yx)$ (согласно (a)).

Если бы п. f в определении подстановки был опущен, то мы столкнулись бы со следующим нежелательным явлением. Хотя $\lambda v.x$ и $\lambda u.x$ обозначают одну и ту же функцию (константу, значение которой всегда есть x), после подстановки v вместо x они стали бы обозначать разные функции: $[v/x](\lambda y.x) \equiv \lambda y.v$, $[v/x](\lambda v.x) \equiv \lambda v.v$.

Мы рассмотрели, как λ -нотация может быть использована для представления функциональных выражений, и сейчас готовы к тому, чтобы определить правила конверсии λ -исчисления, которые описывают, как вычислять выражение, т.е. как получать конечное значение выражения из его первоначального вида. Правила конверсии, описанные ниже, являются достаточно общими так, что, например, когда они применяются к λ -терму, представляющему арифметическое выражение, то они моделируют вычисление этого выражения.

Правила конверсии

- **α -конверсия.** Любая абстракция вида $\lambda V. E$ может быть конвертирована к терму $\lambda V'. [V'/V]E$. Мы переименовываем связанные переменные так, чтобы избежать коллизии переменных.

- **β -конверсия.** Любая аппликация вида $(\lambda V. E_1) E_2$ конвертируется к терму $[E_2/V]E_1$.

- **η -конверсия.** Любая абстракция вида $\lambda V. (E V)$, в которой V не имеет свободных вхождений в терме E , может быть конвертирована к E .

Если какой-то λ -терм E_1 α -конвертируется к терму E_2 , то это обозначается как $E_1 \rightarrow_\alpha E_2$. Аналогично определяются обозначения \rightarrow_β и \rightarrow_η . Наиболее важным видом конверсии является β -конверсия; она единственная может использоваться для моделирования произвольного вычислительного механизма. α -конверсия применяется для технических преобразований связанных переменных. Использование η -конверсии приводит к естественному свойству, что две функции, дающие один и тот же результат для любых аргументов, оказываются равными.

Обсудим более подробно правила конверсии. Ламбда-выражение, к которому может быть применено правило α -конверсии, называется **α -редексом**. «Редекс» есть аббревиатура для «редуцируемого выражения»¹¹¹. Правило α -конверсии говорит, что любая связанная переменная может быть корректно переименована. Например, $\lambda x.x \rightarrow_\alpha \lambda y.y$.

Ламбда-выражение, к которому может быть применено правило β -конверсии, называется **β -редексом**. Правило β -конверсии подобно вычислению вызова функции в языке программирования: тело E_1 функции $\lambda V. E_1$ вычисляется в окружении (в контексте), в котором «формальный параметр» V заменяется на «фактический параметр» E_2 .

Пример 3.

$$\begin{aligned} & (\lambda x. fx) E \rightarrow_\beta f E, \\ & (\lambda x. (\lambda y. (\text{add } x y))) <3> \rightarrow_\beta \lambda y. \text{add} <3> y, \\ & (\lambda y. \text{add} <3> y) <4> \rightarrow_\beta \text{add} <3> <4>. \end{aligned}$$

Ламбда-выражение, к которому может быть применено правило η -конверсии, называется **η -редексом**.

Пример 4.

$$\begin{aligned} & \lambda x. \text{add } x \rightarrow_\eta \text{add}, \\ & \lambda y. \text{add } x y \rightarrow_\eta \text{add } x. \end{aligned}$$

Но следующая конверсия

$$\lambda x. \text{add } x x \rightarrow_\eta \text{add } x$$

не имеет места, поскольку переменная x свободна в $\text{add } x$.

¹¹¹ Redex – REDucible EXpression.

Ламбда-исчисление можно рассматривать как формальную теорию с равенством. Отношение равенства формализуется с помощью следующих аксиом и правил вывода.

Равенство.

Для любых λ -термов M, N, P и любой переменной x имеем:

1. Если $M \rightarrow_{\beta} N$, то $M = N$.
2. Если $M \rightarrow_{\alpha} N$, то $M = N$.
3. Если $M \rightarrow_{\eta} N$, то $M = N$.
4. $M = M$.
5. Если $M = N$, то $N = M$.
6. Если $M = N$ и $N = P$, то $M = P$.
7. Если $M = N$, то $M P = N P$.
8. Если $M = N$, то $P M = P N$.
9. ξ -правило: если $M = N$, то $\lambda x. M = \lambda x. N$.

Пример 5.

$$\begin{aligned}\lambda z x. ((\lambda y. y) x) &= \lambda z y. y, \text{ поскольку } \lambda z x. ((\lambda y. y) x) \equiv \lambda z. (\lambda x. ((\lambda y. y) x)) \text{ и } \lambda x. (\lambda y. y) x \rightarrow_{\eta} \lambda y. y; \\ (\lambda z x. ((\lambda y. y) x)) ab &= b, \text{ поскольку } \lambda z x. ((\lambda y. y) x) = \lambda z y. y \text{ и } (\lambda z y. y) ab \rightarrow_{\beta} (\lambda y. y) b \text{ и } (\lambda y. y) b \rightarrow_{\beta} b.\end{aligned}$$

В философском смысле два свойства называются **экстенсионально эквивалентными**, если они принадлежат в точности одним и тем же объектам. В математике, например, принят экстенсиональный взгляд на множества, т.е. два множества считаются одинаковыми, если они содержат одни и те же элементы. Аналогично мы говорим, что две функции равны, если они имеют одну и ту же область определения и для любых значений аргумента из этой области определения вычисляют один и тот же результат. Вследствие наличия η -конверсии отношение равенства ламбда-термов экстенсионально.

Лемма (принцип экстенсиональности). Если переменная x не свободна в M и N , то из $M x = N x$ следует $M = N$.

Доказательство. По ξ -правилу из $M x = N x$ следует $\lambda x. M x = \lambda x. N x$, и в силу η -конверсии получаем $M = N$. ■

Более общим понятием, по сравнению с конверсией, является понятие **обобщенной конверсии** (по причинам, которые станут понятными позже, она также называется **одношаговой редукцией**). Терм M обобщенно α -конвертируется (β -конвертируется, η -конвертируется) к терму N , если последний получается из M в результате конверсии какого-то подтерма в M , являющегося α -редексом (β -редексом, η -редексом соответственно). Обобщенная конверсия обозначается так же, как и просто конверсия: $M \rightarrow_{\alpha} N$ (аналогично и для других видов обобщенной конверсии).

Пример 6. Конвертируемые редексы подчеркнуты:

$$\begin{aligned}((\lambda x. (\lambda y. (\text{add } x y))) <3>) <4> &\rightarrow_{\beta} (\lambda y. \text{add} <3> y) <4>, \\ (\lambda y. \text{add} <3> y) <4> &\rightarrow_{\beta} \text{add} <3> <4>.\end{aligned}$$

Отметим, что в первой конверсии сам терм $((\lambda x. (\lambda y. (\text{add } x y))) <3>) <4>$ не является редексом. Мы будем иногда писать последовательность конверсий, подобных двум предыдущим, как

$$((\lambda x. (\lambda y. (\text{add } x y))) <3>) <4> \rightarrow_{\beta} (\lambda y. \text{add} <3> y) <4> \rightarrow_{\beta} \text{add} <3> <4>.$$

Пример 7. Исходное выражение одно и то же, но последовательности конвертируемых редексов различны (используемые редексы подчеркнуты):

$$\begin{aligned}&(\lambda f. \lambda x. f <3> x) (\lambda y. \lambda x. \text{add } x y) <0> \rightarrow_{\beta} \\ &\rightarrow_{\beta} (\lambda x. (\lambda y. \lambda x. \text{add } x y) <3> x) <0> \rightarrow_{\alpha} \\ &\rightarrow_{\alpha} (\lambda z. (\lambda y. \lambda x. \text{add } x y) <3> z) <0>\end{aligned}$$

(выбрали один из двух возможных редексов) \rightarrow_{α}

$$\begin{aligned}
& \rightarrow_{\beta} (\lambda y. \lambda x. \underline{\text{add}} \ x \ y) <3> <0> \rightarrow_{\beta} \\
& \rightarrow_{\beta} (\lambda z. \underline{\text{add}} \ z <3>) <0> \rightarrow_{\beta} \\
& \rightarrow_{\beta} \underline{\text{add}} <0> <3>. \\
& (\underline{\lambda f. \lambda x. f <3>} x) (\lambda y. \lambda x. \underline{\text{add}} \ x \ y) <0> \rightarrow_{\beta} \\
& \rightarrow_{\beta} (\lambda x. (\lambda y. \lambda x. \underline{\text{add}} \ x \ y) <3> x) <0> \\
& (\text{выбрали один из двух возможных редексов}) \rightarrow_{\beta} \\
& \rightarrow_{\beta} (\lambda x. (\lambda x. \underline{\text{add}} \ x <3>) x) <0> \rightarrow_{\alpha} \\
& \rightarrow_{\alpha} (\lambda z. (\lambda x. \underline{\text{add}} \ x <3>) z) <0> \text{ (снова делаем произвольный выбор)} \rightarrow_{\beta} \\
& \rightarrow_{\beta} (\lambda x. \underline{\text{add}} \ x <3>) <0> \rightarrow_{\beta} \\
& \rightarrow_{\beta} \underline{\text{add}} <0> <3>.
\end{aligned}$$

Заметим, что в данном случае независимо от выбора редексов мы пришли к одному результату.

Нормальные формы

Если λ -выражение E' получается из λ -выражения E с помощью последовательности обобщенных конверсий, то естественно считать, что E' получается в результате «вычисления» E , которое более точно выражается через понятие **редукции**.

Определение отношения редукции

Пусть E и E' есть λ -выражения. Говорят, что терм E редуцируется к терму E' (обозначают как $E \rightarrow E'$), если $E \equiv E'$ или существуют выражения E_1, E_2, \dots, E_n , такие что $E \equiv E_1, E_n \equiv E'$, и для каждого i выполнено одно из трех отношений: $E_i \rightarrow_{\alpha} E_{i+1}$, $E_i \rightarrow_{\beta} E_{i+1}$ или $E_i \rightarrow_{\eta} E_{i+1}$.

Пример 7 говорит о том, что $(\lambda f. \lambda x. f <3> x) (\lambda y. \lambda x. \underline{\text{add}} \ x \ y) <0> \rightarrow \underline{\text{add}} <0> <3>$.

Три правила конверсии сохраняют значения λ -выражений, т.е. если терм E редуцируется к терму E' , то имеем $E = E'$. Это следствие нашего определения равенства λ -выражений.

Несмотря на то что термин «редукция» подразумевает уменьшение размера ламбда-терма, в действительности это может быть не так, что показывает следующий пример:

$$\begin{aligned}
(\lambda x. \underline{xxx}) (\lambda x. \underline{xxx}) & \rightarrow (\lambda x. \underline{xxx}) (\lambda x. \underline{xxx}) (\lambda x. \underline{xxx}) \rightarrow \\
& \rightarrow (\lambda x. \underline{xxx}) (\lambda x. \underline{xxx}) (\lambda x. \underline{xxx}) \rightarrow \dots .
\end{aligned}$$

Говорят, что λ -выражение **находится в нормальной форме**, если к нему нельзя применить никакое β - или η -правило конверсии. Другими словами, λ -выражение – в нормальной форме, если оно не содержит β - или η -редексов. Нормальная форма, таким образом, соответствует понятию конца вычислений в традиционном программировании. Отсюда немедленно вытекает наивная схема вычислений:

*while существует хотя бы один β - или η -редекс;
do преобразовывать один из редексов;
end (выражение теперь в нормальной форме).*

Будем говорить, что λ -выражение M имеет **нормальную форму**, если существует выражение N в нормальной форме, причем $M = N$.

Пример 8. Различные варианты конверсии в процессе редукции могут приводить к принципиально различным последствиям (конвертируемые редексы подчеркнуты):

$$\begin{aligned}
& (\lambda x. \lambda y. y) ((\lambda z. z z) (\lambda z. z z)) \rightarrow \\
& \rightarrow (\lambda x. \lambda y. y) ((\lambda z. z z) (\lambda z. z z)) \rightarrow \\
& \rightarrow (\lambda x. \lambda y. y) ((\lambda z. z z) (\lambda z. z z)) \rightarrow \dots \\
& (\text{бесконечный процесс редукции}),
\end{aligned}$$

$$\begin{aligned}
& (\lambda x. \lambda y. y) ((\lambda z. z z) (\lambda z. z z)) \rightarrow \lambda y. y \\
& (\text{редукция закончилась}).
\end{aligned}$$

Порядок редукций (стратегия выбора редексов):

Самым левым редексом называется редекс, первый символ которого текстуально расположен в λ -выражении левее всех остальных редексов (аналогично определяется **самый правый редекс**). Самым внешним редексом называется редекс, который не содержится внутри никакого другого редекса. Самым внутренним редексом называется редекс, не содержащий других редексов.

В контексте функциональных языков в λ -исчислении существуют два важных порядка редукций [112]:

Аппликативный порядок редукций (АПР) предписывает вначале преобразовывать самый левый из самых внутренних редексов.

Нормальный порядок редукций (НПР) предписывает вначале преобразовывать самый левый из самых внешних редексов.

Пример 9. В терме $(\lambda x. \lambda y. y) ((\lambda z. zz) (\lambda z. z z))$ подчеркнут самый левый из самых внутренних редексов – если его последовательно конвертировать, то редукция никогда не закончится. В терме $(\lambda x. \lambda y. y) ((\lambda z. z z) (\lambda z. .zz))$ подчеркнут самый левый из самых внешних редексов – редукция в этом случае заканчивается за один шаг.

Функция $\lambda x. \lambda y. y$ – это классический пример функции, которая отбрасывает свой аргумент. НПР в таких случаях эффективно откладывает вычисление любых редексов внутри выражения аргумента до тех пор, пока это возможно, в расчете на то, что такое вычисление может оказаться ненужным.

В функциональных языках стратегии НПР соответствуют так называемые **ленивые вычисления** (или отложенные вычисления). «Не делай ничего, пока это не потребуется» – механизм вызова по необходимости (все аргументы передаются функции в невычисленном виде и вычисляются только тогда, когда в них возникает необходимость внутри тела функции). Haskell – один из языков с ленивыми вычислениями.

Стратегия АПР приводит к **энергичным вычислениям**. «Делай все, что можешь», другими словами, не надо заботиться о том, пригодится ли в конечном счете полученный результат. Таким образом, реализуется механизм вызова по значению (значение аргумента передается в тело функции). В языке Лисп реализуются, как правило, энергичные вычисления.

Теорема 1 (Чёрча–Россера) [38. С. 78]. Если $E \rightarrow E_1$ и $E \rightarrow E_2$, то существует терм E' такой, что $E_1 \rightarrow E'$ и $E_2 \rightarrow E'$.

Следствие 1. Если $E_1 = E_2$, то существует терм E' такой, что $E_1 \rightarrow E'$ и $E_2 \rightarrow E'$.

Следствие 2. Если выражение E может быть приведено двумя различными способами к двум нормальным формам, то эти нормальные формы совпадают или могут быть получены одна из другой с помощью замены связанных переменных.

Теорема 2 (стандартизации) [Там же. С. 298–303]. Если выражение E имеет нормальную форму, то НПР гарантирует достижение этой нормальной формы (с точностью до замены связанных переменных).

Приведем сводку наших знаний о нормальных формах λ -выражений.

Любое ли выражение имеет нормальную форму? – Нет.

Влияет ли порядок редукции на достижение нормальной формы? – Да. НПР гарантирует достижение нормальной формы выражения, если она существует.

Как соотносятся две нормальные формы, полученные различными β - или η -конверсиями из одного выражения? – Эти нормальные формы совпадают или отличаются с точностью до α -конверсии.

Если два λ -выражения находятся в нормальной форме и не совпадают (даже после α -конверсии), то эти λ -выражения не равны. Это утверждение следует из предыдущих выводов.

Комбинаторы

Теория комбинаторов была развита российским математиком М.Э. Шейнфинкелем¹¹² [22] перед тем, как ламбда-обозначения были введены Чёрчем. Вскоре Х.Б. Карри¹¹³ переоткрыл эту теорию независимо от Шейнфинкеля и Чёрча. Теорию комбинаторов так же, как и λ -исчисление, можно использовать для представления функций. Комбинаторы также обеспечивают хороший промежуточный код для обычных компьютеров: несколько лучших компиляторов для ленивых функциональных языков базируются на комбинаторах [112].

Существует два эквивалентных способа формализации теории комбинаторов:

- внутри λ -исчисления;
- как полностью независимая теория.

Следуя первому подходу, определим **комбинатор** просто как λ -терм, не имеющий свободных переменных. Такой терм также называется **замкнутым** – он имеет фиксированное значение независимо от значения любой переменной.

Следующие комбинаторы имеют традиционное обозначение и часто встречаются в литературе, посвященной λ -исчислению:

$$\begin{aligned} \mathbf{B} &\equiv \lambda xyz. x(yz), \\ \mathbf{C} &\equiv \lambda xyz. xzy, \\ \mathbf{I} &\equiv \lambda x. x, \\ \mathbf{K} &\equiv \lambda xy. x, \\ \mathbf{M} &\equiv \lambda x. xx, \\ \mathbf{N} &\equiv \lambda fghx. f(gx)(hx), \\ \mathbf{S} &\equiv \lambda xyz. xz(yz), \\ \mathbf{W} &\equiv \lambda xy. xyy, \\ \mathbf{Y} &\equiv \lambda f. ((\lambda x. f(xx)) (\lambda x. f(xx))). \end{aligned}$$

Из этих определений, используя β -конверсию, получаем, что для любых термов E_1 , E_2 и E_3 выполнено:

$$\begin{aligned} \mathbf{B} E_1 E_2 E_3 &= E_1 (E_2 E_3), \\ \mathbf{C} E_1 E_2 E_3 &= E_1 E_3 E_2, \\ \mathbf{I} E_1 &= E_1, \\ \mathbf{K} E_1 E_2 &= E_1, \\ \mathbf{M} E_1 &= E_1 E_1, \\ \mathbf{N} E_1 E_2 E_3 E_4 &= E_1 (E_2 E_4) (E_3 E_4), \\ \mathbf{S} E_1 E_2 E_3 &= E_1 E_3 (E_2 E_3), \\ \mathbf{W} E_1 E_2 &= E_1 E_2 E_2. \end{aligned}$$

Понятие базиса в λ -исчислении аналогично соответствующему понятию в линейной алгебре: базис B для векторного пространства W есть конечное множество векторов, замыкание которого относительно операций сложения и скалярного умножения равно W . Ситуация в λ -исчислении похожа: **базис** B для множества термов W есть множество λ -термов (которое не обязано быть конечным), замыкание которого относительно операции аппликации равно W . Следствием этой аналогии понятий являются такие же вопросы для λ -исчисления, какие возникают и в линейной алгебре: «Как представить произвольный λ -терм в данном базисе?» и «Как мал может быть базис для представления всех комбинаторов?»

¹¹² Моисей Эльевич Шейнфинкель (1889–1942) – русский и советский логик и математик.

¹¹³ Хаскелл Брукс Карри (1900–1982) – американский математик и логик. В честь него назван язык программирования Haskell.

Замыкание относительно аппликации

Пусть S – произвольное множество λ -термов. Множество S^+ термов называется **замыканием множества S относительно операции аппликации**, если оно есть наименьшее множество W , удовлетворяющее условиям:

- 1) $S \subseteq W$;
- 2) для любых $M, N \in W$ имеем $(MN) \in W$.

Базис

Множество термов B называется **базисом** для множества термов L , если для любого $M \in L$ существует $N \in B^+$ такой, что $M = N$.

Алгоритм абстракции

Пусть множество термов B есть базис для множества термов L . Алгоритм, который для каждого $M \in L$ выдает соответствующий терм $N \in B^+$, называется **алгоритмом абстракции**.

Теорема 3.

1. Множество $B = \{I, K, B, C, S\} \cup \{\text{переменные}\}$ является базисом для множества Λ всех λ -выражений.

2. Множество $\{K, S\}$ является базисом для множества всех комбинаторов.

Доказательство. Определим алгоритм абстракции как отображение $\text{comb}: \Lambda \rightarrow B^+$ в виде рекурсивных правил:

1. $\text{comb}(E) \stackrel{\text{def}}{=} E$, если $E \in B$.
2. $\text{comb}(E_1 E_2) \stackrel{\text{def}}{=} \text{comb}(E_1) \text{comb}(E_2)$.
3. $\text{comb}(\lambda x . E) \stackrel{\text{def}}{=} \text{abs}(x, \text{comb}(E))$.

Отображение $\text{abs}: \{\text{переменные}\} \times B^+ \rightarrow B^+$ также задается в виде рекурсивных правил ($\text{FreeVars}(E)$ обозначает множество свободных переменных терма E):

1. $\text{abs}(x, x) \stackrel{\text{def}}{=} I$.
2. $\text{abs}(x, E) \stackrel{\text{def}}{=} KE$, если $E \in B \setminus \{x\}$.
3. $\text{abs}(x, E_1 E_2) \stackrel{\text{def}}{=} C \text{abs}(x, E_1) E_2$, если $x \in \text{FreeVars}(E_1)$ и $x \notin \text{FreeVars}(E_2)$.
4. $\text{abs}(x, E_1 E_2) \stackrel{\text{def}}{=} BE_1 \text{abs}(x, E_2)$, если $x \notin \text{FreeVars}(E_1)$ и $x \in \text{FreeVars}(E_2)$.
5. $\text{abs}(x, E_1 E_2) \stackrel{\text{def}}{=} S \text{abs}(x, E_1) \text{abs}(x, E_2)$, если $x \in \text{FreeVars}(E_1) \cap \text{FreeVars}(E_2)$.

Для доказательства утверждения 1 теоремы мы должны доказать, что для любого λ -выражения E имеем равенство

$$\text{comb}(E) = E. \quad (1)$$

Заметим, что из определения отображения abs следует, что для произвольной переменной x и произвольного аппликативного выражения $E \in B^+$ значение отображения $\text{abs}(x, E)$ не содержит переменной x .

Для доказательства (1) нам понадобятся два вспомогательных утверждения. Сначала докажем, что для произвольной переменной x и произвольного аппликативного выражения $E \in B^+$ имеем равенство

$$\text{abs}(x, E)x = E. \quad (2)$$

Кроме того, покажем, что для произвольной переменной x и произвольного аппликативного выражения $E \in B^+$ имеем равенство

$$\text{abs}(x, E) = \lambda x . E. \quad (3)$$

Равенство (2) будем доказывать, используя индукцию по построению терма.

Базис индукции.

Случай 1 для abs . Имеем $\text{abs}(x, x) x \stackrel{\text{def}}{=} \mathbf{I} x = x$.

Случай 2 для abs . Имеем $\text{abs}(x, E) x \stackrel{\text{def}}{=} \mathbf{K} E x = E$.

Индуктивный переход.

Случай 3 для abs :

$\text{abs}(x, E_1 E_2) x \stackrel{\text{def}}{=} \mathbf{C} \text{abs}(x, E_1) E_2 x = \text{abs}(x, E_1) x E_2 = (\text{abs}(x, E_1) x) E_2 = (\text{по индуктивному предположению}) E_1 E_2$.

Случай 4 для abs :

$\text{abs}(x, E_1 E_2) x \stackrel{\text{def}}{=} \mathbf{B} E_1 \text{abs}(x, E_2) x = E_1 (\text{abs}(x, E_2) x) = (\text{по индуктивному предположению}) E_1 E_2$.

Случай 5 для abs :

$\text{abs}(x, E_1 E_2) x \stackrel{\text{def}}{=} \mathbf{S} \text{abs}(x, E_1) \text{abs}(x, E_2) x = \text{abs}(x, E_1) x (\text{abs}(x, E_2) x) = (\text{по индуктивному предположению}) E_1 E_2$. Таким образом, равенство (2) справедливо.

Теперь докажем (3).

Применяя правило ξ к (2), получаем $\lambda x. \text{abs}(x, E) x = \lambda x. E$. С другой стороны, так как $\text{abs}(x, E)$ не имеет вхождений переменной x , то в силу η -конверсии $\lambda x. \text{abs}(x, E) x = \text{abs}(x, E)$. Поэтому имеем $\text{abs}(x, E) = \lambda x. E$.

Доказательство равенства (1) проведем индукцией по построению λ -терма. Базис индукции (случай 1 для comb) справедлив по определению.

Индуктивный переход.

Случай 2 для comb : $\text{comb}(E_1 E_2) \stackrel{\text{def}}{=} \text{comb}(E_1) \text{comb}(E_2) = E_1 E_2$ по индуктивному предположению.

Случай 3 для comb : $\text{comb}(\lambda x. E) \stackrel{\text{def}}{=} \text{abs}(x, \text{comb}(E)) = (\text{по равенству (3)}) \lambda x. \text{comb}(E) = (\text{по индуктивному предположению}) \lambda x. E$.

Утверждение 1 доказано. Заметим, что все связанные переменные в исходном λ -терме при переводе в комбинаторную форму исчезают, а новые переменные появиться не могут, поэтому любой замкнутый терм представляется в виде аппликативного выражения только из комбинаторов $\mathbf{I}, \mathbf{K}, \mathbf{B}, \mathbf{C}, \mathbf{S}$.

Утверждение 2 усиливает последний вывод. Для его справедливости достаточно обнаружить, что комбинаторы $\mathbf{I}, \mathbf{B}, \mathbf{C}$ можно представить в виде некоторых комбинаций только двух комбинаторов \mathbf{K} и \mathbf{S} . Но это действительно так:

$$\begin{aligned} \mathbf{I} &= \mathbf{SKK}, \\ \mathbf{B} &= \mathbf{S(KS)K}, \end{aligned} \tag{4}$$

$$\mathbf{C} = \mathbf{S(BBS)(KK)} = \mathbf{S(S(KS)K(S(KS)K)S)(KK)}.$$

Для доказательства этих равенств воспользуемся экстенсиональностью. Пусть x, y и z – произвольные переменные. Если мы покажем, что:

a) $\mathbf{Ix} = \mathbf{SKKx}$,

b) $\mathbf{Bxyz} = \mathbf{S(KS)Kxyz}$,

c) $\mathbf{Cxyz} = \mathbf{S(S(KS)K(S(KS)K)S)(KK)} xyz$,

то в силу принципа экстенсиональности равенства (4) будут доказаны.

a. Комбинатор \mathbf{I} обладает свойством $\mathbf{Ix} = x$. С другой стороны, $\mathbf{SKKx} = \mathbf{Kx(Kx)}$ (по свойству комбинатора \mathbf{S}) $= x$ (по свойству комбинатора \mathbf{K}).

b. Комбинатор \mathbf{B} обладает свойством $\mathbf{Bxyz} = x(yz)$. С другой стороны, $\mathbf{S(KS)Kxyz} =$

= (правило для S) $KSx (Kx)yz =$
= (правило для K) $S(Kx)yz =$
= (правило для S) $Kxz (yz) =$
= (правило для K) $x(yz).$

с. Комбинатор C обладает свойством $Cxyz = xzy$. С другой стороны,
 $S(S(KS)K(S(KS)K)S)(KK) xyz =$

= $S(BBS)(KK) xyz =$
= (правило для S) $BBSx (KKx)yz =$
= (правило для K) $BBSxKyz =$
= (правило для B) $B(Sx)Kyz =$
= (правило для B) $(Sx)(Ky)z =$
= (правило для S) $xz (Kyz) =$
= (правило для K) $xzy.$

Доказательство теоремы закончено. ■

Пример 10. Трансляции терма $\lambda xy . xyy$ в комбинаторную форму:

$comb(\lambda xy . xyy) \equiv$
 $\equiv comb(\lambda x.(\lambda y . xyy)) =$
 $= abs(x, comb(\lambda y . xyy)) =$
 $= abs(x, abs(y, comb(xyy))) =$
 $= abs(x, abs(y, comb(xy) comb(y))) =$
 $= abs(x, abs(y, (comb(x) comb(y)) comb(y))) =$
 $= abs(x, abs(y, (xy)y)) =$
 $= abs(x, S abs(y, xy) abs(y, y)) =$
 $= abs(x, S (Bx abs(y, y)) abs(y, y)) =$
 $= abs(x, S (BxI) I) \equiv$
 $\equiv abs(x, (S (BxI)) I) =$
 $= C abs(x, S (BxI)) I =$
 $= C (BS abs(x, BxI)) I =$
 $= C (BS (C abs(x, Bx) I)) I =$
 $= C (BS (C (BB abs(x, x)) I)) I =$
 $= C (BS (C (BB I) I)) I.$

При переводе λ -выражений используется отображение abs с пятью правилами. Можно использовать упрощенную версию abs с правилами:

1. $abs(x, x) \stackrel{\text{def}}{=} I.$
2. $abs(x, E) \stackrel{\text{def}}{=} KE$, если $E \in B \setminus \{x\}.$
- 3а. $abs(x, E_1 E_2) \stackrel{\text{def}}{=} S abs(x, E_1) abs(x, E_2).$

В этом случае трансляция приводит сразу только к комбинаторам I , K и S .

Убедимся, что правило 3а заменяет как правило для случая B , так и правило для случая C . Используем экстенсиональность.

Имеем

$$\begin{aligned} S abs(x, E_1) abs(x, E_2) y &= \\ &= abs(x, E_1) y (abs(x, E_2) y) = \\ &= (\lambda x. E_1) y ((\lambda x. E_2) y) \text{ (равенство (3) в теореме).} \end{aligned}$$

Если $x \notin FreeVars(E_1)$, то $(\lambda x. E_1) y ((\lambda x. E_2) y) = E_1((\lambda x. E_2) y).$

Если же $x \notin FreeVars(E_2)$, то $(\lambda x. E_1) y ((\lambda x. E_2) y) = (\lambda x. E_1) y E_2.$

С другой стороны,

$$C abs(x, E_1) E_2 y = C (\lambda x. E_1) E_2 y = (\lambda x. E_1) y E_2 \text{ и}$$

$$\mathbf{B} E_1 \text{abs}(x, E_2) y = \mathbf{B} E_1 (\lambda x. E_2) y = E_1((\lambda x. E_2) y).$$

Чтобы уменьшить длину получаемого комбинатора, при переводе можно воспользоваться двумя дополнительными правилами:

2a. $\text{abs}(x, E) \stackrel{\text{def}}{=} \mathbf{K} E$, если x не содержится в E .

6. $\text{abs}(x, Ex) \stackrel{\text{def}}{=} E$, если x не содержится в E .

Правило 2а есть обобщение правила 2 и доказывается по индукции. Правило 6 следует из равенства (3) и η -конверсии $\lambda x. Ex \rightarrow E$.

До работ Давида Тёрнера комбинаторы рассматривались как факт чистой математики. Д. Тёрнер предложил (см., например, [30]) транслировать λ -выражения в комбинаторы с дальнейшим редуцированием, как практический способ реализации эффективных функциональных языков программирования.

Часть λ -исчисления, оперирующая только с функциями, оказалась весьма полезной. Используя эту теорию, Чёрч предложил формализацию понятия вычислимости с помощью λ -*определенности*. Прежде чем дать последнему понятию точное определение, необходимо как-то представить натуральные числа с помощью λ -термов. Соответствующие комбинаторы для представления натуральных чисел ввел Алонзо Чёрч, и поэтому они называются в его честь.

Введем новое обозначение. Для произвольных термов A, B и натурального $n > 0$ пусть $A^n B$ обозначает n -кратную аппликацию: $A(A(\dots(A B)\dots))$, где A повторяется n раз. Условимся также, что $A^0 B$ обозначает просто B . Таким образом, выражение $A^n B$ определено для любого целого $n \geq 0$. Очевидно, $A^{n+1} B \equiv A(A^n B) \equiv A^n(AB)$.

Предположим, что мы имеем некоторое λ -выражение z , представляющее число 0, и λ -выражение s , представляющее функцию следования $s: n \rightarrow n+1$ на множестве натуральных чисел. Тогда аппликация $(s z)$ представляет число 1, $(s(s z))$ представляет число 2 и т.д. Поэтому n -й нумерал Чёрча определяется с помощью абстракции над n -кратной аппликацией s к z .

Нумералы Чёрча

$$<0> \equiv \lambda s z . z$$

$$<n+1> \equiv \lambda s z . (s \dots (s z) \dots) \text{ (терм } s \text{ повторяется } n + 1 \text{ раз)} = \lambda s z . (s^{n+1} z).$$

Ламбда-определенные функции

Пусть f – частично-определенная k -местная функция ($k \geq 1$), заданная на натуральных числах и принимающая натуральные значения.

Говорят, что функция f **λ -определенна** термом M , когда

- $M < n_1 > < n_2 > \dots < n_k > = < f(n_1, n_2, \dots, n_k) >$, если значение $f(n_1, n_2, \dots, n_k)$ определено;
- $M < n_1 > < n_2 > \dots < n_k >$ не имеет нормальной формы, если $f(n_1, n_2, \dots, n_k)$ не определено.

В следующей главе данное определение будет обосновано.

Задачи

Задача 1. Докажите с помощью математической индукции свойства функции Аккермана (\S 1): $F_1(x) = x + 2$, $F_2(x) = 2x + 3$, $F_3(x) = 2^{x+3} - 3$ и соответствующее соотношение для $F_4(x)$.

Задача 2. Существуют ли примитивно-рекурсивные функции для решения следующих задач? Если да, то привести алгоритм, если – нет, то обосновать.

- a) Определить факториал натурального числа n .
- b) Найти остаток от деления натурального числа m на натуральное n .
- c) Найти n -ю цифру числа π после запятой.
- d) Найти n -е число ряда Фибоначчи.
- e) Найти наименьшее простое число, следующее за n .

- f) Найти n -е по счету совершенное число (натуральное число x является совершенным, если сумма всех его делителей равна $2x$).
- g) Тест на простоту числа n .
- h) Проверка того, является ли число n совершенным (натуральное число n является совершенным, если сумма всех его делителей равна $2n$).
- i) Для данных натуральных чисел a, b, c и n выполнено ли равенство $a^n + b^n = c^n$?
- j) Для данных натуральных чисел a, b, c существует ли такое натуральное число $n > 1$, что выполнено равенство $a^n + b^n = c^n$?
- k) Для данного натурального числа $n > 1$ существуют ли такие натуральные числа a, b, c , что выполнено равенство $a^n + b^n = c^n$?
- l) Являются ли числа n и $m + n$ простыми?
- m) Для данного натурального числа n найдутся ли простые числа, чья разность равна n ?
- n) Пусть дана произвольная формальная теория. Является ли данная последовательность формул в формальной теории доказательством?
- o) Пусть дана произвольная формальная теория. Является ли данная последовательность формул в формальной теории доказательством данной теоремы?
- p) Пусть дана произвольная формальная теория. Является ли данная формула в формальной теории теоремой?
- q) Является ли данная формула в исчислении высказываний выполнимой?
- r) Является ли данная формула в исчислении высказываний противоречием?
- s) Является ли данная формула в исчислении высказываний тавтологией?
- t) Является ли данное натуральное число точным квадратом?
- u) Является ли данное натуральное число целой степенью двойки?
- v) Пусть множество X – конечное множество упорядоченных пар. Является ли множество X отношением эквивалентности?
- w) Пусть множество X – конечное множество упорядоченных пар. Является ли множество X отношением частичного порядка?
- x) Для формальных систем, имеющих только удлиняющие правила, всегда существует разрешающий алгоритм. Реализуется ли этот алгоритм с помощью примитивно рекурсивной функции?
- y) Найти наименьшую пару простых чисел-близнецов, больших данного натурального числа (простые числа называются простыми числами-близнецами, если разность между ними равна 2).
- z) Является ли данная формула исчисления высказываний противоречием?

Задача 3. Найдите нормальную форму для выражения $SK(IK)$.

Задача 4. Найдите нормальную форму для выражения $SKIK$.

Задача 5. Найдите нормальную форму для выражения $K(KKK)$.

Задача 6. Пусть $B \equiv S(KS)K$. Покажите, что для любых термов F, G, X имеем $BFGX \rightarrow F(GX)$.

Задача 7. Пусть $W \equiv SS(KI)$. Покажите, что для любых термов F, X имеем $WFX \rightarrow FXX$.

Задача 8. Показать, что аппликация комбинаторов не ассоциативна. Точнее, существуют такие комбинаторы A, B и C , что $A(BC) \neq (AB)C$.

Задача 9. Докажите, что $(\lambda fgx. fx(gx)) (\lambda xy. x) (\lambda xy. x) = \lambda x. x$.

Задача 10. Пусть $B \equiv \lambda fgx. f(gx)$, $C \equiv \lambda fgx. f(xg)$, $S \equiv \lambda xyz. xz(yz)$. Докажите, что $S (KE_1)E_2 \equiv BE_1E_2$ и $SE_1(KE_2) \equiv CE_1E_2$.

Все, что может быть сказано,
может быть сказано ясно.
Людвиг Витгенштейн (1889–1938),
австрийский философ

Глава 10. Алгоритмически неразрешимые проблемы

Глава содержит больше, чем говорит ее название. Первый параграф посвящен доказательству того, что любая частично-рекурсивная функция является ламбда-определенной. Но этот факт оказывается частным случаем общей теоремы: все три рассмотренные формализации вычислимости оказываются эквивалентны. Об этом говорится в § 1 данной главы. И глава заканчивается рассмотрением ряда алгоритмически неразрешимых проблем.

§ 1. Ламбда-определенные функции

В этом параграфе доказывается, что λ -определенные функции – это в точности частично-рекурсивные функции. Начнем с того, что покажем возможности λ -исчисления для представления данных и функций современного функционального языка программирования¹¹⁴. Идея состоит в представлении данных и функций в виде λ -выражений таким образом, чтобы они обладали требуемыми свойствами.

В конце предыдущей главы были определены комбинаторы – нумералы Чёрча, представляющие натуральные числа. Требуется определение основных арифметических операций: сложение, умножение, тест на ноль и т.д. Также, конечно, необходимы истинностные значения и булевские операции.

Выбор λ -выражений для представления программных объектов достаточно произволен, но все предлагаемые определения согласованы так, что они могут работать в унисон. Поиск подходящих комбинаторов требует некоторого искусства. Впрочем, мы стараемся указать те идеи, которые приводят к предложенным определениям комбинаторов.

Нумералы Чёрча называются также **итераторами**. Из определения следует, что для произвольных термов M и E имеем

$$\begin{aligned} & \langle 0 \rangle M E \rightarrow E, \\ & \langle n+1 \rangle M E \rightarrow M(M(\dots(M E)\dots)), \end{aligned}$$

где M повторяется $n+1$ раз. Таким образом, видим, что итератор $\langle n \rangle$ применяет n раз терм M к терму E . Имеем следующее важное свойство:

$$\langle n \rangle M E \rightarrow M^n E. \quad (1)$$

Используя определение нумералов Чёрча, определим элементарные функции над числами, начиная с функции следования. Пусть x и y – произвольные переменные. Имеем, по определению, $\langle n \rangle x y \rightarrow x^n y$. Применяя x к обеим сторонам, получаем

$$x (\langle n \rangle x y) \rightarrow x (x^n y).$$

Применяя абстракцию с переменными x и y к обеим частям равенства, получаем

$$\lambda x y . x (\langle n \rangle x y) \rightarrow \lambda x y . x (x^n y),$$

что дает $\langle n+1 \rangle = \lambda x y . x (\langle n \rangle x y)$.

Если терм $\langle n \rangle$ заменить переменной n и провести абстракцию относительно этой переменной, то получаем комбинатор, представляющий функцию $\langle n \rangle \rightarrow \langle n+1 \rangle$.

¹¹⁴ В «чистом» функциональном языке, как правило, данные и функции синтаксически не различаются.

Комбинатор $\text{succ} \equiv \lambda nxy . x (n x y)$ представляет функцию следования на нумералах Чёрча. Проверим:

$$\begin{aligned}\text{succ } & <n> \equiv \\ & \equiv (\lambda nxy . x (n x y)) <n> \rightarrow \\ & \rightarrow \lambda xy . x (<n> x y) \rightarrow \\ & \rightarrow (\text{в силу (1)}) \lambda xy . x (x^n y) \equiv \\ & \equiv <n + 1>.\end{aligned}$$

Комбинатор succ равен простой комбинации SB основных комбинаторов. Докажем это, используя экстенсиональность: $\text{SB } nxy = \text{Bx}(nx)y = x(nx) = \text{succ } nxy$.

Применим отношение (1), чтобы определить комбинатор, с помощью которого представляется сложение нумералов Чёрча: терм $<n> \text{ succ}$ обозначает функцию, которая n раз увеличивает свой аргумент на 1. Таким образом,

$$(<a> \text{ succ}) \rightarrow <a + b>. \quad (2)$$

Заменим $<a>$ и $$ на соответствующие переменные a и b и, применяя абстракцию относительно переменных a и b над левой частью (2), получаем комбинатор сложения:

Комбинатор $\text{add} \equiv \lambda ab. a \text{ succ } b$ представляет функцию сложения над нумералами Чёрча.

Проверим:

$$\begin{aligned}\text{add } & <a> \equiv \\ & \equiv (\lambda ab. a \text{ succ } b) <a> \rightarrow \\ & \rightarrow <a> \text{ succ } \rightarrow <a + b>.\end{aligned}$$

Комбинатор NB также представляет сложение нумералов Чёрча. Проверим это. Сначала вычислим выражение

$$\begin{aligned}\text{NBm} & nfx = \\ & = \text{B}(mf)(nf)x = \\ & = (mf)(nfx).\end{aligned}$$

Поэтому имеем

$$\begin{aligned}\text{NB} & <m> <n> fx = \\ & = (<m>f)(<n>fx) = \\ & = (\text{используя свойство (1)}) (<m>f) (f^n x) = \\ & = (\text{используя свойство (1)}) f^m (f^n x) \equiv \\ & \equiv f^{m+n} x.\end{aligned}$$

Но точно такое же выражение мы получаем при вычислении

$$<m+n>fx \equiv (\lambda sz. s^{m+n} z)fx = f^{m+n} x.$$

Поэтому, в силу экстенсиональности, $\text{NB} <m> <n> = <m + n>$.

Хотя на нумералах Чёрча два комбинатора add и NB действуют одинаково, они не равны. Докажем от противного. Из равенства $\text{add} = \text{NB}$ следует равенство $\text{add K } hxy = \text{NBK } hxy$. Но имеем $\text{NBK } hxy = \text{B(Kx)(hx)}y = \text{Kx(hxy)} = x$. С другой стороны,

$$\begin{aligned}\text{add K} & hxy \equiv \\ & \equiv (\lambda ab. a (\text{SB}) b) \text{K} hxy = \\ & = \text{K} (\text{SB}) hxy = \\ & = \text{SB} xy = \\ & = \text{By}(xy) = \\ & = (\lambda xyz . x(yz)) y(xy) =\end{aligned}$$

$$= \lambda z . y(xyz).$$

Термы x и $\lambda z . y(xyz)$ находятся в нормальной форме и не совпадают, что противоречит следствию из теоремы Чёрча–Россера.

Понятно, что $\text{add } < a >$ представляет функцию, которая прибавляет к своему аргументу нумерал $< a >$. Следовательно, $< b > (\text{add } < a >)$ делает такое сложение b раз, и поэтому

$$< b > (\text{add } < a >) < 0 > \rightarrow < a \times b >. \quad (3)$$

Заменим $< a >$ и $< b >$ на соответствующие переменные a и b и, применяя абстракцию относительно переменных a и b над левой частью (3), получаем комбинатор умножения:

Комбинатор $\text{times} \equiv \lambda ab. b (\text{add } a) < 0 >$ представляет функцию умножения над нумералами Чёрча.

Проверим:

$$\begin{aligned} \text{times } &< a > < b > = \\ &\equiv (\lambda ab. b (\text{add } a) < 0 >) < a > < b > = \\ &= < b > (\text{add } < a >) < 0 > = \\ &= (\text{add } < a >)^b < 0 > = \\ &\equiv \text{add } < a > (\text{add } < a > (\dots (\text{add } < a > < 0 > \dots))) \text{ (терм add повторяется } b \text{ раз)} = \\ &= < a \times b >. \end{aligned}$$

Комбинатор B также представляет умножение нумералов Чёрча. Проверим это. Пусть x и y – переменные. Тогда $B < n > < m > x y = < n > (< m > x) y$. Так как $< n >$ и $< m >$ – итераторы, то $< n > (< m > x)$ есть функция, которая применяет терм $(< m > x)$ n раз к терму y . Но $< m > x$ есть m -кратная аппликация x , поэтому $< n > (< m > x)$ применяет x к y всего $m \times n$ раз. Получили $B < n > < m > x y = x^{m \times n} y$, но имеем также $< n \times m > x y = x^{m \times n} y$, поэтому по экстенсиональности $B < n > < m > = < n \times m >$.

Хотя на нумералах Чёрча два комбинатора times и B действуют одинаково, они не равны. Докажем от противного. Из равенства $\text{times} = B$ следует равенство $\text{times} < 0 > K < 0 > = B < 0 > K < 0 >$. Но имеем

$$\begin{aligned} \text{times } &< 0 > K < 0 > = \\ &\equiv (\lambda ab. b (\text{add } a) < 0 >) < 0 > K < 0 > \rightarrow \\ &\rightarrow K (\text{add } < 0 >) < 0 > < 0 > \rightarrow \\ &\rightarrow (\text{add } < 0 >) < 0 > \rightarrow \\ &\rightarrow < 0 >. \end{aligned}$$

С другой стороны,

$$\begin{aligned} B < 0 > K < 0 > &= \\ &= < 0 > (K < 0 >) \equiv \\ &\equiv (\lambda xy. y) (K < 0 >) \rightarrow \\ &\rightarrow \lambda y. y. \end{aligned}$$

Термы $< 0 >$ и $\lambda y. y$ находятся в нормальной форме и не совпадают, что противоречит следствию из теоремы Чёрча–Россера.

Понятно, что $\text{times } < a >$ представляет функцию, которая умножает свой аргумент на нумерал $< a >$. Следовательно, $< b > (\text{times } < a >)$ делает такое умножение b раз, и поэтому

$$< b > (\text{times } < a >) < 1 > \rightarrow < a^b >. \quad (4)$$

Заменим $< a >$ и $< b >$ на соответствующие переменные a и b и, применяя абстракцию относительно переменных a и b над левой частью (4), получаем комбинатор для возведения в степень:

Комбинатор $\text{power} \equiv \lambda ab. b (\text{times } a) <1>$ представляет возвведение в степень над нумералами Чёрча.

Проверим:

$$\begin{aligned}\text{power } &<a> \equiv \\ &\equiv (\lambda ab. b (\text{times } a) <1>) <a> = \\ &= (\text{times } <a>) <1> = \\ &= (\text{times } <a>)^b <1> = \\ &\equiv \text{times } <a> (\text{times } <a> (\dots (\text{times } <a> <1>) \dots)) \text{ (терм } \text{times} \text{ повторяется } b \text{ раз)} = <a^b>.\end{aligned}$$

Истинностные значения и условное выражение

Определим булевские значения true , false и условное выражение if так, чтобы выполнялись следующие свойства:

$$\begin{aligned}\text{if true } A B &= A, \\ \text{if false } A B &= B.\end{aligned}\tag{5}$$

Существует много различных способов для представления истинностных значений – для кодирования булевых значений «истина» и «ложь» можно использовать два любых неравных ламбда-терма. Здесь предлагаются традиционные комбинаторные определения.

$$\begin{aligned}\text{true} &\equiv K, \\ \text{false} &\equiv KI.\end{aligned}$$

Как известно, $K A B = A$. Комбинатор KI , в свою очередь, отбрасывает свой первый аргумент: $(KI) A B \equiv (KI A) B = I B = B$. Комбинатор if должен удовлетворять уравнениям (5); если if будет обладать свойством $\text{if } M A B = M A B$ для произвольных комбинаторов M , A и B , то для if будет выполнено и (5). Поэтому условное выражение определяем следующим образом:

$$\text{if} \equiv \lambda x. \lambda y. \lambda z. x y z.$$

В комбинаторной записи $\text{if} = I$. Это легко доказать, используя экстенсиональность. Следуя [38. С. 142], будем записывать $\text{if } M A B$ в виде выражения

$$\text{если } M, \text{ то } A, \text{ иначе } B.$$

Комбинаторное выражение $M A B$ легко вычисляется, если M равно true или false . Это наблюдение помогает определить комбинатор not для операции отрицания. Тогда not есть решение уравнения $\text{not } A = A \text{ false true}$. Пусть not обладает данным свойством, тогда

$$\begin{aligned}\text{not true} &= \text{true false true} = \text{false}, \\ \text{not false} &= \text{false false true} = \text{true}.\end{aligned}$$

Поэтому not определяем следующим образом:

$$\text{not} \equiv \lambda x. x \text{ false true}.$$

В комбинаторной записи $\text{not} = S(SI(K(KI)))(KK)$.

Комбинаторы для операций конъюнкции и дизъюнкции также являются решениями соответствующих уравнений:

$$\begin{aligned}\text{and } A B &= A B \text{ false}, \\ \text{or } A B &= A \text{ true } B.\end{aligned}$$

Поэтому комбинаторы and и or определяем следующим образом:

$$\begin{aligned}\text{and} &\equiv \lambda xy. x y \text{ false}, \\ \text{or} &\equiv \lambda xy. x \text{ true } y.\end{aligned}$$

В комбинаторной записи

$$\begin{aligned} \text{and} &= SS(K(K(KI))), \\ \text{or} &= SI(KK). \end{aligned}$$

Пары и кортежи

Следующие комбинаторы используются для представления пар в λ -исчислении:

$$\begin{aligned} \text{fst} &\equiv \lambda x. x \text{ true}, \\ \text{snd} &\equiv \lambda x. x \text{ false}, \\ (E_1, E_2) &\equiv \lambda f. f E_1 E_2. \end{aligned}$$

Выражение (E_1, E_2) представляет упорядоченную пару, причем доступ к первой компоненте осуществляется с помощью функции fst , а вторую компоненту возвращает функция snd . Проверим:

$$\begin{aligned} \text{fst} (E_1, E_2) &\equiv \\ &\equiv (\lambda x. x \text{ true}) (\lambda f. f E_1 E_2) \rightarrow_{\beta} \\ &\rightarrow_{\beta} (\lambda f. f E_1 E_2) \text{ true} \rightarrow_{\beta} \\ &\rightarrow_{\beta} \text{true} E_1 E_2 \rightarrow_{\beta} \\ &\rightarrow_{\beta} E_1. \end{aligned}$$

Пара есть структура данных с двумя компонентами. Обобщенная структура с n компонентами называется **n -кой** или **кортежем** и легко определяется через пары.

$$(E_1, E_2, \dots, E_n) \equiv (E_1, (E_2, (\dots(E_{n-1}, E_n)\dots))).$$

Выражение (E_1, E_2, \dots, E_n) есть n -кортеж с компонентами E_1, E_2, \dots, E_n и длиной n . Пары суть кортежи длиной 2. С помощью следующих выражений получаем доступ к отдельным компонентам кортежа:

$$\begin{aligned} E \downarrow 1 &\equiv \text{fst } E, \\ E \downarrow 2 &\equiv \text{fst} (\text{snd } E), \end{aligned}$$

$E \downarrow i \equiv \text{fst} (\text{snd} (\text{snd} (\dots (\text{snd } E) \dots)))$, если i меньше длины E (комбинатор snd повторяется $i-1$ раз),
 $E \downarrow n \equiv \text{snd} (\text{snd} (\dots (\text{snd } E) \dots))$, если n равно длине E (комбинатор snd повторяется $n-1$ раз).

Проверим, что эти определения правильно работают:

$$\begin{aligned} (E_1, E_2, \dots, E_n) \downarrow 1 &\equiv \\ &\equiv \text{fst} (E_1, (E_2, (\dots(E_{n-1}, E_n)\dots))) \rightarrow \\ &\rightarrow E_1. \\ (E_1, E_2, \dots, E_n) \downarrow 2 &\equiv \\ &\equiv \text{fst} (\text{snd} (E_1, (E_2, (\dots(E_{n-1}, E_n)\dots)))) \rightarrow \\ &\rightarrow \text{fst} (E_2, (\dots(E_{n-1}, E_n)\dots)) \rightarrow \\ &\rightarrow E_2. \end{aligned}$$

В общем случае $(E_1, E_2, \dots, E_n) \downarrow i = E_i$ для $1 \leq i \leq n$.

Тест на ноль, предшествование, вычитание и сравнение

Введенных функций для чисел явно недостаточно, чтобы с удобством использовать λ -исчисление как язык программирования. Необходимо также ввести еще некоторые функции: pred , zero? (представляющие функции предшествования $n \rightarrow n-1$ и тест для нуля) и другие.

Будем искать комбинатор zero? в виде $\lambda n. n A B$, где A и B – некоторые пока еще неизвестные нам λ -термы. Комбинатор должен удовлетворять следующим свойствам:

$$\text{zero? } <0> \rightarrow \text{true},$$

$$\text{zero? } \langle n+1 \rangle \rightarrow \text{false}.$$

Поэтому должно выполняться (так как $\text{zero? } n \rightarrow n A B$):

$$\begin{aligned} \langle 0 \rangle A B &\rightarrow \text{true}, \\ \langle n+1 \rangle A B &\rightarrow \text{false}. \end{aligned}$$

Но $\langle 0 \rangle A B \equiv (\lambda ab.b) A B \rightarrow B$. Значит, $B \equiv \text{true}$. Теперь найдем A . Имеем $\langle n+1 \rangle \equiv \lambda ab. a M_{a,b}$, где $M_{a,b}$ есть одно из выражений b , $(a b)$, $a(a b)$, $a(a(a b))$ и т.п. Поэтому

$$\langle n+1 \rangle A B \rightarrow A M_{A,B} \rightarrow \text{false}.$$

Таким образом, комбинатор A , действуя на любой терм $M_{A,B}$, дает false . Следовательно, можно взять постоянную функцию $A \equiv \lambda x. \text{false}$.

Поэтому zero? определяем следующим образом:

$$\text{zero?} \equiv \lambda n. n (\lambda x. \text{false}) \text{ true} .$$

Определим на натуральных числах **усеченное вычитание** (функцию **монус**):

$$a \div b = \begin{cases} a - b, & \text{если } a \geq b, \\ 0 & \text{иначе.} \end{cases}$$

Функция предшествования pred моделирует $a \div 1$, и на нумералах Чёрча удовлетворяет соотношениям (для любого натурального числа n):

$$\begin{aligned} \text{pred } \langle 0 \rangle &= \langle 0 \rangle, \\ \text{pred } \langle n+1 \rangle &= \langle n \rangle. \end{aligned}$$

Функция предшествования pred определяется с большим трудом, чем предыдущие функции. Сам Алонзо Чёрч бился несколько месяцев над тем, чтобы определить эту функцию, но так и не справился с этой задачей и уверился в неполноте своего исчисления. Но в 1932 г. Стивен Клини, тогда молодой аспирант, нашел решение, и это было его первым математическим результатом.

Трудность в определении функции предшествования состоит в том, что, имея терм $\lambda y. u^n x$, надо избавиться от первой аппликации y в u^n .

Клини рассмотрел функцию f , отображающую пару (a, b) в пару $(\text{succ } a, a)$. Можно определить f следующим образом: $\lambda p. (\text{succ } (\text{fst } p), \text{fst } p)$.

Заметим, для любого λ -терма E имеем

$$\begin{aligned} \langle n+1 \rangle f(\langle 0 \rangle, E) &\rightarrow_{\beta} \\ \rightarrow_{\beta} f^{n+1}(\langle 0 \rangle, E) &\rightarrow \\ \rightarrow(\langle n+1 \rangle, \langle n \rangle). & \end{aligned}$$

Если взять $E \equiv \langle 0 \rangle$, то получим $\langle n \rangle f(\langle 0 \rangle, \langle 0 \rangle) \rightarrow (\langle n \rangle, \langle n \div 1 \rangle)$ и, следовательно, для любого натурального n имеем $\text{snd } (\langle n \rangle f (\langle 0 \rangle, \langle 0 \rangle)) \rightarrow \langle n \div 1 \rangle$. Поэтому pred определяем следующим образом (заменяя $\langle n \rangle$ на n и проводя абстракцию относительно n):

$$\text{pred} \equiv \lambda n. \text{snd } (n (\lambda p. (\text{succ } (\text{fst } p), \text{fst } p)) (\langle 0 \rangle, \langle 0 \rangle)).$$

Пример 1. Ту же самую технику можно применить и для создания других теоретико-числовых функций. Например, рассмотрим функцию f , отображающую пару (a, b) в пару $(\text{succ } a, \text{times } a b)$. Легко видеть, что функцию f можно определить как

$$\lambda p. (\text{succ } (\text{fst } p), \text{times } (\text{fst } p) (\text{snd } p)).$$

Заметим, что

$$\begin{aligned} & \langle n \rangle f(\langle 1 \rangle, \langle 1 \rangle) \rightarrow_{\beta} \\ & \rightarrow_{\beta} f^n(\langle 1 \rangle, \langle 1 \rangle) \rightarrow \\ & \rightarrow (\langle n+1 \rangle, \langle n! \rangle). \end{aligned}$$

Подставим в выражение $\langle n \rangle f(\langle 1 \rangle, \langle 1 \rangle)$ определение функции f , применим комбинатор snd , заменим $\langle n \rangle$ на переменную n и окончательно проведем λ -абстракцию над этой переменной. Получается определение функции, вычисляющей факториал

$$fact \equiv \lambda n. \, snd(n(\lambda p. (succ(fst p), times(fst p)(snd p))) (\langle 1 \rangle, \langle 1 \rangle)).$$

Имея определение функции предшествования, мы можем определить усеченное вычитание (функцию монус) над нумералами Чёрча. Необходимо только сделать b -кратную итерацию аппликации функции $pred$ к терму $\langle a \rangle$, чтобы получить $\langle a \div b \rangle$:

$$monus \equiv \lambda ab. (b pred a).$$

Для доказательства достаточно проверить, что $monus \langle a \rangle \langle b \rangle \rightarrow \langle a \div b \rangle$.

Равенство двух нумералов Чёрча можно определить через усеченное вычитание:

$$equal? \equiv \lambda ab. (and(zero?(monus a b)) (zero?(monus b a))).$$

Для доказательства надо проверить, что для любых $a, b \in N$, $a \neq b$ выполнено

$$\begin{aligned} equal? \langle a \rangle \langle a \rangle & \rightarrow true, \\ equal? \langle a \rangle \langle b \rangle & \rightarrow false. \end{aligned}$$

Следующие функции сравнения получаются подобным (как и для $equal?$) образом:

$$\begin{aligned} notEqual? & \equiv \lambda ab. not(equal? a b), \\ lessThanOrEqual? & \equiv \lambda ab. zero?(monus a b), \\ greaterThanOrEqual? & \equiv \lambda ab. zero?(monus b a), \\ lessThan? & \equiv \lambda ab. not(greaterThanOrEqual? a b), \\ greaterThan? & \equiv \lambda ab. not(lessThanOrEqual? a b). \end{aligned}$$

Рекурсия

Использование рекурсивных¹¹⁵ функций – одна из важнейших особенностей функционального программирования: все итерации заменяются рекурсивными вызовами. На первый взгляд это невозможно сделать в ламбда-исчислении, поскольку в λ -исчислении все функции анонимны и мы не можем использовать их имена, чтобы организовать рекурсивный вызов. Как это ни удивительно, но рекурсия в λ -исчислении возможна! Но этот факт, как и существование функции предшествования, был открыт только после значительных усилий.

Ключевой идеей послужило использование так называемого **комбинатора неподвижной точки**. В математике неподвижной точкой для данной функции $f : X \rightarrow X$ называется точка $x_0 \in X$, такая что $f(x_0) = x_0$. В λ -исчислении имеется подобное определение: **неподвижной точкой** λ -терма M называется λ -терм N , для которого выполнено $M N = N$.

Замкнутый λ -терм Y называется комбинатором неподвижной точки, если для любого терма f выполнено соотношение $f(Yf) = Yf$. Другими словами, комбинатор неподвижной точки, примененный для любой функции f , возвращает неподвижную точку этой функции. Первый такой комбинатор был найден Хаскеллом Карри и обычно обозначается Y . Этот комбинатор напоминает парадокс Рассела и поэтому называется «парадоксальным комбинатором». Если мы определим $R = \lambda x. not(x x)$, то обнаружим, что $R R = not(R R)$.

¹¹⁵ Имеется в виду метод определения функций, так как это понимается в программировании.

Таким образом, терм $R R$ служит неподвижной точкой для оператора отрицания¹¹⁶. Для того чтобы получить общий комбинатор неподвижной точки, мы должны заменить отрицание **not** на произвольный терм f . Поэтому определяем

$$Y \equiv \lambda f. (\lambda x . f(x x)) (\lambda x . f(x x)).$$

Проверим, что Y удовлетворяет требуемым условиям. С одной стороны,

$$\begin{aligned} YE &\equiv (\lambda f. (\lambda x . f(x x)) (\lambda x . f(x x))) E \rightarrow_{\beta} \\ &\rightarrow_{\beta} (\lambda x . E(x x)) (\lambda x . E(x x)) \rightarrow_{\beta} \\ &\rightarrow_{\beta} E((\lambda x . E(x x)) (\lambda x . E(x x))). \end{aligned}$$

С другой стороны,

$$\begin{aligned} E(YE) &\equiv E((\lambda f. (\lambda x . f(x x)) (\lambda x . f(x x))) E) \rightarrow_{\beta} \\ &\rightarrow_{\beta} E((\lambda x . E(x x)) (\lambda x . E(x x))). \end{aligned}$$

Так как оба терма YE и $E(YE)$ редуцируются к терму $E((\lambda x . E(x x)) (\lambda x . E(x x)))$, то $E(YE) = YE$. Таким образом, мы получили, что каждое λ -выражение E имеет неподвижную точку YE .

Комбинатор Карри Y представляется в базисе $\{S, K, I\}$ как

$$Y = S(K(SII))(S(S(KS)K)(K(SIII))).$$

Рассмотрим теперь представление рекурсивных функций в λ -исчислении. В качестве примера попробуем определить λ -выражение **summa**, такое что

$$\text{summa } <m> = \text{add } <m> (\text{add } <m-1> (\dots (\text{add } <1> <0>) \dots)).$$

Нетрудно увидеть, что **summa** должно удовлетворять уравнению

$$\text{summa } <m> = \text{если zero? } <m>, \text{то } <0>, \text{иначе add } <m> (\text{summa } (\text{pred } <m>)).$$

Пусть это имеет место, тогда, например,

$$\begin{aligned} \text{summa } <2> \text{ если zero? } <2>, \text{то } <0>, \text{иначе add } <2> (\text{summa } (\text{pred } <2>)) &= \\ &= \text{add } <2> (\text{summa } (\text{pred } <2>)) = \\ &= \text{add } <2> (\text{summa } <1>) = \\ &= \text{add } <2> (\text{если zero? } <1>, \text{то } <0>, \text{иначе add } <1> (\text{summa } (\text{pred } <1>))) = \\ &= \text{add } <2> (\text{add } <1> (\text{summa } (\text{pred } <1>))) = \\ &= \text{add } <2> (\text{add } <1> (\text{summa } <0>)) = \\ &= \text{add } <2> (\text{add } <1> (\text{если zero? } <0>, \text{то } <0>, \text{иначе add } <0> (\text{summa } (\text{pred } <0>)))) = \\ &= \text{add } <2> (\text{add } <1> <0>) = \\ &= \text{add } <2> <1> = \\ &= <3>. \end{aligned}$$

Приведенное выше уравнение для **summa** предполагает, что терм **summa** может быть определен как

$$\text{summa} = \lambda m. \text{если zero? } m, \text{то } <0>, \text{иначе add } m (\text{summa } (\text{pred } m)).$$

Но такое определение невозможно в λ -исчислении, поскольку определяемый терм не может присутствовать в правой части определения. И здесь на помощь приходит комбинатор неподвижной точки. Определим вспомогательный терм:

$$\text{summaf} = \lambda f m. \text{если zero? } m, \text{то } <0>, \text{иначе add } m (f(\text{pred } m)),$$

затем определим $\text{summa} = Y \text{summaf}$. Получаем искомое уравнение:

¹¹⁶ Последнее равенство не является противоречием, поскольку $R R$ не является термом, представляющим булевское значение.

$$\begin{aligned}
\text{summa } <\!m\!> &= (Y \text{ summaf}) <\!m\!> = \\
&= \text{summaf} (Y \text{ summaf}) <\!m\!> = \\
&= (\text{по определению } \text{summa}) \text{ summaf summa } <\!m\!> = \\
&= (\lambda f m. \text{ если zero? } m, \text{ то } <\!0\!>, \text{ иначе add } m (f(\text{pred } m))) \text{ summa } <\!m\!> = \\
&= \text{если zero? } <\!m\!>, \text{ то } <\!0\!>, \text{ иначе add } <\!m\!> (\text{summa} (\text{pred } <\!m\!>)).
\end{aligned}$$

Уравнение вида $f x_1 \dots x_n = E$ называется рекурсивным, если f имеет свободное вхождение в E . Комбинатор Y обеспечивает общий путь решения такого уравнения. Начинаем с уравнения в форме $f x_1 \dots x_n = \sim f \sim$, где $\sim f \sim$ есть некоторое λ -выражение, содержащее f . Затем определяем f как

$$f = Y(\lambda f x_1 \dots x_n . \sim f \sim).$$

Проверим, что f удовлетворяет необходимому уравнению:

$$\begin{aligned}
f x_1 \dots x_n &= \\
&= (Y(\lambda f x_1 \dots x_n . \sim f \sim)) x_1 \dots x_n = \\
&= (\text{по свойству } Y) (\lambda f x_1 \dots x_n . \sim f \sim) (Y(\lambda f x_1 \dots x_n . \sim f \sim)) x_1 \dots x_n = \\
&= (\text{по определению } f) (\lambda f x_1 \dots x_n . \sim f \sim) f x_1 \dots x_n = \\
&= \sim f \sim.
\end{aligned}$$

Хотя с математической точки зрения использование комбинатора Карри совершенно безусловно, но с точки зрения программирования вычислительный переход от выражения E (YE) к выражению YE и обратно нельзя осуществить только с помощью β -конверсии. По этой причине более удобен комбинатор неподвижной точки, предложенный Тьюрингом:

$$T \equiv (\lambda x y. y(x x y)) (\lambda x y. y(x x y)).$$

Для того чтобы проверить необходимое свойство, обозначим через a терм $\lambda x y. y(x x y)$. Тогда имеем

$$Tf \equiv (\lambda x y. y(x x y)) af \rightarrow_{\beta} f(a a f) \equiv f(Tf).$$

Функции с несколькими аргументами

В математических обозначениях применение n -местной функции f к аргументам x_1, \dots, x_n записывается как $f(x_1, \dots, x_n)$. Существует два способа представления n -кратной аппликации в λ -исчислении:

- 1) как $(fx_1 \dots x_n)$ или
- 2) как аппликация f к n -ке (x_1, \dots, x_n) .

В первом случае f применяется к своим аргументам по очереди. М. Шейнфинкель заметил, что не обязательно вводить функции более чем одной переменной [22]. Действительно, для функции, скажем, от двух переменных $f(x, y)$ мы можем рассмотреть функцию g_x с соотношением $g_x(y) = f(x, y)$, а затем h с соотношением $h'(x) = g_x$. Отсюда $(h(x))(y) = f(x, y)$. Позднее Карри [8] переоткрыл это свойство, и поэтому сейчас сведение функций с несколькими переменными только к функциям одного переменного носит название **карринг**. Функции **and**, **or** или **add**, определенные ранее, применяют карринг. Преимущество функций с каррингом заключается в том, что такие функции можно применять частично с меньшим числом аргументов, чем требуется по определению этих функций. Например, $\text{add } <1>$ есть результат частичного применения функции **add** к $<1>$ и обозначает функцию $n \rightarrow n + 1$.

Хотя часто удобно представлять n -местные функции с помощью карринга, полезно также иметь возможность представлять аргументы с помощью единственной n -ки. Например, вместо представления сложения λ -термом **add**, так что выполняется условие $\text{add } <m> <n> = <m + n>$,

может быть, более удобно представить λ -термом sum , для которого выполнено $\text{sum} (< m >, < n >) = < m + n >$.

Таким образом, n -местные функции можно определить как с каррингом, так и без карринга. Можно определить два комбинатора, применяя которые к функциям, можно менять наличие карринга у последних:

$$\begin{aligned}\text{curry} &\equiv \lambda f x y. f(x, y), \\ \text{uncurry} &\equiv \lambda f p. f(\text{fst } p) (\text{snd } p).\end{aligned}$$

Имеем для произвольного комбинатора E :

$$\begin{aligned}\text{curry} (\text{uncurry } E) &= E, \\ \text{uncurry} (\text{curry } E) &= E.\end{aligned}$$

Проверим первое равенство:

$$\begin{aligned}\text{curry} (\text{uncurry } E) &\equiv \\ &\equiv (\lambda f x y. f(x, y)) (\text{uncurry } E) = \\ &= \lambda x y. ((\text{uncurry } E) (x, y)) \equiv \\ &\equiv \lambda x y. ((\lambda f p. f(\text{fst } p) (\text{snd } p)) E (x, y)) = \\ &= \lambda x y. (E (\text{fst } (x, y)) (\text{snd } (x, y))) = \\ &= \lambda x y. E x y \rightarrow_{\eta} \\ &\quad \rightarrow_{\eta} E.\end{aligned}$$

Аналогично доказывается второе равенство. Нетрудно увидеть, что

$$\begin{aligned}\text{sum} &= \text{uncurry add}, \\ \text{add} &= \text{curry sum}.\end{aligned}$$

Представление вычислимых функций

После того как Чёрч ввел λ -исчисление, Клини доказал, что множество частично-рекурсивных функций совпадает с множеством λ -определимых функций.

Доказательство теоремы Клини в двух различных вариантах представлено в [38. С. 143–147; 121. С. 91–122]. Проведем доказательство только половины теоремы: любая частично-рекурсивная функция является λ -определимой. Вторая часть теоремы требует описания λ -исчисления в виде аксиоматической теории, что выходит за рамки данной книги.

Для большей наглядности изложения доказательства введем обозначение.

- Для частично-определенной функции, имеющей более одного аргумента, например $f(x, y_1, y_2, \dots, y_k)$ и $g(y_1, y_2, \dots, y_k)$, будем писать $f(x, \vec{y})$ и $g(\vec{y})$ соответственно.
- Для λ -переменных в λ -абстракциях, например $\lambda x y_1 y_2 \dots y_k. A$ и $\lambda y_1 y_2 \dots y_k. A$, будем писать $\lambda x \vec{y}. A$ и $\lambda \vec{y}. A$ соответственно.
- Для последовательности λ -переменных в λ -аппликациях, например $A x y_1 y_2 \dots y_k$ и $A y_1 y_2 \dots y_k$, будем писать $A x \vec{y}$ и $A \vec{y}$, соответственно.
- Для последовательности нумералов Чёрча в λ -аппликациях, например $A < x > < y_1 > < y_2 > \dots < y_k >$ и $A < y_1 > < y_2 > \dots < y_k >$, будем писать $A < x > < \vec{y} >$ и $A < \vec{y} >$ соответственно.

Теорема 1. Любая частично-рекурсивная функция является λ -определимой.

Доказательство. Ламбда-определимость базисных функций показана ранее. Суперпозиция функций f и g , λ -определимых соответственно термами F и G , выражается через терм $\lambda \vec{x}. F(G \vec{x})$.

Осталось доказать только λ -определимость примитивной рекурсии и минимизации.

Примитивная рекурсия. Пусть имеется примитивно рекурсивная функция f с определением:

$$\begin{aligned} f(0, \vec{n}) &= g(\vec{n}), \\ f(m+1, \vec{n}) &= h(m, \vec{n}, f(m, \vec{n})), \end{aligned}$$

где функция g λ -определенна термом $\mathbf{G} : \mathbf{G} < \vec{n} > = < g(\vec{n}) >$ и функция h λ -определенна термом $\mathbf{H} : \mathbf{H} < m > < \vec{n} > < y > = < h(m, \vec{n}, y) >$. Докажем, что f также λ -определенна. Возьмем терм \mathbf{F} , который удовлетворяет рекурсивному уравнению

$$\mathbf{F} = \lambda \vec{x} \vec{y}. \text{если } (\text{zero? } x), \text{mo } (\mathbf{G} \vec{y}), \text{иначе } \mathbf{H}(\text{pred } x) \vec{y} (\mathbf{F}(\text{pred } x) \vec{y}).$$

Такой терм существует, он представляется с помощью комбинатора неподвижной точки

$$\mathbf{F} = \mathbf{Y}(\lambda \vec{x} \vec{y}. \text{если } (\text{zero? } x), \text{mo } (\mathbf{G} \vec{y}), \text{иначе } \mathbf{H}(\text{pred } x) \vec{y} (\mathbf{f}(\text{pred } x) \vec{y})).$$

По свойству комбинатора неподвижной точки имеем

$$\mathbf{F} < m > < \vec{n} > = (\lambda \vec{x} \vec{y}. \text{если } (\text{zero? } x), \text{mo } (\mathbf{G} \vec{y}), \text{иначе } \mathbf{H}(\text{pred } x) \vec{y} (\mathbf{f}(\text{pred } x) \vec{y})) \mathbf{F} < m > < \vec{n} >.$$

Докажем индукцией по m , что

$$\mathbf{F} < m > < \vec{n} > = < f(m, \vec{n}) >. \quad (6)$$

Базис $m = 0$.

$$\begin{aligned} \mathbf{F} < 0 > < \vec{n} > &= (\lambda \vec{x} \vec{y}. \text{если } (\text{zero? } x), \text{mo } (\mathbf{G} \vec{y}), \text{иначе } \mathbf{H}(\text{pred } x) \vec{y} (\mathbf{f}(\text{pred } x) \vec{y})) \mathbf{F} < 0 > < \vec{n} > = \\ &= \text{если } (\text{zero? } < 0 >), \text{mo } (\mathbf{G} < \vec{n} >), \text{иначе } \mathbf{H}(\text{pred } < 0 >) < \vec{n} > (\mathbf{F}(\text{pred } < 0 >) < \vec{n} >) = \\ &= \mathbf{G} < \vec{n} > = < g(\vec{n}) > = < f(0, \vec{n}) >. \end{aligned}$$

Индуктивный переход. Пусть (6) доказано для m , докажем для $m + 1$.

$$\begin{aligned} \mathbf{F} < m + 1 > < \vec{n} > &= \\ &= (\lambda \vec{x} \vec{y}. \text{если } (\text{zero? } x), \text{mo } (\mathbf{G} \vec{y}), \\ &\text{иначе } \mathbf{H}(\text{pred } x) \vec{y} (\mathbf{f}(\text{pred } x) \vec{y})) \mathbf{F} < m + 1 > < \vec{n} > = \\ &= \text{если } (\text{zero? } < m + 1 >), \text{mo } (\mathbf{G} < \vec{n} >), \\ &\text{иначе } \mathbf{H}(\text{pred } < m + 1 >) < \vec{n} > (\mathbf{F}(\text{pred } < m + 1 >) < \vec{n} >) = \\ &= \mathbf{H}(\text{pred } < m + 1 >) < \vec{n} > (\mathbf{F}(\text{pred } < m + 1 >) < \vec{n} >) = \\ &= \mathbf{H} < m > < \vec{n} > (\mathbf{F} < m > < \vec{n} >) = \\ &= (\text{применяя индуктивное предположение}) \mathbf{H} < m > < \vec{n} > < f(m, \vec{n}) > = \\ &= < h(m, \vec{n}, f(m, \vec{n})) > = < f(m + 1, \vec{n}) >. \end{aligned}$$

Минимизация. Пусть функция $f(m, \vec{n})$ — λ -определенна с помощью терма \mathbf{F} :

$$\mathbf{F} < m > < \vec{n} > = < f(m, \vec{n}) >.$$

Требуется доказать, что существует такой терм \mathbf{G} , для которого

$$\mathbf{G} < \vec{x} > = < \mu y [f(y, \vec{x}) = 0] >.$$

Рассмотрим рекурсивное уравнение

$$\mathbf{H} = \lambda y \vec{x}. \text{если zero? } (\mathbf{F} y \vec{x}), \text{то } y, \text{иначе } \mathbf{H}(\text{succ } y) \vec{x}.$$

Решение этого уравнения существует:

$$\mathbf{H} = \mathbf{Y}(\lambda hy \vec{x}. \text{если zero? } (\mathbf{F} y \vec{x}), \text{то } y, \text{иначе } h(\text{succ } y) \vec{x}).$$

По свойству комбинатора неподвижной точки имеем

$$\mathbf{H} < y > < \vec{x} > = (\lambda hy \vec{x}. \text{если zero? } (\mathbf{F} y \vec{x}), \text{то } y, \text{иначе } h(\text{succ } y) \vec{x}) \mathbf{H} < y > < \vec{x} >.$$

Если в качестве комбинатора неподвижной точки взять комбинатор Тьюринга, то дополнительно получаем

$$H < y > < \vec{x} > \rightarrow (\lambda h y \vec{x}. \text{если } zero? (F y \vec{x}), \text{то } y, \text{иначе } h(succ\ y) \vec{x}) H < y > < \vec{x} >.$$

Отсюда следует

$H < y > < \vec{x} > \rightarrow \text{если } zero? (F < y > < \vec{x} >), \text{то } < y >, \text{иначе } H(succ < y >) < \vec{x} >$
и, далее,

$$H < y > < \vec{x} > \rightarrow \text{если } zero? < f(y, \vec{x}) >, \text{то } < y >, \text{иначе } H < y+1 > < \vec{x} >.$$

Имеем свойства:

- если $f(y, \vec{x}) = 0$, то $H < y > < \vec{x} > \rightarrow < y >$;
- если $f(y, \vec{x}) \neq 0$, то $H < y > < \vec{x} > \rightarrow H < y+1 > < \vec{x} >$.

Пусть функция $g(\vec{x}) = \mu y [f(y, \vec{x}) = 0]$ и для данного значения \vec{x} существует $m = g(\vec{x})$. Тогда цепочка заканчивается:

$$H < 0 > < \vec{x} > \rightarrow H < 1 > < \vec{x} > \rightarrow H < 2 > < \vec{x} > \rightarrow \dots \rightarrow < m >.$$

Определим теперь комбинатор $G \equiv \lambda \vec{x}. H < 0 > \vec{x}$. Имеем

$$G < \vec{x} > = H < 0 > < \vec{x} > \rightarrow < \mu y [f(y, \vec{x}) = 0] >,$$

если $g(\vec{x}) = \mu y [f(y, \vec{x}) = 0]$ – определено. Если же нет, то редукция

$$H < 0 > < x > \rightarrow H < 1 > < x > \rightarrow H < 2 > < x > \rightarrow \dots$$

не заканчивается. Получили, что терм G λ -определяет минимизацию $\mu y [f(y, \vec{x}) = 0]$. ■

Таким образом, получаем, что множество λ -определимых функций также является формализацией интуитивного понятия алгоритма.

– 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.

*A. и B. Стругацкие.
Понедельник начинается в субботу*

§ 2. Тезис Чёрча и алгоритмическая неразрешимость

С 30-х гг. XX в. было предложено много различных математических уточнений интуитивного понятия алгоритма. Три из этих подходов мы разобрали. Перечислим некоторые другие альтернативные способы, которые предлагались следующими авторами:

- Гёдель–Эрбран¹¹⁷–Клини. Общерекурсивные функции, определенные с помощью исчисления рекурсивных уравнений [64. Глава XI].
- Пост. Функции, определяемые каноническими дедуктивными системами [61. С. 66–72; 105].
- Марков¹¹⁸. Функции, задаваемые некоторыми алгоритмами (известными под названием «нормальные алгорифмы») над конечным алфавитом [80].

¹¹⁷ Эрбран Жак (1908–1931) – французский математик и логик.

¹¹⁸ Марков Андрей Андреевич (1903–1979) – основоположник советской школы конструктивной математики.

- Шепердсон–Стерджис. МНР-вычислимые функции (МНР – машина с неограниченными регистрами – расширенный вариант машины Тьюринга: добавлены команды *обнуление*, *прибавление единицы*, *переадресация*, *условный переход*; в отличии от современного компьютера проще и обозримее) [24, 61].

Между этими подходами (в том числе и тремя рассмотренными ранее) имеются большие различия; каждый из них имеет свои преимущества для соответствующего описания вычислимости. Следующий замечательный результат получен усилиями многих исследователей.

Теорема 2 (основной результат) [61. 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 [61. 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 § 1 главы 9 и в § 1 данной главы, образуют исходную часть этого семейства, которую можно расширять до бесконечности методами из указанных параграфов 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.

После принятия тезиса Чёрча эквивалентной заменой машине Тьюринга может служить программа вычислений на любом универсальном языке программирования. Программной реализацией λ -исчисления можно считать Haskell [59].

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 данный предикат **разрешимым** или нет (т.е. существует ли алгоритм, который позволил бы распознать, является предикат истинным или ложным). 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.

Теорема 3. Проблема остановки неразрешима. 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. Смысль этого утверждения для теоретического программирования очевиден: не существует совершенно общего метода проверки программ на наличие в них бесконечных циклов.

Приведем два варианта доказательства. Первый вариант использует неформальное определение вычислимости доказательства [89. С. 123–125], и рассуждение следует первоначальному доказательству Тьюринга.

Второй вариант – строгое доказательство, сделанное в рамках λ -исчисления.

Доказательство 1. Не теряя общности, мы можем рассматривать только программы, вычисляющие одноместные функции от натуральных чисел. Поскольку вычислимых одноместных функций счетное число, то пусть последовательность c_1, c_2, c_3, \dots содержит все такие функции. Доказательство проведем от противного.

Пусть имеется такая программа (двуместная функция) $a(q, n)$, что:

1) если завершается $a(q, n)$, то не завершается $c_q(n)$ (т.е. мы считаем, что алгоритм a проверяет, остановится или нет вычисление функции). Тогда, в частности, для $q = n$

2) если завершается $a(n, n)$, то не завершается $c_n(n)$. Функция $a(n, n)$ зависит от одного параметра, следовательно, существует такое k , что

3) $a(n, n) = c_k(n)$. Тогда

4) $a(k, k) = c_k(k)$ (следует из п. 3 при $n = k$). Имеем из п. 2 при $n = k$

5) если завершается $a(k, k)$, то не завершается $c_k(k)$. Подставляя п. 4 в п. 5, получаем

6) если завершается $c_k(k)$, то не завершается $c_k(k)$.

Однозначное следствие: $c_k(k)$ не завершается, а $a(k, k)$ не может это установить (поскольку $a(k, k) = c_k(k)$ и, следовательно, не останавливается). ■

Доказательство 2 [121. С. 122]. Поскольку вычислимые функции – это в точности те, которые λ -представимы (теорема 1), то проблему остановки можно сформулировать в терминах λ -исчисления: «Существует ли алгоритм, с помощью которого можно установить, имеет ли нормальную форму данный λ -терм?»

Доказывать будем от противного. Предположим, что искомый алгоритм существует: если терм t имеет нормальную форму, то алгоритм выдает 0, а если нет, то алгоритм выдает 1. В силу тезиса Чёрча такой алгоритм представляется в виде λ -определенной функции, следовательно, существует комбинатор H , такой что

$$Ht = \begin{cases} <0>, & \text{если терм } t \text{ имеет нормальную форму,} \\ <1> & \text{в противном случае.} \end{cases}$$

Комбинаторы $<0>$ и $<1>$ – произвольные нумералы, кодирующие соответственно 0 и 1. Обозначим через zero? , как обычно, комбинатор – тест на ноль:

$$\begin{aligned} \text{zero? } &<0> \rightarrow \text{true}, \\ &<1> \rightarrow \text{false}. \end{aligned}$$

Как обычно, $\text{true} \equiv K$, $\text{false} \equiv KI$.

Мы используем комбинатор H , чтобы построить комбинатор D , такой что

$$Dt = \begin{cases} K(tt), & \text{если терм } (tt) \text{ имеет нормальную форму,} \\ S & \text{в противном случае.} \end{cases}$$

Он строится очевидным образом:

$$D \equiv \lambda t. \text{zero?}(H(tt))(K(tt))S.$$

Действительно, пусть терм (tt) имеет нормальную форму, тогда

$$\begin{aligned} Dt &\equiv (\lambda t. \text{zero?}(H(tt))(K(tt))S) t = \text{zero?}(H(tt))(K(tt))S = \\ &= \text{zero?} <0> (K(tt))S = \text{true} (K(tt))S \equiv K (K(tt))S = K(tt). \end{aligned}$$

Если же терм (tt) не имеет нормальную форму, то

$$\begin{aligned} Dt &\equiv (\lambda t. \text{zero?}(H(tt))(K(tt))S) t = \text{zero?}(H(tt))(K(tt))S = \\ &= \text{zero?} <1> (K(tt))S = \text{false} (K(tt))S \equiv (KI)(K(tt))S = IS = S. \end{aligned}$$

Для любого t терм Dt имеет нормальную форму (поскольку он равен либо $K(tt)$, имеющему нормальную форму, либо равен S), поэтому терм DD также имеет нормальную форму (скажем, некий комбинатор α). Согласно определению D комбинатор DD равен $K(DD)$, т.е. $D = \alpha$ и $D = K\alpha \rightarrow \lambda y. \alpha$. Но комбинаторы α и $\lambda y. \alpha$ оба находятся в нормальной форме и не совпадают. Получили противоречие. ■

Многие результаты о неразрешимости в теории вычислимости являются следствием следующей теоремы.

Теорема 4 (Райс¹¹⁹) [19]. Любое нетривиальное свойство вычислимых функций алгоритмически неразрешимо. (Свойство нетривиально, если имеются функции, обладающие этим свойством и не обладающие.)

Оказывается, по программе, вычисляющей частично определенную функцию $f(n)$, невозможно в общем случае установить, обладает или нет функция следующими свойствами:

- является ли функция f всюду неопределенной;
- конечно ли множество решений $f(n) = 0$;
- конечно или бесконечно множество значений функции f ;
- является ли функция f периодической;
- является ли функция f ограниченной;
- является ли функция f постоянной.

Из того, что нельзя определить, вычисляет ли функция тождественный ноль, следует, 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.

Неразрешимые проблемы встречаются не только в теории вычислимости. Одним из первых результатов была уже рассмотренная в главе 6, § 5 **теорема Чёрча о неразрешимости логики предикатов**: *не существует алгоритма, который для любой формулы логики предикатов устанавливает, общезначима она или нет*.

Чёрч доказывал свою теорему, используя λ -исчисление [6].

Диофантовы уравнения

Рассмотрим проблему нахождения универсального алгоритма для распознавания разрешимости диофантовых уравнений.

Пусть $p(z_1, \dots, z_n)$ – полином с целыми коэффициентами типа

$$p(z_1, z_2) = z_1^5 - 4z_1z_2^3 + 32.$$

¹¹⁹ Генри Гордон Райс (1920–2003) – американский логик и математик.

Диофантовы уравнения $p(z_1, \dots, z_n) = 0$ подразумевают решение в целых числах. Первым диофантовые уравнения систематизировал и изучил математик Диофант¹²⁰ в III в. н.э.

Пример 2. Рассмотрим две системы диофантовых уравнений:

$$\begin{cases} 6w + 2x^2 - y^3 = 0, \\ 5xy - z^2 + 6 = 0, \\ w^2 - w + 2x - y + z - 4 = 0. \end{cases}$$

$$\begin{cases} 6w + 2x^2 - y^3 = 0, \\ 5xy - z^2 + 6 = 0, \\ w^2 - w + 2x - y + z - 3 = 0. \end{cases}$$

Решением первой системы, 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 временем 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.

Рассмотрим проблему нахождения универсального алгоритма для распознавания разрешимости диофантовых уравнений.

Часть переменных в диофантовом уравнении выделим в качестве параметров и перепишем уравнение в виде $p(\mathbf{a}, \mathbf{x}) = 0$, т.е.

$$p(\mathbf{a}, x_1, \dots, x_m) = 0, \quad (7)$$

где параметр \mathbf{a} в общем случае является векторным, $\mathbf{a} = \langle a_1, \dots, a_k \rangle$. Причем все a_i и x_j являются положительными целыми числами.

Множество A положительных векторов $\mathbf{a} = \langle a_1, \dots, a_k \rangle$ называется **диофантовым**, если при любом $\mathbf{a} \in A$ и только при $\mathbf{a} \in A$ уравнение (7) разрешимо в целых положительных x_1, \dots, x_m .

Требование положительности переменных, вообще говоря, не принципиально и связано с техническими причинами. Отрицательные коэффициенты полинома $p(\mathbf{a}, \mathbf{x}) = 0$ при этом не исключены, например

$$p(z_1, z_2) = z_1^5 - 4z_1z_2^3 + 32,$$

т.е. минусы берет на себя запись полинома.

Пример 3. Множество всех составных чисел является диофантовым – достаточно взять полином $p(a, x_1, x_2) \equiv a - (x_1 + 1)(x_2 + 1)$.

С виду определение устанавливает жесткие ограничения, и кажется маловероятным, что диофантовыми будут сколько-нибудь нетривиальные множества.

Можно дать эквивалентное определение диофантовых множеств.

¹²⁰ Диофант Александрийский – древнегреческий математик.

Теорема 5. Множество A натуральных чисел является диофантовым тогда и только тогда, когда оно является множеством всех положительных значений некоторого полинома с целыми коэффициентами при натуральных значениях переменных.

Доказательство. Если множество A является множеством всех положительных значений некоторого полинома $p(x_1, \dots, x_k)$, то уравнение

$$a - p(x_1, \dots, x_k) = 0$$

определяет A как диофантово.

Обратно. Пусть A – множество тех положительных a , при которых диофантово уравнение

$$q(a, x_1, \dots, x_k) = 0$$

разрешимо. Тогда A – множество положительных значений полинома

$$a [1 - (q(a, x_1, \dots, x_k))^2]. \blacksquare$$

За двадцать лет усилиями многих математиков (последнюю точку в доказательстве поставил советский математик Юрий Матиясевич) в 1970 г. получен неожиданный результат:

Теорема 6 [81]. Диофантовость множества равносильна его перечислимости¹²¹.

В частности, любое множество положительных целых чисел, являющееся результатом работы некоторого алгоритма, может быть получено при нахождении положительных значений некоторого полинома.

Пример 4. Числа Фибоначчи порождаются положительными значениями многочлена пятой степени от двух переменных:

$$2a^4b + a^3b^2 - 2a^2b^3 - a^5 - ab^4 + 2a.$$

Но данный многочлен бесполезен для практических вычислений. Это нетрудно утврдить. Возьмем значения переменных a и b от 1 до 1000 и получим миллион значений многочлена, из которых наибольшее число равно 1 080 971 238 104 521, а неповторяющихся чисел будет 999 135. Но если удалить все отрицательные значения многочлена, то останется всего 16 первых чисел Фибоначчи.

Так как множество простых чисел перечислимо, то оно диофантово. Найдено несколько соответствующих многочленов для этого множества. Например, множество простых чисел порождают положительные значения следующего полинома от 26 переменных от a до z степени 25 [14]:

$$\begin{aligned} (k+2)\{ &1 - [n+l+v-y]^2 - \\ &[wz+h+j-q]^2 - \\ &[ai+k+1-l-i]^2 - \\ &[2n+p+q+z-e]^2 - \\ &[(a^2-1)l^2+1-m^2]^2 - \\ &[(a^2-1)y^2+1-x^2]^2 - \\ &[(gk+2g+k+1)(h+j)+h-z]^2 - \\ &[e^3(e+2)(a+1)^2+1-o^2]^2 - \\ &[16r^2y^4(a^2-1)+1-u^2]^2 - \\ &[z+pl(a-p)+t(2ap-p^2-1)-pm]^2 - \\ &[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2 - \\ &[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2 - \\ &[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2 - \\ &[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2 \}. \end{aligned}$$

¹²¹ См. главу 8.

Если каждую квадратную скобку приравнять нулю, получится система из 14 полиномиальных уравнений. Извлекая из ее положительных решений $\{a, b, \dots, z\}$ значения k , получаем список простых чисел $v = k + 2$, но в крайне запутанном порядке. И здесь такая же ситуация с получением простых чисел, как в примере 4.

Насколько сложны полиномы, описывающие нетривиальные множества?

Каждый полином характеризуется (суммарной) степенью n и числом m переменных x . Для любого диофанта множества A можно указать полином с $n \leq 4$ (но, возможно, большим m) либо $m \leq 9$ (но, может быть, большим n). Чисел n и m порядка двух-трех десятков, как правило, достаточно для самых сложных случаев.

После того как были получены результаты:

- о существовании перечислимого, но не разрешимого множества (см. теорему 14 в главе 8);
- перечислимость множеств равносильна их диофантовости, сразу последовало отрицательное решение 10-й проблемы Гильберта [82]:

Теорема 7. Существует такой полином $P(x_1, x_2, \dots, x_k)$, что неразрешимость уравнения $P(x_1, x_2, \dots, x_k) - y = 0$ по x_1, x_2, \dots, x_k при некоторых положительных y алгоритмически непроверяется.

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) [15].

Задачи

Задача 1. Покажите, что $\text{uncurry}(\text{curry } E) = E$.

Задача 2. Пусть F – комбинатор неподвижной точки и $F_1 \equiv F(\lambda y. f(f(yf)))$. Докажите, что F_1 – также комбинатор неподвижной точки, т.е. для любого E имеем $F_1 E = E (F_1 E)$.

Задача 3. Пусть Y – комбинатор неподвижной точки и $Y^0 \equiv Y, Y^{n+1} \equiv (Y^n) (SI)$. Докажите, что все термы Y^0, Y^1, Y^2, \dots – комбинаторы неподвижной точки.

Задача 4 [38. С. 156]. Пусть $L \equiv \lambda abcde\bar{f}ghijklmnpqrstuvwxyz.r$ (*this is a fixed point combinator*) и $\$ \equiv LLLLLLLLLLLLLLLLLL$. Докажите, что $\$$ – комбинатор неподвижной точки. Переведите пример на русский язык (так, чтобы в терме читалась русская фраза с аналогичным значением, а алфавит, в отличие от латинского, присутствовал бы в неизменном порядке).

Задача 5. Определим нумералы следующим образом: $(M, N) \equiv \lambda z. zMN, \langle 0 \rangle \equiv I, \langle n+1 \rangle \equiv (\text{false}, \langle n \rangle)$. Пусть $S^+ \equiv \lambda x. (\text{false}, x), P^- \equiv \lambda x. x \text{ false}, \text{zero} \equiv \lambda x. x \text{ true}$. Доказать, что $S^+ \langle n \rangle = \langle n+1 \rangle, P^- \langle n+1 \rangle = \langle n \rangle, \text{zero} \langle 0 \rangle = \text{true}, \text{zero} \langle n+1 \rangle = \text{false}$.

Задача 6. Докажите, что нумералы Чёрча можно представить с помощью основных комбинаторов в следующем виде: $\langle n \rangle = (SB)^n(KI)$.

Задача 7. Пусть $V \equiv \lambda xy. ux$. Докажите для нумералов Чёрча, что $V \langle 2 \rangle \langle 2 \rangle = \langle 4 \rangle$.

Задача 8. Пусть $C \equiv \lambda fgx. fgx$ и $\langle n \rangle$ – нумерал Чёрча. Докажите, что $\langle 2n+1 \rangle C = C$ и $\langle 2n \rangle C = I$ для натуральных n . Используйте математическую индукцию.

Задача 9. Пусть $Y_M \equiv \lambda f. WWM$, где $W \equiv \lambda xz. f(xxz)$. Доказать, что для каждого терма M терм Y_M – комбинатор неподвижной точки.

Задача 10. Пусть $B \equiv \lambda fgx. f(gx)$. Доказать, что для любых нумералов Чёрча $\langle m \rangle$ и $\langle n \rangle$ имеет место равенство $B \langle m \rangle \langle n \rangle = B \langle n \rangle \langle m \rangle$.

Задача 11. Докажите для нумералов Чёрча ($m > 0$), что $\langle m \rangle \langle n \rangle = \langle n^m \rangle$. Используйте математическую индукцию по m .

Задача 12. Пусть $W \equiv \lambda xy. x y y$. Докажите, что для нумералов Чёрча имеет место равенство $\langle n \rangle Wxy = x y \dots y$ (терм y повторяется $n+1$ раз). Используйте математическую индукцию.

Задача 13. Пусть $K \equiv \lambda xy. x$. Докажите, что для нумералов Чёрча имеет место равенство $\langle n \rangle K x_1 x_2 \dots x_{n+1} = x_1$ ($n > 0$). Используйте математическую индукцию.

Задача 14. Пусть $B \equiv \lambda f g x. f(gx)$ и $C \equiv \lambda f g x. f x g$. Докажите, что для нумералов Чёрча при $n > 0$ имеем $\langle n \rangle BC f x_1 x_2 \dots x_{n+1} x_{n+2} = f x_1 x_2 \dots x_{n+2} x_{n+1}$ (последние два аргумента меняются местами). Используйте математическую индукцию.

Задача 15. Пусть $B \equiv \lambda f g x. f(gx)$. Доказать, что для любого нумерала Чёрча при $n > 0$ имеет место равенство $\langle n \rangle B f g x_1 \dots x_n = f(g x_1 \dots x_n)$. ($\langle n \rangle B f g$ – аналог композиции функций f и g , когда g имеет n аргументов.) Используйте математическую индукцию.

Задача 16. Пусть $B \equiv \lambda f g x. f(gx)$ и $W \equiv \lambda xy. x y y$. Доказать, что для любого нумерала Чёрча при $n > 0$ имеет место равенство $\langle n \rangle BW f x_1 \dots x_n x_{n+1} = f x_1 \dots x_n x_{n+1} x_{n+1}$ (удваивается последний аргумент). Используйте математическую индукцию.

Задача 17. Пусть $B \equiv \lambda f g x. f(gx)$ и $K \equiv \lambda xy. x$. Доказать, что для любого нумерала Чёрча имеет место равенство $\langle n \rangle BK f x_1 \dots x_n x_{n+1} = f x_1 \dots x_n$ (удаляется последний аргумент). Используйте математическую индукцию.

Задача 18. Пусть $B \equiv \lambda f g x. f(gx)$. Доказать, что для любого нумерала Чёрча при $n > 0$ имеет место равенство $\langle n \rangle BB f x_1 \dots x_n x_{n+1} x_{n+2} = f x_1 \dots x_n (x_{n+1} x_{n+2})$. Используйте математическую индукцию.

Задача 19. Пусть N есть комбинатор со свойством $N fghx = f(gx)(hx)$. Доказать, что при $n > 0$ имеет место $\langle n \rangle N fgh x_1 \dots x_n = f(g x_1 \dots x_n)(h x_1 \dots x_n)$.

Задача 20. Доказать, что для любого нумерала Чёрча имеет место равенство $\langle n \rangle (BK) f x_1 \dots x_{n+1} = f x_1$.

Задача 21. Пусть $Z_1 \equiv S(KI)$ и для $n > 1$ положим $Z_{n+1} \equiv S(KZ_1)(S(KZ_n))$. Докажите, что для любого $n > 1$ комбинатор $Z_n = I$.

У логики один недостаток: она не останавливается на полпути.
Д. Уиндем. День триффиодов

Глава 11. Теоремы Гёделя о неполноте

Можно ли доказать все математические истины? – Нет. Даже для всех арифметических истин это невозможно. Оказывается, что не любая формула, истинная в стандартной интерпретации формальной арифметики, выводима из аксиом теории PA . В этом заключается основное содержание первой теоремы Гёделя о неполноте формальной арифметики.

§ 1. Гёделева нумерация

Продолжим рассмотрение теории формальной арифметики PA , начатое в примере 6 главы 5 и в § 6 главы 6. Мы будем рассматривать теорию PA только в стандартной интерпретации.

Как можно трактовать в теории PA операцию возведения в степень, если соответствующего символа в языке теории нет? Другой вопрос, мы пишем формулы, заменяющие в PA интуитивно понимаемые предикаты вроде « x – простое число»:

$$\langle\langle 1 < x \rangle\rangle \& \neg \exists y \exists z (\langle\langle y < x \rangle\rangle \& \langle\langle z < x \rangle\rangle \& x = y \times z).$$

Какие требования мы должны предъявлять к такого рода формулам? Если кто-то предлагает формулу и утверждает, что она «выражает» то-то и то-то, как это проверить?

Множество $A \subseteq \mathbb{N}^k$ называется **арифметическим**, если существует формула $F(x_1, x_2, \dots, x_k)$ языка PA , которая его представляет в следующем смысле: кортеж $\langle n_1, n_2, \dots, n_k \rangle$ принадлежит множеству A тогда и только тогда, когда формула F истинна при значениях параметров $x_1 = n_1, x_2 = n_2, \dots, x_k = n_k$.

Теорема 1. График любой вычислимой функции является арифметическим множеством.

Доказательство теоремы в [47. С. 122–124] использует формализацию вычислимости с помощью машин Тьюринга.

Следствие. Любое перечислимое множество A является арифметическим.

Доказательство. Пусть множество $A \subseteq \mathbb{N}^k$ перечислимо, тогда, очевидно, множество $Q = \{\langle x_1, x_2, \dots, x_k, 0 \rangle \mid \{\langle x_1, x_2, \dots, x_k \rangle \in A\}\}$ является графиком вычислимой постоянной функции $\langle x_1, x_2, \dots, x_k \rangle \rightarrow 0$ и, следовательно, представляется арифметической формулой $F(x_1, x_2, \dots, x_k, y)$. Тогда множество A является арифметическим, так как представляется формулой

$$\exists x_1 \exists x_2 \dots \exists x_k F(x_1, x_2, \dots, x_k, 0). \blacksquare$$

Каждое одноместное отношение (свойство) натуральных чисел определяет некоторое множество натуральных чисел, а именно состоящее из чисел, обладающих данным свойством. Очевидно, множество различных формул в теории первого порядка является счетным. С другой стороны, множество всех подмножеств, составленных из натуральных чисел, имеет мощность больше счетного (теорема Кантора), отсюда следует, что существуют свойства натуральных чисел, невыразимые в PA , и существуют неарифметические множества натуральных чисел. Пример такого множества дает теорема 2 в конце данного параграфа.

Таким образом, мы теперь знаем, какие свойства натуральных чисел и отношений между ними выражаются формулами формальной арифметики. Но как выразить в теории PA , что данная конечная последовательность формул является логическим выводом

некоторой формулы **PA**? Предложение, утверждающее, что некоторая последовательность формул образует (или не образует) вывод некоей формулы, уже не является доказательством в самой этой формальной системе. Это утверждение о системе; такие утверждения обычно называют **метаматематическими**. Необходимо тщательно различать математические и метаматематические рассуждения. Нарушение этого условия приводит к парадоксам.

У Курта Гёделя возникла великая идея **арифметизации метаматематики**, т.е. замены утверждений о формальной системе эквивалентными высказываниями о натуральных числах с последующим выражением этих высказываний в формальной системе. Идея арифметизации стала ключом к решению многих важных проблем математической логики.

Пусть дана произвольная теория первого порядка T . Пусть множество S есть объединение $A \cup B \cup F \cup D$, где A, B, F суть соответственно множества символов алфавита, термов и формул теории T ; D – множество всех конечных последовательностей формул теории T .

Арифметизацией данной теории первого порядка мы называем всякую инъективную вычислимую функцию $h: S \rightarrow \mathbb{N}$. При этом требуется, чтобы обратное частичное отображение $h^{-1}: \mathbb{N} \rightarrow S$ было вычислимым. Про функцию h говорят, что она осуществляет **кодирование** теории T , а значение функции h для элемента $x \in S$ называется **гёделевым номером (кодом)** соответствующего объекта x .

Существуют различные способы построения гёделевых номеров для системы **PA** [83. С. 151–152]. Изложим одну из возможных гёделевых нумераций. Рассмотрим алфавит теории **PA**. Выберем 10 основных символов этого алфавита: **0**, S , $($, $)$, $+$, \times , \supset , \neg , \forall и $=$. Другие логические связки можно выразить через \supset , \neg и \forall . Например, $A \vee B \equiv \neg A \supset B$, а $\exists x A(x) \equiv \neg \forall x \neg A(x)$.

Таким образом, основной символ алфавита получает в качестве гёделева номера число, не превосходящее 10. Например, соответствие может быть задано таблицей:

0	S	$($	$)$	$+$	\times	\supset	\neg	\forall	$=$
1	2	3	4	5	6	7	8	9	10

Предметным переменным сопоставляются простые числа, большие 10 (скажем, x получает номер 11, y – номер 13 и т.д.).

Язык теории **PA** (как и любой язык теории первого порядка) можно расширить, введя новые функциональные символы и константы, которые «доказуемо выражимы» в языке. Это просто формальный вариант «введения новых обозначений». Их добавление к алфавиту сокращает формульные выводы и записи формул, но не увеличивает множество выводимых формул¹²².

Формула получает номер по правилу, которое лучше всего пояснить на примере. Рассмотрим формулу $\forall x (x \times S(0) = x)$, которая утверждает, что число не меняется при умножении на 1. Эта формула содержит 12 символов, причем некоторые из них (скажем, x) входят несколько раз. Возьмем первые 12 простых чисел, возведем каждое из них в степень, равную номеру соответствующего символа, и перемножим полученные числа. Найденное так число

$$2^9 \times 3^{11} \times 5^3 \times 7^{11} \times 11^6 \times 13^2 \times 17^3 \times 19^1 \times 23^4 \times 29^{10} \times 31^{11} \times 37^4 = \\ = 3512466963791134964962551783462053411408361516343794496506561501312862272000$$

и будет гёделевым номером этой формулы.

¹²² Если мы расширяем язык, добавляя счетное число новых функциональных символов, то нумерацию символов алфавита меняем следующим образом: предметным переменным сопоставляются простые числа, большие 10 и имеющие вид $3n + 1$, а новым функционаторам сопоставляются простые числа, большие 10 и имеющие вид $3n + 2$.

Последовательность формул (которая может составлять доказательство) F_1, F_2, \dots, F_m получает гёделевый номер

$$2^{G_1} \times 3^{G_2} \times \dots \times p_m^{G_m},$$

где p_m есть m -е простое число, а G_1, G_2, \dots – гёделевы номера соответственно формул F_1, F_2, \dots .

Таким образом, каждой формуле или последовательности формул ставится в соответствие единственное натуральное число. Не всякое натуральное число является гёделевым номером, но всякий гёделевый номер однозначно определяет соответствующее выражение. Это следует из теоремы 7 главы 7 о единственности разложения на простые множители.

Оказывается, функцию, осуществляющую гёделеву нумерацию формул элементарной арифметики, можно сделать даже примитивно-рекурсивной (каковой она и была у Гёделя).

Заметим, что метаматематическое утверждение « $\forall x$ есть начальная часть формулы $\forall x (x \times S(0) = x)$ » отражается внутрь теории, переходя в чисто арифметическое предложение «гёделевый номер выражения $\forall x$, равный $2^9 \times 3^{11}$, является делителем гёделевого номера полной формулы».

Обещанный пример неарифметического множества дает следующая теорема.

Теорема 2 (теорема Тарского¹²³) [83. С. 168]. Множество гёделевых номеров замкнутых формул теории PA , истинных в стандартной интерпретации, не является арифметическим множеством. Грубо говоря, понятие арифметической истины арифметически неопределимо.

§ 2. Первая теорема Гёделя о неполноте: семантическая версия

Первая теорема Гёделя о неполноте формальной арифметики имеет две версии: семантическую и синтаксическую.

Семантическая версия говорит, что если теория PA непротиворечива, то существует истинная формула¹²⁴ в стандартной интерпретации PA , но она является недоказуемой в PA .

Синтаксическая версия утверждает, что если теория PA непротиворечива, то существует такая формула A , что ни сама A и ни отрицание $\neg A$ не имеют доказательства в теории PA .

Сам Курт Гёдель доказал синтаксическую версию теоремы [9]. Идея его доказательства основывается на парадоксе лжеца (см. главу 1, § 3) и работает также и в семантической версии. Парадокс заключается в следующем: истинно или ложно высказывание «Высказывание, которое я сейчас произношу, ложно»? Оно не может быть ни истинным, ни ложным. Гёдель нашел формулу, высказывающую недоказуемость самой себя. Легко понять, что эта формула истинна, но недоказуема. В самом деле, если бы она была доказуема, то утверждение, которое она выражает, было бы истинным. Утверждение же это состоит в её недоказуемости. Следовательно, она недоказуема. Значит, формула, высказывающая эту недоказуемость (т.е. она сама) истинна. Вот мы вслед за Гёделем и нашли истинную, но недоказуемую формулу.

Утверждение об арифметичности любого перечислимого множества помогает избавиться от технических трудностей при доказательстве семантической версии. Мы приводим доказательство В.А. Успенского [107].

Теорема 3 (о неполноте PA : семантическая версия). Если теория PA непротиворечива, то существует истинная формула в стандартной интерпретации PA , но она является недоказуемой в PA .

¹²³ Альфред Тарский (1901–1983) – польско-американский математик, логик, философ.

¹²⁴ То, что формула является истинной, доказывается неформально.

Доказательство. Пусть для теории PA проведена арифметизация и каждая формула и каждое доказательство идентифицируются натуральными числами – гёделевыми номерами. Тогда множество всех формул и множество всех формальных доказательств (рассматриваемые как множества натуральных чисел) разрешимы, следовательно, перечислимы. Поэтому каждое из них можно без повторений расположить в вычислимую последовательность или, как говорят, перечислить без повторений.

Условимся об обозначениях. Пусть A – некоторая формула. Мы не должны забывать, что вместо свободных переменных формулы мы имеем право подставлять не числа, а нумералы – термы, обозначающие числа в теории PA . Поэтому через $A(r)$ обозначаем результат подстановки в формулу A нумерала r , обозначающего число r , вместо параметра x ; через $A(r, s)$ – результат подстановки в A нумералов r и s , обозначающих числа r и s , вместо параметров x и y ; через $A(r, s, t)$ – результат подстановки в A нумералов r , s и t , обозначающих числа r , s и t вместо параметров x , y и z .

1. Перечисляем без повторений все формулы:

$$C_1, C_2, C_3, \dots$$

2. Перечисляем без повторений все формальные доказательства:

$$\Gamma_1, \Gamma_2, \Gamma_3, \dots$$

3. Рассматриваем функцию g :

$$g(s) = t$$

тогда и только тогда, когда Γ_s есть доказательство формулы C_t .

Ясно, что функция g вычислима. Поэтому её выражает некоторая формула G с параметрами x и y . Когда, для каких пар чисел формула $G(s, t)$ истинна? Она истинна тогда только тогда, когда доказательство с номером s является доказательством формулы с номером t .

4. Для каждого числа t формула $\exists w G(w, t)$ означает доказуемость формулы C_t .

5. Для каждого числа t формула $\neg \exists w G(w, t)$ означает недоказуемость формулы C_t .

6. Перечисляем без повторений все открытые формулы с параметром x :

$$A_1, A_2, A_3, \dots$$

7. Рассматриваем функцию f :

$$f(m, n) \text{ есть номер формулы } A_m(n).$$

Ясно, что f – вычислимая функция. Поэтому её выражает некоторая формула F с параметрами x , y и z . Когда для каких троек чисел формула $F(m, n, p)$ истинна? Она истинна тогда и только тогда, когда p есть номер формулы $A_m(n)$.

8. Для чисел e, m, n формула

$$\exists u (G(e, u) \& F(m, n, u))$$

означает, что число e есть номер доказательства формулы $A_m(n)$, имеющей номер $f(m, n)$.

9. Для чисел m, n формула

$$\neg \exists w \exists u (G(w, u) \& F(m, n, u))$$

означает недоказуемость формулы $A_m(n)$, имеющей номер $f(m, n)$.

10. Для каждого числа n формула

$$\neg \exists w \exists u (G(w, u) \& F(n, n, u))$$

означает недоказуемость формулы $A_n(n)$, имеющей номер $f(n, n)$.

11. Теперь рассматриваем формулу

$$\neg \exists w \exists u (G(w, u) \& F(x, x, u))$$

с параметром x . Эта формула есть A_q при некотором q .

12. В силу п. 7 формула $A_q(q)$, т.е. формула

$$\neg \exists w \exists u (G(w, u) \& F(q, q, u)),$$

имеет номер $f(q, q)$.

13. В силу п. 10 формула

$$\neg \exists w \exists u (G(w, u) \& F(q, q, u))$$

означает недоказуемость формулы с номером $f(q, q)$.

14. Сравнивая п. 12 и 13, убеждаемся, что присутствующая в них формула (одна и та же!) означает недоказуемость самой себя. Построение закончено. ■

§ 3. Первая теорема Гёделя о неполноте: синтаксическая версия

В синтаксической версии теоремы о неполноте вместо истинности формул используется понятие доказуемости формул.

Последовательно сформулируем необходимые понятия и докажем необходимые леммы, чтобы, следуя идеям Гёделя, получить доказательство синтаксической версии теоремы.

Если в семантической версии в доказательстве применяется понятие арифметического множества, то в доказательстве Гёделя применяется понятие выразимого предиката.

Предикат $R(x_1, \dots, x_n)$, определенный на натуральных числах, называется **выразимым** в \mathbf{PA} , если существует формула $A(x_1, \dots, x_n)$ теории \mathbf{PA} с n свободными переменными, такая что для любых натуральных чисел k_1, \dots, k_n выполнено:

- 1) если $R(k_1, \dots, k_n)$ истинно, то $\vdash A(k_1, \dots, k_n)$;
- 2) если $R(k_1, \dots, k_n)$ ложно, то $\vdash \neg A(k_1, \dots, k_n)$.

В данном случае мы рассматриваем доказуемость в теории \mathbf{PA} .

Существенной частью доказательства Гёделя является следующее утверждение об арифметике Пеано.

Теорема 4 [83. С. 134]. Предикат $R(x_1, \dots, x_n)$ выразим в \mathbf{PA} тогда и только тогда, когда множество $X = \{ \langle k_1, \dots, k_n \rangle \mid R(k_1, \dots, k_n) \}$ истинных значений предиката R разрешимо.

Из определения разрешимости множества (глава 8, § 2) следует, что характеристическая функция выразимого предиката $R(x_1, \dots, x_n)$

$$\chi_R(\langle k_1, \dots, k_n \rangle) = \begin{cases} 1, & \text{если } R(k_1, \dots, k_n) = \text{И}, \\ 0, & \text{если } R(k_1, \dots, k_n) = \text{Л} \end{cases}$$

является вычислимой. Вслед за множеством X предикат R также называется **разрешимым**.

Гёдель в своей теореме требовал от теории \mathbf{PA} более сильное условие, чем непротиворечивость. Он назвал это условие ω -непротиворечивостью.

Определение ω -непротиворечивости. Говорят, что арифметика Пеано является **ω -непротиворечивой**, если следующие два условия не выполняются вместе ни для какой формулы φ :

- (i) $\vdash \exists y \varphi(y)$;
- (ii) $\vdash \neg \varphi(0), \vdash \neg \varphi(1), \vdash \neg \varphi(2), \dots$.

Если теория \mathbf{PA} противоречива, то она и ω -противоречива, поскольку в противоречивой теории доказывается все, что угодно. Сам Гёдель не пытался освободиться от условия ω -непротиворечивости.

Следуя Гёделю, проведем арифметизацию теории \mathbf{PA} , тогда предикат $\text{Provable}(n, m)$: «формула с гёделевым номером n является доказуемой в \mathbf{PA} и ее доказательство имеет номер

m » является разрешимым. Следовательно, по теореме 4 предикат $\text{Provable}(n, m)$ выражим в PA некоторой формулой $\text{Pr}(x, y)$, т.е.:

- 1) если $\text{Provable}(n, m)$ истинно, то $\vdash \text{Pr}(\mathbf{n}, \mathbf{m})$,
- 2) если $\text{Provable}(n, m)$ ложно, то $\vdash \neg \text{Pr}(\mathbf{n}, \mathbf{m})$.

Формула $P(\mathbf{n}) \equiv \exists y \text{Pr}(\mathbf{n}, y)$ выражает свойство «формула с гёделевым номером n является доказуемой в PA ».

Введем новое обозначение. Если M является выражением (термом, формулой, доказательством) с гёделевым номером n , то определим $\lceil M \rceil$ как нумерал \mathbf{n} . Тогда если A – формула PA , то формула $P(\lceil A \rceil)$ выражает свойство «формула A доказуема в PA ». Или если теперь для некоторых формул $B(x)$ и A удается установить, что $\vdash B(\lceil A \rceil)$, то можно сказать: в теории PA доказано, что формула A «обладает свойством B ».

Замечание 1. Гёделеву нумерацию PA можно провести таким образом, что для любой формулы A из $\vdash A$ следует $\vdash P(\lceil A \rceil)$ [102. С. 15].

В формальной арифметике PA некоторые функции представимы формулами в следующем смысле [44. С. 214].

Функция $f(x_1, \dots, x_n)$ с натуральными аргументами и значениями называется **представимой** в PA , если существует формула $A(x_1, \dots, x_n, y)$ формальной арифметики со свободными переменными x_1, \dots, x_n, y , такая что для любых натуральных чисел k_1, \dots, k_n, m из равенства $f(k_1, \dots, k_n) = m$ следует

$$\vdash \forall y ((\mathbf{m} = y) \sim A(k_1, \dots, k_n, y)). \quad (1)$$

В этом случае формула $A(x_1, \dots, x_n, y)$ называется **представляющей** функцию f в PA .

Теорема 5 [83. С. 158]. Функция $f: \mathbb{N}^n \rightarrow \mathbb{N}$ представима в PA тогда и только тогда, когда f вычислима.

Определим понятие диагонализации. Пусть B – формула теории PA со свободной переменной x . Назовем **диагонализацией** формулы B формулу $C \equiv \exists x (x = \lceil B \rceil \& B)$.

Лемма 1. Существует вычислимая функция d , такая что если n – гёделевый номер формулы B , то $d(n)$ – гёделевый номер формулы C – диагонализации формулы B .

Доказательство. Для произвольного натурального числа m определим $d(m)$ как гёделевый код формулы

$$\exists x (x = \mathbf{m} \& B).$$

Функция d вычислима. Действительно, зная m , можно алгоритмически построить нумерал \mathbf{m} . Далее гёделевый код формулы $\exists x (x = \mathbf{m} \& B)$ вычисляется в соответствии с определением арифметизации теории. Если теперь в качестве аргумента функции d взять код n формулы B , то значение функции $d(n)$ равно коду формулы C . ■

Лемма 2 (о рефлексии или о диагонализации). Пусть B – формула теории PA со свободной переменной x . Тогда существуют такая формула G , что

$$\vdash G \sim B(\lceil G \rceil)$$

в теории PA .

Доказательство. Пусть d – функция из леммы 1. Вычислимые функции представимы в теории PA (теорема 4), поэтому существует формула $D(x, y)$ такая, что если для любых m и k имеем $d(m) = k$, то

$$\vdash \forall y (D(\mathbf{m}, y) \sim y = \mathbf{k})$$

в теории PA .

Определим формулу

$$F(x) \equiv \exists y (D(x, y) \& B(y)).$$

Пусть s – гёделев номер формулы F . Определим замкнутую формулу

$$G \equiv \exists x (x = s \& F(x)) \equiv \exists x (x = s \& \exists y (D(x, y) \& B(y))).$$

Так как G логически эквивалентно

$$\exists y (D(s, y) \& B(y)),$$

то имеем

$$\vdash G \sim \exists y (D(s, y) \& B(y)).$$

Формула G является диагонализацией формулы F . Пусть k – гёделевый номер формулы G . Имеем

$$\vdash \forall y (D(s, y) \sim y = k).$$

Значит,

$$\vdash G \sim \exists y (y = k \& B(y)).$$

Следовательно,

$$\vdash G \sim B(k).$$

То есть имеем

$$\vdash G \sim B(\lceil G \rceil). \blacksquare$$

Хотя Гёдель не использовал лемму о рефлексии в явном виде, но её частный случай присутствует в его доказательстве.

Теорема 6 (неполнота PA : синтаксическая версия с ω -непротиворечивостью).

Существует замкнутая формула G языка PA , такая что:

- а) если G доказуема в PA , то теория PA противоречива,
- б) если $\neg G$ доказуема в PA , то теория PA ω -противоречива.

Доказательство. Как мы уже установили в этой параграфе, разрешимый предикат, выражающий свойство натуральных чисел «формула с гёделевым номером x является доказуемой в PA », выражим некоторой формулой $P(x)$. Мы собираемся воспользоваться леммой о рефлексии, и для этого определим формулу $B(x)$ как отрицание формулы $P(x)$. Тогда по лемме о рефлексии существует замкнутая формула G языка PA , такая что

$$\vdash G \sim \neg P(\lceil G \rceil). \quad (2)$$

Формула G «утверждает», что она недоказуема. Мы собираемся выяснить, доказуема или опровергнута формула G .

1. Предположим, что $\vdash G$. Используя замечание 1, получаем, что $\vdash P(\lceil G \rceil)$. Далее из (2), используя тавтологию $(\alpha \sim \beta) \supset (\neg \alpha \sim \neg \beta)$, получаем

$$\vdash \neg G \sim P(\lceil G \rceil). \quad (3)$$

Но (3) вместе с $\vdash P(\lceil G \rceil)$ дают $\vdash \neg \neg G$. Итак, если дано доказательство (средствами PA) для формулы G , то найдется также доказательство и для отрицания $\neg G$, т.е. теория PA окажется в таком случае противоречивой.

2. Предположим, что $\vdash \neg \neg G$. Тогда, так как $P(x) \equiv \exists y Pr(x, y)$ и согласно (2), имеем

$$\vdash \exists d Pr(\lceil G \rceil, d).$$

В нашем интуитивном понимании формула

$$\exists d Pr(\lceil G \rceil, d)$$

утверждает, что в PA существует доказательство формулы G . Это вроде бы опять должно означать, что теория PA противоречива. Не может ли случиться, однако, что, доказав средствами PA формулу

$$\vdash \exists d \Pr(\Gamma G], d),$$

мы, тем не менее, не в состоянии найти конкретное значение d ? Разве, перебирая подряд: 0, 1, 2, ..., мы не должны натолкнуться однажды на номер доказательства G ?

К сожалению, у нас нет достаточных оснований для такого заключения. Если мы найдем номер доказательства G , то теория PA окажется противоречивой. Но в этом случае теория PA будет и ω -противоречивой.

Но если не найдем? Тогда никакое n не будет номером PA -доказательства формулы G , т.е. для любого n : $\vdash \neg \Pr(\Gamma G], n)$. С другой стороны, мы знаем, что $\vdash \exists d \Pr(\Gamma G], d)$. Противоречие? Не совсем, поскольку формула $\exists d \Pr(\Gamma G], d)$ противоречит на самом деле формуле $\forall d \neg \Pr(\Gamma G], d)$, но ее мы еще не доказали в PA . Все, что мы пока имеем, это бесконечная серия отдельных доказательств: для $\neg \Pr(\Gamma G], 0)$, для $\neg \Pr(\Gamma G], 1)$, $\neg \Pr(\Gamma G], 2)$ и т.д. Можем ли мы надеяться свернуть всю серию в единое конечное PA -доказательство формулы $\forall d \neg \Pr(\Gamma G], d)$? До сих пор это никому не удалось.

Если положить $\varphi(y) \equiv \Pr(\Gamma G], y)$, то одновременно выполнено:

$$\begin{aligned} &\vdash \exists y \varphi(y); \\ &\vdash \neg \varphi(0), \vdash \neg \varphi(1), \vdash \neg \varphi(2), \dots, \end{aligned}$$

что означает ω -противоречивость формальной арифметики. ■

Напомним общепринятый термин. Замкнутую формулу F из языка теории первого порядка T называют **неразрешимой в T** , если ни F , и ни $\neg F$ не имеют логического вывода в теории T .

Теорема 6 утверждает, что теория PA или ω -противоречива, или имеет неразрешимую формулу.

Бог существует,
поскольку Арифметика непротиворечива.
Дьявол существует,
поскольку мы не можем доказать это¹²⁵.
*Андре Вейль*¹²⁶

§ 4. Обобщения и вторая теорема Гёделя

Понятие ω -противоречивости несколько «портит» формулировку теоремы 6. Первым от этого понятия освободился Б. Россер в 1936 г. Если неразрешимая формула Гёделя «говорит» о своей недоказуемости, то неразрешимая формула Россера «утверждает» о себе: «для каждого доказательства меня существует более короткое доказательство отрицания меня».

В настоящее время, используя теорию вычислимости, получены более простые доказательства первой теоремы Гёделя о неполноте. Рассмотрим одно из таких доказательств, в которых не требуется ω -непротиворечивость PA .

Замечание 2. Представимость функции $f(x)$ формулой $F(x, y)$ в PA означает: для любых натуральных чисел m и n , если $f(m) = n$, то

¹²⁵ Раймонд Смаллиан [97. С. 136]: «Это остроумное изречение хотя и восхитительно, на самом деле вводит в заблуждение. Дело не в том, что мы не можем доказать непротиворечивость Арифметики, а в том, что эта Арифметика не может доказать непротиворечивость Арифметики! Мы определенно можем доказать непротиворечивость Арифметики, но наше доказательство не может быть formalизовано в самой Арифметике».

¹²⁶ Андре Вейль (1906–1998) – французский математик.

$$\vdash \forall y ((\mathbf{n} = y) \sim A(\mathbf{m}, y)).$$

Но это утверждение эквивалентно двум условиям:

- 1) для любых чисел m и n , если $f(m) = n$, то $\vdash F(\mathbf{m}, \mathbf{n})$;
- 2) для любых чисел m , n_1 и n_2 , если $\vdash F(\mathbf{m}, \mathbf{n}_1)$ и $\vdash F(\mathbf{m}, \mathbf{n}_2)$, то $\vdash (\mathbf{n}_1 = \mathbf{n}_2)$.

Лемма 3. Пусть формула $F(x, y)$ представляет функцию f , и пусть числа m и n таковы, что f определена на m и $f(m) \neq n$. Тогда, если теория полна, то $\vdash \neg F(\mathbf{m}, \mathbf{n})$.

Доказательство. Поскольку f определена на m , то для некоторого числа p , отличного от n , будет $f(m) = p$. В силу п. 1 $\vdash F(\mathbf{m}, \mathbf{p})$. Если бы было $\vdash F(\mathbf{m}, \mathbf{n})$, то в силу п. 2 было бы $\vdash (\mathbf{n} = \mathbf{p})$. Но такое невозможно в силу $n \neq p$. Итак, формула $F(\mathbf{m}, \mathbf{n})$ недоказуема, а тогда, согласно предположению о полноте, доказуема формула $\neg F(\mathbf{m}, \mathbf{n})$. ■

Теорема 7 (неполнота PA: синтаксическая версия). Если теория PA непротиворечива, то она неполна.

Доказательство. Пусть теория PA непротиворечива. Доказательство неполноты теории проводим от противного.

Теорема 13 из главы 8 утверждает существование пары неотделимых перечислимых множеств натуральных чисел. Пусть (A, B) – такая пара. Рассмотрим функцию f , принимающую значение 0 на A , значение 1 на B и не определённую на остальных натуральных числах. Её график, как легко видеть, перечислим, поэтому она вычислима. Пусть $F(x, y)$ – какая-либо представляющая её формула. Положим

$$\begin{aligned} A^* &= \{n \mid \vdash F(n, 0)\}, \\ B^* &= \{n \mid \vdash \neg F(n, 0)\}. \end{aligned}$$

Множества A^* и B^* очевидным образом перечислимы. В силу непротиворечивости и полноты они взаимно дополнительны, а потому разрешимы. Если мы обнаружим, что 1) $A \subseteq A^*$ и 2) $B \subseteq B^*$, то A и B окажутся отделимыми. Утверждение 1 вытекает из утверждения 1 в замечании 2. Убедимся в справедливости утверждения 2. Если $m \in B$, то $f(m) = 1$. Беря 0 в качестве числа n в лемме 3, получаем $\vdash \neg F(m, 0)$, что приводит к (2). ■

Приведенное доказательство принадлежит В.А. Успенскому и Л.Д. Беклемишеву [107]. В статье [39] Л.Д. Беклемишев приводит другое доказательство синтаксического варианта теоремы Гёделя, используя также существование пары неотделимых перечислимых множеств натуральных чисел. Но вместо понятия *представимости функций* он использует понятие *представимости множеств*.

Современные доказательства первой теоремы Гёделя о неполноте часто используют существование пары неотделимых перечислимых множеств, как в доказательстве теоремы 7. Но доказательство самого Гёделя первой теоремы о неполноте, где он сумел сконструировать предложение теории PA , утверждающее, что оно недоказуемо в PA , сохранило свое значение в связи с доказательством второй теоремы о неполноте.

Теорема 8 (вторая теорема Гёделя о неполноте). Если формальная арифметика PA непротиворечива, то недоказуема в PA формула *Con*, выражающая непротиворечивость теории PA .

Доказательство. Приведем доказательство теоремы, опуская важную часть (см. п. 3 доказательства).

1. Сначала о существовании формулы *Con*. Рассмотрим арифметизацию PA и пусть x – гёделевый номер некоторой формулы A из теории PA . По свойствам кодирования формул, мы алгоритмически можем найти по номеру x саму формулу A , а потом вычислить гёделевый номер формулы $\neg A$. Таким образом, получаем вычислимую функцию *neg*(x), которая по номеру любой формулы выдает номер отрицания этой формулы. Поскольку *neg* – вычислимая функция, то по теореме 5 функция *neg* представима в PA некоторой формулой *Neg*(x_1, x_2).

Ранее в § 3 нами введен предикат $Prov\text{able}(x, y)$, истинный тогда и только тогда, когда x есть гёделевый номер некоторой формулы A теории \textbf{PA} , а y есть гёдельевый номер некоторого вывода A в \textbf{PA} . Как мы установили, предикат $Prov\text{able}(x, y)$ выражим в \textbf{PA} формулой $Pr(x_1, x_2)$.

Обозначим через Con формулу $\forall x \ y \ z \ w \ \neg(Pr(x, z) \ \& \ Pr(y, w) \ \& \ Neg(x, y))$. Содержательно, т.е. в соответствии со стандартной интерпретацией, Con выражает невозможность вывода в \textbf{PA} какой-либо формулы A (с кодом x) вместе с ее отрицанием $\neg A$ (с кодом y) и Con является истинной в том и только в том случае, когда теория \textbf{PA} непротиворечива. Иными словами, формулу Con можно интерпретировать как утверждение непротиворечивости теории \textbf{PA} .

2. Вспомним теперь, что в соответствии со стандартной интерпретацией гёделева неразрешимая формула G (теорема 6) содержательно выражает свою собственную невыводимость. Тогда формула $Con \supset G$ содержательно утверждает, что если теория \textbf{PA} непротиворечива, то формула G в ней невыводима. Но в этом и состоит первая часть теоремы 5 (первой теоремы Гёделя о неполноте).

3. Неформальные рассуждения, доказывающие теорему 5, могут быть выражены и проведены средствами теории \textbf{PA} , так что в результате оказывается возможным получить вывод формулы $Con \supset G$ в теории \textbf{PA} (см.: [83. С. 165]).

4. Итак, $\neg Con \supset G$. Согласно первой теореме Гёделя, однако, если теория \textbf{PA} непротиворечива, то формула G в ней невыводима. Отсюда следует, что если теория \textbf{PA} непротиворечива, то в ней невыводима и формула Con ; иными словами, если теория \textbf{PA} непротиворечива, то в ней невыводима некоторая формула, содержательно утверждающая непротиворечивость теории \textbf{PA} . ■

Неформально, вторая теорема о неполноте утверждает, что если теория формальной арифметики \textbf{PA} непротиворечива, то доказательство непротиворечивости теории не может быть проведено средствами самой теории \textbf{PA} , т.е. всякое такое доказательство обязательно должно использовать невыразимые в теории \textbf{PA} идеи или методы. Одно из таких доказательств непротиворечивости \textbf{PA} , предложенное К. Шютте¹²⁷, изложено в [Там же. С. 282–295].

Заметим, что в доказательстве теоремы 8 не требуется ω -непротиворечивость \textbf{PA} .

Наличие неразрешимых формул в \textbf{PA} , возможно, говорит о несовершенстве аксиом \textbf{PA} . С их помощью нельзя решить некоторые проблемы, касающиеся натуральных чисел (одна такая проблема выражена в формуле G – несмотря на все разговоры о том, что G «занимается» собственной доказуемостью, G – замкнутая формула в языке \textbf{PA} и как таковая выражает вполне определенное свойство натуральных чисел).

Несовершенную систему аксиом следует совершенствовать. Может быть, мы «забыли» какие-то важные аксиомы? Следует найти их, присоединить к аксиомам \textbf{PA} , и в результате мы получим, возможно, совершенную систему?

К сожалению, рассуждения К. Гёделя проходят и для любого расширения \textbf{PA} . Никакие новые аксиомы не могут привести к «совершенной» системе аксиом арифметики. Усовершенствованный метод Гёделя позволяет доказать *принципиальное* несовершенство всякой системы аксиом арифметики: каждая такая система неизбежно является либо противоречивой, либо недостаточной для решения некоторых проблем, касающихся свойств натуральных чисел.

Мы доказали теоремы Гёделя для теории \textbf{PA} . Формальная арифметика \textbf{PA} представляет простейший уровень математических рассуждений, в которых участвуют только целые числа (и не участвуют произвольные действительные числа, не говоря уже о произвольных множествах Кантора). Более сложные рассуждения формализуются более сложными (по сравнению с \textbf{PA}) формальными теориями. «Силу» этих более сложных теорий составляет,

¹²⁷ Курт Шютте (Kurt Schütte; 1909–1998) – немецкий математик.

прежде всего, их способность обсуждать более сложные объекты (действительные числа, функции действительных и комплексных переменных и т.д.), которые недоступны в PA .

Каким образом выделить в некоторой формальной теории T ту ее часть, которая относится к компетенции PA ? Этот вопрос решается очень естественно с помощью так называемых, **относительных интерпретаций**. Чтобы воспроизвести в теории T арифметику, прежде всего какие-то объекты из области значений переменных T должны быть объявлены натуральными числами. Это связано с выделением в языке T некоторой формулы $N(x)$ (с единственной свободной переменной x), которая «утверждает», что x является натуральным числом. Далее необходимо отобразить в теории T элементарные формулы PA , т.е. формулы вида $t_1 = t_2$, трактующие о значениях полиномов t_1, t_2 с натуральными коэффициентами.

Имея относительную интерпретацию PA в T , в теории T можно доказать любое свойство натуральных чисел, которое доказуемо в PA . Учитывая роль системы натуральных чисел в математике, формальную теорию, в которой относительно интерпретируема теория PA (и которая содержит в этом смысле полноценное понятие натурального числа), будем называть **фундаментальной теорией**. Простейшей из фундаментальных теорий является, конечно, сама теория PA .

Теоремы Гёделя оказываются справедливы для любой фундаментальной теории [102. С. 9–53].

Теорема 9 (первая теорема Гёделя в форме Россера). В языке всякой фундаментальной теории T найдется замкнутая формула R_T («выражающая» некоторое свойство натуральных чисел), такая что если $\vdash_T R_T$ или $\vdash_T \neg R_T$, то теория T противоречива.

Следствие. Так как теория множеств ZFC является фундаментальной, то справедливо утверждение: теория множеств ZFC неполна (при условии своей непротиворечивости).

В формулировке теоремы 9 сделано еще одно усиление теоремы о неполноте, не имеющее отношения к методу Россера. Сейчас речь идет о теории T с произвольным языком первого порядка, которая содержит в себе элементарную арифметику. Это освобождает нас от подозрений, что принципиальное несовершенство всякой системы аксиом арифметики кроется в неудачном выборе языка PA .

Теорема 10 (вторая теорема о неполноте в общем виде). Пусть Con – любая формула фундаментальной теории T , выражающая непротиворечивость теории T . Тогда формула Con не доказуема в теории T .

Замечание Л.Д. Беклемишева [39]. Речь в теореме 8 не идет о том, что непротиворечивость PA может вызывать сомнения, а лишь о том, что обоснование (очевидным образом) верного факта непротиворечивости PA требует допущений, выходящих за рамки этой теории. Ситуация менее очевидная с теорией ZFC : мы также верим в непротиворечивость ZFC , но предположения, на основании которых мы могли бы обосновать этот факт, не могут быть formalизованы внутри самой ZFC , т.е. должны выходить за рамки «обычной», общепринятой математики! Поэтому, в частности, в формулировке следствия из теоремы 8 сделана оговорка относительно условия о непротиворечивости ZFC .

Мы можем сформулировать «**Принцип несовершенства**» К. Гёделя:

Всякая фундаментальная теория несовершена – она либо противоречива, либо недостаточна для решения всех возникающих в ней проблем.

В частности, если бы удалось аксиоматизировать всю математику, то она была бы несовершенной.

Из теорем Гёделя вытекает следующий интересный факт. Согласно закону исключенного третьего, принятого в классической логике, $\vdash A \vee \neg A$ для любой формулы A . Однако следует ли отсюда, что если A – замкнутая формула, то либо $\vdash A$, либо $\vdash \neg A$? Если взять в качестве A неразрешимую формулу, то из первой теоремы Гёделя о неполноте

следует, что ни *PA*, ни какая-либо другая фундаментальная математическая теория этим идеальным свойством обладать не могут – несмотря на постулирование закона исключенного третьего в их аксиомах!

Р. Смаллиан во многих своих книгах, в том числе и популярных, рассматривает доказательство первой теоремы Гёделя о неполноте [25, 26, 28, 97–99], стараясь очистить доказательство от технических сложностей, и явно показать основные идеи, приводящие к неполноте теории.

Остановимся на одной такой интерпретации теоремы Гёделя, сделанной Смаллианом [97].

Задача. На острове рыцарей и лжецов каждый обитатель есть либо рыцарь, либо лжец. Рыцари могут делать только истинные утверждения, а лжецы – только ложные. Предположим, что на этом острове есть два клуба – Клуб 1 и Клуб 2. Только рыцарям позволяет быть членами любого из клубов, а лжецам строго запрещено быть членами любого из них. Также каждый рыцарь есть член одного и только одного из двух клубов. Вы однажды посещаете остров и встречаете незнакомого аборигена – жителя острова, который делает утверждение, из которого вы делаете вывод, что он должен быть членом Клуба 1. Какое утверждение сделал абориген, чтобы из него можно было сделать такой вывод?

Решение. Абориген мог произнести следующее: «Я не член Клуба 2». Если абориген – лжец, то он не является членом Клуба 2 и, следовательно, это утверждение было истинно. Поэтому абориген является рыцарем, и согласно своему утверждению, принадлежит Клубу 1.

Комментарий. Это задача воплощает в себе существенные идеи, лежащей в основе знаменитого гёделевого предложения, которое утверждает свою собственную недоказуемость в данной математической теории. Аналогия заключается в следующем:

- рыцари – это истинные утверждения математической теории;
- лжецы – ложные утверждения;
- рыцари из Клуба 2 – доказуемые истинные утверждения;
- рыцари из Клуба 1 – недоказуемые истинные утверждения.

Когда рыцарь говорит, что он не принадлежит Клубу 2, то это означает, что имеется некоторое истинное утверждение, говорящее о том, что оно недоказуемо.

§ 5. Теорема Гудстейна

Хотя неразрешимое самоссыльное утверждение Гёделя, несомненно, также говорит о каком-то свойстве натуральных чисел, математикам хотелось бы также обнаружить более «естественное» верное, но недоказуемое в арифметике Пеано утверждение. Одно из таких утверждений есть теорема Гудстейна.

Нам понадобится следующее представление натуральных чисел.

Наследственным представлением натурального числа называется его представление в виде суммы степеней с основанием b , причем показатели степени также представляются в виде суммы степеней числа b и т.д., пока процесс не остановится.

Например, наследственное представление 266 по основанию 2 есть

$$266 = 2^8 + 2^3 + 2 = 2^{(2+1)} + 2^{(2+1)} + 2.$$

Для данного наследственного представления числа n по основанию b пусть $F_b(n)$ – неотрицательное целое число, равное результату синтаксической замены в представлении n каждого b на $b+1$, т.е. F_b есть оператор замены b на $b+1$.

Так как $266 = 2^{(2+1)} + 2^{(2+1)} + 2$, то замена основания 2 на 3 дает

$$F_2(266) = 3^{(3+1)} + 3^{(3+1)} + 3.$$

В построении следующей последовательности повторяется применение оператора F_b с последующим вычитанием 1. Первые девять членов суть

$$\begin{aligned}
G_0(266) &= 266 = 2^{(2^{2+1})} + 2^{2+1} + 2. \\
G_1(266) &= F_2(266) - 1 = 3^{(3^{3+1})} + 3^{3+1} + 2 = \\
&= 443426488243037769948249630619149892886 \text{ (39 цифр).} \\
G_2(266) &= F_3(G_1(266)) - 1 = 4^{(4^{4+1})} + 4^{4+1} + 1 = \\
&= 3231700607\dots853611059596231681 \text{ (617 цифр).} \\
G_3(266) &= F_4(G_2(266)) - 1 = 5^{(5^{5+1})} + 5^{5+1} \text{ (10 922 цифры).} \\
G_4(266) &= F_5(G_3(266)) - 1 = 6^{(6^{6+1})} + 6^{6+1} - 1 = \\
&= 6^{(6^{6+1})} + 5 \cdot 6^6 + 5 \cdot 6^5 + \dots + 5 \cdot 6 + 5 \approx 4 \cdot 10^{217832}. \\
G_5(266) &= F_6(G_4(266)) - 1 = \\
&= 7^{(7^{7+1})} + 5 \cdot 7^7 + 5 \cdot 7^5 + \dots + 5 \cdot 7 + 4 \approx 10^{4871822}. \\
G_6(266) &= F_7(G_5(266)) - 1 = \\
&= 8^{(8^{8+1})} + 5 \cdot 8^8 + 5 \cdot 8^5 + \dots + 5 \cdot 8 + 3 \approx 2 \cdot 10^{121210686}. \\
G_7(266) &= F_8(G_6(266)) - 1 = \\
&= 9^{(9^{9+1})} + 5 \cdot 9^9 + 5 \cdot 9^5 + \dots + 5 \cdot 9 + 2 \approx 5 \cdot 10^{3327237896}. \\
G_8(266) &= F_9(G_7(266)) - 1 = \\
&= 10^{(10^{10+1})} + 5 \cdot 10^{10} + 5 \cdot 10^5 + \dots + 5 \cdot 10 + 1 \approx 10^{10^{11}}.
\end{aligned}$$

Последовательность $\{G_k(n)\}$ называется последовательностью Гудстейна для числа n .

Теорема 11 (Гудстейн¹²⁸). Для любого n существует такое k , что $G_k(n) = 0$.

Кажется невероятным, но это так. А чтобы в это поверить, мы рекомендовали бы читателю проделать вышеописанную процедуру, для начала – с числом 3.

$$\begin{aligned}
G_0(3) &= 2 + 1. \\
G_1(3) &= F_2(3) - 1 = 3. \\
G_2(3) &= F_3(G_1) - 1 = 4 - 1 = 3. \\
G_3(3) &= F_4(G_2) - 1 = 2. \\
G_4(3) &= F_5(G_3) - 1 = 1. \\
G_5(3) &= F_6(G_4) - 1 = 0.
\end{aligned}$$

Попробуем проверить утверждение теоремы для $n = 4$:

$$\begin{aligned}
2^2. \\
3^3 - 1 &= 2 \times 3^2 + 2 \times 3 + 2. \\
2 \times 4^2 + 2 \times 4 + 1. \\
2 \times 5^2 + 2 \times 5. \\
2 \times 6^2 + 6 + 5. \\
2 \times 7^2 + 7 + 4. \\
2 \times 8^2 + 8 + 3. \\
2 \times 9^2 + 9 + 2. \\
2 \times 10^2 + 10 + 1. \\
2 \times 11^2 + 11. \\
2 \times 12^2 + 12 - 1 &= 2 \times 12^2 + 11.
\end{aligned}$$

¹²⁸ Рувим Луи Гудстейн (1912–1985) – английский математик.

$$\begin{aligned}
& 2 \times 13^2 + 10. \\
& \dots \\
& 2 \times 23^2. \\
& 2 \times 24^2 - 1 = 24^2 + 23 \times 24 + 23. \\
& 25^2 + 23 \times 25 + 22. \\
& \dots \\
& 47^2 + 23 \times 47. \\
& 48^2 + 23 \times 48 - 1 = 48^2 + 22 \times 48 + 47. \\
& 49^2 + 22 \times 49 + 46. \\
& \dots \\
& 95^2 + 22 \times 95. \\
& 96^2 + 22 \times 96 - 1 = 96^2 + 21 \times 96 + 95. \\
& 97^2 + 21 \times 97 + 94. \\
& \dots \\
& 191^2 + 21 \times 191. \\
& 192^2 + 21 \times 192 - 1 = 192^2 + 20 \times 192 + 191. \\
& 193^2 + 20 \times 193 + 190. \\
& \dots \\
& 383^2 + 20 \times 383. \\
& 384^2 + 20 \times 384 - 1 = 384^2 + 19 \times 384 + 383. \\
& 385^2 + 19 \times 385 + 382. \\
& \dots \\
& 767^2 + 19 \times 767. \\
& 768^2 + 19 \times 768 - 1 = 768^2 + 18 \times 768 + 767. \\
& 769^2 + 18 \times 769 + 766. \\
& \dots \\
& 1535^2 + 18 \times 1535. \\
& 1536^2 + 18 \times 1536 - 1 = 1536^2 + 17 \times 1536 + 1535. \\
& 1537^2 + 17 \times 1537 + 1534. \\
& \dots \\
& \dots \\
& \dots
\end{aligned}$$

Эта последовательность доходит до числа из 121 210 695 цифр (для сравнения заметим, что $1000000!$ содержит около пяти с половиной миллионов цифр), но потом числа только уменьшаются (так как уже не содержат в наследственном представлении основания) вплоть до 0. Последовательность $G_k(4)$ впервые достигает 0 для $k = 3(2^{402653211} - 1) \approx 10^{121210695}$.

Набросок доказательства теоремы Гудстейна. Будем использовать трансфинитные ординалы (см. например, [46]). Пусть, как обычно, ω обозначает ординал, равный порядковому типу множества натуральных чисел, а ординал ε_0 обозначает $\sup(\omega, \omega^\omega, \omega^{\omega^\omega}, \dots)$.

Для любого натурального числа n и любого основания b пусть $B_b(n)$ обозначает выражение, полученное из наследственного представления числа n по основанию b , после синтаксической замены b на ординал ω . Например, так как наследственное представление 266 есть $2^{2^{2+1}} + 2^2 + 2$, то $B_2(266) = \omega^{\omega^{\omega+1}} + \omega^\omega + \omega$.

Очевидно, $B_b(n)$ есть ординал, меньший ε_0 и представленный в виде «экспоненциального полинома» относительно ω (канторова нормальная форма).

Имеем следующие свойства (для любых натуральных n и m и основания $b > 1$):

- 1) $B_b(n) = 0 \Leftrightarrow n = 0;$

- 2) $m < n \Leftrightarrow B_b(m) < B_b(n)$;
 3) $B_b(n) = B_{b+1}(F_b(n))$ (поскольку в правой части основание b в наследственном представлении n сначала заменяется на $b+1$, а потом $b+1$ заменяется на ω).

Зафиксируем $n > 0$, и пусть g_0, g_1, g_2, \dots – последовательность Гудстейна для данного числа n , т.е. $g_k = G_k(n)$ при $k = 0, 1, 2, \dots$. Определим теперь соответствующую последовательность ординалов a_0, a_1, a_2, \dots по правилу $a_k = B_{k+2}(g_k)$ при $k = 0, 1, 2, \dots$. Пусть для всех $k = 0, 1, 2, \dots$ выполнено $g_k > 0$. Придем к противоречию, и тем самым теорема будет доказана.

Сравним a_k и a_{k+1} . Имеем $g_{k+1} = F_{k+2}(g_k) - 1$ (здесь как раз используется предположение, что последовательность Гудстейна не содержит 0), поэтому

$$\begin{aligned} a_{k+1} &= B_{k+3}(g_{k+1}) = B_{k+3}(F_{k+2}(g_k) - 1) < B_{k+3}(F_{k+2}(g_k)) = \\ &= (\text{по свойству (3)}) B_{k+2}(g_k) = a_k. \end{aligned}$$

Проиллюстрируем предыдущее неравенство на примере: пусть $n = 266$. Тогда

$$g_0 = 266 = 2^{2^{2+1}} + 2^2 + 2 \text{ и } a_0 = B_2(g_0) = \omega^{\omega^{\omega+1}} + \omega^\omega + \omega.$$

Также имеем

$$g_1 = 3^{3^{3+1}} + 3^3 + 2, \text{ и } a_1 = B_3(g_1) = \omega^{\omega^{\omega+1}} + \omega^\omega + 2.$$

Очевидно, $a_1 < a_0$.

Таким образом, получили бесконечную убывающую последовательность ординалов $a_0 > a_1 > a_2 > a_3 > \dots$, что противоречит вполне упорядоченности ординалов. ■

Гудстейн доказал теорему в 1944 г., используя трансфинитную индукцию [11]. В 1982 г. Л. Кирби и Дж. Парис получили результат того, что теорема Гудстейна формально недоказуема в рамках теории формальной арифметики [16].

Все, что завершается, начинается.
Явилем ванн де Ватеринг. Пустое зеркало

– Хотелось бы более четких инструкций.
 – Полной ясности не будет никогда.
 Не жди ее, привыкай действовать в
 условиях частичной неопределенности.

B. Серкин. Хохот шамана

Решения избранных задач

Задачи из главы 3

Задача 3. а) $A = \emptyset, B = U$ (универсум); $B = \emptyset, A = U$ (универсум); $A = B$.

Задача 4. Выделим три непересекающихся множества для произвольных множеств A и B :

$$A \setminus B = X, A \cap B = Y, B \setminus A = Z.$$

По построению, $A \cup B = X \cup Y \cup Z$. Поскольку X, Y, Z не пересекаются друг с другом, для этих множеств мы имеем

$$X \Delta Y = (X \cup Y) \setminus (X \cap Y) = (X \cup Y) \setminus \emptyset = X \cup Y.$$

Следовательно, $X \cup Y \cup Z = (X \cup Y) \cup Z = (X \Delta Y) \cup Z = (X \Delta Y) \Delta Z$. Значит, для исходных множеств мы имеем

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

Таким образом, мы выразили объединение через пересечение, разность и симметрическую разность. Нам остается только выразить разность через симметрическую разность. Для этого заметим, что если одно множество включено в другое, например $P \subseteq Q$, то для этих множеств имеем

$$P \Delta Q = (P \setminus Q) \cup (Q \setminus P) = (P \setminus Q) \cup \emptyset = P \setminus Q.$$

Для множеств A, B верно $A \cap B \subseteq A$ и $A \setminus B = A \setminus (A \cap B)$. Поэтому

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

Тем самым разность выражена через симметрическую разность и пересечение. Подставим это выражение в формулу, полученную для объединения:

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

Оба выражения получены.

Задача 5. Определим операцию $A \otimes B = \{x \mid x \notin A \text{ и } x \notin B\}$. Тогда имеем

$$\neg A = A \otimes A;$$

$$A \cup B = \neg(\neg A \cap \neg B) = \neg(A \otimes B) = (A \otimes B) \otimes (A \otimes B);$$

$$A \setminus B = A \cap \neg B = (\neg A) \otimes B = (A \otimes A) \otimes B;$$

$$A \Delta B = (A \setminus B) \cup (B \setminus A) = ((A \setminus B) \otimes (B \setminus A)) \otimes ((A \setminus B) \otimes (B \setminus A)) =$$

$$= (((A \otimes A) \otimes B) \otimes ((B \otimes B) \otimes A)) \otimes (((A \otimes A) \otimes B) \otimes ((B \otimes B) \otimes A));$$

$$A \cap B = \neg(\neg A \cup \neg B) = \neg((A \otimes A) \cup (B \otimes B)) = \neg(((A \otimes A) \otimes (B \otimes B)) \otimes (B \otimes B)) =$$

$$= (((A \otimes A) \otimes (B \otimes B)) \otimes (B \otimes B)) \otimes (((A \otimes A) \otimes (B \otimes B)) \otimes (B \otimes B)).$$

Задача 12. $x = 6, y = 4$.

Задача 15. $x \rho y \Leftrightarrow x + y \in \mathbb{N} \vee x - y \in \mathbb{N}$.

Задача 29. Используйте диаграммы Венна.

Задача 30. $X = (C \setminus A) \cup B$.

Задача 35. Доказывайте от противного: предположите, что существует $x \in A$. Рассмотрите два случая: а) $x \notin B$ и б) $x \in B$ и придите в обоих случаях к противоречию. Это покажет, что $A = \emptyset$.

Задача 43. Используйте ассоциативность симметрической разности (задача 29).

Задача 44. Доказательство.

а) Пусть ρ симметрично. Возьмем $\langle x, y \rangle \in \rho^{-1} \Leftrightarrow \langle y, x \rangle \in \rho$ (по определению ρ^{-1}) $\Leftrightarrow \Leftrightarrow \langle x, y \rangle \in \rho$ (так как ρ симметрично). Пусть теперь $\rho^{-1} = \rho$. Тогда $\langle x, y \rangle \in \rho \Leftrightarrow \langle x, y \rangle \in \rho^{-1} \Leftrightarrow \Leftrightarrow \langle y, x \rangle \in \rho \Leftrightarrow \rho$ симметрично.

б) Пусть ρ транзитивно. Тогда $\langle x, y \rangle \in \rho \circ \rho \Rightarrow$ существует такое z , что $\langle x, z \rangle \in \rho$ и $\langle z, y \rangle \in \rho \Rightarrow \langle x, y \rangle \in \rho$ (так как ρ транзитивно). Пусть теперь $\rho \circ \rho \subseteq \rho$. Тогда $\langle x, y \rangle \in \rho$, $\langle y, z \rangle \in \rho \Rightarrow \langle x, z \rangle \in \rho \circ \rho \Rightarrow \langle x, z \rangle \in \rho$ (по условию, $\rho \circ \rho \subseteq \rho$) $\Rightarrow \rho$ транзитивно.

в) Пусть ρ рефлексивно. Тогда $\langle x, y \rangle \in \rho \Rightarrow \langle x, x \rangle \in \rho$ (так как ρ рефлексивно) и $\langle x, y \rangle \in \rho \Rightarrow \langle x, y \rangle \in \rho \circ \rho$ (по определению композиции отношений).

г) это утверждение следует из б и в.

Задачи из главы 4

Задача 1. Доказательство. Пусть формула $(A_1 \vee A_2 \vee \dots \vee A_n) \supset B$ ложна (то, что мы начинаем доказательство, предполагая, что формула ложна, а не истинна, продиктовано тем обстоятельством, что при этом выборе доказательство короче), тогда формула B ложна, а $A_1 \vee A_2 \vee \dots \vee A_n$ истинна. Следовательно, существует такое i ($1 \leq i \leq n$), что A_i истинна и поэтому $A_i \supset B$ ложна. Отсюда следует, формула $(A_1 \supset B) \wedge (A_2 \supset B) \wedge \dots \wedge (A_n \supset B)$ ложна.

В обратную сторону: пусть формула $(A_1 \supset B) \wedge (A_2 \supset B) \wedge \dots \wedge (A_n \supset B)$ ложна. Следовательно, существует такое i ($1 \leq i \leq n$), что $A_i \supset B$ ложна. Отсюда получаем, что A_i истинна и B ложна и, следовательно, $A_1 \vee A_2 \vee \dots \vee A_n$ истинна и, наконец, $(A_1 \vee A_2 \vee \dots \vee A_n) \supset B$ ложна.

Задача 15. Ответ: A – лжец; B – рыцарь; C – лжец; D – рыцарь.

Задача 16. Ответ: A – лжец; B – рыцарь; C – лжец; D – рыцарь; E – рыцарь.

Задачи из главы 5

Задача 1. Сюръективность:

$f: X \rightarrow Y$ – сюръективное отображение $\Leftrightarrow \forall y (y \in Y \supset \exists x ((x \in X) \wedge (f(x) = y)))$.

Инъективность:

$f: X \rightarrow Y$ – инъективное отображение $\Leftrightarrow \forall x_1 x_2 ((x_1 \in X) \wedge (x_2 \in X) \supset (f(x_1) = f(x_2)))$.

Задача 8. а) Число A есть предел функции $f(x)$ при $x \rightarrow x_0$. б) Функция f непрерывна в точке x_0 . в) Функция f непрерывна на отрезке $[a, b]$.

Задача 9. Функция должна быть постоянной.

Задача 10.

$\forall \varepsilon \exists \delta \forall a \forall x ((\varepsilon > 0) \wedge (\delta > 0) \wedge (a \in \mathbb{R}) \wedge (x \in \mathbb{R}) \wedge (|x - a| \leq \delta) \rightarrow (|f(x) - f(a)| \leq \varepsilon))$.

Задача 11. Пусть высказанное утверждение ложно. Тогда жители острова – разного типа, и среди них рыцари утверждают, что они одного типа с лжецами. Получили противоречие. Рассмотрим другой вариант: утверждение истинно. Тогда получаем решение задачи: все жители острова – рыцари, и они говорят об этом.

Задача 12. Среди сказавших нет рыцарей, так как тогда они говорили бы о себе ложь. Следовательно, говорящие были лжецами, но для того чтобы их утверждение было ложным, необходимо, чтобы спящий был рыцарь. Этот рыцарь на следующий день, очевидно, на вопрос ответил «нет».

Задача 13. Пусть предикат $K(x)$ истинен, если островитянин x есть рыцарь, а предикат $S(x)$ истинен, если x курит. Тогда высказанное утверждение можно записать в виде формулы $\forall x(K(x) \supset S(x))$. Если эта формула ложна, то все жители острова – лжецы. И для некоторого лжеца x_0 формула $K(x_0) \supset S(x_0)$ должна быть ложной. Но по свойству импликации это возможно только тогда когда $K(x_0)$ – истина. Получили противоречие. Значит, все жители острова – рыцари, и они курят.

Задача 14. Пусть высказанное утверждение истинно. Тогда среди жителей острова есть и рыцари, и лжецы. Причем лжецы в данном утверждении говорят правду. Это невозможно. Рассмотрим другой вариант: утверждение ложно. Тогда все жители острова – лжецы, и, как должно быть, они говорят ложь.

Задача 15. Пусть предикат $L(x)$ истинен, если островитянин x есть лжец, а предикат $S(x)$ истинен, если x курит. Тогда высказанное утверждение можно записать в виде формулы $\exists x(L(x) \& S(x))$. Если эта формула истина, то каждый житель – рыцарь и он утверждает, что есть лжецы на острове. Получили противоречие. Значит, все жители острова являются лжецами. Так как мы знаем, что для любого x формула $L(x)$ – истина, то в силу того, что лжецы высказывают ложь, необходимо, чтобы $\exists xS(x)$ было ложью. Ответ: все жители острова лжецы и ни один из них не курит.

Задача 16. Пусть предикат $S(x)$ истинен, если островитянин x курит. Для каждого жителя x_0 острова мы можем записать его утверждение в виде формулы $S(x_0) \supset \forall xS(x)$. Если эта формула – ложь, то $S(x_0)$ – истина, а $\forall xS(x)$ – ложь. Но поскольку для каждого x_0 формула $S(x_0)$ должна быть истиной, поэтому формула $\forall xS(x)$ ложной не может быть. Следовательно, любой житель x_0 острова есть рыцарь и формула $S(x_0) \supset \forall xS(x)$ является истинной. Если $S(x_0)$ – ложь, то все курить не могут и, следовательно, $\forall xS(x)$ – ложь. Если $S(x_0)$ – истина, то по свойству импликации $\forall xS(x)$ – истина. Получили, что все жители острова – рыцари, и они либо все не курят, либо все курят.

Задача 17. Используя предикат S из предыдущих задач, мы можем записать высказанное каждым жителем x_0 острова утверждение в виде формулы $\forall xS(x) \supset S(x_0)$. Эта формула ложной быть не может, поэтому все жители острова – рыцари. А что касается курения, то здесь ничего сказать нельзя. Может быть любое распределение курильщиков на острове, в том числе все могут быть некурящими или все могут курить.

Задача 18. Используя предикат S из предыдущих задач, мы можем записать высказанное каждым жителем x_0 острова утверждение в виде формулы $\exists xS(x) \& \neg S(x_0)$. Если эта формула истина для любого x_0 , то тогда получаем, что все жители острова не курят, но есть курящие среди них. Получили противоречие. Поэтому формула должна быть ложной и поэтому жители острова – лжецы. Если бы часть жителей была курящей, а другая – некурящей, то тогда формула была бы истинной для некурящего x_0 . Но эта формула будет ложной, если все курят или все не курят. Ответ: на острове живут лжецы, они все курят или все не курят, но точнее сказать нельзя.

Задача 19. Пусть все жители острова – рыцари. Тогда оба утверждения есть истина и, в частности, каждый говорит, что он некурящий, но это противоречит тому, что некоторые из них курят. Пусть теперь все жители острова – лжецы. Тогда из высказывания «Некоторые из нас курят» получаем, что все не курят, но это делает истинным высказывание «Я не курю». Снова противоречие. Жители острова не могут сделать эти высказывания при данных условиях задачи.

Задача 20. Утверждение «Все жители этого острова – рыцари» может быть истиной, а может быть ложью. Пусть это истина. Тогда оба племени состоят из рыцарей и рыцари племени B высказали ложь: «Некоторые из жителей этого острова есть лжецы». Противоречие. Следовательно, люди племени A высказывают ложь, т.е. они лжецы. Поэтому «Некоторые из жителей этого острова есть лжецы» – истина и племя B состоит из рыцарей. Ответ: племя A – лжецы, племя B – рыцари, и никто не курит на острове.

Задача 21. Решения:

- a) $\forall x (A(x, \text{Мориарти}) \supset A(\text{Холмс}, x));$
- c) $\exists x A(x, \text{Мориарти}) \supset A(\text{Холмс}, \text{Мориарти});$
- e) $\forall x (A(x, \text{Холмс}) \supset A(x, \text{Мориарти}));$
- g) $\forall x \exists y (A(x, y) \& \neg A(y, \text{Мориарти}));$
- i) $\forall x (A(x, \text{Холмс}) \supset \forall y (A(\text{Холмс}, y) \supset A(x, y))).$

Задача 22. Решения: b) $\exists x \forall y K(x, y);$ d) $\forall x \exists y (K(x, y) \& \neg K(y, x)).$

Задачи из главы 6

Задача 3. Разрешающий алгоритм для формальных систем, имеющих только удлиняющие правила, можно сформулировать в следующем виде:

Пусть F – проверяемая формула и M – множество всех аксиом теории.

While $\forall x \in M ((\text{длина}(x) \leq \text{длина}(F)) \& F \notin M)$ **do**

Begin

Для каждой формулы $x \in M$ выполняем следующее:

Begin

Пусть R_x обозначает множество всех формул, получаемых из x однократным применением правил вывода.

Полагаем M равным $(M \cup R_x) \setminus \{x\}.$

End

End

If $F \in M$ **then** F – теорема **else** F – не теорема.

Задача 4.

- a) Возможны варианты формулы: $S(\mathbf{0}) = x$ и $\forall y (y \times x = y);$
- b) Очевидная формула $\exists x (a \times x = b);$
- c) $S(S(S(S(S(\mathbf{0})))))$;
- d) $\exists x y z (\neg(x = \mathbf{0}) \& \neg(y = \mathbf{0}) \& \neg(z = \mathbf{0}) \& \neg(x = y) \& \neg(y = z) \& \neg(z = x) \& (n = x \times x + y \times y + z \times z));$
- e) $\exists z (\neg(z = 0) \& (x = y + z));$
- f) $\neg \exists x (\neg(\langle x > 1)) \& \langle x \rangle \text{ делит } a \& \langle x \rangle \text{ делит } b),$ где формулы в кавычках определены в пунктах e и b;
- g) $\exists r ((a = b \times q + r) \& (\langle r > 0 \rangle \vee (r = 0)) \& \langle b > r)),$ где формулы в кавычках определены ранее;
- h) $\exists q ((a = b \times q + r) \& (\langle r > 0 \rangle \vee (r = 0)) \& \langle b > r)),$ где формулы в кавычках определены ранее;

i) ($\ll x > 1$) & ($\forall y ((\ll y \text{ делит } x \gg) \supset ((y = S(0)) \vee (y = x)))$), где формулы в кавычках определены ранее;

j) $\forall x y z ((x + y = z) \supset (y + x = z))$;

k) $\forall x ((\ll x > 1) \& \ll x \text{ делит } n \gg \supset \exists y (x = y + y))$, где формулы в кавычках определены ранее.

Задачи из главы 7

Задача 6.

a) Имеем в силу

$$F_{n+1}(x) = F_n(F_n(\dots F_n(1)\dots)) \quad (*)$$

равенства

$$F_1(x) = \underbrace{F_0(F_0(\dots F_0(1)\dots))}_{F_0 \text{ повторяется } x+1 \text{ раз}} ,$$

$$F_1(x+1) = \underbrace{F_0(F_0(\dots F_0(1)\dots))}_{F_0 \text{ повторяется } x+2 \text{ раза}} .$$

Поэтому получаем $F_1(x+1) = F_0(F_1(x))$.

b) Проводим математическую индукцию по n . Базис индукции для $n = 0$ доказан в пункте a. Для доказательства индуктивного перехода предположим, что для $n = k$ выполнено $F_{k+1}(x+1) = F_k(F_{k+1}(x))$. Имеем в силу (*)

$$F_{k+2}(x+1) = \underbrace{F_{k+1}(F_{k+1}(\dots F_{k+1}(1)\dots))}_{F_{k+1} \text{ повторяется } x+2 \text{ раза}},$$

$$\underbrace{F_{k+1}(F_{k+1}(\dots F_{k+1}(1)\dots))}_{F_{k+1} \text{ повторяется } x+1 \text{ раз}} = F_{k+2}(x).$$

Отсюда получаем $F_{k+2}(x+1) = F_{k+1}(F_{k+2}(x))$.

c) Проводим математическую индукцию по x . Базис индукции для $x = 0$: $F_1(0) = F_0(1) = 2$. Для доказательства индуктивного перехода предположим, что для $x = y$ выполнено $F_1(y) = y + 2$. Имеем по свойству b $F_1(y+1) = F_0(F_1(y)) = F_0(y+2) = y + 2 + 1 = (y+1) + 2$. Что и требовалось доказать.

d) Проводим математическую индукцию по x . Базис индукции для $x = 0$: $F_2(0) = F_1(1) =$ (используем c) $= 3 = 2 \cdot 0 + 3$. Для доказательства индуктивного перехода предположим, что для $x = y$ выполнено $F_2(y) = 2y + 3$. Имеем по свойству b $F_2(y+1) = F_1(F_2(y)) = F_1(2y+3) = = 2y + 3 + 2 = 2(y+1) + 3$. Что и требовалось доказать.

e) Проводим математическую индукцию по x . Базис индукции для $x = 0$: $F_3(0) =$ (используем *) $F_2(1) =$ (используем d) $= 5 = 2^{0+3} - 3$. Для доказательства индуктивного перехода предположим, что для $x = y$ выполнено $F_3(y) = 2^{y+3} - 3$. Имеем по свойству 2 $F_3(y+1) = F_2(F_3(y)) = F_2(2^{y+3} - 3) = 2(2^{y+3} - 3) + 3 = 2^{(y+1)+3} - 3$. Что и требовалось доказать.

f) Проводим математическую индукцию по x . Базис индукции для $x = 0$: $F_4(0) =$ (используем *) $F_3(1) =$ (используем 5) $= 13 = 2^{2^2} - 3$. Для доказательства индуктивного

перехода предположим, что для $x = y$ выполнено $F_4(y) = \underbrace{2^{2^2}}_{y+3 \text{ раза}} - 3$. Имеем по свойству b $F_4(y+1) = F_3(F_4(y)) = 2^{F_4(y)+3} - 3 = 2^{(2^{2^2}-3)+3} - 3 = 2^{2^{2^2}} - 3$. Что и требовалось доказать.

+ 1) $= F_3(F_4(y)) = 2^{F_4(y)+3} - 3 = 2^{(2^{2^2}-3)+3} - 3 = 2^{2^{2^2}} - 3$. Что и требовалось доказать.

Задача 20. Задачу можно решить, используя только бумагу и карандаш. Но если использовать удобный язык программирования (который, например, имеет операции со списками чисел), то получится быстрее.

Задачи из главы 9

Задача 2. р) Если теория неразрешима, то алгоритма для решения задачи не существует. Если алгоритм существует, то он не обязан использовать только примитивную рекурсию.

Задача 3. $SK(IK) \equiv (\lambda xyz. xz(yz))IK \rightarrow (\lambda z. Kz(IKz)) = (\lambda z. z) \equiv I$.

Задача 7. $WFX \equiv SS(KI)FX \rightarrow SF((KI)F)X \rightarrow FX((KI)F)X \rightarrow FX(KIFX) \rightarrow FX(IX) \rightarrow FXX$.

Задача 9.

$$\begin{aligned} & (\lambda fgx. fx(gx)) (\lambda xy. x) (\lambda xy. x) \rightarrow_a (\lambda fgw. fw(gw)) (\lambda xy. x) (\lambda xy. x) \rightarrow \\ & \rightarrow (\lambda gw. (\lambda xy. x)w(gw)) (\lambda xy. x) \rightarrow \lambda w. (\lambda xy. x)w((\lambda xy. x)w) \rightarrow \lambda w. (\lambda y. w)(\lambda y. w) \rightarrow \\ & \rightarrow \lambda w. w \rightarrow_a \lambda x. x. \end{aligned}$$

Задачи из главы 10

Задача 3. Используем математическую индукцию по n . Базис индукции: $Y^0 \equiv Y$, поэтому Y^0 – комбинатор неподвижной точки. Индуктивный переход: пусть $n > 0$ и Y^n – комбинатор неподвижной точки. Докажем, что Y^{n+1} – комбинатор неподвижной точки. Имеем $Y^{n+1}E \equiv (Y^n(SI))E = SI(Y^n(SI))E = IE(Y^n(SI)E) = E(Y^n(SI)E) \equiv E(Y^{n+1}E)$. Поэтому Y^{n+1} – комбинатор неподвижной точки. Утверждение доказано.

Задача 4. Например, можно выбрать в качестве L терм

$L \equiv \text{лабвгдеёжзийклмнопрстуфхччищъыъюя. я(комбинаторнеподвижнойточкиугадала})$ и взять $\$ \equiv LLLLLLLLLLLLLLLLLLLLLLLLLLLLLL$, где L повторяется 33 раза.

Задача 8. Используем математическую индукцию по n . Базис индукции: $\langle 0 \rangle Cx = x = Ix$, поэтому по аксиоме экстенсиональности $\langle 0 \rangle C = I$. $\langle 1 \rangle Cx = Cx$, поэтому по аксиоме экстенсиональности $\langle 1 \rangle C = C$. Индуктивный переход: случай четного n : пусть $\langle n \rangle C = I$. Имеем $\langle n+1 \rangle Cx \equiv C(\langle n \rangle Cx) = C(Ix) = Cx$, поэтому по аксиоме экстенсиональности $\langle n+1 \rangle C = C$. Случай нечетного n : пусть $\langle n \rangle C = C$. Имеем $\langle n+1 \rangle Cxyz \equiv C(\langle n \rangle Cx)yz = C(Cx)yz = Cxzy = xyz = Ixyz$, поэтому по аксиоме экстенсиональности $\langle n+1 \rangle C = I$. Утверждение доказано.

Задача 16. Используем математическую индукцию по n . Базис индукции: $\langle 1 \rangle BWf x_1x_2 \rightarrow BWfx_1x_2 \rightarrow W(fx_1)x_2 \rightarrow fx_1x_2x_2$. Индуктивный переход: пусть $\langle n \rangle BWfx_1\dots x_n x_{n+1} = fx_1\dots x_n x_{n+1} x_{n+1}$. Тогда $\langle n+1 \rangle BWfx_1\dots x_{n+1} x_{n+2} = B(\langle n \rangle BW)f x_1\dots x_{n+1} x_{n+2} = \langle n \rangle BW(fx_1)x_2\dots x_{n+1} x_{n+2} = (\text{по индуктивному предположению})fx_1x_2\dots x_{n+1}x_{n+2}x_{n+2}$.

На высокую башню можно подняться

лишь по винтовой лестнице.

Фрэнсис Бэкон

Литература

1. *Appel K., Haken W.* Every Planar Map is Four-Colorable. Providence, RI : Amer. Math. Soc., 1989.
2. *Appel K., Haken W.* The Solution of the Four-Color Map Problem. Sci. Amer. 237, 108–121, 1977.
3. *Bailey D.* Mathematics by Experiment: Plausible Reasoning in the 21st Century. Wellesley, MA : A K Peters, 2003.
4. *Bishop E., Bridges D.* Constructive Analysis. New York : Springer-Verlag, 1985.
5. *Borwein J., Bailey D., Gkgensohn R.* Experimentation in Mathematics. Wellesley, MA : AK Peters, 2003. 358 p.
6. *Church A.* A note on the Entscheidungsproblem // Journal Symbolic logic. 1936. Vol. 1. P. 40–41; Correction. Ibid. P. 101–102.
7. *Church A.* The Calculi of Lambda Conversion. Princeton : Princeton University Press, 1941.
8. *Curry H.B., Feys R.* Combinatory Logic. Amsterdam : North Holland Co., 1958. Vol. 1.
9. *Gödel K.* Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I // Monatsh. Math. Phys. 1931. Vol. 38:1. P. 173–198.
10. *Gonthier G.* Formal Proof – The Four-Color Theorem // Notices of the American Mathematical Society. 2008. Vol. 55 (11). P. 1382–1393.
11. *Goodstein R.L.* On the Restricted Ordinal Theorem // Journal Symb. Logic. 1944. Vol. 9. P. 33–41.
12. *Hales, Thomas C.* The Jordan curve theorem, formally and informally // The American Mathematical Mounthly. 2007. Vol. 114 (10). P. 882–894.
13. *Harrison J.* Formalizing an analytic proof of the Prime Number Theorem // Journal of Automated Reasoning. 2009. Vol. 43. P. 243–261.
14. *Jones J.P., Sato D., Wada H., Wiens D.* Diophantine representation of the set of prime numbers // Amer. Mathem. Monthly. 1976. Vol. 83 (6). P. 449–464.
15. *Jones J.P.* Universal diophantine equation // Journal Symbol Logic. 1982. Vol. 47, № 3. P. 549–571.
16. *Kirbi L., Paris J.* Accessible independence result for Peano arithmetic // Bulletin of the London Mathematical Society. 1982. Vol. 14. P. 285–293.
17. *Mathias A.R.D.* A Term of Length 4 529 659 424 929 // Synthese. 2002. Vol. 133. P. 75–86.
18. *O'Connor R.* Essential Incompleteness of Arithmetic Verified by Coq // Lecture Notes in Computer Science. 2005. Vol. 3603. P. 245–260.
19. *Rice H.G.* Classes of Recursively Enumerable Sets and Their Decision Proems // Transactions of the American Mathematical Society. American Mathematical Society. 1953 (March). Vol. 74 (2). P. 358–366.
20. *Robertson N., Sanders D.P., Seymour P.D., Thomas R.* A New Proof of the Four Colour Theorem // Electron. Res. Announc. Amer. Math. Soc. 1996. Vol. 2. P. 17–25.
21. *Robinson J.A.* A machine-oriented logic based on resolution principle // Journal of the ACM. 1965. № 12. P. 23–41.
22. *Schönfincel M.* Über die Bausteine der mathematischen // Logik. Math. Annalen. 1924. № 92. S. 305–316.
23. *Shankar N.* Metamathematics, Machines and Gödel's Proof // Cambridge tracts in theoretical computer science. 1994. Vol. 38.
24. *Shepherdson J.C., Sturgis H.E.* Computability of recursive functions // Journal Assoc. Comput. Machinery. 1963. № 10. P. 217–255.
25. *Smullyan R.* Diagonalization and Self-reference. Clarendon Press, 1984. 396 p.

26. Smullyan R. Godel's Incompleteness Theorems. Oxford University Press, 1992. 160 p.
27. Smullyan R. M. Logical labyrinths. A K Peters, 2009. 327 p.
28. Smullyan R. Recursion Theory for Metamathematics. Oxford University Press, 1993. 163 p.
29. Thurber J. The Thirteen Clocks. Simon & Schuster, 1950. 124 p.
30. Turner D.A. A new implementstion technique for applicative languages // Software – Practice and Experience. 1979. № 9. P. 31–49.
31. The Seventeen Provers of the World / ed. by F. Wiedijk // Lecture Notes in Artificial Intelligence. Vol. 3600. Springer, Heidelberg, 2006.
32. Wilson R. Four Colors Suffice: How the Map Problem Was Solved. Princeton, NJ : Princeton University Press, 2004.
33. Wolfram Mathematica. URL: <http://www.wolfram.com/mathematica/>
34. Wolfram S. A New Kind of Science. Champaign, Illinois : Wolfram Media, Inc., 2002. 1197 p. URL: <http://www.wolframscience.com/>
35. Wolfram S. Mathematical Notation: Past and Future. URL: <http://www.stephenwolfram.com/publications/mathematical-notation-past-future/>
36. Айгнер М., Циглер Г. Доказательства из Книги. Лучшие доказательства со времен Евклида до наших дней : пер. с англ. М. : Мир, 2006. 256 с.
37. Александрова Н.В. История математических терминов, понятий, обозначений: словарь-справочник. М. : Изд-во ЛКИ, 2007. 248 с.
38. Барендрегт Х. Ламбда-исчисление. Его синтаксис и семантика. М. : Мир, 1985. 606 с.
39. Беклемишев Л.Д. Теоремы Гёделя о неполноте и границы их применимости. I // Успехи математических наук. 2010. Т. 65, вып. 5 (395). С. 61–105.
40. Бирс A. Словарь Сатаны. М. : Центрполиграф, 2003.
41. Босс В. Лекции по математике. Т. 16: Теория множеств: от Кантора до Коэна : учеб. пособие. М. : ЛИБРОКОМ, 2011. 208 с.
42. Босс В. Лекции по математике. Т. 6: Алгоритмы, логика, вычислимость. От Диофанта до Тьюринга и Гёделя : учеб. пособие. М. : ЛИБРОКОМ, 2013. 208 с.
43. Братко И. Алгоритмы искусственного интеллекта на языке PROLOG. 3-е изд. М. : Вильямс, 2004. 640 с.
44. Бунос Дж., Джессифри Р. Вычислимость и логика. М. : Мир, 1994. 396 с.
45. Бурбаки Н. Теория множеств. Начала математики : пер. с фр. М. : Мир, 1965. 456 с.
46. Верещагин Н.К., Шень А. Лекции по математической логике и теории алгоритмов. Ч. 1: Начала теории множеств. 4-е изд., доп. М. : МЦНМО, 2012. 112 с.
47. Верещагин Н.К., Шень А. Лекции по математической логике и теории алгоритмов. Ч. 3: Вычислимые функции. 4-е изд., исправл. М. : МЦНМО, 2012. 160 с.
48. Гарднер М. Математические досуги. М. : Оникс, 1995. 496 с.
49. Гейтинг А. Интуиционизм. М. : Мир, 1965.
50. Гильберт Д. Основания геометрии. Л. : Сеятель, 1923. 152 с.
51. Губа В.С., Львовский С.М. «Парадокс» Банаха–Тарского. М. : МЦНМО, 2012. 48 с.
52. Деза Е.И. Специальные числа натурального ряда : учеб. пособие. М. : ЛИБРОКОМ, 2011. 240 с.
53. Дербшишир Д. Простая одержимость. Бернхард Риман и величайшая нерешенная проблема в математике. М. : Астрель, 2010. 464 с.
54. Дрёссер К. Обольстить логикой. Выводы на все случаи жизни. М. : БИНОМ. Лаборатория знаний, 2014. 176 с.
55. Дьёдонне Ж. О деятельности Бурбаки // Успехи математических наук. 1973. Т. XXVIII, вып. 3 (171).
56. Дьёдонне Ж. Основы современного анализа. М. : Мир, 1964. 430 с.
57. Дэвенпорт Г. Высшая арифметика: Введение в теорию чисел. 2-е изд. : пер. с англ. М. : ЛИБРОКОМ, 2010. 176 с.

58. Емельяненков А. С учёным видом. Как за 4,5 тысячи рублей в журнале опубликовали заведомую галиматью // Российская газета (Федеральный выпуск). № 4782 от 29 октября 2008 г. URL: <http://www.rg.ru/2008/10/29/journal-nauka.html>
59. Зюзьков В.М. Ленивое функциональное программирование : учеб. пособие. 2-е изд., перераб. и доп. Томск : Изд-во Том. ун-та, 2007. 294 с.
60. История математики : в 3 т. / под ред. А.П. Юшкевича. М. : Наука, 1972. Т. III.
61. Катленд Н. Вычислимость. Введение в теорию рекурсивных функций / пер. с англ. М. : Мир, 1983. 256 с.
62. Катракарт Т., Клейн Д. Как-то раз Платон зашел в бар...: Понимание философии через шутки. М. : Альпина нон-фикшн, 2012. 236 с.
63. Клейн М. Математика. Утрата определенности. М. : Мир, 1984. 434 с.
64. Клини С.К. Введение в метаматематику. М. : ЛИБРОКОМ, 2009. 582 с.
65. Клини С.К. Математическая логика. 2-е изд. М.: Едиториал УРСС, 2005. 480 с.
66. Колмогоров А.Н., Драгалин А.И. Математическая логика. 3-е изд. М. : КомКнига, 2006. 240 с.
67. Кормен Т., Лейзерсон Ч., Ривест Р. Алгоритмы: построение и анализ. М. : МЦНМО, 2001. 960 с.
68. Кранц С. Изменчивая природа математического доказательства. Доказать нельзя поверить. М. : Лаборатория знаний, 2016. 320 с.
69. Кроновер Р.М. Фракталы и хаос в динамических системах. Основы теории. М. : Постмаркет, 2000. 352 с.
70. Лавров И.А. Математическая логика : учеб. пособие. М. : Академия, 2006. 240 с.
71. Лакатос И. Доказательства и опровержения: Как доказываются теоремы. 2-е изд. М. : Изд-во ЛКИ, 2010. 152 с.
72. Лем С. Сумма технологий. М. : ACT ; СПб. : Terra Fantastica, 2002. 668 с.
73. Логический подход к искусенному интеллекту: От классической логики к логическому программированию / А. Тейз, П. Грибоман, Ж. Луи и др. М. : Мир, 1990. 432 с.
74. Маковельский А.О. История логики. М. : Кучково поле, 2004. 480 с.
75. Манин Ю.И. «Не мы выбираем математику своей профессией, а она нас выбирает» (интервью) // Троицкий вариант. 30 сентября 2008. № 13N (839). URL: <http://www.mcsite.ru/edu/statii/Manin-13N.pdf>
76. Манин Ю.И. Вычислимое и невычислимое. М. : Светское радио, 1980. 128 с.
77. Манин Ю.И. Математика как метафора. 2-е изд., доп. М. : МЦНМО, 2010. 424 с.
78. Манин Ю.И. Доказуемое и недоказуемое. М. : Мир; Советское радио, 1979. 168 с.
79. Марков А.А. Избранные труды. М. : Изд-во МЦНМО, 2003. Т. II. Теория алгоритмов и конструктивная математика, математическая логика, информатика и смежные вопросы. 626 с.
80. Марков А.А. Теория алгорифмов // Труды Математического института АН СССР. М. ; Л., 1954. Т. 42.
81. Матиясевич Ю.В. Диофантовы множества // УМН. 1972. Т. 22, вып. 5. С. 185–222.
82. Матиясевич Ю.В. Десятая проблема Гильберта. М. : Физматлит, 1993. 224 с.
83. Мендельсон Э. Введение в математическую логику. М. : Наука, 1984. 320 с.
84. Милль Дж.Ст. Система логики силлогистической и индуктивной: Изложение принципов доказательства в связи с методами научного исследования / пер. с англ. 5-е изд., испр. и доп. М. : ЛЕНАНД, 2011. 832 с.
85. Минский. М. Вычисления и автоматы. М. : Мир, 1971. 360 с.
86. Непейвода Н.Н. Прикладная логика : учеб. пособие. Новосибирск : Изд-во Новосиб. ун-та, 2000. 521 с.
87. Непейвода Н.Н., Скопин И.Н. Основания программирования. Москва ; Ижевск :

- Регулярная и хаотическая динамика, 2003. 913 с. URL: <http://ulm.uni.udm.ru/~nnn/>
88. Никифоров А. Книга о логике. М. : Гнозис, 1996. 240 с.
 89. Пенроуз Р. Тени разума: в поисках науки о сознании. Ч. 1: Понимание разума и новая физика. Москва ; Ижевск: Институт компьютерных исследований, 2003. 368 с.
 90. Подниекс К.М. Вокруг теоремы Геделя. Рига : Зинатне, 1992. 191 с.
 91. Пойа Д. Как решать задачу / пер. с англ. 4-е изд. М. : ЛИБРОКОМ, 2010. 208 с.
 92. Пойа Д. Математика и правдоподобные рассуждения. М. : Наука, 1975. 464 с.
 93. Пойа Д. Математическое открытие: Решение задач: основные понятия, изучение и преподавание. 3-е изд. М. : КомКнига, 2010. 448 с.
 94. Попов Г. Ошибка в проекте. Ленинский тупик. М. : Изд. дом Междунар. ун-та в Москве, 2008. 512 с.
 95. Проблемы Гильберта : сб. / под ред. П.С. Александрова. М. : Наука, 1969. 237 с.
 96. Рассел Б. Философский словарь разума, материи и морали. Киев : Port-Royal, 1996.
 97. Смаллан Р. Вовеки неразрешимое. Путь к Гёделю через занимательные загадки. М. : Канон⁺; РООИ «Реабилитация», 2013. 303 с.
 98. Смаллан Р. Как же называется эта книга? М. : Мир, 1981. 238 с.
 99. Смаллан Р. Теория формальных систем. М. : Наука, 1981. 104 с.
 100. Сосинский А.Б. Умер ли Бурбаки? // Математическое просвещение. 1998. Сер. 3, вып. 2.
 101. Справочная книга по математической логике : в 4 ч. / под ред. Дж. Барвайса. Ч. 3: Теория рекурсии : пер. с англ. М. : Наука, 1982. 360 с.
 102. Справочная книга по математической логике : в 4 ч. / под ред. Дж. Барвайса. Ч. IV: Теория доказательств и конструктивная математика. М. : Наука, 1983. 392 с.
 103. Тегмарк М. Наша математическая Вселенная. В поисках фундаментальной природы реальности. М. : АСТ; CORPUS, 2017. 592 с.
 104. Уайтхед А., Рассел Б. Основания математики : в 3 т. / под ред. Г.П. Ярового, Ю.Н. Радаева. Самара : Самар. ун-т, 2005–2006.
 105. Успенский В.А. Машина Поста. М. : Наука, 1988. 96 с.
 106. Успенский В.А. Предисловие к математике. СПб. : Торгово-издательский дом «Амфора», 2015. 474 с.
 107. Успенский В.А. Теорема Гёделя о неполноте и четыре дороги, ведущие к ней // Математическое просвещение. 2011. Сер. 3, вып. 15. С. 37–75.
 108. Успенский В.А. Что такое аксиоматический метод? Ижевск : Регулярная и хаотическая динамика, 2001. 96 с.
 109. Успенский В.А., Верещагин Н.К., Плиско В.Е. Вводный курс математической логики. М. : ФИЗМАТЛИТ, 2004. 128 с.
 110. Успенский. В.А. Апология математики. СПб. : Амфора, 2009. 554 с.
 111. Ученые шутят / авт.-сост. С.Н. Федин, Б.С. Горобец, Ю.А. Золотов. М. : ЛКИ, 2010. 248 с.
 112. Филд А., Харрисон П. Функциональное программирование. М. : Мир, 1993. 637 с.
 113. Френкель А.А., Бар-Хиллел И. Основания теории множеств. М. : КомКнига, 2006. 552 с.
 114. Френкель Э. Любовь и математика. Сердце скрытой реальности. СПб. : Питер, 2015. 352 с.
 115. Хайрер Э., Ваннер Г. Математический анализ в свете его истории. М. : Научный мир, 2008. 396 с.
 116. Харди Г.Г. Апология математика. Ижевск : Регулярная и хаотическая динамика, 2000. 104 с.
 117. Хоффштадтер Д. Гёдель, Эшер, Бах: эта бесконечная гирлянда. Самара : Бахрах-М, 2001. 752 с.
 118. Чёрч А. Введение в математическую логику. 2-е изд., испр. М. : Либроком, 2009. Т. 1. 480 с.
 119. Штейнгауз Г. Математика – посредник между духом и материей. М. : БИНОМ.

- Лаборатория знаний, 2005. 351 с.
- 120. Эббинхауз Г.-Д., Якобс К., Ман Ф.-К., Хермес Г. Машины Тьюринга и рекурсивные функции. М. : Мир, 1972. 264 с.
 - 121. Энгелер Э. Метаматематика элементарной математики. М. : Мир, 1987. 128 с.
 - 122. Энциклопедия для детей. Т. 11: Математика. М. : Аванта+, 2003. 688 с.

Предметный и персональный указатели

W

Wolfram Mathematica, 87, 173

A

аксиома, 26, 124, 126
выбора, 148, 149
аксиома о параллельности, 138
аксиоматическая теория, 125
Ch, 125
L, 126
MIU, 130
PR, 130
PR1, 131
UR, 131
ZFC, 147
алфавит, 126
геометрия, 138
неформальная, 144
полная, 129
полуразрешимая, 129
правило вывода, 126
разрешимая, 129
семантически непротиворечивая, 129
синтаксически непротиворечивая, 129
формальная, 125, 126, 144
формальной арифметики *PA*, 145
Цермело-Френкеля, 146
аксиоматический метод, 124, 165
неформальный, 124
формальный, 124
алгоритм, 180
алгоритмически неразрешимая задача, 36
Аппель Кеннет, 175
Аристотель, 25
арифметизация метаматематики, 228

Б

Беклемишев Лев Дмитриевич, 176, 235
бесконечность
актуальная, 169
потенциальная, 169
Бирс Амброз, 7
Бойян Янош, 138
Брауэр Лейтзен, 169, 180
булевы алгебра, 30, 92
булевы функции, 94
вырожденная, 93
двоичная интерпретация, 93
двоичными функциями, 94
логика высказываний, 94
многочлены Жегалкина, 97
нейтральные элементы, 93
нормальная форма, 95
переключательные функции, 94
полная система функций, 97
совершенная конъюнкция, 96
теоретико-множественная интерпретация, 94
булевы выражения, 45
булевы операции, 45
Буль Джордж, 30
Бурбаки Николя, 37

Начала математики, 37
Бэкон Фрэнсис, 27

В

Вейерштрас Карл, 30
Вейль Герман, 7, 180
Венн Джон, 46
Венна диаграммы, 46
взаимно-однозначное соответствие. См. функция
биективная
Вольфганг Хакен, 175
выводимость
вывод, 127
выводимая формула, 127
гипотеза, 127
заключение, 127
непосредственный вывод, 127
посылка, 127
теорема, 127
выполнимое множество формул, 91
высказывание, 73
автореферентное, 79
автореференция, 86
истина, 73
квазивысказывание, 73
логическое значение, 73
ложь, 73
модальность, 75
простое, 73
сложное, 75
высказывательная форма, 75

Г

Гаусс Карл, 138
гёделевый номер, 228
Гёдель Курт, 35, 149, 172, 188, 219, 228
принцип несовершенства, 237
Гейтинг Аренд, 170
геометрия Евклида, 139
геометрия Лобачевского, 138
Геттингенская программа, 34, 180
Гильберт Давид, 32, 33, 180
гипотеза континуума, 149
Гудстейн Луи, 238

Д

Дедекинд Юлиус, 30
дедуктивная система, 125
дедукция, 9
декартова степень, 49
декартово произведение, 49
Делоне Шарль-Эжен, 172
диагонализация формулы, 232
Диофантовы уравнения, 222
догадка, 151
доказательство, 8, 123, 151
Бхаскара, 123
доказательство от противного, 88
использование теоремы о дедукции, 166
компьютерное, 172, 174, 176
конструктивное, 170, 180

контрпримером, 168
косвенное, 166
логический вывод, 164
математический интуиционизм, 169
методом перебора, 166
неформальное, 124
определение Непейводы Н.Н., 166
от противного, 167
поиском от цели, 167
прямая волна, 167
прямое, 166
с помощью контрапозиции, 166
существования, 170
формальное, 124, 164, 165

Е

Евклид, 26, 168, 180

З

задача о двух шкатулках, 21
закон де Моргана, 90
закон исключенного третьего, 87, 136, 170
закон контрапозиции, 90
закон поглощения, 90
закон расщепления, 90
Зенон, 18

И

именная форма, 75
индуктивное определение, 163
индукции принцип, 153
индукция, 9, 151
интерпретация, 128
истинностное значение формулы, 109
носитель, 106
общезначимая формула, 110
сигнатуры, 107
интерпретация относительная, 236
интерпретация языка логики высказываний, 81
интуиция, 123
исчислением высказываний, 132

К

канонические дедуктивные системы, 219
Кантор Георг, 30, 41
канторово множество, 149
Карри Хаскелл, 202, 214, 216
Кассини Джованни, 156
квантор, 33, 75
существования, 101
универсальный, 101
Клейн Морис, 29
класс вычетов по модулю, 55
класс эквивалентности, 55
Клини Стивен, 180, 188, 213, 217, 219
кодирование теории, 228
конструктивная математика, 171
контрапозиция, 166
контрпример, 153, 168
кортеж, 49
Коши Огюстен, 30, 152
Коэн Пол, 149

Кронекер Леопольд, 31
Кэрролл Льюис, 6

Л

Лакатос Имре, 173
ламбда-исчисление, 36, 195
алгоритм абстракции, 203
альфа-конверсия, 198
альфа-редекс, 198
арифметические операторы, 208
базис, 203
бета-конверсия, 198
бета-редекс, 198
булевы операции, 211
замыкание относительно аппликации, 203
итератор, 208
карринг, 216
комбинатор, 202
комбинатор неподвижной точки, 214
комбинатор Тьюринга, 216
кортеж, 212
ламбда-абстракция, 196
ламбда-аппликация, 196
ламбда-термы, 196
ленивые вычисления, 201
нормальная форма, 200
нумерал Чёрча, 206
обобщенная конверсия, 199
пара, 212
парадоксальный комбинатор, 214
подстановка, 197
порядок редукции, 201
принцип экстенсиональности, 199
редукция, 200
свободная переменная, 197
связанная переменная, 196
тело абстракции, 196
функция предшествования, 213
экстенсиональная эквивалентность, 199
энергичные вычисления, 201
этा-конверсия, 198
этा-редекс, 198
Леверье Урбен, 172
Лейбниц Готфрид, 28
Лем Станислав, 12
лемма о диагонализации, 232
Лобачевский Николай, 138
логика, 8, 24, 29
интуиционистская, 170
классическая, 36
неклассическая, 36
логика высказываний, 32, 73
язык, 80
логика предикатов, 32
логика пропозициональная. См. логика высказываний
логика символическая, 30
логики многозначные, 36
логически эквивалентные формулы, 111, 128
логические операции. См. логические связки
логические связки, 75
дизъюнкция, 77
импликация, 77
конъюнкция, 76
отрицание, 76
эквиваленция, 78

логическое следствие, 91, 114, 128
Локк Джон, 6
Лукасевич Ян, 36

M

Манин Юрий Иванович, 22, 39, 171
Марков Андрей Андреевич, 219
математическая индукция, 154
возвратная индукция, 157
индуктивный базис, 156
индуктивный шаг, 156
по построению, 163
принцип, 156
принцип бесконечного спуска, 158
строго убывающая последовательность
натуральных чисел конечна, 158
существование наименьшего элемента в
непустом множестве, 157
математическая логика, 11, 20
математический платонизм, 25
Матиясевич Юрий, 223
метатеорема, 128
Милль Джон Стюарт, 6
многоугольные числа, 152
множество, 31, 41
абсолютное дополнение, 44
арифметическое, 227
бесконечное, 65
включение, 42
выразимое, 113
диофантово, 223
множество-степень, 43
объединение, 43
относительное дополнение, 43
отношение принадлежности, 41
пересечение, 43
перечислимое, 183
подмножество, 42
принцип абстракции, 41
принцип объемности, 41
пустое, 42
разность, 43
разрешимое, 184
собственное подмножество, 42
строгое включение, 42
характеристическое свойство, 41
элемент, 41
МНР-машина с неограниченными регистрами, 219
модель множества формул, 91, 114, 128
модель теории, 128
модус поненс, 27, 132
мощность множества, 31
континуум, 68
континуум-гипотеза, 69
отель Гильберта, 62
равномощные, 62
счетное, 65

H

наследственное представление, 238
Непейвода Николай Николаевич, 7, 13, 163
нормальные алгорифмы, 219
нумерал, 107

O

общерекурсивные функции, 219
омега-непротиворечивость, 231
отделимые множества, 187
отношение множеств, 50
 n -местное, 50
антисимметричное, 53
бинарное, 50
композиция, 52
компоненты, 50
множество значений, 50
область определения, 50
обратное, 52
рефлексивное, 53
симметричное, 53
транзитивное, 53
отношение эквивалентности, 54
отображение. См. функция

P

парадокс, 15
Ахиллес и черепаха, 18
Берри, 18
брадобрейя, 19
Гемпеля, 153
Грэллинга, 19
изобретателя, 162
Карри, 86
крокодила, 18
лжец, 18
неожиданной казни, 19
Рассела, 43
Ришара, 161
Пеано Джузеппе, 30
переменная, 74
вхождение, 74
высказывательная, 80
параметр, 75
свободная, 74
связанная, 74
Пифагор, 24, 167
Платон, 24
подформула, 81
Пойа Дьёрдь, 154, 163, 173
Попов Гавриил, 9
порочный круг в доказательстве, 15
порядок
лексикографический, 57
линейный, 56
частичный, 56
Шарковского, 58
Пост Эмиль, 180, 219
предикат, 32, 100
выразимый, 113, 231
разрешимый, 220
разрешимый, 231
принцип пьяницы, 110
проблема остановки, 37, 220
пропозициональная формула, 80
прувер, 174

R

равносильные формулы, 89
разбиение, 55

Рамануджан Сриниваса, 177
Рассел Берtrand, 7, 33
Робинсон Джон, 143
рыцари и лжецы, 84, 121

C

Саккери Джироламо, 138
семантическая полнота, 114
семантическая система, 125
семейство множеств, 48
 объединение, 48
 пересечение, 48
система аксиом независимая, 129
системы компьютерной алгебры, 173
сложность алгоритма, 39
Смаллиан Рэймонд, 20, 84, 121, 237
Сократ, 24
сократовский диалог, 25
софизм, 15
 все лошади одной масти, 161
 единица – наибольшее натуральное число, 168
карта России, 17
Эватл и Протагор, 15
Стивен Вольфрам, 173, 174

T

таблица истинности, 82
Тегмарк Макс, 12
тезис Чёрча, 220
теодиция наоборот, 136
теорема, 26, 124, 125
 Банаха–Тарского, 149
 Венна, 46
 Гёделя о полноте исчисления предикатов, 144
 Гудстейна, 238
 диофантовость равносильна перечислимости, 224
 Жордана о кривой, 174
 Кантора, 67
 Кантора–Шрёдера–Бернштейна, 64
 Клини, 217
 о бесконечности простых чисел, 168
 о дедукции для теории первого порядка, 144
 о корректности исчисления предикатов, 144
 о неподвижной точке, 170
 об отрицательном решении 10-й проблемы Гильbertа, 224
 о распределении простых чисел, 174
 о четырех красках, 175
 основная теорема арифметики, 159
Поста о полноте исчисления высказываний, 135
Райса, 222
Тарского, 229
Чёрча о неразрешимости исчисления предикатов, 145, 222
Чёрча–Россера, 201
теорема Гёделя
 о неполноте, 35, 174
 о неполноте – семантическая версия, 229
 о неполноте – синтаксическая версия, 231
 о неполноте – синтаксическая версия с ω -непротиворечивостью, 233
о неполноте без ω -непротиворечивости, 235
о неполноте в форме Россера, 237

о непротиворечивости, 35, 235
о непротиворечивости в общем виде, 237
теория вычислимости, 180
теория вычислительной сложности, 40
теория первого порядка, 141, 142
 аксиомы равенства, 142
 исчисление предикатов первого порядка, 143
логические аксиомы, 142
логическое программирование, 143
правила вывода, 143
собственные аксиомы, 143
чистое исчисление предикатов, 143
теория формальной арифметики PA, 227
теория фундаментальная, 237
Тёрбер Джеймс, 7
Тьюринг Аллан, 36, 181, 192
 машина, 37, 192, 227
 универсальная машина, 194

У

Уайтхед Альфред, 33
универсум, 74
универсум фон Неймана, 147
упорядоченная пара, 49
Успенский Владимир Андреевич, 11, 235

Ф

фактор-множество, 56
Фалес, 24
Ферма Пьер, 152
формула
 выполнимая, 87, 111
 общезначимая, 128
 опровергимая, 87
 противоречие, 87, 128
 совместное множество формул, 114, 128
 тавтология, 87, 111
Фреге Готлоб, 30
Френкель Эдуард, 14
функция, 58
 k-местная частичная, 181
 Аккермана, 191
 биективная, 61
 всюду определенная, 181
 вычислимая, 181, 188, 192, 195
 вычислимой по Тьюрингу, 193
 инъективная, 60
 композиция, 61
 ламбда-определенная, 206, 208
 область значений, 59
 область определения, 58
 область потенциальных значений, 58
 образ множества, 59
 обратная, 61
 полухарактеристическая, 183
 представимой в PA, 232
 прообраз множества, 59
 сюръективная, 60
 универсальная, 185
 характеристическая, 184

Х

Харди Годфри, 10
Хофштадтер Дуглас, 129

Ч

частично-рекурсивная функция, 188
базисная, 188
минимизация, 189
общерекурсивная, 189
прimitивная рекурсия, 188
прimitивно-рекурсивная, 189
суперпозиция, 188
Чёрч Алонзо, 36, 180, 195, 213, 220

Ш

Шварц Герман, 31
Шейнфинкель Моисей, 202, 216
Шенкс Вильям, 172
Штейнгауз Гуго, 10
Шютте Курт, 236

Э

Эйлер Леонардо, 44, 172

Эйлера круги, 44

экспериментальная математика, 173
Эрбран Жак, 219
Эрдёш Пол, 177

Я

язык первого порядка, 100
атомарная формула, 104
замкнутая формула, 105
константы, 103
предикатные символы, 103
сигнатура, 103
терм, 103
формула, 104
функциональные символы, 103
язык программирования Haskell, 196
язык программирования Prolog, 143
язык теории множеств, 106
язык формальной арифметики, 106
стандартная интерпретация, 107

Учебное издание

ЗЮЗЬКОВ Валентин Михайлович

Введение в математическую логику

Учебное пособие

Редактор Н.А. Афанасьева
Оригинал-макет А.И. Лелоюор
Дизайн обложки Л.Д. Кривцовой

Подписано к печати 13.06.2017 г. Формат 60×84^{1/8}.
Бумага для офисной техники. Гарнитура Times.
Усл. печ. л. 30,2.
Тираж 50 экз. Заказ № 2568.

Отпечатано на оборудовании
Издательского Дома
Томского государственного университета
634050, г. Томск, пр. Ленина, 36
Тел. 8+(382-2)-53-15-28
Сайт: <http://publish.tsu.ru>
E-mail: rio.tsu@mail.ru

ISBN 978-5-94621-617-3

