МАТЕМАТИЧЕСКОЕ ПРОСВЕЩЕНИЕ

Третья серия

выпуск 4

МЦНМО
Москва 2000

ББК 22.1
М34

Адрес редакции:
121002, Москва, Б. Власьевский пер., д. 11, к. 202
(с пометкой «Математическое просвещение»)
Email: matpros@mccme.ru Web-page: www.mccme.ru/free-books

М34 **Математическое просвещение.** Третья серия, вып. 4. — М.: МЦНМО, 2000. — 232 с.

Темой номера очередного сборника «Математическое просвещение» выбрана теория сложности вычислений. Публикуемые здесь материалы дают представление как о классических разделах этой теории, так и о новых, нетрадиционных (вариант теории сложности по Л. Блюм, С. Смейлу и М. Шубу в популярном изложении С. Смейла). Раздел «Математический мир» содержит материалы, посвященные памяти А. Б. Ходулёва (1953–1999), замечательного математика и эксперта в области программирования. Там же, в продолжение материалов предыдущих номеров, помещен очерк творчества двух выдающихся советских математиков А. О. Гельфонда и Л. Г. Шнирельмана. Помимо этого, сборник содержит ряд статей, посвященных интересным математическим сюжетам: элементарному изложению теории препятствий, простоте числа $2^{127}-1$, доказательству квадратичного закона взаимности, дискретному преобразованию Фурье. В разделе «Олимпиады» обсуждаются некоторые избранные задачи математических соревнований 1999 г. В задачном разделе, кроме новых задач, помещены решения некоторых задач из предыдущих выпусков.

ISBN 5–900916–51–0

РФФИ
Выпуск данного сборника поддержан грантом Российского Фонда Фундаментальных Исследований (номер проекта 99-01-14033)

Содержание

Математический мир

А. Б. Ходулёв (1953 – 1999)

10 сентября 1999 года ушел из жизни Андрей Борисович Ходулёв.

Он представлялся мне человеком, опередившим своё время, человеком XXI века. В нём ярко сочеталось то, что ныне свойственно лишь избранным: талант исследователя-математика, глубокий интерес к естествознанию (и науке вообще), с одной стороны, и исключительная сила в том, что называется ныне Computer Science — с другой.

...Если человечество сумеет справиться со своими проблемами (экологическими, энергетическими, народонаселенческими и т. п.), если оно сумеет победить язву терроризма, его ждут в самом недалеком будущем великие свершения, о которых сейчас невозможно даже помыслить. Ещё несколько шагов, и каждый сможет моделировать звучание той музыки, которую слышит его внутренний голос, доказывать математические теоремы, открывать новые явления природы, создавать инженерные проекты и т. п., совещаясь со своим несравненным соперником по разуму и другом в творческой работе — компьютером. И дорогу к этому будут пролагать люди, подобные А. Б. Ходулёву.

Андрей был необыкновенной личностью. Это очень выразительно описал его друг ещё со школьных времён — Г. А. Гальперин, статья которого, посвящённая Ходулёву, печатается следом за этим моим кратким словом. Но вот ещё несколько моих воспоминаний об этой его необычности. Он казался неспортивным и производил впечатление учёного-неумехи. Но на самом деле у него были замечательные руки, он знал электронику так, как её знают не все профессионалы, что в сочетании с высочайшим интеллектом давало ему возможность рассчитывать и собирать схемы, которые не мог бы сделать никто. Он был первоклассным горнолыжником, воднолыжником, виндсерфистом, скейтбортистом. При этом все

пользовались его умелыми руками, чтобы исправить всякое оборудование — лодки, лыжи, паруса... Не наделённый от природы кошачьей ловкостью, присущей спортсменам-профессионалам, он с необыкновенной скоростью осваивал все новые спортивные профессии за счет опять-таки силы своего характера и интеллекта.

* * * * * *

Андрей Ходулёв родился 7 октября 1953 года в городе Калинине. Никто из его родни не занимался математикой. Математическая одарённость проявилась в самом раннем детстве. Как-то он рассказывал мне, что когда его, младенца, спрашивали до скольких ты умеешь считать (по-видимому, желая восхититься тем, что мальчик умеет считать до десяти), он затруднялся с ответом. Как сказать: числам нет предела, а названия где-то обрываются — миллион, миллиард, он, конечно, знал и дальнейшие названия, но не был уверен, что знает все.

Очень рано он ощутил интерес к естественным наукам. В 1968 году Андрей поступает в Колмогоровский интернат. В следующем едет — девятиклассником — на олимпиаду в Бухарест, где получает вторую премию (первой из наших школьников был награждён тогда лишь Володя Дринфельд — будущий филдсовский лауреат, второй, вместе с Андреем Ходулёвым, — Андрей Зелевинский и Андрей Прасолов). В 1970 году Андрей снова принимает участие в международной олимпиаде в Кештели (Венгрия), где получает высший балл и первую премию.

В том же году он поступает на мехмат. Его сразу увлекает программирование. Он начинает работать в группе студентов, которыми руководил Всеволод Серафимович Штаркман. После окончания Университета Ходулёв поступает в аспирантуру в Институт прикладной математики им. Келдыша, потом остаётся в этом Институте и вскоре становится одним из самых крупных специалистов в области программирования. Русский LaTeX во многом, как принято сейчас говорить, его «продукт».

* * * * * *

Я познакомился с Андреем Ходулёвым, когда он, будучи студентом 4 курса, слушал мои лекции по «Оптимальному управлению». Он, безусловно, был самым внимательным слушателем за всё время моего преподавания в Университете. В частности, он указал мне на существенную и достаточно глубоко скрытую ошибку при доказательстве принципа максимума, исправление которой сыграло довольно значительную роль в моём собственном понимании сути дела. Потом в течение нескольких лет Ходулёв был участником моего семинара по теории аппроксимации. В этом семинаре он сделал несколько работ, две из которых были опубликованы, а одна занимает краеугольное положение в весьма существенном разделе теории.

А теперь позвольте мне предоставить слово его другу Григорию Александровичу Гальперину, которому 11 сентября 1999 года, через день после смерти Андрея Борисовича Ходулёва (по просьбе покойного) было по e-mail'у отправлено его последнее послание (The last letter), начинавшееся словами:

```
I have died...
```

В. М. Тихомиров

Мой друг Андрей Ходулёв

Г. А. Гальперин

О жизни и творчестве А. Б. Ходулёва

Ушёл из жизни замечательный математик и выдающийся эксперт в области программирования Андрей Ходулёв. Он был одним из самых близких мне друзей. Смерть наступила 10 сентября 1999 г., когда Андрею было лишь немногим больше 45 лет. Его смерть ошеломила меня. Андрей находился в самом расцвете своих творческих сил. Наше интенсивное общение продолжалось непрерывно почти 30 лет, с момента моего знакомства с Андреем в Колмогоровском интернате №18 в 1969 году, когда оба мы были ещё школьниками. Уже тогда Андрей поразил меня независимостью и яркостью своего мышления.

Андрей Ходулёв был замечательным, добрым и скромным человеком, обладая при этом поистине неординарным и гибким умом, широта и глубина которого всегда поражали. Он, будучи выдающимся математиком, глубоко знал физику, астрономию и химию. Я часто заставал Андрея с журналом «Радио» в руках и неоднократно был свидетелем, как он играючи собирал сложные электронные «штучки», состоящие из транзисторов, микросхем и других устройств. Выписывал Андрей также журнал «Земля и Вселенная», из которого он цитировал интересные сведения: о расположении планет вдоль одной прямой («сизигии») в 1805, 1845, 1982 и 2357 годах и влиянии этого события на земную орбиту; о солнечной активности; о чёрных дырах; и о многом другом, не менее интересном. Андрей высчитывал все затмения и расположения звёзд на небе, и он так мечтал увидеть солнечное затмение в августе 1999 года! В начале 90-х годов мы как-то разговорились с ним о связи математики, физики и астрономии, и Андрей заметил: «Ты забыл ещё химию, которая не менее интересна. К сожалению, я не силён в биологии, но судя по генетике (её математической части), биологию тоже было бы здóрово изучить!» Вот выдержка из его письма: «Занимаюсь химией. Ещё читаю книги. Посылаю тебе некоторые фотографии (абстрактные). На досуге можешь подумать, что там изображено, я тебе сообщать не буду».

При обсуждении той или иной математической теории Андрей зачастую привлекал известные ему факты и идеи из других естественных

наук. Вот один пример: мы писали с ним совместную работу по небесной механике [1] (частный случай задачи четырёх тел с нулевой массой), и нужно было доказать одну лемму, которая не сразу далась нам, но после нескольких попыток и одного замечания Андрея (которое я сейчас не помню) это удалось сделать. Я спросил, как ему пришло в голову такое соображение, и он ответил: «Как-то я наблюдал движение роя мух в комнате. По-моему, оно напоминает движение галактик: сначала мухи разлетаются далеко, а потом сближаются, их скорости возрастают, они делают $1 \div 1{,}5$ оборота друг вокруг друга и разлетаются, а потом сближаются и разбиваются на группы, которые затем движутся независимо; в каждой же группе мухи летают вокруг некоторого центра по эллиптическим орбитам, причём они, как и галактики, стремятся попасть в одну плоскость, а не образовывать, например, нечто вроде шара. Это наблюдение и подало мне мысль, как подойти к решению. Иногда бывают и тройные сближения. Чаще всего они происходят по такой схеме: после взаимодействия двух мух, одна из них, не погасив скорости, сразу же сталкивается с третьей. По-видимому, собрав большую кучу мух — штук 1000 или больше, можно наблюдать явления, характерные для астрономических масштабов, — неоднородность, спирали, волокна». В другой раз мы обсуждали с Андреем отрывок из книги Анри Пуанкаре «Наука и гипотеза» ([2, стр. 122–125]), связанный с вероятным распределением малых планет на зодиаке. Пуанкаре подробно рассмотрел случай равномерного распределения материи и лишь вскользь упомянул о её действительном распределении, в котором изображающие точки образуют как бы дискретные атомы. Андрей сейчас же выдвинул более реальную гипотезу («сферическое распределение») и стал заниматься вычислением соответствующего интеграла, используя по ходу вычислений разнообразные физические соображения, помогающие упростить эти вычисления. В результате он подтвердил утверждение Пуанкаре о маловероятном распределении малых планет вдоль спиралей специальной формы.

Незадолго до окончания школы-интерната Андрей выбирал, в какой Международной Олимпиаде ему лучше участвовать — в математической или физической, и он выбрал математическую (на которой он получил первую премию, как до этого получал на Всесоюзных математических олимпиадах и на физико-математических олимпиадах Физтеха). В результате Андрей был принят без экзаменов на мехмат МГУ, с успехом закончил его, а затем поступил в аспирантуру[1)] ИПМ (Институт

[1)] При поступлении в аспирантуру у Андрея, как и у многих его сокурсников, возникли трудности со сдачей экзамена по истории КПСС. Сейчас можно только шутить по этому поводу, но тогда нам было не до шуток. Но и в истории КПСС Андрей умудрялся находить математические закономерности. Вот составленная им таблица годов съездов партии, начиная с XIV съезда:

прикладной математики), после окончания которой стал сотрудником ИПМ.

Любовь Андрея к программированию проявилась ещё на первом курсе мехмата, когда нам начал читаться курс программирования. Андрей сразу стал среди студентов признанным авторитетом в этой области; это проявлялось, в частности, в том, что чуть ли не весь курс ходил к нему сверяться в правильности составления того или иного алгоритма или программы для ЭВМ. За последующие годы талант и мастерство Ходулёва в программировании отшлифовались настолько, что он стал одним из крупнейших специалистов в этой области не только в России, но и во всём мире (его приглашали консультировать в разные страны Европы и в Японию). Недаром Андрею был поручен в 80-х годах перевод (вместе с его бывшими сокурсниками Надей Вьюковой и Володей Галатенко) книги Дональда Кнута «Искусство программирования для ЭВМ», а в 90-х годах он стал редактором перевода другой книги Д. Кнута «Concrete Mathematics» (авторы R. L. Graham, D. E. Knuth, O. Patashnik), вышедшей в издательстве «Мир» (перевод Б. Б. Походзея и А. Б. Ходулёва). Кроме того, Ходулёв является создателем шрифтов для русского LaTeX'а, о чём я узнал весной 1999 г. от него самого.

К его компьютерным талантам я отношу также особую способность и любовь Андрея к головоломкам. (Цитата из его письма: «Во время отдыха я, от нечего делать, рассчитал очко (карточную игру). Я раньше рассчитывал его с меньшей точностью. В этот раз результаты оказались существенно другими. Но выяснилось, что и нынешняя точность недостаточна — надо привлекать компьютер».) Андрей участвовал, с момента их возникновения, в нескольких мировых чемпионатах по головоломкам (World Puzzle Championships), как член команды России, и неизменно показывал на этих соревнованиях высокий результат. И, несмотря на смертельную болезнь, которая стала проявляться уже и внешне, Андрей решил и в этот, последний раз (1998), участвовать в соревновании и занял одно из первых мест. Как написала мне Ольга Леонтьева (председатель жюри этого чемпионата в том году, хорошо знавшая Андрея и уговаривавшая его не ездить на соревнования 1998 года), «только потом я поняла, насколько это было правильно, важно и красиво: он ушёл непобеждённым!»

№ съезда	XIV		XV		XVI		XVII		XVIII	
Год	25		27		30		34		39	
Разность		2		3		4		5		
№ съезда	XIX		XX		XXI		XXII		XXIII	XXIV
Год	52		56		59		61		66	71
Разность		4		3		2		5	5	

Ну чем не таблица в стиле аналогичных таблиц из книги В. И. Арнольда [3]?!

О компьютерных талантах Ходулёва должны свидетельствовать его коллеги по работе. Я же ограничусь тем, что написал выше, и далее коснусь только его математических талантов и удивительной (иногда непостижимой для меня) интуиции Андрея, его способности «видеть» ответы на очень трудные математические вопросы и одновременно предчувствовать направление, в котором следует искать решение. Особенно здорово это ему удавалось, когда он опирался на аналогии из других естественных наук. Одну из таких аналогий я уже упомянул, и ниже я приведу другие примеры, заимствованные мной из нашей с Андреем многолетней переписки по разным вопросам.

Эта переписка была особенно интенсивной в годы нашего студенчества и аспирантуры (1972–77) и в последние 5 лет (1994–99) по e-mail'у (всего более 100 писем). В 80-е и в начале 90-х годов мы поддерживали интенсивное интеллектуальное общение «устно», когда встречались в МГУ на Московском Математическом Обществе или же у Андрея дома (а иногда в редакции журнала «Квант») и обсуждали разные теории и конкретные задачи. Часть этих обсуждений вылилась в статьи (совместные и порознь), препринты и заметки (например, в решения задач в «Задачнике Кванта», см. [1], [4], [5]), ещё большая часть «осела» в черновых бумагах, многие из которых, увы, с течением лет бесследно пропали, хотя кое-что и сохранилось).

Как правило, идеи и решения Андрея Ходулёва были не только глубоки, но и изобретательны — он умел находить «изюминку» в даже, казалось бы, рутинных вычислениях. Андрей любил и «чувствовал» числа — см. его решение задачи №12 во второй части статьи. Упомянутая уже страсть Андрея к программированию (в широком смысле этого слова), сплавленная с глубокими знаниями, позволяли ему делать «синтетические ходы» в решении трудных задач и видеть в них «невидимое». Особенно изобретателен Андрей был в придумывании примеров и контрпримеров, поэтому довольно часто он находил неожиданные возражения к ясным, казалось бы, формулировкам или гипотезам. Один его неожиданный пример состоял в том, что если хорда, как жесткий отрезок, скользит своими концами по внутренности *выпуклой* гладкой кривой, то фиксированная точка на хорде не обязательно будет описывать *выпуклую* кривую![2)]

А вот какой контраргумент привел Андрей по поводу общепринятого взгляда на поведение фигур Лиссажу на экране осциллографа. (И опять этот сплав математики и физики, и даже нейрофизиологии!). Если подавать два независимых гармонических колебания с частотами ω_1 и ω_2 на

[2)] Читатель, попробуй и ты самостоятельно привести такой пример! Казалось бы, просто как Колумбово яйцо, но сразу не получится. А если не знать о его существовании, — пример с окружностью вводит в заблуждение! — то можно подумать, что такого не бывает.

горизонтальную и вертикальную развёртки осциллографа, то на экране будет видна кривая (как правило, медленно вращающаяся), похожая на параболу, или эллипс, или «восьмёрку», или несколько соединённых вместе «восьмёрок». Известно (см. задачу на стр. 26 книги В. И. Арнольда [6]), что если отношение частот $\omega = \omega_1/\omega_2$ *рационально*, то фигура Лиссажу — замкнутая алгебраическая кривая (при целом ω это график многочлена Чебышёва), а если ω *иррационально*, то она заполняет экран осциллографа всюду плотно. (Таково же поведение частицы в прямоугольном биллиарде). Отсюда, казалось бы, должно следовать, что при иррациональном отношении частот мы должны видеть весь экран осциллографа полностью светящимся. Каково же было моё удивление, когда я узнал от Андрея, что иррациональность ω никакой роли не играет и никакого свечения экрана не будет!

Цитирую Андрея: «Утверждение о вращающейся фигуре Лиссажу верно лишь в очень грубой абстракции. На самом деле, вращение связано с инерцией зрения, и условие вращения может быть записано в таком виде:

$$\frac{\omega_1}{2\pi m} \gg \frac{1}{\tau}\,, \quad \frac{\omega_2}{2\pi n} \gg \frac{1}{\tau}\,, \quad \frac{|2\pi n\omega_1 - 2\pi m\omega_2|}{\max(m,n)} \ll \frac{1}{\tau}\,,$$

где τ — время инерции глаза. Мы будем видеть вращающуюся фигуру Лиссажу с m колебаниями по одной оси и с n — по другой, при этом неважно, рационально или нет отношение ω. Вообще, как известно, рациональность или иррациональность непрерывной физической величины нельзя установить с помощью эксперимента».

Андрея Ходулёва любили все — его друзья, его учителя, его коллеги: со всеми он щедро делился своими знаниями и многочисленными идеями. Ему всегда было интересно, что же происходит в действительности, он всегда стремился узнать как можно больше нового, и он неустанно думал о том, как бы попроще и элегантнее объяснить то или иное явление, будь оно из математики, физики, химии или астрономии. Андрею удалось сохранить до конца своих дней юношеский задор, стремление ко всему новому, умение удивляться и полнокровно жить. Он заряжал своей энергией всех, кто оказывался рядом, и мы, его друзья, благодарны Андрею за то, что нам посчастливилось с ним общаться и «подзаряжаться» частицами его «научной» энергии.

Мне хочется закончить этот рассказ следующей цитатой из письма Андрея ко мне, датированного 13 июля 1973 г.: «...Вскоре (с 17 июля) я уеду отдыхать в точку $44°34'$ с. ш. и $38°12'$ в. д. Я пробуду там секунд $1{,}8 \cdot 10^6$, так что ты не сможешь написать мне вскоре. До свидания. Андрей». Это письмо — одно из десятков других типично ходулёвских писем, которые я получил от Андрея.

Последнее из них датировано 11 сентября 1999 года...

Задачи, проблемы, идеи, конструкции

Мы с Андреем обсуждали множество разнообразных и интересных вопросов, часть из которых я излагаю ниже. Однако еще большее число проблем (и подходов к их решению) так и остались нерешенными. Я решил взять на себя смелость привести примеры обсуждавшихся вопросов и идей из обеих групп.

Изложенный ниже материал носит «мозаичный» характер в стиле «Математической смеси» Дж. Литтлвуда и не претендует на полноту или завершенность. В его основу положено содержание примерно 100 писем и e-mail'ов, которыми мы обменялись, и тех черновиков, которые мне удалось сохранить. Здесь я описываю наиболее яркие и интересные задачи, которыми мы обменивались, а также частичные результаты, которые мы получили или надеялись получить. К сожалению, из-за ограниченности журнального объёма, я могу привести лишь малую долю этих материалов. Естественно, я выбрал задачи по своему вкусу; возможно, Андрей выбрал бы другое их подмножество.

♦♦♦

№1 (Многочлен от многочленов). *Пусть $f(x)$ и $\varphi(x)$ — два вещественных многочлена. Всегда ли существует такой многочлен от двух переменных $R(u,t)$, что $R(f(x),\varphi(x))=0$?*

Решение. Ответ: «всегда». Пусть $\deg f \cdot \deg\varphi = mn$. Рассмотрим «квадрант» многочленов $\{f^k\cdot\varphi^s\}$, $k,s\geqslant 0$, и большой прямоугольный треугольник, отсекаемый прямой от квадранта (см. рис. 1). Тогда среди многочленов, лежащих в треугольнике, лишь часть линейно независима в пространстве многочленов степени $\leqslant mn$; действительно, количество

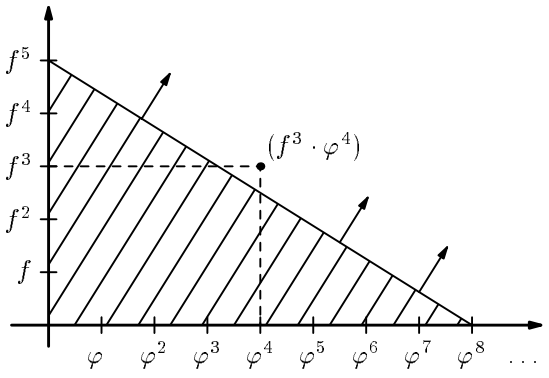


Рис. 1. *Квадрант и треугольник многочленов*

точек в треугольнике растет квадратично, а движение гипотенузы происходит линейно. Следовательно, имеется нетривиальная линейная комбинация многочленов, тождественно равная 0. Она и есть искомый многочлен.

♦♦♦

№2 (Шкаф в комнате). *Может ли треугольный шкаф «заклинить» в треугольной комнате (т. е. не существует движения шкафа, оставляющего его внутри комнаты)? А многоугольный шкаф в многоугольной комнате? (Оба многоугольника — выпуклые.)*

Обсуждение. Замечание Ходулёва: «Я не совсем понимаю, что значит „заклинить“. Я считаю, что это означает следующее: все вершины шкафа лежат на разных сторонах комнаты — но не в углах — и шкаф не может осуществить никакое малое движение. Иначе неинтересно (рис. 2).

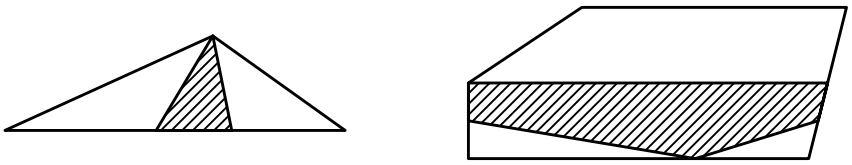


Рис. 2. *«Заклинившие» шкафы (вырожденный случай)*

В этой постановке я полностью решил задачу. Ответ: при $n = 3$ не может заклинить, хотя решение непростое, с несколькими случаями (между прочим, используется утверждение, которое мы с тобой обсуждали: *если есть 3 полуплоскости, то либо их пересечение имеет непустую внутренность, либо пересечение их дополнений имеет непустую внутренность, либо их границы пересекаются*)».

На это я ответил Андрею, что возможно такое решение (рис. 3): если шкаф-треугольник ABC лежит внутри комнаты $\triangle XYZ$ и $A \in XY$, $B \in \in YZ$, то геометрическое место точек C во время движения отрезка AB вдоль стен — дуга эллипса с центром в Y (при этом Y — пересечение осей

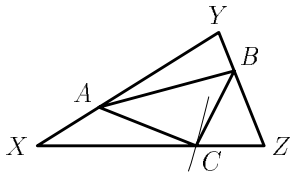


Рис. 3. *C движется по дуге эллипса*

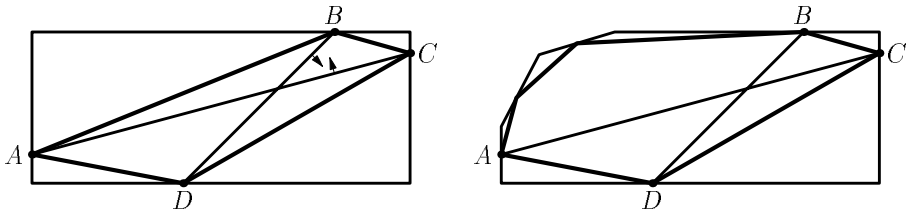


Рис. 4. *«Заклинившие» шкафы* ($n \geqslant 4$) *(невырожденный случай)*

эллипса). Кусочек этой дуги лежит внутри $\triangle XYZ$, поэтому «шевеление» шкафа внутри комнаты осуществимо.

Он согласился со мной и не стал присылать своего решения, о чём я сейчас сожалею. Для $n > 3$ Ходулёв построил примеры, в которых шкаф заклинивает (рис. 4). Для $n = 4$ диагональ AC может повернуться только против часовой стрелки, а диагональ BD — только по часовой (рис. 4а). Полученное противоречие и доказывает «заклинивание» шкафа. Для любого $n > 4$ пример «заклинившего» шкафа можно построить, исходя из этого примера (рис. 4б).

Я хочу отметить здесь ту самую «изюминку», которую нашел Андрей: противоречие возникает из-за того, что «что-то вращается не в ту сторону» (в данном случае, отрезки AC и BD).

В таких вот «изюминках» и проявлялся талант Андрея.

♦♦♦

№3 (Предел). *Пусть z — комплексное число. Найти предел*

$$\lim_{m\to\infty} \sum_{n=-m}^{m} \frac{1}{z+n}$$

для тех z, для которых он существует.

Решение. Рассмотрим следующую 2π-периодическую функцию $f(x)$ вещественного переменного:

$$f(x) = e^{-izx} \text{ при } |x| < \pi,$$
$$f(x+2\pi) = f(x).$$

Разложим ее в ряд Фурье. Коэффициент a_n равен

$$a_n = \frac{1}{2\pi}\int_{-\pi}^{\pi} e^{-izx}e^{-inx}\,dx = \frac{1}{2\pi}\int_{-\pi}^{\pi} e^{-i(z+n)x}\,dx =$$

$$= -\frac{1}{2\pi i(z+n)}\left(e^{-i(z+n)\pi} - e^{i(z+n)\pi}\right) = -\frac{e^{in\pi}}{2\pi i(z+n)}\left(e^{-iz\pi} - e^{iz\pi}\right) =$$
$$= -\frac{(-1)^n}{\pi(z+n)}\frac{e^{iz\pi} - e^{-iz\pi}}{2i} = \frac{(-1)^n \sin \pi z}{\pi(z+n)}\,.$$

Поскольку $f(x)$ кусочно непрерывна и дифференцируема, имеем

$$\frac{f(x^+)+f(x^-)}{2} = \lim_{m\to\infty}\sum_{n=-m}^{m} a_n e^{inx} = \lim_{m\to\infty}\sum_{n=-m}^{m}\frac{(-1)^n \sin \pi z}{\pi(z+n)}e^{inx} =$$
$$= \frac{\sin \pi z}{\pi}\lim_{m\to\infty}\sum_{n=-m}^{m}\frac{(-1)^n e^{inx}}{z+n} = \frac{\sin \pi z}{\pi}\lim_{m\to\infty}\sum_{n=-m}^{m}\frac{e^{in(x-\pi)}}{z+n}\,.$$

Подставим $x = \pi$ в эту формулу, тогда в силу периодичности f

$$\frac{f(\pi^+)+f(\pi^-)}{2} = \frac{f(\pi^-)+f(-\pi^-)}{2} = \frac{e^{-iz\pi}+e^{iz\pi}}{2} = \cos \pi z.$$

Таким образом,

$$\cos \pi z = \frac{\sin \pi z}{\pi}\lim_{m\to\infty}\sum_{n=-m}^{m}\frac{1}{z+n},$$

откуда

$$\lim_{m\to\infty}\sum_{n=-m}^{m}\frac{1}{z+n} = \pi \cdot \operatorname{ctg} \pi z.$$

Равенство выполняется для любого комплексного z, для которого $\sin \pi z \neq$ $\neq 0$, т. е. для всех комплексных $z \notin \mathbb{Z}$. При $z \in \mathbb{Z}$ предел не существует по очевидным причинам.

♦♦♦

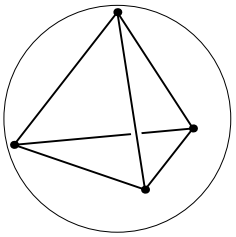
№4 (Электроны на сфере). *На внутренней стороне металлической сферы располагаются N электронов — точечных частиц равной (единичной) массы и равного отрицательного заряда (полагаем его равным -1). В силу отталкивания электронов, они стремятся улететь на бесконечность, но им мешает сфера, и поэтому электроны «разбегаются» по сфере так, чтобы минимизировать потенциальную энергию системы*

$$U = \sum_{i\neq j}\frac{1}{|\vec{r}_i - \vec{r}_j|}\,,$$

здесь $\vec{r}_i$ и $\vec{r}_j$ — радиус-векторы, идущие из центра сферы в электроны i и j, $|\vec{r}_i - \vec{r}_j|$ — расстояние между электронами. Для каждого числа $N = 2, 3, 4, \ldots$ электронов указать их расположения на сфере, минимизирующие потенциальную энергию.

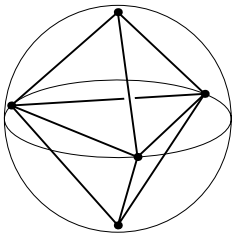
Таблица расположения электронов на сфере

$N = 4$

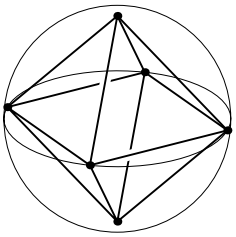


правильный тетраэдр

$N = 5$

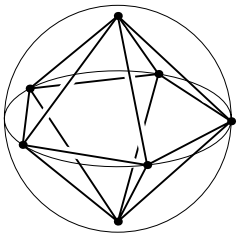


$N = 6$



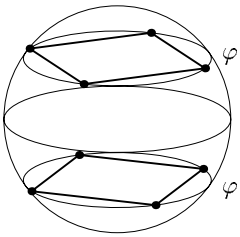
правильный октаэдр

$N = 7$



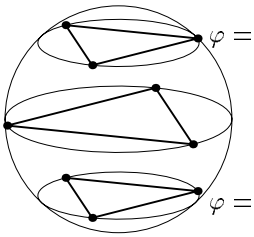
правильный пятиугольник в
экваториальной плоскости

$N = 8$



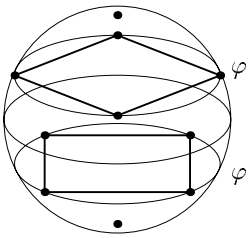
квадраты развернуты на 45°

$N = 9$



правильные треугольники,
экваториальный развернут на 180°

$N = 10$



квадраты развернуты на 45°

$N = 11$

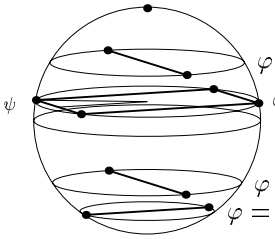
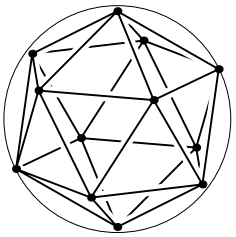


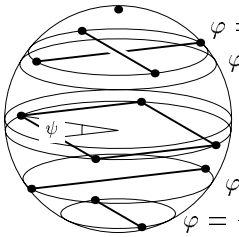
Таблица расположения электронов на сфере (продолжение)

$N = 12$

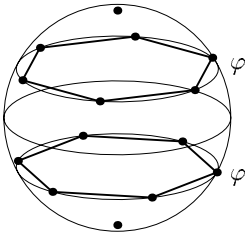


правильный икосаэдр

$N = 13$

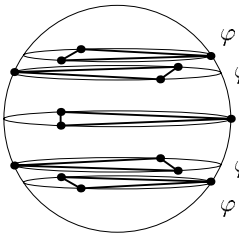


$N = 14$



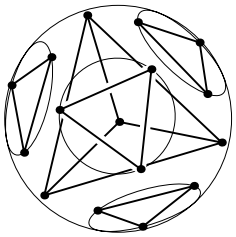
правильные шестиугольники развернуты на 30°

$N = 15$



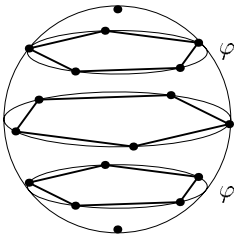
все треугольники — правильные; крайние развернуты относительно экваториального на угол $\pm 6{,}96°$, средние развернуты на $180° \pm 5{,}62°$

$N = 16$



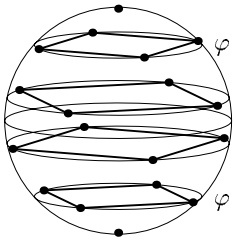
правильные треугольники над гранями тетраэдра имеют угловой размер $30{,}7°$, каждый из них повернут относительно прямой, соединяющей его центр и противоположную вершину тетраэдра на $7{,}29°$

$N = 17$



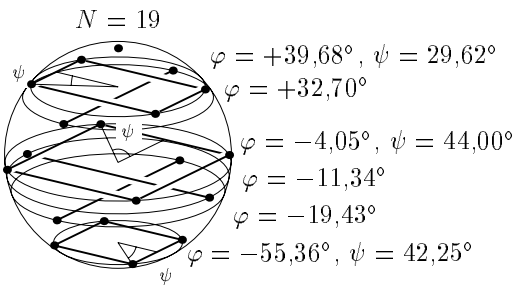
все пятиугольники — правильные

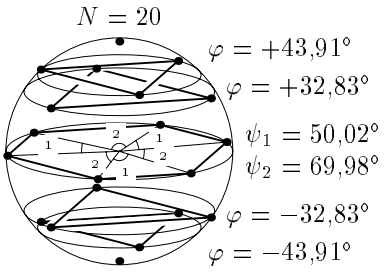
$N = 18$



квадраты последовательно сверху вниз разворачиваются на 45°

Таблица расположения электронов на сфере (окончание)





плоскости симметрии правильных треугольников совпадают с плоскостями симметрии центрального шестиугольника

Обсуждение. Решение этой задачи для $N = 2, 3, 4, 6$ и 12 приведено в статье Н. Н. Андреева и В. А. Юдина [7]. Я привел эту задачу здесь для того, чтобы показать результаты работы на ЭВМ, проделанной А. Ходулёвым. Я поставил этот вопрос перед Андреем в 1974 году на четвертом курсе мехмата, когда стал преподаваться курс «Оптимальное управление» (ОПУ) под руководством «двух Владимиров Михайловичей» — профессоров МГУ В. М. Алексеева и В. М. Тихомирова. Мне он сразу пришел в голову, когда я соединил две идеи — задачу о минимизации расположения точек на сфере, в которой целевая функция $\min\limits_{i\neq j} |\vec{r}_i - \vec{r}_j| \to \max$ (эта задача частично исследовалась в известной книге по геометрии Шклярского, Ченцова и Яглома [9]), и новые сведения из ОПУ. Андрей с радостью воспринял эту задачу, но через некоторое время написал мне: «ОПУ не особенно применимо к задаче про электроны. Здесь годится только обычное конечномерное правило множителей Лагранжа, но оно мало помогает. Эту задачу можно решить на ЭВМ». Что он с блеском и проделал! (См. таблицу расположения N электронов для $N = 4, \ldots, 20$ на сс. 17–19). Задача про электроны воодушевила Андрея еще и тем, что он «...смог почерпнуть некоторые сведения в учебнике по химии. Рассмотрим атом A, имеющий N валентных электронов и пусть он образует молекулу AB_N. Из соображений симметрии, N атомов элемента B расположатся на равном расстоянии от A, т. е. на поверхности сферы, и между ними будет действовать сила электростатического отталкивания. Экспериментально установлены конфигурации таких молекул с разными $N = 1, \ldots, 7$. Там же приведены картинки: для $N = 4$ — тетраэдр, для $N = 5$ — два тетраэдра с общей треугольной гранью; для $N = 6$ — октаэдр и для $N = 7$ — две пятиугольные пирамиды, прикреплённые друг к другу своими общими пятиугольными основаниями. Можно предположить, что

электроны займут на сфере такое же положение. Так химия помогает математике».

Я считаю эту задачу достойной того, чтобы передоказать результаты Ходулёва, объяснить их теоретически (т. е. переоткрыть метод, которым он нашёл глобальные минимумы) и продолжить таблицу для $N > 20$.

♦♦♦

№5 (Шахматный король[3]). *Шахматный король обошел все клетки шахматной доски ровно по одному разу и вернулся в исходную клетку, причём он нигде не пересекал своего следа. Доказать, что король сделал не менее* 28 *коротких ходов* (*см. рис.* 5). *Найти верхнюю оценку числа коротких ходов для шахматной доски* $m \times n$. *Точна ли эта оценка?*

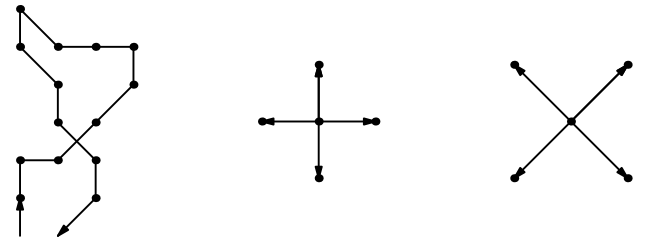


Рис. 5. *Ходы короля*

Решение. Маршрут короля — замкнутая несамопересекающаяся ломаная. Король побывал везде, в частности, во всех $2m + 2n - 4$ клетках периметра. Эти клетки разбивают всю ломаную на $2m + 2n - 4$ кусков. Основное утверждение:

Каждый кусок соединяет две соседние клетки периметра.

Действительно, если бы кусок соединял не соседние клетки, то клетки периметра оказались бы разделенными на две части и король не смог бы побывать в обеих частях, не пересекая куска (рис.6). Основное утверждение доказано.

Теперь заметим, что соседние клетки периметра разноцветны, а единственная возможность для короля перейти на клетку другого цвета — это сделать короткий ход. Значит, в каждом куске будет по крайней мере один короткий ход, а кусков по крайней мере $2m + 2n - 4$.

[3] Из письма Ходулёва: «Теперь у меня есть время сообщить тебе мою задачу, про которую я недавно говорил. По-моему, она достойна II тура Московской олимпиады или даже Всесоюзной». Действительно, достойна! Я тут же сообщил об этой задаче Н. Б. Васильеву, и она попала на 7-ю Всесоюзную олимпиаду по математике (Кишинёв, 1973), а потом была опубликована под номером 184 в сборнике задач [8].

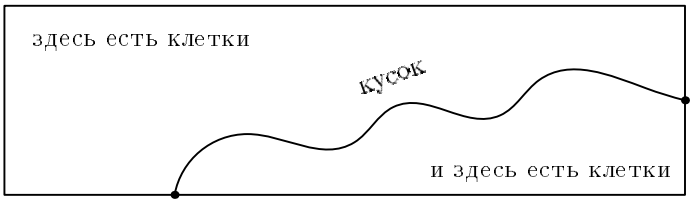


Рис. 6. *Основное утверждение*

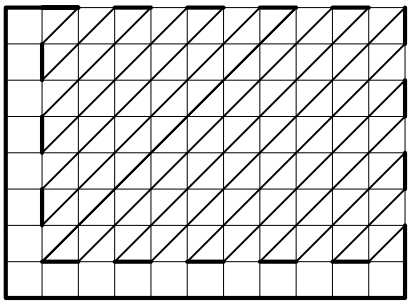


Рис. 7. $2m + 2n - 4$ *хода короля, покрывающих всю доску*

Поэтому ответ: $\geqslant 2m + 2n - 4$ *коротких хода.* Эта оценка точная. Пример, из которого ясна общая конструкция, приведён на рис. 7 (узлам решётки соответствуют центры клеток). Легко убедиться, что тут в каждом куске содержится ровно один *короткий* ход. «Это, конечно, не строго доказано, но что поделаешь», — добавляет Ходулёв. «Однако в случае обычной шахматной доски никаких неясностей, конечно же, нет».

♦♦♦

№6 (Минимальное число распилов[4)]). *Имеется некоторое тело, требуется распилить его определённым образом (известно, по каким линиям (в двумерном случае) или поверхностям (для трёх и большего числа измерений) это тело надо пилить). За какое минимальное число распилов это можно сделать, если разрешается накладывать части друг на друга и пилить их вместе?*

Мы рассмотрим здесь лишь частный случай этой задачи: *Распилить параллелепипед* $m \times n \times k$ *на кубики* $1 \times 1 \times 1$. *Аналогичная задача для многомерного параллелепипеда.*

[4)] В 70-е годы мы увлекались чтением недавно переведённых книг Мартина Гарднера. Мы с Андреем решили обобщить задачу Гарднера о распиле куба на 27 маленьких кубиков, если разрешается накладывать распиленные части одну на другую.

Решение. Сначала ответ: минимальное число распилов равно $N = \lceil \log_2 m \rceil + \lceil \log_2 n \rceil + \lceil \log_2 k \rceil$ (такой же ответ — только с большим числом слагаемых — справедлив и в многомерном пространстве).

Замечание. $\lceil x \rceil = \inf\{n \mid n \geqslant x;\ n \in \mathbb{Z}\} = -\lfloor -x \rfloor$, где $\lfloor \cdot \rfloor$ — целая часть числа.

Приведём сначала решение гарднеровской задачи: $m = n = k = 3$; $N = 3\lceil \log_2 3 \rceil = 3 \cdot 2 = 6$ распилов. Довольно красиво доказывается, что за меньшее число распилов нельзя получить 27 кубиков. Действительно, у центрального кубика надо выпилить все 6 граней, а за один распил нельзя выпилить сразу две грани! Решение в одну строчку!

Теперь общий случай. У каждой части, появившейся в процессе разрезания, имеются размеры, которые обозначим x, y и z. Мы считаем, что оси координат «вморожены» в эту часть с самого начала, так что размеры x, y и z не меняются при её повёртывании (которое может понадобиться для очередного распила).

После каждого распила мы выберем одну из полученных частей в соответствии со следующим индуктивным правилом:

1. До всех разрезаний мы выбираем единственную существующую часть — сам параллелепипед.

2. Пусть после предыдущего распила была выбрана часть с размерами x, y и z. Тогда после очередного распила эта часть может быть распилена на две, отличающиеся лишь в одной координате. (Например, если эта часть была распилена параллельно плоскости xz, то получатся части с размерами

$$x'_1 = x'_2 = x, \quad y'_1 + y'_2 = y, \quad z'_1 = z'_2 = z;$$

штрихи здесь означают новые размеры). После очередного распила выбирается та из двух частей, у которой «спиленная» координата (в данном случае y) *больше*. (Например, если часть $1\times5\times7$ распилена на части $1\times2\times7$ и $1\times3\times7$, то выбирается часть $1\times3\times7$). Если очередной распил не коснулся этой части, то она же и остаётся выбранной.

Таким образом, у нас получается последовательность выбранных убывающих частей, у каждой из которых некоторая (но только одна!) координата меньше, чем у предыдущей, но не более, чем в два раза; возможно, что у некоторых частей все координаты совпадают с предыдущими. Последняя часть, очевидно, имеет размер $1 \times 1 \times 1$ (слова «координата» и «размер» синонимы в данном контексте).

Рассмотрим теперь по-отдельности каждую из координат у выбранных частей. Поскольку каждый распил уменьшает каждую координату не

более чем вдвое, потребуется не менее $\lceil \log_2 m \rceil$ распилов, чтобы уменьшить x-координату с m до 1, и аналогично $\lceil \log_2 n \rceil$ и $\lceil \log_2 k \rceil$ распилов, уменьшающих y- и z-координату до 1.

Так как каждый распил уменьшает только одну координату (или ни одной), то всего потребуется *не менее*

$$N = \lceil \log_2 m \rceil + \lceil \log_2 n \rceil + \lceil \log_2 k \rceil$$

распилов.

Приведённого числа распилов достаточно. Надо сначала при помощи $\lceil \log_2 m \rceil$ распилов разрезать параллелепипед на слои $1 \times n \times k$, затем сложить все слои вместе и разрезать их за $\lceil \log_2 m \rceil$ распилов на полоски $1 \times 1 \times k$, и наконец, сложив все полоски вместе, разрезать их на кубики $1 \times 1 \times 1$.

Многомерный случай рассматривается аналогично.

♦♦♦

№7 (Солнечная система). *Некоторая солнечная система состоит из солнца и 8 вращающихся вокруг него по круговым орбитам планет, каждая планета со своей постоянной скоростью. Может ли случиться так, что в каждый момент все планеты располагаются в вершинах (движущегося во времени) куба с фиксированным ребром a? (Центр куба — не обязательно солнце. Солнце и все планеты предполагаются точечными и не взаимодействуют друг с другом).*

Обсуждение. Андрей и я придумали два независимых решения этой задачи, оба приведены ниже. Позже, разобравшись в существе дела, мы написали совместную статью на эту тему («Уплощение в задаче четырёх тел»), опубликованную в виде препринта ИПМ (см. [1]). Ответ в задаче отрицательный: *планеты не могут в каждый момент располагаться в вершинах некоторого движущегося куба фиксированного размера.*

♦♦♦

Решение 1 (А. Ходулёв). Предположим противное. Пусть A и B — вершины куба, плоскости орбит которых не совпадают. Рассмотрим произвольную сферу с центром в солнце O и спроецируем точки A и B радиально на эту сферу (рис. 8а). Тогда их проекции C и D будут двигаться равномерно по двум несовпадающим большим кругам, причём дуга CD будет оставаться постоянной: $\smile CD = \angle AOB$ и в треугольнике AOB все стороны постоянны. Обозначим через v_1 и v_2 скорости точек C и D, а их траектории — через γ_1 и γ_2. Пусть P — одна из точек пересечения $\gamma_1 \cap \gamma_2$, а угол между траекториями равен φ. Допустим, что в момент времени t точка C проходит через P.

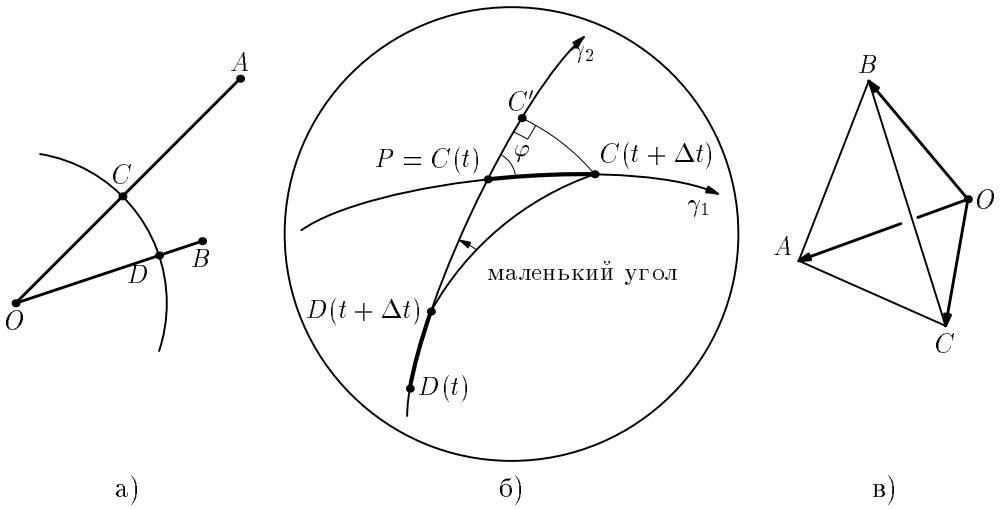


Рис. 8. *Движение проекций планет по сфере и тетраэдр $OABC$*

Выберем малое $\Delta t > 0$ и рассмотрим момент $t + \Delta t$. Имеем

$$\smile C(t+\Delta t)D(t+\Delta t) = \smile CD.$$

Повернём дугу $\smile C(t+\Delta t)D(t+\Delta t)$ вокруг точки $D(t+\Delta t)$ на соответствующий — очень маленький — угол так, чтобы точка $C(t+\Delta t)$ попала в некоторую точку C' круга γ_2 (рис. 8 б). Поскольку угол поворота мал, можно считать, что отрезок дуги $C(t+\Delta t)C'$ примерно перпендикулярен окружности γ_2. Тогда $\smile C(t)C(t+\Delta t) = v_1\Delta t$ и $\smile C(t)C' = v_1\Delta t\cos\varphi$. Из равенства

$$\smile D(t+\Delta t)C' = \smile D(t+\Delta t)C(t+\Delta t) = \smile D(t)C(t)$$

следует

$$\smile C(t)C' = \smile D(t)D(t+\Delta t) = v_2\Delta t.$$

Следовательно, $v_2\Delta t = v_1\Delta t\cos\varphi$, откуда

$$v_2 = v_1\cos\varphi. \qquad (*)$$

Проведя аналогичное рассуждение, когда точка D проходит через P, получаем

$$v_1 = v_2\cos\varphi, \qquad (**)$$

т. е. $\cos\varphi = \pm 1$, что означает, что орбиты γ_1 и γ_2 совпадают. Противоречие. Значит, искомого движения планет не существует.

♦♦♦

Решение 2 (Г. Гальперин). Ключом к этому решению является

Лемма. *Если расстояние между двумя планетами постоянно во времени, то периоды обращения планет совпадают.*

Итак, периоды обращения всех восьми планет одинаковы, и пусть они равны T.

Выберем из куба такие его вершины A, B и C, чтобы точки O, A, B и C не лежали в одной плоскости (рис. 8 в). В тетраэдре $OABC$ все рёбра постоянные (их длины не зависят от времени), поэтому ни в один момент эти четыре точки не лежат в одной плоскости. Следовательно, смешанное произведение векторов $\overrightarrow{OA}$, $\overrightarrow{OB}$, $\overrightarrow{OC}$ (ориентированный объем параллелепипеда, натянутого на эти векторы) не равно нулю:

$$V(t) \stackrel{\text{def}}{=} (\overrightarrow{OA}, [\overrightarrow{OB}, \overrightarrow{OC}]) \neq 0.$$

Однако через полпериода $t = T/2$, все планеты переместятся в диаметрально противоположные позиции и, следовательно, все векторы $\overrightarrow{OA}$, $\overrightarrow{OB}$, $\overrightarrow{OC}$ изменят свой знак на противоположный. Отсюда $V(T/2) = -V(0)$. Поскольку V непрерывно зависит от параметра t, найдётся момент времени t_0, в который $V(t_0) = 0$. В этот момент точки O, A, B, C становятся компланарными и мы получаем противоречие.

♦♦♦

№8 (Вращение и гомотетия). *В $\mathbb{R}^{13}$ расположено 7-мерное тело. Можно ли его так вращать, чтобы ортогональная проекция этого тела («тень») на подпространство $\{\vec{e}_1, \ldots, \vec{e}_7\}$ уменьшалась бы гомотетично?*

Решение. Ответ: «нельзя». Пусть, напротив, можно, и пусть A — соответствующий поворот. В базисе $E = \{\vec{e}_1, \ldots, \vec{e}_7, \ldots, \vec{e}_{12}, \vec{e}_{13}\}$ матрица A размера 13×13 имеет вид ($0 < \lambda < 1$ — коэффициент гомотетии):

$$A = \begin{pmatrix} \lambda & \ldots\ldots & 0 & \ldots \\ 0 & \lambda \ \ldots & 0 & \ldots \\ 0 & 0 \ \ldots & 0 & \ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots & & & \\ 0 & 0 \ \ldots & \lambda & \ldots \\ \alpha_{8,1} & \ldots\ldots & \alpha_{8,7} & \ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots & & & \\ \alpha_{13,1} & \ldots\ldots & \alpha_{13,7} & \ldots \end{pmatrix}.$$

Напишем условия ортогональности матрицы A для первых 7 столбцов:

7 уравнений	$\alpha_{8,r}^2 + \ldots + \alpha_{13,r}^2 = 1 - \lambda^2$	$(r = 1, \ldots, 7)$,
21 уравнение	$\alpha_{8,r}\alpha_{8,k} + \ldots + \alpha_{13,r}\alpha_{13,k} = 0$	$(1 \leqslant r < k \leqslant 7)$.

Рассмотрим теперь семь 6-мерных векторов

$$\vec{a}_1 = (\alpha_{8,1}, \ldots, \alpha_{13,1}),\ \ldots,\ \vec{a}_7 = (\alpha_{8,7}, \ldots, \alpha_{13,7}) \in \mathbb{R}^6$$

одинаковой длины $\sqrt{1-\lambda^2}$ и попарно ортогональных. А тогда векторы $\vec{a}_1, \ldots, \vec{a}_7$ линейно независимы в $\mathbb{R}^6$ — противоречие.

♦♦♦

№9 (Рациональные расстояния и пифагоровы тройки).
В 1975 году я предложил следующую задачу на Международную Математическую олимпиаду:

Задача А. *Можно ли на окружности радиуса* 1 *расположить* 1975 *точек так, чтобы все попарные расстояния между ними были рациональными числами?*

Идея решения этой задачи основывалась на том, что существуют пифагоровы тройки: $a = q^2 - p^2$, $b = 2pq$, $c = p^2 + q^2$, так что треугольник со сторонами a, b, c — прямоугольный.

Позже я поставил другой вопрос:

Задача Б. *Пусть имеется множество S точек в $\mathbb{R}^n$, все попарные расстояния между которыми — рациональные числа. Верно ли, что это множество конечно или счётно?*

Я решил эту задачу положительно следующим образом. Пусть сначала $n = 2$ (плоскость). Возьмём две точки $A, B \in S$ и сопоставим каждой точке $X \in S$ пару расстояний до точек A и B. Хотя по расстояниям AX и BX точка X не восстанавливается однозначно, но — не более, чем двузначно, как пересечение двух окружностей с центрами A, B и радиусами AX, BX (рис. 9а). Таким образом, каждая точка $X \in S$ имеет рациональные координаты в построенной системе координат, откуда мощность множества S не превышает $\aleph_0$. Аналогично решение и для $\mathbb{R}^n$: выбираем n «базовых» точек из S и приписываем каждой точке $X \in S$ n координат — расстояний от X до базовых точек. Получаем множество «рациональных» точек в $\mathbb{R}^n$, так что $|S| \leqslant \aleph_0$. (Точка X определяется неоднозначно, но не более, чем двузначно, — как пересечение n сфер размерности $n-1$. Детали довольно хлопотно описывать, и мы их здесь опускаем).

Я предложил обе задачи Андрею Ходулёву и получил от него очень интересный и неожиданный ответ. Решал он их в обратном порядке, сначала задачу Б, потом А. Его решение основывалось на следующей лемме.

Лемма. *На любой сфере $S^k \subset \mathbb{R}^n$ размерности $k = 0, 1, \ldots, n-1$ с любым центром содержится не более чем счётное множество точек из S.*

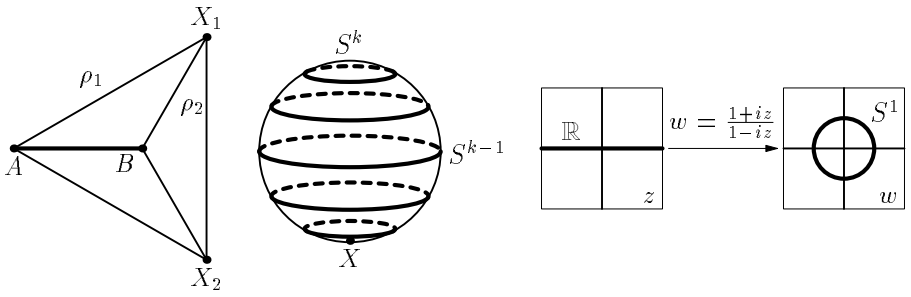


Рис. 9.

Доказательство. Индукция по k. Если на сфере S^k имеется ненулевое число точек нашего множества, то выберем одну из них — X. Разобьём S^k на «параллели» S^{k-1}: каждая сфера S^{k-1} состоит из точек, равноудалённых от X (см. рис. 9б). Тогда всё множество $S \cap S^k$ должно быть сосредоточено на не более чем счётном числе таких $k-1$-мерных сфер, соответствующих рациональным расстояниям, и на каждой сфере содержится не более, чем счётное число точек из S. □

Возьмём теперь любую точку $O \in S$ и рассмотрим всевозможные сферы S^{n-1} с центром O, объединение которых содержит всё множество S. В силу рациональности всех расстояний от O до остальных точек множества S, число сфер S^{n-1} не более чем счётно. Согласно лемме на каждой сфере S^{n-1} имеется не более чем счётное множество точек из S. Не более чем счётное множество не более чем счётных множеств даёт нам не более чем счётное множество, и утверждение о счётности S, тем самым, завершено.

Решив задачу Б, Андрей перешел к задаче А: «Думая над этой задачей (Б), я, во-первых, придумал счётное множество точек на окружности с рациональными расстояниями между ними (усиление задачи А). А во-вторых, я придумал очень простой способ доказательства формул для пифагоровых троек чисел». Вот что он придумал.

Решение задачи А. Возьмём все рациональные точки на единичной окружности — углы α с рациональным $\sin\alpha$ и $\cos\alpha$. Удвоим их аргументы — получим подмножество $\mathcal{A}$ предыдущего множества (поскольку $\sin 2\alpha$ и $\cos 2\alpha$ тоже будут рациональными числами). Расстояние между двумя такими точками 2α и 2β, равно (как легко проверить)

$$2\sin(\alpha-\beta) = 2(\sin\alpha\cos\beta - \cos\alpha\sin\beta) \in \mathbb{Q}.$$

Итак, множество $\mathcal{A}$ на окружности удовлетворяет условию и счётно.

Формулы для пифагоровых троек чисел. Пифагоровы треугольники это всё равно, что рациональные точки на окружности.

Возьмём (и в этом состоит неожиданность!) дробно-линейное отображение $w = \dfrac{1+iz}{1-iz}$. Образ вещественной прямой $\mathbb{R}$ при этом отображении — единичная окружностью S^1 на комплексной плоскости (рис. 9в). Отображение w осуществляет взаимно однозначное соответствие между рациональными точками расширенной комплексной плоскости $\bar{\mathbb{C}}$ и, в частности, между рациональными точками прямой $\mathbb{R}$ и окружностью S^1, поскольку прямое и обратное отображения в действительной записи представляют рациональные функции с рациональными коэффициентами.

Подставляя теперь $z = \dfrac{p}{q}$ и записывая в действительном виде, получаем формулы для пифагоровых троек: $a = q^2 - p^2$, $b = 2pq$, $c = p^2 + q^2$.

Суть этого рассуждения состоит не в том, что полученная тройка пифагорова (это было известно с самого начала), а в том, что без всяких усилий доказано, что эти формулы дают *все* пифагоровы тройки!

№10 (Сопротивление графа). *Найти сопротивление между соседними узлами*

а) проволочного правильного многогранника (тетраэдра, куба, октаэдра, додекаэдра и икосаэдра);

б) бесконечной правильной сетки на плоскости (квадратной, треугольной, шестиугольной).

Сопротивление отдельно взятого ребра (между двумя вершинами) равно 1 *ом. На какие графы можно обобщить эту задачу?*

Обсуждение. Для куба и тетраэдра ответы приводятся в некоторых задачниках по физике в разделе «Электричество». Для решения задачи надо привлечь законы Кирхгофа о токах, протекающих через вершины сети.

Ответ: сопротивление между соседними вершинами для куба равно $P_{\text{куб}} = 7/12$, а для тетраэдра $P_{\text{тетр.}} = 1/2$.

Даже в этих двух случаях решение не очень простое, и оно намного сложнее для остальных многогранников. Ответы для них такие: $P_{\text{октаэдр}} = 5/12$, $P_{\text{додекаэдр}} = 19/30$, и $P_{\text{икосаэдр}} = 11/30$.

Для квадратной решетки задача ещё сложнее, так как граф бесконечный. Однако ответ для решетки не очень сложен. Он естественно обобщается на так называемые «правильные» графы. Я нашел этот замечательный ответ в одном из писем Андрея и сейчас приведу соответствующую выдержку из этого письма.

«Недавно я получил обобщение одного интересного факта, который мы как-то с тобой обсуждали: найти сопротивление между соседними

узлами бесконечной квадратной решетки, составленной из сопротивлений по одному ому. Оно равно 1/2 ом, как и для тетраэдра.

Обобщение таково. Сначала определения. Возьмем в графе Γ два смежных ребра AB и AC. Эти ребра назовем *эквивалентными*, если существует автоморфизм графа, переводящий A в A и B в C. Вершину графа назовем *центром симметрии* графа Γ, если все ребра, инцидентные ей, эквивалентны. Граф Γ называется *правильным*, если все его вершины — центры симметрии графа. Примеры правильных графов: правильные многогранники любой размерности; правильные решетки на евклидовой плоскости и плоскости Лобачевского и их многомерных аналогах; симметричные решетки на сфере или торе и т.п. Нетривиальный пример: граф многогранника, полученного из куба приставлением к каждой грани по четырехугольной пирамиде (поверхность этого многогранника состоит из 12 ромбов). Он нетривиален тем, что его вершины имеют разную степень (4 и 6).

Задача. *Найти сопротивление между соседними вершинами X и Y правильного графа* Γ, *если все его ребра имеют сопротивление* 1 *ом.*

Пусть n — общее число вершин графа (если $n = \infty$, то полагаем $\frac{1}{n} = 0$), k_1 и k_2 — степени вершин X и Y. Тогда

$$P_\Gamma = \left(\frac{1}{k_1} + \frac{1}{k_2}\right)\left(1 - \frac{1}{n}\right).$$

Доказательство этого факта не отличается по существу от доказательства для квадратной решетки».

Я предлагаю всем заинтересовавшимся этим результатом попытаться доказать его самостоятельно[5)].

♦♦♦

№11 (Делимость чисел). *Доказать, что для любого натурального числа k существует такое* **нецелое** *число α, что для всякого натурального числа n число $\lfloor \alpha^n \rfloor$ делится на k.*

Решение. Фиксируем k. Назовем *отрезком n-го порядка* любой отрезок вида $\left[\sqrt[n]{N + \frac{1}{3}}, \sqrt[n]{N + \frac{2}{3}}\right]$, где N — натуральное число, кратное k. Таким образом, если Δ — отрезок n-го порядка, то для любой точки $X \in \Delta$, $\lfloor X^n \rfloor$ кратно k.

[5)] В следующем письме Андрей написал мне, что ему удалось обобщить этот результат для нахождения сопротивления между *несоседними* вершинами графа. Однако на граф ему пришлось наложить существенно более сильное ограничение, и формула для сопротивления также существенно усложнилась.

Лемма. *Если* $\Delta = [a, b]$ *— отрезок* n*-го порядка и* $a \geqslant 3k + 1$*, то в* Δ *содержится какой-то отрезок* $(n + 1)$*-го порядка.*

Доказательство. Действительно, $b^n - a^n = \frac{1}{3}$, откуда

$$b^{n+1} - a^{n+1} > b^n a - a^{n+1} = a(b^n - a^n) = \frac{1}{3}a \geqslant k + \frac{1}{3}\ .$$

Поэтому между числами a^{n+1} и b^{n+1} обязательно найдется отрезок вида $\left[N + \frac{1}{3}, N + \frac{2}{3}\right]$, где N делится на k. Следовательно, $\left[\sqrt[n]{N + \frac{1}{3}}, \sqrt[n]{N + \frac{2}{3}}\right] \subset$ $\subset \Delta$. Лемма доказана. □

Рассмотрим теперь вложенную (согласно лемме) систему отрезков первого, второго, третьего, и т. д. порядков. Их пересечение непусто, и любое число α из этого пересечения дает решение нашей задачи. Действительно, уже отрезок первого порядка не содержит целых точек, так что α не может быть целым.

♦ ♦ ♦

№12 (Последние цифры степени числа). *Как меняются последние* 200000 *цифр числа*

$$N = 11^{10^{9^{8^7}}} - 6^{5^{4^{3^2}}}$$

при его возведении в степень $n = 1, 2, 3, \ldots$*?*

Решение. Ответ: 200000 *последних цифр чисел* N *и* N^n *совпадают.*

Надо доказать, что для каждого натурального n

$$N^n \equiv N \pmod{10^{200000}}. \tag{1}$$

Найдем сначала $N \bmod 10^{200000}$. Воспользуемся для этого φ-функцией Эйлера: $\varphi(k)$ *равно числу натуральных чисел, не превышающих числа* k *и взаимно простых с* k. Число $\varphi(k)$ легко находится по такой формуле:

$$\varphi(k) = k \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_s}\right),$$

где $p_1 < p_2 < \ldots < p_s$ — все различные простые делители k. Если $k =$ $= 10^{200000}$, то единственные простые делители k равны 2 и 5, так что $\varphi(k) = k\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 4 \cdot 10^{199999}$. Напомним также знаменитую теорему Эйлера о φ-функции:

Теорема Эйлера. *Если числа* a *и* k *взаимно просты, т. е.* $(a, k) = 1$*, то* $a^{\varphi(k)} \equiv 1 \pmod{m}$.

Так как $9^{8^7} > 200001$, число $10^{9^{8^7}}$ делится на $\varphi(10^{200000})$, откуда по теореме Эйлера

$$11^{10^{9^{8^7}}} \equiv 1 \pmod{10^{200000}}.$$

Обозначим $m = 5^{4^{3^2}}$, тогда

$$N \equiv 1 - 6^m \pmod{10^{200000}}. \tag{2}$$

Нам достаточно доказать равенство (1) для $n = 2$, тогда оно верно и для всех $n > 2$. Возведем (2) в квадрат:

$$N^2 \equiv 1 + 6^{2m} - 2 \cdot 6^m \equiv N + 6^{2m} - 6^m \pmod{10^{200000}}.$$

Поэтому достаточно доказать, что

$$6^{2m} \equiv 6^m \pmod{10^{200000}}.$$

Поскольку $m \geqslant 200000$, $6^{2m} \equiv 6^m \pmod{2^{200000}}$ (обе части сравнимы с 0), так что достаточно доказать, что

$$6^m \equiv 1 \pmod{5^{200000}}. \tag{3}$$

Однако доказательство сравнения (3) нельзя получить непосредственно из теоремы Эйлера, поскольку m не делится на $\varphi(5^{200000}) = 4 \cdot 5^{199999}$.

Поэтому поступим так: распишем 6^m как бином,

$$6^m = (1+5)^m = 1 + C_m^1 \cdot 5 + C_m^2 \cdot 5^2 + \ldots + C_m^m \cdot 5^m;$$

надо доказать, что

$$C_m^1 \cdot 5 + C_m^2 \cdot 5^2 + \ldots + C_m^m \cdot 5^m \text{ делится на } 5^{200000}. \tag{4}$$

Обозначим через $\deg_5 L$ наибольшую степень пятерки, на которую делится L, и дообозначим $\deg_5 \dfrac{L}{M} = \deg_5 L - \deg_5 M$. Тогда

$$\deg_5 C_m^r = \deg_5 \frac{m(m-1)\ldots(m-r+1)}{1 \cdot 2 \cdot \ldots \cdot r} =$$

$$= \deg_5 \left(m \cdot \frac{m-1}{1} \cdot \frac{m-2}{2} \cdot \ldots \cdot \frac{m-r+1}{r-1} \cdot \frac{1}{r} \right) =$$

$$= \deg_5 \frac{m}{r} + \deg_5 \frac{m-1}{1} + \deg_5 \frac{m-2}{2} + \ldots + \deg_5 \frac{m-r+1}{r-1}.$$

Учитывая, что $m = 5^l$, где $l = 4^{3^2}$, получаем, что $\deg_5 \dfrac{m-k}{k} = 0$ для всех $k = 1, 2, \ldots, r-1$. Поэтому $\deg_5 C_m^r = \deg_5 \dfrac{m}{r}$. Значит,

$$\deg_5 (C_m^r \cdot 5^r) = \deg_5 \left(\frac{m}{r} \cdot 5^r \right) > \deg_5 m = 4^{3^2} > 200000.$$

Итак, утверждение (4), а с ним и (3), доказаны. Этим задача решена.

♦♦♦

Список литературы

[1] *Гальперин Г. А., Ходулёв А. Б.* Случаи плоского расположения в пространственной задаче четырех тел с одним притягивающим центром. Препринт ИПМ №41. Москва, 1983. С. 1–27.

[2] *Пуанкаре А.* О науке. М.: Наука, 1983. С. 122–125.

[3] *Арнольд В. И.* Избранное – 60. М.: Фазис, 1997. С. 127, 196, 213, 240, 256, 307, 474, 586, 588.

[4] *Гальперин Г. А., Ходулёв А. Б.* Решение задачи М229 // Квант, №6, 1974. С. 24–27.

[5] *Ходулёв А. Б.* Расселение фишек // Квант, №7, 1982. С. 28.

[6] *Арнольд В. И.* Математические методы классической механики. М.: Наука, 1979. С. 26.

[7] *Андреев Н. Н., Юдин В. А.* Экстремальные расположения точек на сфере // Математическое Просвещение. Сер. 3, вып. 1, 1997. С. 116–125.

[8] *Васильев Н. Б., Егоров А. А.* Задачи Всесоюзных математических олимпиад. М.: Наука, 1988. Задача 184.

[9] *Шклярский Д. О., Ченцов Н. Н., Яглом И. М.* Избранные задачи и теоремы элементарной математики. Часть 2, геометрия (планиметрия). М.: Наука, 1952. С. 22, зад. 53.

[10] Труды А. Б. Ходулёва по Computer Science за 1985–1998 г. см. по адресу `cgd_publ.htm at rmp.kiam1.rssi.ru`

Советская математика 30-х годов (II): А. О. Гельфонд и Л. Г. Шнирельман

В. М. Тихомиров В. В. Успенский

Во втором выпуске сборника «Математическое просвещение», в связи с присуждением первых филдсовских медалей, мы рассказывали о Колмогорове и Понтрягине (см. [3]). Здесь речь пойдёт о двух других советских математиках, получивших выдающиеся результаты в 30-е годы: о Гельфонде и Шнирельмане.

Александр Осипович Гельфонд и седьмая проблема Гильберта

Комплексное число называется *алгебраическим*, если оно является корнем некоторого многочлена с целыми коэффициентами. Таково, например, число $\sqrt{2}$, являющееся корнем уравнения $x^2 - 2 = 0$. Еще в далекой античности было доказано, что $\sqrt{2}$ не является рациональным числом. Числа, не являющиеся алгебраическими, называются *трансцендентными*. Лейбниц упоминает, что число $2^{\sqrt{2}/2}$ «интерцендентно», не определяя это понятие. Явное указание на то, что $a^{\sqrt{n}}$ трансцендентно, если a — рациональное, а n — натуральное, не являющееся квадратом, содержится у Эйлера.

Первый пример трансцендентных чисел построил Ж.Лиувилль в 1844 г. Он доказал, что алгебраическое число не может «слишком хорошо» аппроксимироваться рациональными [6]. Так называемое «число Лиувилля» $\sum_{n=1}^{\infty} 10^{-n!}$, имеющее в десятичной записи единицы на позициях с номерами $1, 2, 6, 24, \ldots$ и нули на остальных, «слишком хорошо» приближается своими «начальными кусками» и потому (как доказал Лиувилль) трансцендентно. Существование трансцендентных чисел вытекает также из результатов Кантора: множество $\mathbb{A}$ алгебраических чисел счётно, в то время как множество $\mathbb{R}$ действительных чисел несчётно. Метод Кантора даёт и алгоритм построения трансцендентных чисел. Но естественно возник вопрос о том, являются ли трансцендентными всем известные числа e и π. Вопрос о трансцендентности π был особо актуален, ибо от ответа на него во многом зависело решение одной из известнейших задач античной математики — задачи о квадратуре круга. Трансцендентность числа e

доказал Эрмит в 1873 г. Через девять лет, в 1882 г., Линдеман доказал трансцендентность чисел вида e^α, где $\alpha \neq 0$ — алгебраическое. Отсюда вытекает, что π трансцендентно (ибо $e^{\pi i} = -1$). Тем самым была решена (в отрицательном смысле) проблема квадратуры круга.

(Говорят, Линдеман получил этот выдающийся результат в день своего тридцатилетия. Кто-то из друзей, пришедших на празднование дня рождения, сказал ему: «Ты выглядишь таким счастливым, как будто решил проблему квадратуры круга!» Линдеман отвечал, что так оно и есть. В последующие годы Линдеман был ректором университета в Мюнхене и пытался решить проблему Ферма — говорят, под давлением жены, которая требовала от мужа не останавливаться на достигнутом.)

Среди 23 математических проблем, которые Гильберт сформулировал в своём знаменитом докладе на парижском конгрессе 1900 г., седьмая проблема посвящена трасцендентным числам. Гильберт спрашивает, всегда ли трансцендентно число вида α^β, где α и β алгебраические, α отлично от 0 и 1, а β не является рациональным. В частности, Гильберт указывает конкретные числа $2^{\sqrt{2}}$ и $e^\pi = i^{-2i}$ и предлагает доказать, что они трансцендентны.

Поясним равенство $e^\pi = i^{-2i}$. Если α не является положительным вещественным числом, выражение α^β определено неоднозначно. По определению $\alpha^\beta = e^{\beta \log \alpha}$, где $e^z = \sum z^n/n!$, а $\log \alpha$ — какое-либо решение уравнения $e^x = \alpha$. Последнее уравнение имеет бесконечно много решений, отличающихся между собой на целое кратное числа $2\pi i$. Если β не является рациональным, отсюда получается бесконечное множество значений для выражения α^β. Так как $e^{\pi i/2} = i$, одним из значений для $\log i$ является $\pi i/2$, а одним из значений для i^{-2i} является $e^{-2i\pi i/2} = e^\pi$.

Гильберт считал свою седьмую проблему очень трудной. Он полагал, что её решение принадлежит ещё более далекому будущему, чем решение проблем Римана и Ферма. Но здесь он ошибся.

Первое частичное решение седьмой проблемы было получено А. О. Гельфондом в 1929 г. и Р. О. Кузьминым в 1930 г. В 1934 г. Гельфонд получил окончательное решение. Несколько позже решение седьмой проблемы независимо получил немецкий математик Т. Шнейдер.

Александр Осипович Гельфонд родился 24 (11) октября 1906 г. в Петербурге в семье врача. Окончив среднюю школу, он поступил в училище им. Баумана, но вскоре перевелся на физико-математический факультет Московского Университета. Студенческие и аспирантские годы Александра Осиповича прошли под руководством В. В. Степанова и А. Я. Хинчина. Решение седьмой проблемы Гильберта принесло ему всемирную известность. В 1935 г. Гельфонду без защиты диссертации была присвоена ученая степень доктора физико-математических наук, а

в 1939 г. он был избран членом-корреспондентом АН СССР. С 1933 г. А. О. Гельфонд был старшим научным сотрудником Математического института им. В. А. Стеклова АН СССР, с 1938 г. — заведующим кафедрой теории чисел механико-математического факультета МГУ. А. О. Гельфонд умер 7 ноября 1968 г.

Приведем решение седьмой проблемы Гильберта. Основные понятия и определения, связанные с алгебраическими числами, мы предполагаем известными; найти их, например, можно в книгах [2, 6].

Теорема Гельфонда – Шнейдера. *Пусть α — алгебраическое число, отличное от 0 и 1, а β — алгебраическое число, не являющееся рациональным. Тогда каждое значение выражения α^β трансцендентно.*

Гельфонд был приглашён принять участие в Международном конгрессе в Осло в 1932 году. Но он не получил разрешения на выезд. Контакты между советскими математиками и математиками остального мира в те годы фактически прекратились. Кандидатуры советских математиков на соискание международных премий не рассматривались. Но нет никакого сомнения в том, что решение седьмой проблемы Гильберта могло бы претендовать на филдсовскую медаль в 1936 году.

Из теоремы Гельфонда – Шнейдера вытекает, в частности, трансцендентность чисел $2^{\sqrt{2}}$ (это предполагали ещё Лейбниц и Эйлер!) и $e^{\pi\beta} = i^{-2i\beta}$, где $\beta \neq 0$ вещественное алгебраическое. Отметим, что до сих пор неизвестно, являются ли трансцендентными (или хотя бы иррациональными!) числа $e + \pi$ и $e\pi$.

Доказательство теоремы Гельфонда – Шнейдера можно найти в [1], [4], [6]. Весьма общий результат о значениях функций, удовлетворяющих алгебраическим дифференциальным уравнениям, из которого вытекает как теорема Гельфонда – Шнейдера, так и теорема Линдемана, доказан в добавлении к [2]. Наше изложение заимствовано из статьи А. И. Галочкина [1] (где теорема Линдемана также доказана на сходных идеях).

Общий замысел доказательства таков. Допустим, что α^β алгебраическое. Для каждого натурального $n > 1$ мы построим ненулевую функцию $f = f_n$ вида

$$f(z) = \sum_{k=0}^{n-1} \sum_{l=0}^{n-1} a_{kl} e^{(k+l\beta)z}, \tag{1}$$

имеющую нуль высокого порядка (точнее, порядка $\geqslant [n^{3/2}]$) в точке $z = 0$. При этом коэффициенты функции f_n — целые числа, которые «не слишком быстро» растут с ростом n: справедлива оценка $|a_{kl}| < n^{\gamma_1 n}$, где γ_1 — не зависящая от n положительная константа (в дальнейшем аналогичный смысл имеют $\gamma_2, \gamma_3, \ldots$). Тогда на любом круге $|z| \leqslant R$ функции f_n быстро сходятся к нулю вместе со всеми своими производными. С другой

стороны, для натуральных x и t значение производной $f_n^{(t)}$ в точке $x\log\alpha$ есть многочлен с целыми коэффициентами от алгебраических чисел α, β и α^β. Отсюда выводится оценка снизу на $|f_n^{(t)}(x\log\alpha)|$, противоречащая оценке сверху на скорость сходимости последовательности (f_n) к нулю.

Предположим, что для каждого n функция f_n с указанными свойствами уже построена. Покажем, как получаются упомянутые оценки.

Обозначим через $\operatorname{ord}_{z=a} F(z)$ порядок нуля функции F в точке $z=a$.

Лемма 1. *Пусть $\omega_1,\dots,\omega_m$ — различные комплексные числа,*

$$g_m(z)=a_1e^{\omega_1 z}+\dots+a_me^{\omega_m z},$$

где коэффициенты a_k не все равны нулю. Тогда

$$\operatorname{ord}_{z=0} g_m(z)<m.$$

Доказательство. Индукция по m. Производная

$$g_{m-1}(z)=(e^{-\omega_m z}g_m(z))'$$

имеет вид

$$g_{m-1}(z)=b_1e^{(\omega_1-\omega_m)z}+\dots+b_{m-1}e^{(\omega_{m-1}-\omega_m)z}.$$

По предположению индукции, $\operatorname{ord}_{z=0} g_{m-1}(z)<m-1$, откуда вытекает требуемое заключение. □

Пусть m, m_1 и m_2 — степени алгебраических чисел β, α и α^β соответственно. Положим $X=3mm_1m_2+6$. Зафиксируем какое-нибудь значение $\log\alpha$. Из леммы 1 вытекает, что $\operatorname{ord}_{z=0} f(z)<n^2$. Таким образом,

$$N=\min_{0\leqslant x\leqslant X}\operatorname{ord}_{z=x\log\alpha} f(z)<n^2.$$

Лемма 2. *Для любого $R>0$ при достаточно больших n справедливо неравенство*

$$\max_{|z|\leqslant R}|f^{(N)}(z)|<n^{-1/3n^{3/2}-1/3(X-6)N}.$$

Доказательство. Функция

$$g(z)=f(z)z^{-[n^{3/2}]}(z-\log\alpha)^{-N}\cdot\ldots\cdot(z-X\log\alpha)^{-N}$$

имеет только устранимые особенности и может рассматриваться как всюду определённая целая функция. Применим к этой функции принцип максимума. Пусть n таково, что $R+1<\sqrt{n}$. Тогда

$$\max_{|z|\leqslant R+1}|g(z)|\leqslant\max_{u=\sqrt{n}}|g(u)|,$$

откуда

$$M = \max_{|z|\leqslant R+1} |f(z)| \leqslant$$

$$\leqslant \max_{|u|=\sqrt{n}} |f(u)| \cdot \max_{\substack{|z|\leqslant R+1,\\ |u|=\sqrt{n}}} \left| \left(\frac{z}{u}\right)^{[n^{3/2}]} \left(\frac{z-\log\alpha}{u-\log\alpha}\right)^N \cdot \ldots \cdot \left(\frac{z-X\log\alpha}{u-X\log\alpha}\right)^N \right|. \tag{2}$$

Первый сомножитель в правой части не превосходит $n^2 n^{\gamma_1 n} e^{(1+|\beta|)n^{3/2}}$ (здесь n^2 — число слагаемых в (1), $n^{\gamma_1 n}$ — верхняя оценка для коэффициентов a_{kl}), и для любого $\varepsilon > 0$ второй сомножитель не превосходит

$$n^{-(1/2-\varepsilon)(n^{3/2}+XN)}$$

при больших n. Отсюда

$$M \leqslant n^{-1/3n^{3/2}-1/3XN}. \tag{3}$$

Далее,

$$f^{(N)}(z) = \frac{N!}{2\pi i} \int\limits_{|\zeta-z|=1} \frac{f(\zeta)\,d\zeta}{(\zeta-z)^{N+1}},$$

поэтому для любого z с $|z| \leqslant R$ имеем

$$|f^{(N)}(z)| \leqslant (N!)M \leqslant N^N M \leqslant n^{2N} M,$$

и из (3) следует утверждение леммы. □

Из леммы 2 вытекает, что при больших n выполняется

$$|f^{(N)}(x\log\alpha)| < n^{-1/3n^{3/2}-mm_1m_2N}, \quad x = 0, \ldots, X. \tag{4}$$

Теперь установим оценку снизу на $f^{(N)}(x\log\alpha)$, несовместимую с (4). Эта оценка основана на следующей лемме.

Назовем длиной многочлена P сумму модулей его коэффициентов. Обозначим длину многочлена P через $L(P)$.

Лемма 3. *Пусть $\alpha_1, \ldots, \alpha_s$ — алгебраические числа степеней соответственно $m_1, \ldots, m_s$. Тогда существует такая положительная постоянная $C = C(\alpha_1, \ldots, \alpha_s)$, что для любого многочлена $P(x_1, \ldots, x_s) \in \in \mathbb{Z}[x_1, \ldots, x_s]$ либо $P(\alpha_1, \ldots, \alpha_s) = 0$, либо выполняется $|P(\alpha_1, \ldots, \alpha_s)| \geqslant \geqslant L^{1-m_1\cdot\ldots\cdot m_s} C^{-d}$, где d и L — соответственно степень и длина многочлена $P(x_1, \ldots, x_s)$.*

Доказательство. Пусть a — такое натуральное число, что все числа $a\alpha_1, \ldots, a\alpha_s$ целые алгебраические. Тогда целым алгебраическим является и $\beta = a^d P(\alpha_1, \ldots, \alpha_s)$. Предположим, что $\beta \neq 0$. Минимальный

многочлен $B(x)$ числа β имеет целые коэффициенты. Пусть

$$B(x) = x^n + b_{n-1}x^{n-1} + \ldots + b_0 = (x - \beta_1) \cdot \ldots \cdot (x - \beta_n),$$

где $\beta = \beta_1$. Тогда

$$|\beta\beta_2 \cdot \ldots \cdot \beta_n| = |b_0| \geqslant 1. \tag{5}$$

Пусть $\alpha_{i1}, \ldots, \alpha_{im_i}$ — числа, сопряженные с алгебраическим числом α_i $(1 \leqslant i \leqslant s)$, $C_1 = a \max_{i,j}(1, |\alpha_{i,j}|)$. Каждое β_i сопряжено с β и имеет вид $a^d P(\alpha_{1r_1}, \ldots, \alpha_{sr_s})$, поэтому

$$|\beta_i| = |a^d P(\alpha_{1r_1}, \ldots, \alpha_{sr_s})| \leqslant C_1^d L. \tag{6}$$

Из (5) и (6) вытекает

$$1 \leqslant |\beta| \cdot |\beta_2 \cdot \ldots \cdot \beta_n| \leqslant a^d |P(\alpha_1, \ldots, \alpha_s|(C_1^d L)^{n-1}.$$

Так как $n \leqslant m_1 \cdot \ldots \cdot m_s$, то из этого неравенства следует утверждение леммы с $C = aC_1^{m_1 \cdot \ldots \cdot m_s - 1}$. □

По определению числа N найдется такое целое x, $0 \leqslant x \leqslant X$, что $f^{(N)}(x \log \alpha) \neq 0$. Так как

$$f^{(N)}(z) = \sum_{k,l=0}^{n-1} a_{kl}(k + l\beta)^N e^{(k+l\beta)z},$$

то

$$f^{(N)}(x \log \alpha) = \sum_{k,l=0}^{n-1} a_{kl}(k + l\beta)^N \alpha^{xk} (\alpha^\beta)^{xl} = P(\beta, \alpha, \alpha^\beta),$$

где P — многочлен с целыми коэффициентами. При этом

$$L(P) \leqslant n^2 n^{\gamma_1 n} (2n)^N, \quad \deg P \leqslant N + 2nX.$$

Из леммы 3 получаем, что при достаточно больших n

$$f^{(N)}(x \log \alpha) = P(\beta, \alpha, \alpha^\beta) \geqslant (L(P))^{1 - mm_1m_2} C^{-\deg P} > \\ > n^{-\gamma_2 n} (2n)^{N(1-mm_1m_2)} C^{-N} > n^{-\gamma_2 n - mm_1m_2 N}.$$

При больших n это противоречит (4).

Остается построить функцию $f(z) = \sum_{k=0}^{n-1} \sum_{l=0}^{n-1} a_{kl} e^{(k+l\beta)z}$, такую, что $\operatorname{ord}_{z=0} f(z) \geqslant [n^{3/2}]$ и $|a_{kl}| < n^{\gamma_1 n}$.

Лемма 4 (Зигель). *Пусть* $a_{ij} \in \mathbb{Z}$, $|a_{ij}| \leqslant A$, $\xi = (x_1, \ldots, x_q)$ *и*

$$L_i(\xi) = \sum_{j=1}^{q} a_{ij} x_j, \quad 1 \leqslant i \leqslant p, \quad p < q.$$

Тогда система уравнений

$$L_i(\xi) = 0, \quad 1 \leqslant i \leqslant p$$

имеет ненулевое решение $(x_1, \ldots, x_q) \in \mathbb{Z}^q$, *для которого* $\max_j |x_j| \leqslant 1 + (qA)^{p/(q-p)}$.

Доказательство. Рассмотрим нашу систему как линейное уравнение $L(\xi) = 0$, где $L = (L_1, \ldots, L_p)$ — линейное отображение $\mathbb{Z}^q \to \mathbb{Z}^p$. Для всякого целого положительного числа B обозначим через $\mathbb{Z}^q(B)$ множество таких векторов ξ из $\mathbb{Z}^q$, что $|\xi| = \max_j |x_j| \leqslant B$. Тогда L отображает $\mathbb{Z}^q(B)$ в $\mathbb{Z}^p(qBA)$. Число элементов в $\mathbb{Z}^q(B)$ равно $(2B+1)^q$. Найдем значение B, для которого существуют два различных элемента ξ, η из $\mathbb{Z}^q(B)$, имеющих один и тот же образ $L(\xi) = L(\eta)$. Для этого достаточно, чтобы выполнялось неравенство $(2B+1)^q > (2qBA+1)^p$. Это неравенство выполняется при $B = [(1+(qA)^{p/(q-p)})/2]$, так как тогда $2B+1 > (qA)^{p/(q-p)}$ и $(2B+1)^{q-p} > (qA)^p \geqslant ((2qAB+1)/(2B+1))^p$. В качестве решения нашей системы берем вектор $\xi - \eta$, для которого $|\xi - \eta| \leqslant 2B \leqslant 1 + (qA)^{p/(q-p)}$. □

Лемма 5. *Пусть* β — *целое алгебраическое число,*

$$\beta^m = b_{m-1}\beta^{m-1} + \ldots + b_1\beta + b_0, \quad b_j \in \mathbb{Z}, \quad |b_j| \leqslant B.$$

Если k *и* l — *неотрицательные целые числа, не превосходящие* n, *то для всякого натурального* t

$$(k + l\beta)^t = c_{m-1}\beta^{m-1} + \ldots + c_1\beta + c_0, \quad c_j \in \mathbb{Z}, \quad |c_j| \leqslant (B+2)^t n^t.$$

Доказательство. Для начала заметим, что для всякого натурального t выполняется

$$\beta^t = b_{t,m-1}\beta^{m-1} + \ldots + b_{t,1}\beta + b_{t,0}, \quad b_{t,j} \in \mathbb{Z}, \quad |b_{t,j}| \leqslant (B+1)^t.$$

Это верно при $t \leqslant m$, а равенство

$$\beta^{t+1} = b_{t,m-1}(b_{m-1}\beta^{m-1} + \ldots + b_0) + b_{t,m-2}\beta^{m-1} + \ldots + b_{t,0}\beta$$

позволяет сделать переход от t к $t+1$.

Теперь из равенства

$$(k + l\beta)^t = \sum_{s=0}^{t} C_t^s k^{t-s} l^s \sum_{j=0}^{m-1} b_{sj}\beta^j$$

следует, что коэффициенты при β^j не превосходят

$$\sum_{s=0}^{t} C_t^s k^{t-s} l^s (B+1)^s = (k + l(B+1))^t \leqslant (B+2)^t n^t.$$

□

У нас все готово для завершения доказательства теоремы Гельфонда – Шнейдера. Мы можем считать, что β — целое алгебраическое число.

Иначе $k\beta$ является целым алгебраическим для некоторого целого $k > 0$, и если мы докажем, что $\alpha^{k\beta}$ трансцендентно, то таково же и α^{β}.

Мы хотим построить ненулевую функцию

$$f(z) = \sum_{k=0}^{n-1} \sum_{l=0}^{n-1} a_{kl} e^{(k+l\beta)z}$$

с коэффициентами $a_{kl} \in \mathbb{Z}$, такую, что $|a_{kl}| < n^{\gamma_1 n}$ и $f^{(t)}(0) = 0$, $0 \leqslant t \leqslant [n^{3/2}] - 1$. Так как

$$f^{(t)}(0) = \sum_{k,l=0}^{n-1} a_{kl}(k + l\beta)^t = \sum_{k,l=0}^{n-1} \sum_{s=0}^{m-1} B_{t,k,l,s} \beta^s a_{kl},$$

нам надо найти целочисленное решение системы линейных уравнений

$$\sum_{k,l=0}^{n-1} B_{t,k,l,s} a_{kl} = 0, \quad 0 \leqslant t \leqslant [n^{3/2}] - 1, \quad 0 \leqslant s \leqslant m - 1, \tag{7}$$

состоящей из $p = m[n^{3/2}]$ уравнений относительно $q = n^2$ неизвестных a_{kl}. По лемме 5

$$|B_{t,k,l,s}| \leqslant (B + 2)^t n^t < n^{\gamma_3 n^{3/2}}$$

(мы воспользовались тем, что $t < n^{3/2}$). Согласно лемме 4, система (7) имеет такое ненулевое целочисленное решение (a_{kl}), что все числа a_{kl} по модулю не превосходят $1 + (qn^{\gamma_3 n^{3/2}})^{p/(q-p)} < n^{\gamma_4 n^{3/2} n^{3/2}/(n^2 - m[n^{3/2}])} < n^{\gamma_1 n}$. Это завершает доказательство теоремы Гельфонда — Шнейдера.

Лев Генрихович Шнирельман, антиподы на сфере и квадрат, вписанный в кривую

Лев Генрихович Шнирельман родился 2 января 1905 года в Гомеле. Там он прожил до 16 лет. Отец его был учителем русского языка.

Лев Генрихович очень рано обнаружил выдающиеся способности. Он рисовал, писал стихи, в 12 лет самостоятельно прошел курс элементарной математики. В течение нескольких месяцев мальчик посещал физико-математические курсы для окончивших среднюю школу. Там на него обратил внимание преподаватель, который добился того, чтобы мальчика направили в Москву для продолжения образования.

В 15 лет он испробовал свои силы в самостоятельной работе. Согласно одной из легенд (которые всегда сопровождают жизненный путь выдающегося человека), он приехал в Москву в шестнадцатилетнем возрасте поступать в Московский университет, привезя с собой записанную в школьной тетради (на ужасной бумаге — другой в ту трудную по-

ру не было) теорему о раскраске сферы (мы обсудим её чуть дальше). Эта теорема сыграла основополагающую роль при решении (найденном Шнирельманом совместно с Лазарем Ароновичем Люстерником) проблемы Пуанкаре о трёх геодезических. Решение проблемы Пуанкаре сделало имя Шнирельмана известным всему миру.

Окончив Университет за два с половиной года, Шнирельман поступил в аспирантуру «Института математики и механики Первого МГУ». Он был учеником Николая Николаевича Лузина. Лазарь Аронович вспоминал, что Лузину (по-видимому, склонному в некоторой мере к мистическому восприятию мира) как-то приснился сон, что к нему придет юноша («с теми же анкетными данными», что и Лев Генрихович, как писал Л. А.) и решит проблему континуума. И когда к нему явился юный Шнирельман, Лузин воспринял его как посланца небес. Увы, Шнирельман проблему континуума не решил, решения её пришлось ждать до 60-х годов, когда её осилил Пол Коэн.

Свои самые замечательные результаты Шнирельман опубликовал в течение двух лет — 1929 и 1930. Вот их формулировки.

Теорема 1 (о вписанном квадрате). *В любую замкнутую кривую на плоскости можно вписать квадрат.*

Точнее, можно найти 4 точки на кривой, служащие вершинами квадрата (если кривая ограничивает невыпуклую область, то квадрату разрешается вылезать из этой области). В работе Шнирельмана кривая предполагается достаточно гладкой. Когда цитируют теорему Шнирельмана, её часто формулируют для произвольной *непрерывной* кривой. Авторам неизвестно, опубликовано ли где-нибудь доказательство для этого случая. В 1996 г. один из нас (В. В. Успенский) спросил знаменитого Пола Эрдёша, каков статус теоремы о вписанном квадрате в случае произвольной непрерывной кривой. Эрдеш ответил, что это открытая проблема.

Теорема 2 (о трёх геодезических). *На любой гладкой поверхности, гомеоморфной сфере S^2, имеется по меньшей мере три замкнутых геодезических.*

Найдите на берегу моря (или мысленно) какой-нибудь гладкий камешек. И тонкую аптечную резиночку. Попробуйте надеть резиночку на камешек, чтобы она «не сползала». Если вам это удастся, вы нашли замкнутую геодезическую. На шарообразном мячике замкнутые геодезические — большие круги: если вы чуть-чуть собъетесь с большого круга, резиночка соскочит. А на эллипсоиде — всего три замкнутых геодезических: сечения этого эллипсоида плоскостями, проходящими через его оси. Гипотеза Пуанкаре состояла в том, что «на любом гладеньком камешке» имеется не меньше трёх различных замкнутых геодезических.

В 1929 году Люстерник и Шнирельман доказали гипотезу Пуанкаре, и это стало всемирной сенсацией. (Правда, впоследствии в доказательстве был обнаружен пробел, но его удалось залатать.)

Теорема 3. *Существует натуральное N такое, что любое натуральное число есть сумма не более чем N простых чисел.*

Всякое ли натуральное число, большее или равное шести, может быть представлено в виде суммы трёх простых чисел? Такой вопрос поставил перед Эйлером Христиан Гольдбах — немецкий математик, полжизни проживший в России и умерший в Москве. Он задал этот вопрос в письме от 7.6.1742. В ответном письме (от 30.6.1742) Эйлер указывал, что для решения этой проблемы достаточно доказать, что любое чётное число $\geqslant 4$ есть сумма двух простых.

Первым сдвигом в исследовании этих проблем (до конца не решенных по сей день) был результат Шнирельмана. (Впрочем, к тому времени были опубликованы исследования Харди и Литтлвуда, в которых гипотеза Гольдбаха доказывалась (для достаточно больших нечётных чисел) в предположении, что верны некоторые другие (не доказанные и по сей день) гипотезы. В 1937 году И. М. Виноградов доказал гипотезу Гольдбаха для достаточно больших нечётных чисел.) Но особое значение имел не сам факт представимости любого числа суммой ограниченного числа простых (тем более, что у самого Шнирельмана число слагаемых оценивалось в несколько сотен тысяч), а своеобразный и очень оригинальный метод, с помощью которого удалось сдвинуть эту и множество других проблем. Мы расскажем об этом методе ниже.

В 1931 году Шнирельман был командирован за границу на три месяца и там имел огромный успех. Он работал некоторое время в Геттингене — Мекке математики того времени, где жил и творил в ту пору великий Гильберт. (Шнирельман запомнился многим тогда не только своими феноменальными результатами, но и тем, что «walked barefoot through the streets of Göttingen» — прогуливался босиком по улицам Геттингена, — как писала Констант Рид в книге о Куранте.) Ему было предложено написать монографию для престижного немецкого издательства, но этому не дано было осуществиться: в Германию пришли фашисты.

В 1933 году Шнирельман был избран членом-корреспондентом Академии наук СССР.

В 1934 году Правление Московского математического общества приняло решение о проведении первой Московской школьной олимпиады по математике. В оргкомитет по проведению олимпиады вошел Л. Г. Шнирельман. Он был одним из инициаторов Школьного математического кружка при МГУ (наряду с Люстерником и Гельфандом). Тогда же профессора и преподаватели два раза в месяц по воскресеньям читали лек-

ции в университете для школьников. И снова Шнирельман был одним из организаторов этих лекций. Он прочитал, в частности, лекции по многомерной геометрии, по теории групп.

Одним из первых Шнирельман стал культивировать в Москве выпуклую геометрию. Он написал замечательную работу по приложению выпуклой геометрии к теории наилучшего приближения (опубликованную посмертно).

Еще об одной работе Шнирельмана надо сказать — о его статье (написанной совместно с Л. С. Понтрягиным), посвящённой метрическому определению размерности. Эта работа оказала влияние на разработку концепции ε-энтропии Колмогорова. Статья Понтрягина и Шнирельмана помещена в качестве приложения к русскому переводу «Теории размерности» Гуревича и Волмэна.

Лев Генрихович очень дружил с Люстерником, Гельфондом, Гельфандом. Многие вспоминали о нём, как о личности большого масштаба, человеке мягком и деликатном, имевшем самые многогранные интеллектуальные запросы, человеке остроумном, наблюдательном, одухотворенном и очень обаятельном.

Жизнь его оборвалась трагически: 24 сентября 1938 года он покончил с собой. Те люди старшего поколения, с кем нам доводилось говорить на эту тему, связывали этот шаг Льва Генриховича с кровавым безумием того времени: они говорили, что Лев Генрихович попал в поле зрения НКВД и, устрашившись этого, решил покончить с жизнью. Быть может, истина откроется, когда кто-то из людей, желающих узнать правду, доберется до архивов КГБ.

А теперь расскажем чуть подробнее о теоремах Шнирельмана. Начнём с уже упоминавшегося результата из юношеской тетради.

Теорема 4 (о раскраске сферы). *Пусть сфера S^2 покрыта тремя замкнутыми множествами. Тогда одно из них содержит пару антиподов (т. е. диаметрально противоположных точек).*

Иными словами, если сферу S^2 раскрасить в три цвета, то найдется пара одноцветных антиподов. Шнирельман доказал свою теорему и для сфер произвольной размерности: *если n-мерная сфера S^n раскрашена в $n+1$ цветов (т. е. покрыта замкнутыми множествами $F_1, \ldots, F_{n+1}$), то найдется пара одноцветных антиподов.*

Теорема Шнирельмана эквивалентна другой теореме, которую доказали в тридцатые годы польские математики К. Борсук и С. Улам: *всякое отображение f сферы S^n в евклидово пространство $\mathbb{R}^n$ склеивает некоторую пару антиподов.* Иными словами, найдется такое $x \in S^n$, что $f(x) = f(-x)$. (Все отображения здесь и далее предполагаются непрерывными.) Еще одна эвивалентная формулировка теоремы Борсука –

Улама такова: *не существует нечётного отображения* $f\colon S^n \to S^{n-1}$. При этом отображение f называется нечётным, если $f(-x) = -f(x)$.

Покажем, как вывести теорему о раскраске сферы из теоремы Борсука – Улама. Пусть $F_1, \ldots, F_{n+1}$ — замкнутые подмножества сферы S^n, объединение которых равно S^n. Нам надо доказать, что при некотором i, $1 \leqslant i \leqslant n+1$, множество F_i содержит пару антиподов. Если существует точка x, принадлежащая всем множествам F_i, то все ясно: некоторое F_i содержит пару антиподов x, $-x$. Предположим, что $F_1 \cap \ldots \cap F_{n+1}$ пусто. Для каждого $x \in S^n$ пусть $f_i(x)$ — расстояние от точки x до множества F_i. Тогда $f_i\colon S^n \to \mathbb{R}$ — непрерывная неотрицательная функция, и $f_i(x) = 0$ тогда и только тогда, когда $x \in F_i$. Согласно нашему предположению, функции f_i, $1 \leqslant i \leqslant n+1$, нигде не обращаются в нуль одновременно, поэтому функция $h = \sum_{i=1}^{n+1} f_i$ всюду положительна. Положим $g_i = f_i/h$, $1 \leqslant i \leqslant n+1$, и $G(x) = (g_1(x), \ldots, g_n(x))$. Тогда $G\colon S^n \to \mathbb{R}^n$ — непрерывное отображение. Применяя к нему теорему Борсука – Улама, находим такое $x \in S^n$, что $g_i(x) = g_i(-x)$ при каждом $i = 1, \ldots, n$. Так как $g_{n+1} = 1 - \sum_{i=1}^{n} g_i$, имеем также $g_{n+1}(x) = g_{n+1}(-x)$. Если i таково, что $x \in F_i$, то $g_i(-x) = g_i(x) = 0$, так что F_i содержит пару антиподов x и $-x$.

Что касается теоремы Борсука – Улама, то ей можно придать более сильную форму, используя понятие степени отображения сферы в себя:

Теорема Борсука. *Всякое нечётное отображение* $f\colon S^n \to S^n$ *имеет нечётную степень.*

Отсюда следует, что *всякое отображение* $f\colon S^n \to S^n$ *чётной степени склеивает пару антиподов.* Действительно, если отображение f не склеивает антиподов, то его можно продеформировать в нечётное отображение, а при непрерывной деформации степень отображения не меняется. Деформацию можно осуществить так: для каждого $x \in S^n$ точки $f(x)$ и $f(-x)$ равномерно двигаются в разные стороны по дуге большого круга, пока они не займут диаметрально противоположные позиции.

Объясним идею доказательства теоремы Борсука. Нечётное отображение $f\colon S^n \to S^n$ приводит к отображению $g\colon \mathbb{RP}^n \to \mathbb{RP}^n$, где $\mathbb{RP}^n$ — вещественное проективное пространство, получающееся из сферы S^n отождествлением антиподов. Для отображения g определена степень по модулю 2. Если g гладко, то эта степень совпадает с чётностью числа прообразов точки общего положения. Если $\#g^{-1}(p) = k$ и точка $p \in \mathbb{RP}^n$ представляется парой антиподов x, $-x$ на сфере, то $\#(f^{-1}(x) \cup f^{-1}(-x)) = 2k$ и $\#f^{-1}(x) = k$, так что f и g имеют одинаковые степени по модулю 2. Нам надо установить, что g имеет ненулевую степень.

Замкнутые кривые в $\mathbb{RP}^n$ бывают двух сортов: образы замкнутых кривых на сфере и образы кривых, соединяющих антиподы. Кривые пер-

вого сорта могут быть стянуты в точку, кривые второго сорта нет. Отображение g переводит нестягиваемые кривые в нестягиваемые, так как f переводит кривые с антиподальными концами на сфере в такие же кривые. Таким образом, все сводится к следующему утверждению: *всякое отображение $\mathbb{RP}^n$ в себя, переводящее нестягиваемые кривые в нестягиваемые, имеет нечётную степень по модулю* 2.

С каждым компактным многообразием X можно связать его *кольцо пересечений по модулю* 2. Элементами этого кольца (обозначим его через $A(X)$) служат классы гомологичных циклов по модулю 2, а умножение соответствует пересечению циклов, находящихся в общем положении. Отображению $h\colon X \to Y$ между компактными многообразиями отвечает гомоморфизм колец $h^*\colon A(Y) \to A(X)$ и гомоморфизм аддитивных групп $h_*\colon A(X) \to A(Y)$. Эти гомоморфизмы можно представлять соответственно как переход к прообразу или образу цикла. Гомоморфизмы h_* и h^* связаны формулой

$$h_*(h^*(\eta)\cdot\xi) = \eta\cdot h_*(\xi) \quad (\eta\in A(Y),\ \xi\in A(X)). \tag{8}$$

Пусть теперь $X=\mathbb{RP}^n$ и $A=A(X)$. Для каждого $k=0,\dots,n$ имеется только один ненулевой класс k-мерных циклов в $\mathbb{RP}^n$, представленный подмногообразием $\mathbb{RP}^k$. Поэтому кольцо A состоит из 2^{n+1} элементов вида $\sum_{i=0}^n a_i x^i$, где $a_i\in\mathbb{Z}/2\mathbb{Z}$, x соответствует гиперплоскости в $\mathbb{RP}^n$, а x^k соответствует подмногообразию $\mathbb{RP}^{n-k}$ коразмерности k. В частности, x^{n-1} — класс окружности $\mathbb{RP}^1$.

Предположим, что $h\colon \mathbb{RP}^n \to \mathbb{RP}^n$ переводит нестягиваемые кривые в нестягиваемые. Тогда $h_*(x^{n-1})$ является классом нестягиваемой кривой $h(\mathbb{RP}^1)$, так что $h_*(x^{n-1}) = x^{n-1}$. Положим $\xi = x^{n-1}$, $\eta = x$ и применим формулу (8). Правая часть $\eta\cdot h_*(\xi) = x\cdot x^{n-1} = x^n$ отлична от нуля. Следовательно, $h^*(\eta)=h^*(x)$ отлично от нуля — иначе левая часть $h_*(h^*(\eta)\cdot\xi)$ была бы нулевой. Класс $h^*(x)$ представляется циклом коразмерности 1. Поскольку этот класс ненулевой, должно быть $h^*(x)=x$. Так как кольцо A порождается элементом x и $h^*\colon A\to A$ — кольцевой гомоморфизм, то этот гомоморфизм должен быть тождественным. В частности, $h^*(x^n)=x^n$. Но x^n — это класс точки, и последнее равенство означает, что h имеет нечётную степень по модулю 2.

Метод Шнирельмана в аддитивной теории чисел. Пусть A и B — два множества натуральных чисел (натуральный ряд $\mathbb{N}$ будем считать начинающимся с единицы). *Суммой* A и B обычно называется множество $A+B$ чисел вида $a+b$, где $a\in A$, $b\in B$. Нам будет удобнее называть суммой A и B множество $A\oplus B = (A+B)\cup A\cup B$, полученное добавлением к $A+B$ элементов множеств A и B. Скажем, что множество A является

базисом натурального ряда, если k-кратная сумма $A \oplus \ldots \oplus A$ при некотором натуральном k совпадает с натуральным рядом. Например, если A — множество всех квадратов, то A — базис, поскольку $A \oplus A \oplus A \oplus A = \mathbb{N}$ по теореме Лагранжа. Пусть P — множество, состоящее из всех простых чисел и единицы. Является ли P базисом? Положительный ответ на этот вопрос был впервые получен Шнирельманом: *P является базисом.* Расскажем об основной идее доказательства.

Сперва введем, следуя Шнирельману, понятие *плотности* множества A натуральных чисел. Для каждого $n \in \mathbb{N}$ пусть $A(n)$ — число элементов множества A на отрезке $[1, n]$. Назовем *плотностью* $d(A)$ множества A нижнюю грань чисел вида $A(n)/n$ по всем $n \in \mathbb{N}$. Таким образом, плотность — это наибольшее α такое, что $A(n) \geqslant \alpha n$ при всех n. Шнирельман доказывает следующий результат:

Теорема 5. *Всякое множество натуральных чисел положительной плотности является базисом.*

Эту теорему нельзя непосредственно применить ко множеству P простых чисел с добавленной единицей, поскольку оно имеет нулевую плотность. (Число $\pi(n)$ простых чисел, не превосходящих n, растет как $n/\log n$: отношение $\pi(n) \log n/n$ стремится к единице.) Однако Шнирельман установил, что $P \oplus P$ имеет положительную плотность, откуда вытекает, что P является базисом. Остается открытым вопрос, содержит ли $P \oplus P$ все чётные числа (это вариант вопроса Эйлера).

Докажем теорему 5. Она вытекает из следующих лемм 1 и 2.

Лемма 1. *Если $A, B \subset \mathbb{N}$ и $d(A) + d(B) > 1$, то $A \oplus B = \mathbb{N}$.*

Доказательство. Зафиксируем $n \in \mathbb{N}$. Если $n \in B$, то $n \in A \oplus B$. Если $n \notin B$, то рассмотрим два подмножества отрезка $[1, n]$: $\{a \in A : a \leqslant n\}$ и $\{n - b : b \in B,\ b \leqslant n\}$. Они обязаны пересекаться, поскольку в первом из них не меньше $n \cdot d(A)$ элементов, во втором не меньше $n \cdot d(B)$ элементов и $n \cdot d(A) + n \cdot d(B) > n$. Следовательно, $a = n - b$ при некоторых $a \in A$, $b \in B$, откуда $n \in A \oplus B$. □

Лемма 2. *Для любых $A, B \subset \mathbb{N}$ имеет место неравенство Шнирельмана*:

$$d(A \oplus B) \geqslant d(A) + d(B) - d(A) \cdot d(B).$$

Доказательство. Положим $C = A \oplus B$, $\alpha = d(A)$, $\beta = d(B)$. Зафиксируем $n \in \mathbb{N}$. Нам надо оценить снизу число $C(n)$. Пусть $a_1 < \ldots < a_r$ — все элементы множества A из отрезка $[1, n]$, где $r = A(n)$. Отрезок $[1, n]$ разбивается числами $a_1, \ldots, a_r$ на $r+1$ отрезков (некоторые из них могут быть пустыми) длины $l_1 = a_1 - 1$, $l_2 = a_2 - a_1 - 1, \ldots, l_{r+1} = n - a_r$, при этом k-й отрезок содержит $\geqslant \beta l_k$ чисел из C: при $k > 1$ это числа вида

$a_{k-1}+b$, где $b\in B$, $b\leqslant l_k$, а при $k=1$ – это числа из B, которые $\leqslant l_1$. Отсюда получается оценка

$$C(n)\geqslant r+\beta\cdot\sum_{k=1}^{k=r+1}l_k=r+\beta(n-r)=(1-\beta)r+\beta n\geqslant(1-\beta)\alpha n+\beta n,$$

означающая, что $d(C)\geqslant(1-\beta)\alpha+\beta=\alpha+\beta-\alpha\beta$. □

Выведем теорему 5 из лемм 1 и 2. Неравенство леммы 2 можно переписать в виде $1-d(A\oplus B)\leqslant(1-d(A))(1-d(B))$. В таком виде оно распространяется (по индукции) на любое число слагаемых: $1-d(A_1\oplus\ldots\oplus A_k)\leqslant\leqslant\prod_{i=1}^{k}(1-d(A_i))$. Пусть теперь A — множество положительной плотности и $A_k=A\oplus\cdots\oplus A$ — сумма k слагаемых, равных A. Предыдущее неравенство показывает, что $d(A_k)$ стремится к единице при возрастании k. Пусть k таково, что $d(A_k)>1/2$. Из леммы 1 вытекает, что $A_{2k}=\mathbb{N}$. Таким образом, A является базисом. Теорема 5 доказана.

При всяком ли $n\in\mathbb{N}$ множество $W_n=\{1^n,2^n,\ldots\}$ всех n-тых степеней является базисом? Это — так называемая *проблема Варинга.* Она была положительно решена Гильбертом в начале века. Решение оказалось весьма сложным. Теорема 5 позволяет получить другое решение: достаточно установить, что k-кратная сумма $W_n\oplus\ldots\oplus W_n$ при больших k имеет положительную плотность. Элементарное (хотя очень непростое) решение проблемы Варинга, основанное на методе Шнирельмана, можно найти в книжке Хинчина [5].

Вот что пишет Хинчин [5] в связи с леммой 2 (цитируем с сокращениями): «Осенью 1931 года Л.Г.Шнирельман, рассказывая о своих беседах с Ландау в Геттингене, сообщил, что они установили следующий интересный факт: для всех примеров, какие им удавалось придумать, неравенство

$$d(A\oplus B)\geqslant d(A)+d(B)-d(A)d(B)$$

можно было заменить более сильным и более простым неравенством:

$$d(A\oplus B)\geqslant d(A)+d(B)$$

(при условии, что $d(A)+d(B)\leqslant 1$). Но доказательство этой гипотезы при первых попытках не удавалось. Проблема стала модной. Ученые общества предлагали её на премию. Добрая половина английских математиков, отложив все дела, занялась решением этой задачи. Но она оказалась очень трудной и целый ряд лет не поддавалась усилиям самых искусных исследователей. Только в 1942 г., наконец, с нею справился молодой американский математик Манн». Доказательство гипотезы Ландау – Шнирельмана можно найти у Хинчина [5]. Мы очень советуем читателю познакомиться с этой замечательной книгой. Не менее достойна вашего внимания книга самого Шнирельмана [7]. Из неё вы узнаете и доказательство теоремы

Лагранжа о сумме четырёх квадратов, и решение великой проблемы Ферма для показателей 3 и 4, и многое другое. О затронутых здесь темах, касающихся творчества Л. Г. Шнирельмана см. также [3].

Список литературы

[1] *Галочкин А. И.* О доказательствах теорем Линдемана и Гельфонда – Шнейдера // Фундаментальная и прикладная математика, 1997. Т. 3, №4. С. 1253–1260.

[2] *Ленг С.* Алгебра. М.: Мир, 1968.

[3] *Тихомиров В. М., Успенский В. В.* Первые филдсовские лауреаты и советская математика 30-х годов. I. // Математическое просвещение, 1998. Сер. 3, вып. 2. С. 21–40.

[4] *Фельдман Н. И.* Седьмая проблема Гильберта. М.: МГУ, 1982.

[5] *Хинчин А. Я.* Три жемчужины теории чисел. М.–Л.: ОГИЗ, 1948.

[6] *Шидловский А. Б.* Диофантовы приближения и трансцендентные числа. М.: МГУ, 1982.

[7] *Шнирельман Л. Г.* Простые числа. М.–Л.: ГИТТЛ, 1940.

Логические формулы и схемы

Н. В. Верещагин А. Шень

Эта статья — сокращенный вариант главы из книги «Вычислимые функции», издание которой планируется в ближайшее время.

1. Высказывания и операции

«Если число π рационально, то π — алгебраическое число. Но оно не алгебраическое. Значит, π не рационально». Мы не обязаны знать, что такое число π, какие числа называют рациональными и какие алгебраическими, чтобы признать, что это рассуждение правильно — в том смысле, что из двух сформулированных посылок действительно вытекает заключение. Такого рода ситуации — когда некоторое утверждение верно независимо от смысла входящий в него высказываний — составляют предмет *логики высказываний*.

Такое начало (особенно если учесть, что курс логики входит в программу философского факультета, где в свое время изучалась и «диалектическая логика») настораживает, но на самом деле наши рассмотрения будут иметь вполне точный математический характер, хотя мы начнём с неформальных мотивировок.

Высказывания могут быть *истинными* и *ложными*. Например, «$2^{16}+1$ — простое число» — истинное высказывание, а «$2^{32}+1$ — простое число» — ложное (это число делится на 641). Про высказывание «существует бесконечно много простых p, для которых $p+2$ — также простое» никто не берётся сказать наверняка, истинно оно или ложно. А фраза «x делится на 2» в этом смысле не является высказыванием, пока не сказано, чему равно x; при разных x получаются разные высказывания, одни истинные (при чётном x), другие — ложные (при нечётном x).

Высказывания можно соединять друг с другом с помощью *логических связок*. Эти связки имеют довольно странные, но традиционные названия и обозначения (табл. 1). Отметим также, что в $A \Rightarrow B$ высказывание A называют *посылкой*, или *антецедентом импликации*, а B — *заключением*, или *консеквентом*.

Говорят также, что высказывание имеет *истинностное значение* **И** (истина), если оно истинно, или **Л** (ложь), если оно ложно. Иногда вместо **И** употребляется буква **Т** (true) или число 1, а вместо **Л** — буква **F**

связка	обозначение	название
A и B	$A\&B$ $A \wedge B$ A `and` B	конъюнкция
A или B	$A \vee B$ A `or` B	дизъюнкция
не A A неверно	$\neg A$ $\sim A$ $\overline{A}$ `not` A	отрицание
из A следует B если A, то B A влечёт B B — следствие A	$A \to B$ $A \Rightarrow B$ $A \supset B$ `if` A `then` B	импликация следование

Табл. 1. *Логические связки, обозначения и названия*

(false) или число 0. (На первый взгляд идея выбрать числа 0 и 1 произвольным образом кажется дикой — какая польза могла бы быть, скажем, от сложения истинностных значений? Удивительным образом в последние годы обнаружилось, что такая польза есть, и если оперировать с истиной и ложью как элементами конечного поля, можно получить много неожиданных результатов.)

Логические связки позволяют составлять сложные высказывания из простых. При этом истинность составного высказывания определяется истинностью его частей в соответствии с таблицей 2.

A	B	$A \wedge B$	$A \vee B$	$A \to B$
Л	**Л**	**Л**	**Л**	**И**
Л	**И**	**Л**	**И**	**И**
И	**Л**	**Л**	**И**	**Л**
И	**И**	**И**	**И**	**И**

A	$\neg A$
Л	**И**
И	**Л**

Табл. 2. *Таблицы истинности для логических связок*

Те же правила можно изложить словесно. Высказывание $A \wedge B$ истинно, если оба высказывания A и B истинны. Высказывание $A \vee B$ истинно, если хотя бы одно из высказываний A и B истинно. Высказывание $A \to B$ ложно в единственном случае: если A истинно, а B ложно. Наконец, $\neg A$ истинно в том и только том случае, когда A ложно.

Из всех связок больше всего вопросов вызывает импликация. В самом деле, не очень понятно, почему надо считать, скажем, высказывания «если $2 \times 2 = 5$, то $2 \times 2 = 4$» и «если $2 \times 2 = 5$, то $3 \times 3 = 1$» истинными. (Именно

так говорят наши таблицы: **Л** $\to$ **И** = **Л** $\to$ **Л** = **И**.) Следующий пример показывает, что в таком определении есть смысл.

Общепризнанно, что если число x делится на 4, то оно делится на 2. Это означает, что высказывание

$$(x \text{ делится на } 4) \;\to\; (x \text{ делится на } 2)$$

истинно при всех x. Подставим сюда $x = 5$: обе части ложны, а импликация истинна. При $x = 6$ посылка импликации ложна, а заключение истинно, и вся импликация истинна. Наконец, при $x = 8$ посылка и заключение истинны и вся импликация истинна. С другой стороны, обратное утверждение (если x делится на 2, то x делится на 4) неверно, и число 2 является контрпримером. При этом посылка импликации истинна, заключение ложно, и сама импликация ложна. Таким образом, если считать, что истинность импликации определяется истинностью её частей (а не наличием между ними каких-то причинно-следственных связей), то все строки таблицы истинности обоснованы. Чтобы подчеркнуть такое узко-формальное понимание импликации, философски настроенные логики называют её «материальной импликацией».

Теперь от неформальных разговоров перейдём к определениям. Элементарные высказывания (из которых составляются более сложные) мы будем обозначать маленькими латинскими буквами (с индексами, если понадобится) и называть *пропозициональными переменными*. Из них строятся *пропозициональные формулы* (слово «пропозициональный» для краткости будем опускать) по таким правилам:

- ▷ Всякая пропозициональная переменная есть формула.
- ▷ Если A — пропозициональная формула, то $\neg A$ — пропозициональная формула.
- ▷ Если A и B — пропозициональные формулы, то $(A \wedge B)$, $(A \vee B)$ и $(A \to B)$ — пропозициональные формулы.

Можно ещё сказать так: формулы — это минимальное множество, обладающее указанными свойствами (слово «минимальное» здесь существенно: ведь если бы мы объявили любую последовательность переменных, скобок и связок формулой, то эти три свойства были бы тоже выполнены).

Пусть формула φ содержит n переменных $p_1, p_2, \ldots, p_n$. Если подставить вместо этих переменных истинностные значения (**И** или **Л**), то по таблицам можно вычислить истинностное значение формулы в целом. Таким образом, формула задаёт некоторую функцию от n аргументов, каждый из которых может принимать значения **Л** и **И**. Значения функции также лежат в множестве $\{\mathbf{Л}, \mathbf{И}\}$, которое мы будем обозначать $\mathbb{B}$. Как

уже говорилось, мы будем следовать традиции и отождествлять **И** с единицей, а **Л** — с нулём, тем самым $\mathbb{B}$ есть $\{0,1\}$. Формула φ задаёт отображение $\mathbb{B}^n \to \mathbb{B}$. Такие отображения называют также *булевыми функциями от n аргументов*.

Пример. Рассмотрим формулу $(p \wedge (q \wedge \neg r))$. Она истинна в единственном случае — когда p и q истинны, а r ложно (см. табл. 3).

p	q	r	$\neg r$	$(q \wedge \neg r)$	$(p \wedge (q \wedge \neg r))$
0	0	0	1	0	0
0	0	1	0	0	0
0	1	0	1	1	0
0	1	1	0	0	0
1	0	0	1	0	0
1	0	1	0	0	0
1	1	0	1	1	1
1	1	1	0	0	0

Табл. 3. *Таблица истинности конъюнкции* $(p \wedge (q \wedge \neg r))$

Некоторые формулы выражают логические законы — составные высказывания, истинные независимо от смысла их частей. Такие формулы (истинные при всех значениях входящих в них переменных) называют *тавтологиями*.

Пример. Формула $((p \wedge q) \to p)$ является тавтологией (это можно проверить, например, составив таблицу). Она выражает такой логический закон: из конъюнкции утверждений следует первое из них.

Задача 1. Как выглядит симметричное утверждение для дизъюнкции?

Две формулы называют *эквивалентными*, если они истинны при одних и тех же значениях переменных (другими словами, если они задают одну и ту же булеву функцию). Например, формула $(p \wedge (p \to q))$ истинна лишь при $p = q =$ **И** и потому эквивалентна формуле $(p \wedge q)$.

Рассмотрим формулу $((p \vee q) \wedge q)$. Она истинна, если и только если переменная q истинна. Хотелось бы сказать, что она эквивалентна формуле q, но тут есть формальная трудность: она содержит две переменные и потому задаёт функцию от двух аргументов (типа $\mathbb{B} \times \mathbb{B} \to \mathbb{B}$), в то время как q задаёт функцию от одного аргумента. Мы не будем обращать на это внимания и будем считать эти формулы эквивалентными. Вообще, если есть список переменных $p_1, \ldots, p_n$, содержащий все переменные некоторой формулы φ (и, возможно, ещё какие-то переменные), можно

считать, что формула φ задаёт функцию от n аргументов, возможно, на деле зависящую не от всех аргументов (постоянную по некоторым аргументам).

После таких оговорок легко проверить следующий факт: формулы φ и ψ эквивалентны тогда и только тогда, когда формула $((\varphi \to \psi) \wedge (\psi \to \varphi))$ является тавтологией. Используя сокращение $(p \leftrightarrow q)$ для $((p \to q) \wedge (q \to p))$, можно записывать утверждения об эквивалентности формул в виде тавтологий. Вот несколько таких эквивалентностей:

Теорема 1. *Следующие формулы являются тавтологиями:*

$$
\begin{aligned}
(p \wedge q) &\leftrightarrow (q \wedge p);\\
((p \wedge q) \wedge r) &\leftrightarrow (p \wedge (q \wedge r));\\
(p \vee q) &\leftrightarrow (q \vee p);\\
((p \vee q) \vee r) &\leftrightarrow (p \vee (q \vee r));\\
(p \wedge (q \vee r)) &\leftrightarrow ((p \wedge q) \vee (p \wedge r));\\
(p \vee (q \wedge r)) &\leftrightarrow ((p \vee q) \wedge (p \vee r));\\
\neg(p \wedge q) &\leftrightarrow (\neg p \vee \neg q);\\
\neg(p \vee q) &\leftrightarrow (\neg p \wedge \neg q);\\
(p \vee (p \wedge q)) &\leftrightarrow p;\\
(p \wedge (p \vee q)) &\leftrightarrow p;\\
(p \to q) &\leftrightarrow (\neg q \to \neg p);\\
p &\leftrightarrow \neg\neg p.
\end{aligned}
$$

Доказательство. Первые четыре эквивалентности выражают коммутативность и ассоциативность конъюнкции и дизъюнкции. Проверим, например, вторую: левая и правая части истинны в единственном случае (когда все переменные истинны), и потому эквивалентны. (Для дизъюнкции удобнее смотреть, когда она ложна.)

Две следующие эквивалентности утверждают дистрибутивность — заметим, что в отличие от сложения и умножения в кольцах здесь верны оба свойства дистрибутивности. Проверить эквивалентность легко, если отдельно рассмотреть случаи истинного и ложного p.

Следующие два свойства называются *законами де Моргана*. Их легко проверить, вспомнив, что конъюнкция истинна, а дизъюнкция ложна ровно в одном случае. Законы де Моргана иногда выражают словами: «конъюнкция двойственна дизъюнкции».

Далее следуют два очевидных *закона поглощения* (один из них мы уже упоминали).

За ними идёт правило *контрапозиции*, которое говорит, в частности, что утверждения «если x совершенно, то x нечётно» и «если x нечётно,

то x несовершенно» равносильны. Хотя оно и очевидно проверяется с помощью таблиц истинности, с ним связан любопытный парадокс. Вот он. Биолог А выдвинул гипотезу: все вороны чёрные. Проверяя её, он вышел во двор и обнаружил на дереве ворону. Она оказалось чёрной. Вроде бы у него есть основания радоваться — гипотеза подтверждается. Биолог Б переформулировал гипотезу так: все не-чёрные предметы — не вороны (применив наше правило контрапозиции) и не стал выходить во двор, а открыл холодильник и нашёл там оранжевый предмет. Он оказался апельсином, а не вороной. Биолог Б обрадовался — гипотеза подтверждается — и позвонил биологу А. Тот удивляется — у него тоже есть апельсин в холодильнике, но с его точки зрения никакого отношения к его гипотезе апельсин не имеет...

Последнее (и очевидное) правило называется *снятием двойного отрицания.*

Задача 2. Перечисленные эквивалентности соответствуют равенствам для множеств: например, первая гарантирует, что $P \cap Q = Q \cap P$ для любых множеств P и Q. Какие утверждения соответствуют остальным эквивалентностям?

Задача 3. Две формулы, содержащие только переменные и связки $\wedge$, $\vee$ и $\neg$, эквивалентны. Докажите, что они останутся эквивалентными, если всюду заменить $\wedge$ на $\vee$ и наоборот.

Заметим, что далеко не все тавтологии имеют ясный интуитивный смысл. Например, формула $(p \to q) \vee (q \to p)$ является тавтологией (если одно из утверждений p и q ложно, то из него следует всё, что угодно; если оба истинны, то тем более формула истинна), хотя и отчасти противоречит нашей интуиции — почему, собственно, из двух никак не связанных утверждений одно влечёт другое? Ещё более загадочна тавтология

$$((p \to q) \to p) \to p$$

(хотя её ничего не стоит проверить с помощью таблиц истинности).

Отступление о пользе скобок. На самом деле наши рассуждения содержат серьёзный пробел. Чтобы обнаружить его, зададим себе вопрос: зачем нужны скобки в формулах? Представим себе, что мы изменим определение формулы, и будем говорить, что $P \wedge Q$ и $P \vee Q$ являются формулами для любых P и Q. Останутся ли наши рассуждения в силе?

Легко понять, что мы столкнёмся с трудностью при определении булевой функции, соответствующей формуле. В этом определении мы подставляли нули и единицы на место переменных и затем вычисляли значение формулы с помощью таблиц истинности для связок. Но теперь, когда мы изменили определение формулы, формула $p \wedge q \vee r$ может быть получена

двумя способами — из формул $p \wedge q$ и r с помощью операции $\vee$ и из формул p и $q \vee r$ с помощью операции $\wedge$. Эти два толкования дадут разный результат при попытке вычислить значение $0 \wedge 0 \vee 1$.

Из сказанного ясно, что скобки нужны, чтобы гарантировать однозначность синтаксического разбора формулы. Точнее говоря, верно такое утверждение:

Теорема 2 (однозначность разбора). *Пропозициональная формула, не являющаяся переменной, может быть представлена ровно в одном из трёх видов* $(A \wedge B)$, $(A \vee B)$ *или* $\neg A$, *где* A *и* B — *некоторые формулы, причём* A *и* B *(в первых двух случаях) восстанавливаются однозначно.*

Доказательство. Формальное доказательство можно провести так: определим понятие *скобочного итога* как разницы между числом открывающихся и закрывающихся скобок. Индукцией по построению формулы легко доказать такую лемму:

> Скобочный итог любой формулы равен нулю. Скобочный итог любого начала формулы неотрицателен и равен нулю, лишь если это начало совпадает со всей формулой, пусто или состоит из одних символов отрицания.

Слова «индукцией по построению» значат вот что: мы проверяем интересующее нас утверждение для переменных, а также доказываем, что если оно верно для формул A и B, то оно верно и для формул $(A \wedge B)$, $(A \vee B)$ и $\neg A$.

После того как лемма доказана, разбор формулы проводится так: если она начинается с отрицания, то может быть образована лишь по третьему правилу. Если же она начинается со скобки, то надо скобку удалить, а потом искать начало, имеющее нулевой скобочный итог. Такое начало единственно. (Это легко проверить, используя лемму.) Тем самым формула разбирается однозначно.

В дальнейшем мы будем опускать скобки, если они либо не играют роли (например, можно написать конъюнкцию трёх членов, не указывая порядок действий в силу ассоциативности), либо ясны из контекста.

Задача 4. Польский логик Лукасевич предлагал обходиться без скобок, записывая в формулах сначала знак операции, а потом операнды (без пробелов и разделителей). Например, $(a + b) \times (c + (d \times e))$ в его обозначениях запишется как $\times + ab + c \times de$. Эту запись ещё называют *польской* записью. Обратная польская запись отличается от неё тем, что знак операции идёт после операндов. Покажите, что в обоих случаях порядок действий восстанавливается однозначно.

2. Полные системы связок

Рассматриваемая нами система пропозициональных связок ($\wedge$, $\vee$, $\neg$) *полна* в следующем смысле:

Теорема 3 (Полнота системы $\vee, \wedge, \neg$). *Любая булева функция от n аргументов может быть записана в виде пропозициональной формулы.*

Доказательство. Проще всего пояснить это на примере. Пусть, например, булева функция $\varphi(p, q, r)$ задана таблицей 4.

p	q	r	$\varphi(p,q,r)$
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

$$\begin{array}{l} (\neg p \wedge \neg q \wedge \neg r) \ \vee \\ \vee\ (\neg p \wedge \ \ q \wedge r\ \ ) \ \vee \\ \vee\ (\ \ p \wedge \ \ q \wedge r\ \ ) \end{array}$$

Табл. 4. *Таблица значений булевой функции и задающая её формула*

В таблице есть три строки с единицами в правой колонке — три случая, когда булева функция истинна (равна 1). Напишем три конъюнкции, каждая из которых покрывает один случай (а в остальных строках ложна), и соединим их дизъюнкцией. Нужная формула построена.

Ясно, что аналогичная конструкция применима и для любой таблицы (и с любым числом переменных).

Для формул подобного вида есть специальное название: формулы в *дизъюнктивной нормальной форме*. Более подробно: *литералом* называется переменная или отрицание переменной, *конъюнктом* называется произвольная конъюнкция литералов, а дизъюнктивной нормальной формой называется дизъюнкция конъюнктов. В нашем случае в каждый конъюнкт входит n литералов (где n — число переменных), а число конъюнктов равно число строк с единицами и может меняться от нуля (тогда, правда, получается не совсем формула, а «пустая дизъюнкция», и её можно заменить какой-нибудь всегда ложной формулой типа $p \wedge \neg p$) до 2^n (если булева функция всегда истинна).

Задача 5. Длина построенной в доказательстве теоремы 3 формулы зависит от числа единиц: формула будет короткой, если единиц в таблице

мало. А как написать (сравнительно) короткую формулу, если в таблице мало нулей, а в основном единицы?

Иногда используется *конъюнктивная нормальная форма*, которая представляет собой конъюнкцию *дизъюнктов*, каждый из которых состоит из литералов, связанных дизъюнкциями. Теорему 3 можно теперь усилить так:

Теорема 4. *Всякая булева функция может быть выражена формулой, находящейся в дизъюнктивной нормальной форме, а также формулой, находящейся в конъюнктивной нормальной форме.*

Доказательство. Первая часть утверждения уже доказана. Вторую часть можно доказать аналогично первой, надо только для каждой строки с нулём написать подходящий дизъюнкт.

Можно также представить функцию $\neg\varphi$ в дизъюнктивной нормальной форме, а затем воспользоваться правилами де Моргана, чтобы внести отрицание внутрь.

Задача 6. Проведите второй вариант рассуждения подробно.

Вообще говоря, определение дизъюнктивной нормальной формы не требует, чтобы в каждом конъюнкте (или дизъюнкте) встречались все переменные. (Повторять переменную больше одного раза смысла нет; если, например, формула и её отрицание входят в одну конъюнкцию, то эта конъюнкция всегда ложна и её можно выбросить.)

Задача 7. Приведите пример булевой функции от n аргументов, у которой любая дизъюнктивная или конъюнктивная нормальная форма содержит лишь члены длины n. (Указание: рассмотрите функцию, которая меняет своё значение при изменении значения любой переменной.)

Заметим, что при доказательстве теоремы 3 мы обошлись без импликации. Это и не удивительно, так как она выражается через дизъюнкцию и отрицание:

$$(p \to q) \;\leftrightarrow\; (\neg p \vee q)$$

(проверьте!). Вообще-то мы могли бы обойтись только конъюнкцией и отрицанием, так как

$$(p \vee q) \;\leftrightarrow\; \neg(\neg p \wedge \neg q),$$

или только дизъюнкцией и отрицанием, так как

$$(p \wedge q) \;\leftrightarrow\; \neg(\neg p \vee \neg q),$$

(обе эквивалентности вытекают из законов де Моргана; их легко проверить и непосредственно). Можно сказать, что система связок $\wedge, \neg$, а также система связок $\vee, \neg$ являются *полными*. (По определению это означает, что с их помощью можно записать любую булеву функцию).

Задача 8. Докажите, что система связок $\neg, \to$ полна. (Указание: как записать через них дизъюнкцию?)

А вот без отрицания обойтись нельзя. Система связок $\wedge, \vee, \to$ неполна — и по очень простой причине: если все переменные истинны, то любая их комбинация, содержащая только указанные связки, истинна. (Как говорят, все эти связки «сохраняют единицу».)

Задача 9. Легко понять, что любая формула, составленная только с помощью связок $\wedge$ и $\vee$, задаёт монотонную булеву функцию (в том смысле, что от увеличения значения любого из аргументов значение функции может только возрасти — или остаться прежним). Покажите, что любая монотонная булева функция может быть выражена формулой, содержащей только $\wedge$ и $\vee$.

Задача 10. Пусть $\varphi \to \psi$ — тавтология. Покажите, что найдётся формула τ, которая включает в себя только общие для φ и ψ переменные, для которой формулы $\varphi \to \tau$ и $\tau \to \psi$ являются тавтологиями. (Более общий вариант этого утверждения, в котором формулы берутся в языке первого порядка, называется леммой Крейга.)

В принципе мы не обязаны ограничиваться четырьмя рассмотренными связками. Любая булева функция может играть роль связки. Например, можно рассмотреть связку $(p \texttt{ notand } q)$, задаваемую эквивалентностью

$$(p \texttt{ notand } q) \leftrightarrow \neg(p \wedge q)$$

(словами: $(p \texttt{ notand } q)$ ложно, лишь если p и q истинны). Через неё выражается отрицание $(p \texttt{ notand } p)$, после чего можно выразить конъюнкцию, а затем, как мы знаем, и вообще любую функцию. (Знакомые с цифровыми логическими схемами малого уровня интеграции хорошо знакомы с этим утверждением: достаточно большой запас схем И-НЕ позволяет реализовать любую требуемую зависимость выхода от входов.)

Другая интересная полная система связок — это сложение по модулю 2, конъюнкция и константа 1 (которую можно считать 0-арной связкой, задающей функцию от нуля аргументов).

Назовём *мономом* конъюнкцию любого набора переменных или константу 1 (которую естественно рассматривать как конъюнкцию нуля переменных). Название это естественно, так как при наших соглашениях (1 — истина, 0 — ложь) конъюнкция соответствует умножению.

Назовём *полиномом* сумму таких мономов по модулю 2 (это значит, что $0+0=0, 0+1=1+0=1$ и $1+1=0$). Ясно, что два повторяющихся монома можно сократить (ведь сложение по модулю 2), так что будем рассматривать только полиномы без повторяющихся мономов. При этом,

естественно, порядок членов в мономе и порядок мономов в полиноме несуществен, их можно переставлять.

Теорема 5 (полиномы Жегалкина). *Всякая булева функция однозначно представляется полиномом указанного вида.*

Доказательство. Чтобы доказать существование искомого полинома, можно сослаться на известное из алгебры утверждение, что всякая функция с аргументами из конечного поля (в данном случае это двухэлементное поле вычетов по модулю 2) задаётся полиномом. Правда, в алгебре понятие полинома более общее, разрешены степени. Но это не важно, так как переменные принимают лишь значения 0 и 1 и потому степени роли не играют.

Далее можно заметить, что полиномов столько же, сколько булевых функций, а именно 2^{2^n}. В самом деле, булева функция может принимать любое из двух значений в каждой из 2^n точек булева куба $\mathbb{B}^n$, а многочлен может включать или не включать любой из 2^n мономов. (Мономов столько, потому что каждой моном включает или не включает любую из n переменных.) Поэтому избытка полиномов нет, и если любая функция представима полиномом, то единственным образом.

Можно и не ссылаться на сведения из алгебры, а дать явную конструкцию. Это удобно сделать индукцией по n. Пусть мы уже умеем представлять любую булеву функцию от $n-1$ аргументов с помощью полинома. Тогда $\varphi(p_1,\ldots,p_n)$ можно представить как

$$\begin{aligned}\varphi(p_1,\ldots,p_n) =& \varphi(0,p_2,\ldots,p_n) + \\ &+ [\varphi(0,p_2,\ldots,p_n) + \varphi(1,p_2,\ldots,p_n)]p_1\end{aligned}$$

(проверьте, что всё сходится). Остаётся заметить, что правую часть можно представить полиномом по предположению индукции.

Для единственности также есть другое доказательство: пусть два многочлена равны. Тогда их сумма (или разность — вычисления происходят по модулю 2) является ненулевым многочленом (содержит какие-то мономы), но тождественно равна нулю. Так не бывает, и это легко доказать по индукции. В самом деле, любой многочлен $A(p_1,\ldots,p_n)$ можно представить в виде

$$A(p_1,\ldots,p_n) = B(p_2,\ldots,p_n) + p_1 C(p_2,\ldots,p_n),$$

где B и C — многочлены от меньшего числа переменных. Подставляя сначала $p_1 = 0$, а затем $p_1 = 1$, убеждаемся, что многочлены B и C равны нулю во всех точках, и потому (согласно предположению индукции) равны нулю как многочлены (не содержат мономов).

Задача 11. Назовём *мультилинейной* функцией полином от n переменных, в котором все показатели степеней равны либо 0, либо 1. (Таким

образом, каждый моном в ней есть произведение коэффициента и некоторого набора переменных без повторений). Пусть F — произвольное поле. Будем рассматривать $\mathbb{B} = \{0, 1\}$ как подмножество F. Докажите, что всякая булева функция $\mathbb{B}^n \to \mathbb{B}$ однозначно продолжается до мультилинейной функции $F^n \to F$, и коэффициенты в мультилинейной функции будут целыми.

Если рассматривать произвольные булевы функции в качестве связок, возникает вопрос: в каком случае они образуют полный базис? Ответ дает следующая теорема.

Теорема 6 (критерий Поста). *Набор булевых функций тогда и только тогда является полным (это значит, что любая булева функция представляется в виде их композиции, т. е. записывается в виде формулы, где связками служат функции набора), когда он не содержится ни в одном из пяти «предполных классов»*:

- ▷ *монотонные функции*;
- ▷ *функции, сохраняющие нуль*;
- ▷ *функции, сохраняющие единицу*;
- ▷ *линейные функции*;
- ▷ *самодвойственные функции.*

(Функция f *монотонна*, если она монотонно неубывает по каждому из своих аргументов. Функция f *сохраняет нуль/единицу*, если $f(0, \ldots, 0) = 0$ (соответственно $f(1, \ldots, 1) = 1$). Функция f *линейна*, если она представима многочленом, в котором все мономы содержат не более одной переменной. Наконец, функция f называется *самодвойственной*, если $f(1 - p_1, \ldots, 1 - p_n) = 1 - f(p_1, \ldots, p_n)$.)

Если набор содержится в одном из классов, то и все композиции также не выходят за пределы этого класса (легко проверить для каждого из классов в отдельности) и поэтому набор не является полным. Доказательство обратного утверждения опустим (читатель может попробовать доказать его самостоятельно).

3. Схемы из функциональных элементов

Формулы представляют собой способ записи композиции функций. Например, если мы сначала применяем функцию f, а потом функцию g, это можно записать формулой $g(f(x))$. Но есть и другой способ: можно изобразить каждую функцию в виде прямоугольника с «входом» и «выходом» и соединить выход функции f со входом функции g (рис. 1).

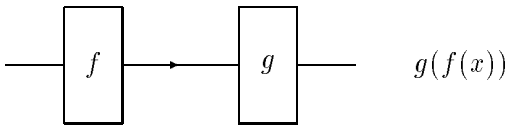


Рис. 1. *Два способа изобразить композицию*

Такое представление отнюдь не является чисто теоретическим. В течение нескольких десятков лет электронная промышленность выпускает микросхемы, которые выполняют логические операции. Такая микросхема имеет электрические контакты, напряжение на которых кодирует логические значения **И** и **Л**. Конкретное напряжение зависит от типа схемы, но обычно это единицы вольт, и высокий потенциал (относительно заземления) считается единицей, а низкий — нулём.

Одной из типичных схем является схема И-НЕ, она имеет два входа и один выход. Сигнал на выходе является отрицанием конъюнкции сигналов на входе. Другими словами, на выходе появляется высокий потенциал (сигнал 1) тогда и только тогда, когда на одном из входов потенциал низкий (0). Из такой схемы легко получить схему НЕ (изменяющую уровень сигнала на противоположный), соединив проводом два входа. При этом на оба входа поступает один и тот же сигнал, и операция И его не меняет ($p \wedge p = p$), а НЕ меняет на противоположный. Взяв два элемента и используя второй из них в качестве элемента НЕ, меняющего сигнал с выхода первого элемента, получаем схему, которая реализует функцию И. А если поставить два элемента НЕ перед каждым из входов элемента И-НЕ, получим схему, реализующую функцию ИЛИ: $\neg(\neg p \wedge \neg q) \leftrightarrow (p \vee q)$.

Теорема 3 о полноте системы связок теперь гарантирует, что любую булеву функцию можно реализовать в виде схемы. Надо иметь в виду, однако, что предлагаемая в её доказательстве конструкция (дизъюнктивная нормальная форма) имеет скорее теоретический интерес, поскольку приводит к схемам очень большого размера даже для простых функций (если число аргументов велико). Например, схема, сравнивающая два 16-битовых числа, должна иметь 32 входа и поэтому в её реализации с помощью дизъюнктивной нормальной формы будет порядка 2^{32} элементов — что мало реально. (Между тем такую схему можно построить гораздо проще, из нескольких сотен элементов.)

Поэтому вопрос о том, сколько элементов нужно для реализации той или иной функции, представляет большой интерес — как практический, так и философский. (Одна из центральных проблем математики и информатики, так называемая «проблема перебора», может быть сформулирована в этих терминах.)

Мы сейчас дадим более формальное определение схемы и реализуемой ею булевой функции. Но прежде всего ответим на такой вопрос — почему мы вообще говорим о схемах? Ведь можно записать композицию булевых функций в виде формулы, не будет ли это то же самое?

Оказывается, не совсем, и разницу легко видеть на примере (рис. 2).

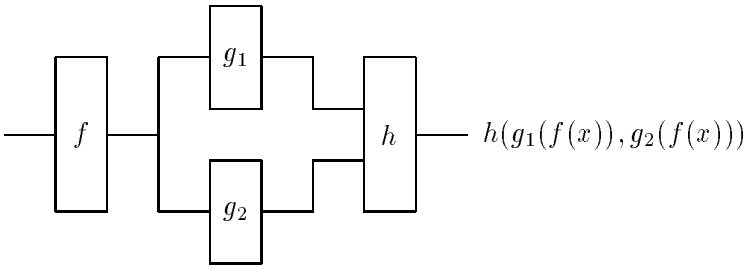


Рис. 2. *Элемент входит в формулу дважды*

Здесь один и тот же элемент схемы (f) приходится указывать в формуле дважды, поскольку его выход используется в качестве входа двух других элементов. Схемы, в которых такого ветвления нет (на практике оно вполне возможно, хотя и ограничено «нагрузочной способностью выхода», как говорят инженеры), как раз и соответствуют формулам. Но в общем случае формула может быть длинной, даже если схема содержит небольшое число элементов, поскольку число копий может расти экспоненциально с ростом глубины схемы.

Хотя идея образования схемы из функциональных элементов, реализующих булевы функции, достаточно наглядна, дадим более формальное определение. Пусть имеется n булевых переменных $x_1, \ldots, x_n$, называемых *входами*. Пусть также имеется некоторое число переменных $y_1, \ldots, y_m$, называемых *проводниками*. Пусть для каждого проводника схемы задана булева функция из некоторого множества B, выражающая его значение через другие проводники и входы. При этом требуется, чтобы не было циклов (когда y_i зависит от y_j, которое зависит от y_k, ..., которое зависит от y_i). Пусть, кроме того, среди проводников выделен один, называемый *выходом*. В таком случае говорят, что задана *схема размера m из функциональных элементов в базисе B* с n входами. (С точки зрения инженера размер — это число использованных элементов, а базис B — это ассортимент доступных ему элементов.)

Отсутствие циклов гарантирует, что есть проводник, зависящий только от входов (иначе можно было бы прийти к циклу: возьмём какой-то проводник, затем возьмём тот проводник, от которого он зависит, и т. д.). Его значение, таким образом, однозначно определяется сигнала-

ми на входах. Среди оставшихся проводников также нет цикла, поэтому можно найти один из них, зависящий только от уже известных, и определить его значение. Перенумеровав проводники в таком порядке, мы можем записать последовательность присваиваний (программу)

$$\begin{aligned} y_1 &:= f_1(\ldots);\\ y_2 &:= f_2(\ldots);\\ &\ldots\\ y_m &:= f_m(\ldots); \end{aligned}$$

в правых частях которых стоят функции из B, применённые ко входам и уже найденным значениям. При этом можно считать, что результат схемы есть y_m (все последующие присваивания уже не нужны). Такая программа определяет y_m при известных значениях входов и тем самым *вычисляет* некоторую булеву функцию.

Набор булевых функций B называется *полным*, если любая булева функция может быть задана схемой из B-элементов (существует программа, её вычисляющая, при этом в правых частях присваиваний стоят функции из B). Ясно, что это равносильно возможности записать булеву функцию в виде формулы со связками из B (как мы говорили, разница только в том, что один и тот же элемент будет фигурировать в формуле многократно).

Сложностью булевой функции f относительно B называется минимальный размер схемы из B-элементов, вычисляющей функцию f. Этот размер будем обозначать $\mathrm{size}_B(f)$.

Теорема 7. *Пусть B_1 и B_2 — два полных набора булевых функций. Тогда соответствующие им сложности отличаются не более чем на постоянный множитель: найдётся такое число C, что $\mathrm{size}_{B_1}(f) \leqslant C\,\mathrm{size}_{B_2}(f)$ и $\mathrm{size}_{B_2}(f) \leqslant C\,\mathrm{size}_{B_1}(f)$ для любой функции f.*

Доказательство. Утверждение почти очевидно: поскольку наборы B_1 и B_2 полны, то каждая функция одного из наборов может быть вычислена какой-то программой, составленной из функций другого набора. Теперь можно взять в качестве C наибольшую длину таких программ, и неравенства будут выполняться: каждую строку программы можно заменить на C (или меньше) строк с использованием функций другого набора.

Что можно сказать о сложности произвольной булевой функции от n аргументов? Следующая теорема показывает, что она экспоненциально зависит от n (для «наугад взятой» функции).

Теорема 8. *а) Сложность любой булевой функции от n аргументов не превосходит C^n для некоторого константы C. б) Сложность*

большинства булевых функций от n аргументов не меньше c^n для некоторой константы c.

Доказательство. Первое утверждение очевидно: размер схемы, реализующей дизъюнктивную нормальную форму, есть $O(n2^n)$ (имеется не более 2^n конъюнктов размера $O(n)$).

Чтобы доказать второе утверждение, оценим число различных схем с n аргументами размера N. Каждая такая схема может быть описана последовательностью из N присваиваний, выражающих одну из переменных через предыдущие. Для каждой формулы есть не более $3(N+n)^2$ вариантов (три типа операций — конъюнкция, дизъюнкция, отрицание, и каждый из не более чем двух аргументов выбирается среди не более чем $N+n$ вариантов). Отсюда легко получить оценку $2^{O(N\log N)}$ на число всех функций сложности не более N (считая $N \geqslant n$).

Всего булевых функций с n аргументами имеется 2^{2^n}. Из сравнения этих формул видно, что что при $c < 2$ и при достаточно больших n булевы функции сложности меньше c^n составляют меньшинство, так как $2^{O(c^n \log c^n)}$ много меньше 2^{2^n}. (Уменьшая константу c, можно добиться, чтобы они составляли меньшинство при всех n, а не только достаточно больших.)

Эта теорема, однако, ничего не говорит о сложности конкретных булевых функций. Ситуация здесь такова. Есть разнообразные методы и приёмы получения верхних оценок. Но про нижние оценки неизвестно практически ничего. Про многие функции мы подозреваем, что их сложность велика (экспоненциальна), но доказать это пока не удаётся. Весьма нетривиальные идеи позволяют доказывать экспоненциальные нижние оценки для некоторых специальных классов схем, например, схем из монотонных элементов или схем ограниченной глубины (использующих элементы И и ИЛИ с произвольным числом входов). Получение экспоненциальных оценок для более общих схем — один из возможных подходов к знаменитой *проблеме перебора*, центральной проблеме теории сложности вычислений.

Мы не будем углубляться в эту теорию, а приведём лишь несколько верхних оценок для конкретных задач. При этом мы не претендуем на полноту, а хотим лишь показать несколько интересных идей и приемов.

Рассмотрим уже упоминавшуюся функцию сравнения двух n-битовых чисел. Она имеет $2n$ аргументов (n для одного числа и n для другого). Обозначим эту функцию Comp_n.

Теорема 9. *Пусть B — полный набор функций. Существует такая константа C, что* $\mathrm{size}_B(\mathrm{Comp}_n) \leqslant Cn$.

Доказательство. Заметим, что поскольку в формулировке теоремы оценка размера проводится с точностью до константы, то выбор конкретного базиса не имеет значения. Другими словами, мы можем предполагать, что любое конечное число необходимых нам функций в этом базисе есть.

Схема сравнения чисел будет рекурсивной (чтобы сравнить два числа, мы отдельно сравниваем их левые и правые половины, а затем объединяем результаты). При этом, как часто бывает, надо усилить утверждение, чтобы индукция прошла. А именно, мы будем строить схему с $2n$ входами $x_1, \ldots, x_n, y_1, \ldots, y_n$ и двумя выходами, которая указывает, какой из трёх случаев $x < y$, $x = y$ или $x > y$ имеет место. (Здесь x — число, записываемое в двоичной системе как $x_1 \ldots x_n$). Два выходных бита кодируют четыре возможности, а нужно только три, так что есть некоторый запас. Для определённости можно считать, что первый выходной бит истинен, если числа равны, а второй — если $x < y$. Тогда возможны три варианта сигналов на выходе: 10 (равенство), 01 (при $x < y$) и 00 (при $x > y$).

Объясним теперь, как собрать, скажем, схему сравнения двух 16-битовых чисел. Соберём отдельно схему сравнения старших 8 битов и младших 8 битов. Каждая из них даст ответ в форме двух битов. Теперь из этих четырёх битов надо собрать два. (Если в старших разрядах неравенство, то оно определяет результат сравнения; если старшие разряды равны, то результат сравнения определяется младшими разрядами.) Написанная в скобках фраза определяет булеву функцию с четырьмя битами на входе и двумя битами на выходе, и может быть реализована некоторой схемой фиксированного размера. Таким образом, если через $T(n)$ обозначить размер схемы, сравнивающей n-битовые числа, то получаем оценку

$$T(2n) \leqslant 2T(n) + c,$$

где c — некоторая константа, зависящая от выбора базиса. Отсюда следует, что $T(2^k) \leqslant c'2^k$ при некотором c'. В самом деле, для достаточно большого c' можно доказать по индукции, что

$$T(m) \leqslant c'm - c$$

(мы должны усилить неравенство, вычтя из правой части c, чтобы индуктивный шаг прошёл; база индукции остается верной, если c' достаточно велико).

Ту же самую оценку можно объяснить и наглядно. Наша схема имеет вид иерархического дерева. На каждом уровне из двух двухбитовых сигналов получается один. Остаётся вспомнить, что в полном двоичном дереве число внутренних вершин (которое определяет размер схемы) на единицу меньше числа листьев. (В турнире по олимпийской системе число

игр на единицу меньше числа команд, так как после каждой игры одна команда выбывает.)

Каждая внутренняя вершина и каждый лист (где сравниваются два бита) представляют собой схемы ограниченного размера, откуда и вытекает оценка $T(2^k) \leqslant c'2^k$.

Осталось лишь сказать, что делать, если размер чисел (который мы обозначали через n) не есть точная степень двойки. В этом случае можно увеличить размер до ближайшей сверху степени двойки (не более чем в два раза) и подать на старшие разряды входов нули. Оба действия приводят к увеличению размера схемы не более чем в константу раз.

Теперь рассмотрим задачу о сложении двух n-битовых чисел. (Строго говоря, тут возникает не булева функция, а функция $\mathbb{B}^n \times \mathbb{B}^n \to \mathbb{B}^{n+1}$, но все наши определения очевидно переносятся на этот случай.)

Теорема 10. *Существует схема сложения двух n-битовых чисел размера $O(n)$.*

Доказательство. Напомним смысл обозначения $O(n)$: нам надо построить схему сложения n-битовых чисел, имеющую размер не более cn для некоторого c и для всех n.

Это совсем просто. Посмотрим на сложение в столбик:

$$\begin{array}{ccccc} & 0 & 1 & 1 & \\ & 1 & 0 & 0 & 1 \\ & 1 & 0 & 1 & 1 \\ \hline 1 & 0 & 1 & 0 & 0 \end{array}$$

Верхняя строка — биты переноса, нижняя — результат. Заметим, что каждый из битов переноса или результата определяется тремя другими битами (бит результата равен сумме двух битов слагаемых и бита переноса по модулю 2, а бит переноса равен 1, если хотя бы два из этих трёх битов равны 1). Поэтому можно составить схему, которая вычисляет эти биты справа налево и имеет размер n.

Заметим, что предыдущее утверждение (теорема 9) является следствием этого: чтобы сравнить числа x и y, сложим число $(2^n - 1) - x$ (то есть число x, в котором все единицы заменены нулями и наоборот) и число y. Если в старшем разряде появится единица, значит, $y > x$, а если нет, то $y \leqslant x$. Остаётся заметить, что и сложение, и обращение битов в числе x реализуются схемами линейного размера.

Тем не менее конструкция, использованная при доказательстве теоремы 9, имеет некоторые преимущества. Назовём *глубиной* схемы максимальное число элементов на пути от входа к выходу. Если представить себе, что сигнал на выходе элемента появляется не сразу после подачи

сигналов на входы, а с некоторой задержкой, то глубина схемы определяет суммарную задержку. Легко понять, что рекурсивная схема сравнения имела глубину $O(\log n)$ (число уровней пропорционально логарифму размера входа), в то время как построенная только что схема сложения имеет глубину, пропорциональную n (биты переноса вычисляются последовательно, справа налево). Но можно соединить эти два результата:

Теорема 11. *Существует схема сложения двух n-битовых чисел размера $O(n)$ и глубины $O(\log n)$.*

Доказательство. Как мы видели, проблема в том, что биты переноса вычисляются последовательно, а не параллельно. Если удастся их все вычислить схемой размера $O(n)$ и глубины $O(\log n)$, то дальнейшее очевидно.

Как мы уже говорили, вычисление битов переноса равносильно сравнению, так что достаточно научиться сравнить параллельно все «суффиксы» чисел, т.е. для каждого i сравнить числа $x_i x_{i+1} \ldots x_n$ и $y_i y_{i+1} \ldots y_n$.

Вспомним, что мы делали при сравнении чисел (скажем, длины 8). На нижнем уровне мы сравнивали биты:

$$\begin{array}{cccccccc} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ y_1 & y_2 & y_3 & y_4 & y_5 & y_6 & y_7 & y_8 \end{array}$$

На следующем уровне мы сравнивали двузначные числа

$$\begin{array}{cccc} x_1x_2 & x_3x_4 & x_5x_6 & x_7x_8 \\ y_1y_2 & y_3y_4 & y_5y_6 & y_7y_8 \end{array}$$

затем четырёхзначные

$$\begin{array}{cc} x_1x_2x_3x_4 & x_5x_6x_7x_8 \\ y_1y_2y_3y_4 & y_5y_6y_7y_8 \end{array}$$

и, наконец, восьмизначные:

$$\begin{array}{c} x_1x_2x_3x_4x_5x_6x_7x_8 \\ y_1y_2y_3y_4y_5y_6y_7y_8 \end{array}$$

Таким образом, для суффиксов длины 8, 4, 2 и 1 результаты сравнения уже есть. Для суффикса длины 6 результат можно получить, комбинируя результат сравнения $x_3x_4?y_3y_4$ и $x_5x_6x_7x_8?y_5y_6y_7y_8$. После этого у нас есть информация о суффиксах всех чётных длин, и соединяя её с информацией с первого этапа, получаем сведения про все суффиксы. Например, для сравнения суффиксов длины 7, то есть $x_2 \ldots x_8$ и $y_2 \ldots y_8$, мы соединяем результаты сравнения x_2 и y_2 с результатами сравнения суффиксов длины 6, то есть $x_3 \ldots x_8$ и $y_3 \ldots y_8$.

В общем случае картина такая: после «сужающегося дерева» мы строим «расширяющееся»; за k шагов до конца мы знаем результаты

сравнения всех суффиксов, длины которых кратны 2^k. Это дерево имеет размер $O(n)$ и глубину $O(\log n)$, что завершает доказательство.

Задача 12. Показать, что вычитание двух n-битовых чисел по модулю 2^n выполняется схемой размера $O(n)$ и глубины $O(\log n)$. (Указание: вычитание легко сводится к сложению, если заменить нули на единицы и наоборот.)

Теперь займёмся умножением. Схема умножения двух n-битовых чисел имеет $2n$ входов (по n для каждого множителя) и $2n$ выходов для произведения.

Посмотрим, какие оценки даёт обычный способ умножения чисел столбиком. В нём умножение двух n-разрядных чисел сводится к сложению n копий первого числа (частично заменённых на нули в зависимости от цифр второго числа) со сдвигами.

Получение этих копий требует схемы размера $O(n^2)$ (общее число цифр в копиях) и глубины $O(1)$. Сложение двух n-разрядных чисел мы можем выполнить с помощью схемы размера $O(n)$ и глубины $O(\log n)$, так что необходимые $n-1$ сложений можно выполнить схемой размера $O(n^2)$ и глубины $O(\log^2 n)$ (если складывать сначала попарно, потом результаты снова попарно и т. д.). Оказывается, этот результат можно улучшить. Наиболее экономные способы основаны на преобразовании Фурье и далеко выходят за рамки нашего обсуждения, но два улучшения мы приведём.

Теорема 12. *Существует схема умножения двух n-битовых чисел размера $O(n^2)$ и глубины $O(\log n)$.*

Доказательство. Как мы уже говорили, умножение двух n-битовых чисел сводится к сложению n таких чисел, и остаётся выполнить такое сложение схемой размера $O(n^2)$ и глубины $O(\log n)$. Ключевым моментом здесь является сведение сложения трёх чисел к сложению двух с помощью простой схемы размера $O(n)$ и глубины $O(1)$. В самом деле, пусть есть три числа x, y и z. Если мы будем складывать отдельно в каждом разряде, то в разряде может накопиться любая сумма от 0 до 3, то есть в двоичной записи от 00 до 11. Сформируем из младших битов этих двухбитовых сумм число u, а из старших (сдвинутых влево) — число v. Тогда, очевидно, $x+y+z=u+v$. Получение цифр числа u и v происходит параллельно во всех разрядах и требует размера $O(n)$ и глубины $O(1)$.

Теперь, если надо сложить n чисел, можно разбить их на тройки и из каждых трёх чисел получить по два. В следующий круг, таким образом, выйдут $(2/3)n$ чисел (примерно — граничные эффекты большой роли не играют). Их снова можно сгруппировать по тройкам и т. д. Получается дерево, в котором размеры уровней образуют геометрическую прогрес-

сию со знаменателем $3/2$, поэтому глубина этого дерева логарифмическая. Число вершин в нём (считая за вершину преобразование трёх чисел в два) будет примерно n, так как при каждом преобразовании число слагаемых уменьшается на единицу. Итак, эта конструкция имеет общий размер $O(n^2)$ и глубину $O(\log n)$. Надо только отметить, что в конце у нас получается не одно число, а два, и их напоследок надо сложить — что мы умеем делать с глубиной $O(\log n)$ и размером $O(n)$.

Задача 13. Доказать, что схема, вычисляющая булеву функцию f от n аргументов, у которой ни один аргумент не является фиктивным, имеет размер не менее cn и глубину не менее $c\log n$ (где c — некоторая константа, зависящая от выбранного набора элементов). (Аргумент функции называют фиктивным, если при его изменении значение функции не меняется.)

Эта задача показывает, что если в процессе умножения двух n-битовых чисел мы суммируем n слагаемых, то оценки $O(n^2)$ для размера и $O(\log n)$ для глубины, полученные при доказательстве теоремы 12, существенно улучшить нельзя.

Однако никто не обязывает нас следовать традиционному способу умножения столбиком — отказавшись от него, мы можем уменьшить размер схемы.

Теорема 13. *Существует схема умножения двух n-битовых чисел размера $O(n^{\log_2 3})$ и глубины $O(\log^2 n)$.*

Доказательство. Начнём с такого замечания. Вычисляя произведение двух комплексных чисел

$$(a+bi)(c+di) = (ac-bd) + (ad+bc)i$$

обычным способом, мы делаем четыре умножения. Но можно обойтись и тремя с помощью такого трюка: вычислить ac, bd и $(a+b)(c+d)$, а потом найти $ad+bc$ как разность $(a+b)(c+d) - ac - bd$.

Аналогичный фокус можно проделать и для целых чисел. Разобьём $2n$-битовое число на две n-битовые части, то есть представим его в виде $a2^n + b$. Теперь запишем произведение двух таких чисел:

$$(a2^n + b)(c2^n + d) = ac2^{2n} + (ad+bc)2^n + bd.$$

Отсюда видно, что для определения всех трех слагаемых в правой части равенства достаточно найти три произведения ac, bd и $(a+b)(c+d)$. Получается, что умножение двух $2n$-битовых чисел сводится к трём умножениям n-битовых и к нескольким сложениям и вычитаниям. (На самом деле при умножении $(a+b)$ на $(c+d)$ сомножители могут быть $(n+1)$-битовыми, но это не страшно, так как обработка лишнего разряда соответствует нескольким сложениям.)

Для размера схемы, таким образом, получается рекурсивная оценка

$$S(2n) \leqslant 3S(n) + O(n),$$

из которой следует, что $S(n) = O(n^{\log_2 3})$. (В самом деле, для умножения n-битовых чисел получается дерево рекурсивных вызовов глубины $\log_2 n$ и степени ветвления 3, так что число его листьев и общее число вершин есть $O(3^{\log_2 n}) = O(n^{\log_2 3})$. Остаётся понять только, что средний размер схемы в каждой вершине есть $O(1)$. В самом деле, он пропорционален числу складываемых битов. При переходе от одного уровня к следующему (более близкому к корню) число битов растёт вдвое, а число вершин уменьшается втрое, поэтому общее число элементов на этом уровне уменьшается в полтора раза. Таким образом, при движении по уровням от листьев к корню получается убывающая геометрическая прогрессия со знаменателем $2/3$, сумма которой всего лишь втрое превосходит её первый член.

Оценка глубины также очевидна: на каждом уровне мы имеем схему сложения глубины $O(\log n)$, а число уровней есть $O(\log n)$.

Рассмотрим теперь функцию *голосования* (majority). Она имеет нечётное число аргументов, и значение её равно 0 или 1 в зависимости от того, какое из двух значений чаще встречается среди входов.

Теорема 14. *Существует вычисляющая функцию голосования схема размера $O(n)$ и глубины $O(\log n \log\log n)$.*

Доказательство. На самом деле можно даже вычислить общее число единиц среди входов. Это делается рекурсивно: считаем отдельно для каждой половины, потом складываем. Получается логарифмическое число уровней. На верхнем уровне надо складывать числа размера $\log n$, на следующем — размера $\log n - 1$ и так до самого низа, где складываются однобитовые числа (то есть биты входа). Какой средний размер складываемых чисел? Половина вершин в дереве приходится на нижний уровень (числа длины 1), четверть — на следующий (числа длины 2) и т. д. Вспоминая, что ряд $\sum(k/2^k)$ сходится, видим, что средний размер складываемых чисел есть $O(1)$ и общий размер схемы есть $O(n)$. А общая глубина есть $O(\log n \log\log n)$, так как на каждом из $\log n$ уровней стоит схема глубины $O(\log\log n)$.

Заметим, что построенная схема вычисления функции голосования содержит в себе немонотонные элементы (поскольку операция сложения не монотонна). Мы уже говорили, что всякую монотонную функцию можно составить из конъюнкций и дизъюнкций. Для функции голосования есть очевидный способ это сделать: написать дизъюнкцию всех конъюнкций размера $(n+1)/2$ (напомним, что число входов n предполагается

нечётным). Однако при этом получится схема экспоненциального по n размера.

Теорема 15. *Существует схема размера $O(n^c)$ и глубины $O(\log n)$, составленная только из элементов И и ИЛИ (с двумя входами), вычисляющая функцию голосования.*

Доказательство. Для начала заметим, что ограничение на размер является следствием ограничения на глубину, так как элементы И и ИЛИ имеют только два входа и число входов схемы глубины d есть $O(2^d)$.

Схема будет строиться из элементов большинства с тремя входами (3-большинства). Каждый из них можно собрать из конъюнкций и дизъюнкций по формуле $(a\wedge b)\vee(a\wedge c)\vee(b\wedge c)$. Выход схемы будет большинством из трёх значений, каждое из которых есть большинство из трёх значений и т. д. (рис. 3).

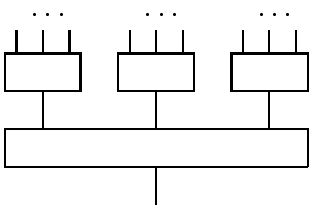


Рис. 3. *Дерево из элементов 3-большинства*

Продолжая эту конструкцию на k уровнях, мы получим схему с 3^k входами. (Отметим, что эта схема не будет вычислять большинство среди своих входов — по той же причине, по которой результат непрямого голосования может отличаться от мнения большинства.) Но мы сделаем вот какую странную вещь: возьмём k равным $c\log n$ при достаточно большом коэффициенте пропорциональности c (при этом число входов такой схемы будет полиномиально зависеть от n) и напишем на входах случайно выбранные переменные из данного нам набора $x_1,\ldots,x_n$. (Переменные, записываемые на разных входах, выбираются независимо.) Оказывается, что с ненулевой вероятностью эта схема будет вычислять функцию большинства среди $x_1,\ldots,x_n$, если константа c достаточно велика. Следовательно, искомая схема существует.

Обратите внимание: нам удастся доказать существование интересующей нас схемы, не предъявив её явно. (Такое использование вероятностных методов в комбинаторных рассуждениях часто бывает полезно.)

Итак, почему же схема с положительной вероятностью вычисляет функцию большинства? Это доказывается так: рассмотрим какой-то один набор значений на входах и докажем, что на этом конкретном

наборе случайная схема выдаёт правильный ответ с вероятностью, очень близкой к единице (равной $1-\varepsilon$ при очень малом ε).

Если число ε настолько мало, что остаётся меньшим единицы даже после умножения на число возможных входов (2^n), то получаем требуемое (каждое из 2^n событий имеет вероятность не меньше $1-\varepsilon$, значит их пересечение имеет вероятность не меньше $1-2^n\varepsilon > 0$).

Итак, осталось оценить вероятность того, что случайная схема даст правильный ответ на данном входе. Пусть доля единиц среди всех входов равна p. Тогда на каждый входной провод схемы подаётся единица с вероятностью p и нуль с вероятностью $1-p$ (выбор случайной переменной даёт единицу с вероятностью p), причём сигналы на всех входах независимы.

Если на трёх входах элемента 3-большинства сигналы независимы, и вероятность появления единицы на входе есть p, то вероятность появления единицы на выходе есть $\varphi(p) = 3p^2(1-p) + p^3 = 3p^2 - 2p^3$. На следующих уровнях вероятность появления единицы будет равна

$$\varphi(\varphi(p)), \varphi(\varphi(\varphi(p))), \ldots$$

График функции $\varphi(x)$ на отрезке $[0,1]$ (рис. 4) показывает, что при итерациях функции φ дисбаланс (отклонение от середины) нарастает. Поэтому последовательность итераций стремится к краю отрезка. Надо только оценить число шагов.

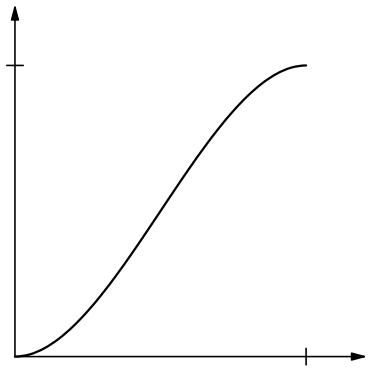


Рис. 4. *Итерируемая функция φ*

Если вначале единицы составляют большинство из n аргументов (напомним, n нечётно), то их как минимум $(n+1)/2$, так что $p \geqslant (n+1)/2n = 1/2 + 1/(2n)$. Таким образом, начальный дисбаланс составляет как минимум $1/2n$. А в конце нам нужно приблизиться к краю отрезка на расстояние 2^{-n}.

Итак, нам осталось доказать такую лемму (относящуюся скорее к математическому анализу):

Лемма. *Пусть функция* $\varphi : [0,1] \to [0,1]$ *задана формулой*

$$\varphi(x) = 3x^2 - 2x^3.$$

Пусть последовательность x_k *определена рекуррентной формулой* $x_{k+1} = \varphi(x_k)$. *Пусть* $x_0 \geqslant 1/2 + 1/(2n)$. *Тогда последовательность* x_k *монотонно возрастает и приближается к* 1 *на расстояние* 2^{-n} *за* $O(\log n)$ *шагов.*

Набросок доказательства: посмотрим на поведение функции в неподвижных точках. В окрестности точки $1/2$ функция близка к линейной и производная больше 1, поэтому удаление от $1/2$ растёт как геометрическая прогрессия, и точка перейдёт какую-то фиксированную границу (например, 0,51) не позднее чем за $O(\log n)$ шагов. Затем потребуется $O(1)$ шагов, чтобы дойти, скажем, до 0,99. В окрестности единицы первая производная функции равна нулю, поэтому расстояние до единицы каждый раз примерно возводится в квадрат, и потому для достижения погрешности 2^{-n} потребуется $O(\log n)$ шагов (каждый раз число совпадающих цифр увеличивается примерно вдвое, как в методе Ньютона отыскания корня). Всего получается $O(\log n) + O(1) + O(\log n)$ шагов, что и требовалось.

На самом деле справедливо гораздо более сильное утверждение: существует схема размера $O(n \log n)$ и глубины $O(\log n)$, состоящая только из элементов И и ИЛИ, которая имеет n входов и n выходов и осуществляет сортировку (это означает, что на выходе столько же единиц, сколько на входе, причём выходная последовательность всегда невозрастающая). Ясно, что средний бит выхода в такой ситуации реализует функцию большинства.

При кажущейся простоте формулировки единственная известная конструкция такой схемы (сортирующая сеть AKS, придуманная Айтаи, Комлошом и Сцемереди сравнительно недавно, в 1983 году[1)]) весьма сложна, и появление какой-то более простой конструкции было бы замечательным достижением.

Вообще многие нетривиальные результаты можно переформулировать в терминах сложности каких-то булевых функций. Например, есть вероятностный алгоритм проверки простоты большого числа (с помощью которого в криптографии проверяются числа из нескольких тысяч цифр). Используя этот алгоритм, можно доказать такое утверждение:

[1)] Ajtai M., Komlós J., Szemerédi E. An $O(n \log n)$ sorting network // Proc. of the 15th Annual ACM Symposium on Theory of Computing. Boston, MA, 1983. P. 1–9.

существует схема проверки простоты n-битового числа (на вход подаются n битов, на выходе появляется единица, если число простое), размер которой ограничен полиномом от n.

Вернёмся к общим утверждениям о схемах и формулах. Мы уже говорили, что с точки зрения измерения размера схемы и формулы — это разные вещи (схемы экономичнее, так как в них одинаковые подформулы учитываются только один раз). Оказывается, что размер формулы можно связать с глубиной схемы.

Будем называть *размером* формулы число логических связок в ней. Мы предполагаем, что формула использует конъюнкции, дизъюнкции и отрицания, и в схемах будем использовать такие же элементы. Напомним, что размером схемы мы называли число элементов, а сложностью булевой функции — минимальный размер схемы, её вычисляющей. Сложность функции h обозначалась $\mathrm{size}(h)$ (точнее $\mathrm{size}_B(h)$, где B — набор разрешённых функциональных элементов, но сейчас мы договорились использовать конъюнкции, дизъюнкции и отрицания и опускаем индекс B).

Минимальный размер формулы, выражающей функцию h, будем обозначать $\mathrm{fsize}(h)$. Очевидно, $\mathrm{size}(h) \leqslant \mathrm{fsize}(h)$. Более интересно, однако, следующее утверждение, связывающее размер схемы с глубиной формулы. Обозначим через $\mathrm{depth}(h)$ минимальную глубину схемы, вычисляющей функцию h.

Теорема 16. *Имеют место оценки* $\mathrm{fsize}(h) \leqslant c_1^{\mathrm{depth}(h)}$ *и* $\mathrm{depth}(h) \leqslant c_2 \log \mathrm{fsize}(h)$ *(для некоторых констант* c_1 *и* c_2 *и для всех* h*). Другими словами, меры сложности* depth *и* $\log$fsize *отличаются не более чем в константу раз.*

Доказательство. Первая оценка очевидна: если мы скопируем повторяющиеся фрагменты схемы, чтобы развернуть её в дерево, то глубина не изменится. Если она равна k, то в полученном дереве будет не больше $2^k - 1$ элементов (напомним, что элементами являются конъюнкции, дизъюнкции и отрицания, и потому ветвление не больше 2). То же самое можно сказать индуктивно. Пусть глубина схемы равна k. Выход схемы является выходом некоторого элемента. Тогда на его входы подаются булевы функции глубины не больше $k - 1$. По предположению индукции их можно записать формулами размера $2^{k-1} - 1$. Таких формул максимум две, так что общий размер не превосходит $2(2^{k-1} - 1) + 1 = 2^k - 1$.

Вторая оценка более сложна. Если мы будем преобразовывать формулу в схему естественным образом (введя по переменной для каждой подформулы), то глубина получившейся схемы может быть близка к размеру формулы, а не к его логарифму. Например, если формула имеет вид $(\ldots((p_1 \wedge p_2) \wedge p_3) \wedge \ldots p_n)$, то у нас получится цепочка элементов И, у

которых каждый следующий подвешен к левому входу предыдущего, и глубина есть $n-1$. Конечно, если использовать ассоциативность конъюнкции, скобки можно переставить и получить более сбалансированное дерево глубины примерно $\log n$, как и требуется. Но как выполнить такое преобразование в случае произвольной формулы?

Обозначим данную нам формулу через F. Выберем у неё некоторую подформулу G (как именно, мы объясним позже). Рассмотрим формулу F_0, которая получится, если вместо G подставить 0 (ложь), а также формулу F_1, которая получится, если подставить 1. Легко понять, что F равносильна формуле

$$((F_0 \wedge \neg G) \vee (F_1 \wedge G)).$$

Если теперь удастся заменить формулы F_0, F_1, G схемами глубины не больше k, то для F получится схема глубины не больше $k+3$.

Такое преобразование полезно, если все три формулы F_1, F_0, G имеют заметно меньший размер, чем исходная формула F.

Лемма. *У любой формулы размера n (при достаточно больших n) есть подформула размера от $n/4$ до $3n/4$.*

Доказательство. Каждая формула есть конъюнкция двух подформул, дизъюнкция двух подформул или отрицание подформулы. Начав со всей формулы, будем переходить к её подформулам, на каждом шаге выбирая из двух подформул наибольшую. Тогда на каждом шаге размер убывает не более чем в два раза, и потому мы не можем миновать промежуток $[n/4, 3n/4]$, концы которого отличаются втрое[2)]. Лемма доказана.

Выбирая подформулу G с помощью этой леммы, мы гарантируем, что размер всех трёх формул F_0, F_1, G не превосходит $3/4$ размера исходной формулы (подстановка нуля или единицы может только уменьшить размер формулы — некоторые части можно будет выбросить).

Применим ко всем трём формулам F_0, F_1 и G тот же приём, выделим в них подформулы среднего размера и так далее, пока мы не спустимся до формул малого размера, которые можно записать в виде схем как угодно. В итоге получится дерево с логарифмическим числом уровней, на каждом из которых стоят схемы глубины 3, а в листьях находятся схемы глубины $O(1)$.

Другими словами, индукцией по размеру формулы, выражающей некоторую функцию h, легко получить оценку $\operatorname{depth}(h) = O(\log \operatorname{fsize}(h))$.

[2)] Тут есть небольшая неточность: размер формулы может убывать чуть быстрее, чем вдвое, так как размер формулы на единицу больше суммы размеров частей, но у нас есть запас, поскольку концы промежутка отличаются втрое, а не вдвое.

Задача 14. Определим глубину формулы как максимальное число вложенных пар скобок; для единообразия будем окружать отрицание скобками и писать $(\neg A)$ вместо $\neg A$. Покажите, что при этом не получится ничего нового: минимальная глубина формулы, записывающей некоторую функцию f, совпадает с минимальной глубиной схемы, вычисляющей f.

Определение формульной сложности $\mathrm{fsize}(h)$ зависит от выбора базиса. Оказывается, что здесь (в отличие от схемной сложности) выбор базиса может изменить $\mathrm{fsize}(h)$ более чем в константу раз.

Задача 15. Объясните, почему доказательство теоремы 7 не переносится на случай формул.

Пример такого рода доставляет функция $p_1 \oplus p_2 \oplus \ldots \oplus p_n$ (знак $\oplus$ обозначает сложение по модулю 2). Эта функция имеет формульную сложность $O(n)$, если сложение по модулю 2 входит в базис. Однако в базисе И, ИЛИ, НЕ она имеет большую сложность, как доказала Б. А. Субботовская. Идея доказательства такова: если заменить случайно выбранную переменную в формуле с конъюнкциями и дизъюнкциями на случайно выбранное значение 0 или 1, то формула упростится (не только эта переменная пропадёт, но с некоторой вероятностью пропадут и другие). Если делать так многократно, то от формулы останется небольшая часть — с другой стороны, эта часть всё равно должна реализовывать сложение оставшихся аргументов по модулю 2.

Задача 16. Доказать, что функция большинства может быть вычислена не только схемой, но и формулой полиномиального размера, содержащей только связки И и ИЛИ.

Задача 17. Доказать, что значения $\mathrm{fsize}_1(h)$ и $\mathrm{fsize}_2(h)$ для одной булевой функции h и различных полных базисов полиномиально связаны: существует полином P (зависящий от выбора базисов), для которого $\mathrm{fsize}_2(h) \leqslant P(\mathrm{fsize}_1(h))$ при всех h. (Указание: использовать теорему 16.)

Сложность вычислительных задач

М. Н. Вялый*

В прошлом номере «Математического просвещения» была опубликована статья А. А. Разборова, в которой излагались основные идеи теории сложности вычислений. Данная статья продолжает эту тему[1)]. Нас будут интересовать два вопроса: «Что такое сложная вычислительная задача?» и «Как доказать, что некоторая вычислительная задача сложна?» В полном объеме эти вопросы слишком широки, поэтому мы сосредоточим внимание на самом интересном случае: тех задачах, которые по всей видимости сложны, но при этом настолько близки к простым задачам, что доказательство их сложности в наиболее естественном понимании этого слова лежит вне возможностей современной науки. Чтобы анализировать сложность таких задач, придуманы особые способы отвечать на первый из сформулированных выше вопросов.

Под вычислительной задачей будем понимать следующую типичную ситуацию: по заданному *входу* нужно получить, если это возможно, *результат*, удовлетворяющий определённым условиям и однозначно определяемый входом. Другими словами, речь всегда будет идти о вычислении некоторой функции, быть может, частично определённой. Поэтому в дальнейшем мы будем использовать выражения «решить задачу» и «вычислить функцию» как синонимические.

Чтобы не вводить читателя в заблуждение относительно возможностей излагаемой теории, предупредим сразу об основном её ограничении. *Вычисление любой функции из конечного множества в конечное множество считается тривиальным.* Очевидно, что в таком контексте бессмысленным становится любой вопрос типа: «смогу ли я решить вот эту задачу за пару часов (недель, лет, веков)?»

Мы будем рассматривать сложность решения задачи на всем (обычно бесконечном) множестве входов. С «практической» точки зрения это означает, что нас интересует как быстро растут ресурсы (время, память и т. п.), требующиеся для решения задачи при увеличении длины входа. Более точное объяснение этой фразы даётся ниже.

* Работа выполнена при поддержке фонда РФФИ (проект №99–01–00122).

[1)] Она написана по материалам первой части книги [4] и существенно опирается на статью [7], помещённую в этом выпуске «Математического Просвещения».

1. Вычисление каких функций рассматривается

Вход и результат предполагаются конечными словами в некотором конечном алфавите (т. е. конечными последовательностями элементов некоторого конечного множества). Более того, часто рассматривается только двоичный алфавит. Такое ограничение по сути не слишком обременительно — данные любой доступной нам задачи можно сформулировать словами, и это будет текст в некотором конечном алфавите (включающем в себя, помимо букв, цифры и все иные специальные знаки, встречающиеся в тексте — знаки пунктуации, математические обозначения и проч.).

Есть некоторая тонкость, связанная с тем, что *кодировок* (способов представить объект словом в конечном алфавите) может быть несколько, а сложность задачи, очевидно, зависит от кодировки. Мы не будем подробно останавливаться на этом вопросе, в дальнейшем кодировки либо будут указываться явно, либо будут подразумеваться наиболее естественные кодировки (скажем, запись числа в позиционной системе счисления; хотя от выбора основания системы ничего не зависит, по умолчанию предполагается использование двоичной системы).

Пока мы говорили о функциях от одного аргумента. В дальнейшем будут возникать и функции от нескольких аргументов. Увеличение алфавита на 1 символ (обозначим его #) позволяет закодировать конечную последовательность слов $\alpha_1, \ldots, \alpha_n$ в алфавите A одним словом

$$\alpha_1 \# \alpha_2 \# \ldots \# \alpha_n \# \tag{1}$$

в алфавите $A \cup \{\#\}$. Будем иметь в виду это преобразование в тех случаях, когда возникает желание рассматривать функцию от нескольких аргументов как функцию от одного аргумента.

Приведем несколько примеров вычислительных задач.

Пример 1. Линейные уравнения над $\mathbb{Q}$.

Даны: матрица A размера $m \times n$, элементы которой — рациональные числа, вектор-столбец b (матрица размера $m \times 1$), также состоящий из рациональных чисел.

Спрашивается: разрешима ли в рациональных числах система

$$Ax = b? \tag{2}$$

Представим эту задачу в виде задачи вычисления некоторой функции. Для начала нужно описать кодировку входа в виде слова в некотором алфавите. В качестве алфавита возьмём

$$\{0, 1, \#, /, -\}.$$

Целые числа будем записывать в двоичной системе, используя знак «$-$» для обозначения отрицательных чисел. Рациональное число p/q будем

записывать словом $код(p)$ / $код(q)$, а последовательность чисел будем записывать, разделяя записи различных чисел знаком #.

В описанной кодировке вход задачи ЛИНЕЙНЫЕ УРАВНЕНИЯ НАД $\mathbb{Q}$ — слово $код(Ax = b)$, кодирующее последовательность чисел

$$m, n, a_{11}, \ldots, a_{1n}, a_{21}, \ldots, a_{2n}, \ldots, a_{m1}, \ldots, a_{mn}, b_1, \ldots, b_m,$$

где a_{ij} — элементы матрицы A, b_i — элементы b.

Функция, которую нужно вычислить, имеет вид

$$\chi(t) = \begin{cases} 1, \text{ если } t = код(Ax = b) \text{ для некоторых } A, b \\ \quad \text{и } Ax = b \text{ имеет решения}, \\ 0, \text{ если } t = код(Ax = b) \text{ для некоторых } A, b \\ \quad \text{и } Ax = b \text{ не имеет решений}, \\ \quad \text{не определено в любом другом случае.} \end{cases} \tag{3}$$

Приведенный пример относится к одному из самых распространенных в математике типов вычислительных задач — проверке разрешимости системы уравнений или, более общо, проверке заданного свойства у объекта, описание которого является входом задачи. В логике принято говорить о проверке *истинности предиката*. Так же, как и в примере 1, такой задаче сопоставляется функция, которая ставит в соответствие описанию объекта 1, если объект удовлетворяет свойству, и 0 в противном случае. Если слово не является описанием объекта, функция на таком слове не определена. Эта функция называется *характеристической функцией* множества описаний объектов, удовлетворяющих заданному свойству.

Сформулируем ещё несколько задач о разрешимости уравнений в виде задач вычисления характеристической функции некоторого предиката. Во всех упомянутых ниже задачах о разрешимости уравнений или систем уравнений подразумевается, что вычисляется характеристическая функция, аналогичная (3).

ПРИМЕР 2. ЛИНЕЙНЫЕ УРАВНЕНИЯ НАД $\mathbb{Z}^+$.

Даны: матрица A размера $m \times n$, элементы которой — целые числа, вектор-столбец b (матрица размера $m \times 1$), также состоящий из целых чисел.

Спрашивается: разрешима ли в неотрицательных целых числах система уравнений

$$Ax = b? \tag{4}$$

ПРИМЕР 3. СИСТЕМА УРАВНЕНИЙ В $\mathbb{F}_2$.

Даны: многочлены $p_1, \ldots, p_k \in \mathbb{F}_2[x_1, \ldots, x_n]$.

Спрашивается: разрешима ли в поле $\mathbb{F}_2$ система уравнений

$$p_i(x_1, \ldots, x_n) = 0, \quad i = 1, \ldots, k? \tag{5}$$

Как кодировать многочлен словом в некотором алфавите? Можно, например, указать степень многочлена d и количество переменных n, представить многочлен в виде суммы мономов

$$p(x_1, \ldots, x_n) = \sum_{\alpha_1 + \ldots + \alpha_n \leqslant d} p_{\alpha_1 \ldots \alpha_n} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n},$$

после чего перечислить коэффициенты его мономов в некотором оговоренном заранее порядке. Другой способ состоит в том, чтобы перечислить все ненулевые мономы, указывая также их коэффициенты. Эти способы могут приводить к записям весьма разной длины: длина записи многочлена $x_1 \cdot \ldots \cdot x_n$ первым способом порядка n^n, а вторым — не больше, чем $n \log n$.

Пример 4. Уравнение над $\mathbb{Z}$.
Дан: многочлен $p \in \mathbb{Z}[x_1, \ldots, x_n]$.
Спрашивается: есть ли решения в целых числах у уравнения

$$p(x_1, \ldots, x_n) = 0? \tag{6}$$

2. Способы решения задач

Когда мы утверждаем, что задачу решить сложно (в предельном случае — невозможно), всегда остается сомнение, что учтены все мыслимые способы её решения. До конца это сомнение снять нельзя — кто может знать, что придумают люди в будущем? Но нужно, по крайней мере, стремиться к тому, чтобы учесть все известные на сегодняшний день способы вычислений.

При этом нас интересуют только такие способы, которые можно явно и однозначно описать и которые можно хотя бы в принципе реализовать. Последнее означает, что все действия, входящие в описание вычисления, должны быть *элементарными*, т. е. доступными всякому (даже самому тупому) исполнителю. Способ вычисления, удовлетворяющий таким свойствам, называется *алгоритмом*.

В 30-ые годы нашего (ещё) века была проделана основная часть работы по формальному определению понятия алгоритма. В результате появилось несколько различных определений и была доказана их эквивалентность. После чего был сформулирован знаменитый *тезис Чёрча*, который утверждает, что более общих определений, удовлетворяющих сформулированным выше условиям, не существует. Тезис Чёрча не является математическим утверждением, потому что приведенные условия не формализованы.

2.1. Исполнитель

Прежде чем давать формальное определение алгоритма, введем в обсуждение неформальный персонаж — Исполнителя. Это довольно ограниченное существо — у него конечная память (размер которой, впрочем, может быть сколь угодно велик). Доступные Исполнителю действия также весьма просты. Исполнитель умеет различать символы некоторого конечного алфавита (сколь угодно большого) и правильно их записывать. Кроме того, он умеет пользоваться таблицами. Это означает, что если выдать ему книжку, в которой приведена таблица некоторой функции из конечного множества в конечное множество, то Исполнитель может находить по аргументам функции её значение.

Помимо этого у Исполнителя есть карандаш, ластик и неограниченной (бесконечной) толщины тетрадь. Страницы тетради имеют ограниченный размер, так что Исполнитель может записать на них лишь ограниченное количество символов. На первых страницах тетради записано задание — вход той функции, которую нужно вычислить. Исполнитель может листать тетрадь, стирать символы, записывать новые. Заканчивается эта его деятельность тем, что он отдаёт тетрадь с результатом своей работы.

Инструкции, которым следует Исполнитель, собраны в отдельную книжечку. Можно считать, что они задают таблицу значений функции

$$\langle\text{состояние Исполнителя, текущая страница}\rangle \mapsto \langle\text{действия Исполнителя}\rangle,$$

где $\langle$действия Исполнителя$\rangle$ — это новое содержание текущей страницы и куда должен Исполнитель пролистать тетрадь — к началу или к концу.

Работа Исполнителя в несколько карикатурной форме отражает те реальные жизненные ситуации, когда мы складываем числа в столбик, приводим подобные члены в записи многочлена, вычисляем наибольший общий делитель двух чисел и т.п., т.е. когда мы «действуем по алгоритму».

С другой стороны, данное выше описание уже легко превратить в формальное определение, что и будет сделано в следующем подразделе. Впрочем, подробности этого формального определения не так уж важны. Единственное существенное в дальнейшем свойство состоит в том, что утверждение «Исполнитель правильно выполнил очередной шаг вычислений» можно записать достаточно короткой логической формулой, переменные которой кодируют описание состояний нашей системы (Исполнитель, тетрадь, книжка с инструкциями) до и после очередного действия Исполнителя. Это свойство хорошо согласуется с неформальным представлением об элементарном действии — если сделано какое-то простое действие, то и утверждение о том, что сделано именно это действие, должно

быть не слишком сложным (длинным). Доказательство этого свойства для используемого ниже формального определения алгоритма легко извлечь из приведенного в разд. 5 наброска доказательства теоремы Кука – Левина.

2.2. Машины Тьюринга

Приведем формальное определение алгоритма, согласованное с предыдущим неформальным обсуждением.

Машина Тьюринга (сокращённо МТ) однозначно задаётся указанием набора $(\mathcal{S}, \text{␣}, \mathcal{A}, \mathcal{Q}, q_0, \delta)$, где

- $\mathcal{S}$ — конечное множество, называемое *алфавитом* МТ (в предыдущем описании элементам этого множества соответствуют все возможные записи на одной странице тетради, выданной Исполнителю);
- $\mathcal{A}$ — также конечное множество, называемое *внешним алфавитом* (в предыдущем описании элементам этого множества соответствуют символы, которыми записывается задание для Исполнителя и результат его работы);
- ␣ — пустой символ (или пробел), это некоторый элемент $\mathcal{S} \setminus \mathcal{A}$ (в предыдущем описании ему соответствует пустая страница в тетради Исполнителя);
- $\mathcal{Q}$ — конечное множество состояний управляющего устройства МТ (неформально — Исполнителя);
- $q_0 \in \mathcal{Q}$ — начальное состояние;
- $\delta\colon \mathcal{Q} \times \mathcal{S} \to \mathcal{Q} \times \mathcal{S} \times \{-1, 0, 1\}$ — (частичная) функция переходов МТ (неформально — книжка с инструкциями для Исполнителя).

Состояние МТ задаётся тройкой (σ, p, q), где σ — бесконечное слово в алфавите $\mathcal{S}$, т.е. произвольная последовательность $s_0, \ldots, s_n, \ldots$ элементов $\mathcal{S}$; p — неотрицательное целое число; $q \in \mathcal{Q}$. Символы слова σ будем, как это принято, представлять записанными на *ленте*, разбитой на *ячейки*, по ячейке на символ. На ленте также имеется *головка*, которая расположена над ячейкой с номером p. Наглядно это изображается так:

Положение головки				∇	
Ячейки	s_0	s_1	$\ldots$	s_p	$\ldots$
Номера ячеек	0	1		p	

Помимо ленты машина Тьюринга имеет *управляющее устройство*, состояние которого задаётся элементом q множества $\mathcal{Q}$.

Состояния МТ меняются дискретно. За один *такт работы* управляющее устройство выполняет следующие действия (полагаем, что МТ находится в состоянии (σ, p, q)):

а) *читает* символ, находящийся под головкой (т.е. определяет s_p);

б) *вычисляет* значение функции переходов: $\delta(q, s_p) = (q', s, \Delta p)$ (если функция переходов на паре (q, s_p) не определена, то останавливает машину Тьюринга);

в) *записывает* на ленту в ячейку p символ s, сдвигает головку на Δp и переходит в состояние q' (другими словами, новое состояние машины задаётся тройкой $((s_0, \ldots, s_{p-1}, s, s_{p+1}, \ldots), p + \Delta p, q'))$;

г) если $p + \Delta p < 0$, то останавливает машину.

Работа машины Тьюринга начинается из состояния $(\alpha\text{␣}\ldots, 0, q_0)$, где за конечным словом α, состоящим из символов внешнего алфавита, (множество таких слов обозначается $\mathcal{A}^*$) следует бесконечное слово, целиком состоящее из пустых символов. Слово α будем называть *входом* МТ. В любой момент времени слово, записанное на ленте, однозначно записывается в виде $\sigma\text{␣}\ldots$, где последний символ слова σ — не пустой, а за ним идут только пустые символы. Будем называть слово σ *используемой частью ленты.*

Выполняя один такт работы за другим, машина Тьюринга порождает последовательность состояний

$$(\sigma_0, 0, q_0),\ (\sigma_1, p_1, q_1),\ (\sigma_2, p_2, q_2),\ \ldots$$

Если МТ останавливается, используемая часть ленты в достигнутом перед остановкой состоянии называется *результатом* работы МТ.

Каждая машина Тьюринга M *вычисляет* частичную функцию φ_M из $\mathcal{A}^*$ в $\mathcal{A}^*$, отображающую вход α в результат работы МТ на входе α при условии, что результат работы является словом во внешнем алфавите. Для входов, на которых машина не останавливается или результат содержит символы из $\mathcal{S} \setminus \mathcal{A}$, функция φ_M не определена. Из определения ясно, что любая МТ вычисляет ровно одну функцию (быть может, нигде не определённую).

Определение 1. *Частичная функция f из $\mathcal{A}^*$ в $\mathcal{A}^*$ называется вычислимой, если существует машина Тьюринга M, для которой $\varphi_M = f$. При этом будем говорить, что f вычислима на M.*

Не все функции вычислимы. Это ясно из сравнения мощности множества функций (континуум) и мощности множества машин Тьюринга (счётное множество). Есть и явные примеры невычислимых функций.

Один из важнейших — *проблема остановки*: дана машина Тьюринга и входное слово; нужно проверить, останавливается ли эта машина Тьюринга на данном входе.

Упражнение 1. *Определите функцию на множестве слов в конечном алфавите, отвечающую проблеме остановки машины Тьюринга.*

Подсказка: хотя машина Тьюринга реализует функцию на бесконечном множестве, она может быть описана конечным словом.

3. Сложность и сложностные классы

3.1. Сложность вычисления

Сложность вычисления (т.е. работы алгоритма на данном входном слове) определяется *ресурсами*, требующимися для этого вычисления. Два важнейших ресурса — *время* (количество тактов работы до остановки или, на другом используемом нами языке, — количество действий Исполнителя) и *память* (наибольший номер ячейки, над которым побывала головка МТ в процессе вычисления, или количество страниц, просмотренных Исполнителем).

Итак, ресурс, требуемый для конкретного вычисления, — это число.

3.2. Сложность алгоритма

Чтобы охарактеризовать сложность работы алгоритма (т.е. способа вычисления функции), мы должны принять во внимание работу алгоритма на всех входах. Сделаем мы это одним из наиболее распространенных способов, который называется «сложность в наихудшем случае».

Будем говорить, что машина Тьюринга M работает за время $T_M(n)$, если максимальное (по всем входам длины n) количество тактов, которое проработает M до остановки, равно $T_M(n)$. Аналогично, машина Тьюринга M работает на памяти $S_M(n)$, если наиболее удалённое от начала ленты положение головки при вычислениях на входах длины n равно $S_M(n)$.

Итак, сложность алгоритма характеризуется некоторой функцией от натурального параметра.

3.3. Сложность задачи

Но давайте вспомним, что нас интересует сложность вычислительной задачи. Решать задачу можно разными способами и есть разные формальные модели вычислений. К тому же (см. [6]), наивный подход — определять сложность задачи по сложности наилучшего алгоритма, её решающего, не работает.

Поэтому принят другой способ характеризации сложности задачи. Он состоит в том, что выделяются классы тех функций, вычисление которых возможно при задаваемых ограничениях на потребляемые ресурсы.

Наиболее важные классы получаются, если накладывать ограничения на рост времени работы и/или используемой памяти в зависимости от длины входного слова. А наиболее важное различие между эффективными и неэффективными вычислениями задаётся функциями *полиномиального роста*. Функция $f(n)$ — полиномиального роста, если для некоторой константы d при достаточно больших n выполняется неравенство $f(n) \leqslant n^d$. В этом случае будем использовать обозначение $f(n) = \mathrm{poly}(n)$.

Определение 2. *Функция f принадлежит классу* P (*и называется полиномиально вычислимой*), *если она вычислима на машине Тьюринга M, для которой $T_M(n) = \mathrm{poly}(n)$.*

Определение 3. *Функция f принадлежит классу* PSPACE (*и называется вычислимой с полиномиальной памятью*), *если она вычислима на машине Тьюринга M, для которой $S_M(n) = \mathrm{poly}(n)$.*

3.4. Почему полиномы?

Почти всякий, кто знакомится с теорией сложности вычислений, задаёт в этом месте вопрос: «почему эффективность вычислений отождествляется с полиномиальностью»? Такой выбор не представляется очевидным, и уж заведомо он не единственно возможный. Поскольку в дальнейшем изложении мы будем без специальных оговорок отождествлять полиномиальную вычислимость и эффективность, стоит сделать отступление и дать хотя бы какие-то пояснения.

Основания для такого выбора делятся на две группы: теоретические и практические. Начнём с первых.

- ▷ Полиномы удобны тем, что они замкнуты относительно композиции. Это обстоятельство будет активно эксплуатироваться в теории, излагаемой ниже.

- ▷ Вспомним, что при формулировке вычислительной задачи как задачи вычисления функции на словах есть произвол, связанный с выбором возможной кодировки входа и результата. Например, перестановку из n элементов можно задавать таблицей значений (как функцию на множестве $\{1, \ldots, n\}$) или матрицей $n \times n$. Последний способ не экономен — нужно задать $O(n^2 \log n)$ битов вместо $O(n \log n)$ битов, как в первом случае, но часто удобен при формулировке задач и алгоритмов. Хотелось бы, чтобы определение сложности задачи не зависело от таких «мелочей», как удобство формулировки.

Как ни странно, отождествление эффективного и полиномиального вычисления имеет смысл и с точки зрения практики вычислений, хотя и не всегда применимо. Напомним, что все наши рассуждения проводятся с точностью до мультипликативной константы, так что применимость рассматриваемой теории к практике нуждается в специальных обоснованиях. Тем не менее, уже к середине 60-ых годов опыт практического программирования показал, что если для полиномиальных алгоритмов есть смысл бороться за эффективную реализацию (практически возникающие задачи решаются за разумное время), то для большинства алгоритмов, не имеющих полиномиальных верхних оценок, решение практически возникающих задач занимает неприемлемо большое время и гораздо разумнее изобретать эвристические приемы решения таких задач, рассматривать приближенные постановки и т. п.

В последующие годы смысл понятия «эффективно вычислимый» уточнялся и несколько изменился. Появилось, скажем, понятие «вычислимый за реальное время». Оно более адекватно описывает ситуации, возникающие в вычислительных системах, от которых требуется по-настоящему быстрая реакция. Ни одного пользователя не устроит текстовый редактор, который вставляет в текст новый символ за время, линейно зависящее от размера текста. Данные выше определения не позволяют формально описать такие ситуации, интересовать они нас не будут. Однако читателю полезно попробовать построить формальное определение, исходя из предложенного примера.

Понятие эффективного алгоритма в последние годы стало включать в себя и вероятностные алгоритмы, работающие за полиномиальное время (о них см. ниже, раздел 8.1).

4. Как различать сложные и простые задачи?

Читатель, не потерявший основную нить рассуждений, должен в этом месте удивиться: «Как? Разве только что не было дано разъяснение этого вопроса? Простые задачи решаются за полиномиальное время, сложные — нет!»

Увы, такой простой ответ применим далеко не всегда. Конечно, есть много задач, для которых построены полиномиальные алгоритмы. Все такие задачи мы считаем простыми. Из примеров, приведенных выше, простой является задача о разрешимости системы линейных уравнений в рациональных числах (пример 1). Полиномиальный алгоритм решения этой задачи строится легко (читателя, интересующегося эффективными алгоритмами, в том числе и алгоритмами решения систем линейных уравнений, отсылаем к книгам [2], [9], [1]).

В некоторых случаях доказано отсутствие алгоритма, решающего задачу; пример 4 — один из них (это вариант десятой проблемы Гильберта; доказательство невычислимости соответствующей функции см., например, в [5]).

Но для огромного числа естественно возникающих вычислительных задач не удаётся ни построить эффективный (=полиномиальный) алгоритм, ни доказать отсутствие такого алгоритма. Именно таковы остальные примеры из раздела 1: решение линейного уравнения в неотрицательных целых числах и решение системы уравнений в поле из двух элементов. Конечно, неудача многолетних усилий по построению эффективного алгоритма для некоторой задачи уже является весомым аргументом в пользу её сложности. Но хочется иметь теорию, в которой такие задачи можно доказуемо отделить от простых задач.

Подходящая теория была построена в начале 70-ых годов и получила с тех пор широкое распространение. Основная идея состоит в том, чтобы ввести на множестве задач отношение *сводимости* («задача A не сложнее задачи B») и характеризовать сложные задачи как задачи, к которым сводятся все задачи из некоторого класса. Ниже в этом разделе описывается самый популярный вариант такой теории, основанный на классе предикатов, вычислимых за полиномиальное время *недетерминированными*[2)] машинами Тьюринга (класс NP).

4.1. Полиномиальная сводимость

Определение 4. Сводимость по Карпу. *Функция f_1 сводится к функции f_2 (обозначение $f_1 \propto f_2$), если существует такая функция $f \in$ $\in$ P, что* $\forall\, x\ f_1(x) = f_2(f(x))$.

Сводимость по Карпу также называют полиномиальной сводимостью, а часто — просто сводимостью. Отношение $\propto$ будем рассматривать как формальный вариант отношения «задача f_1 не сложнее задачи f_2». Действительно, если $f_2 \in$ P, то и $f_1 \in$ P: полиномиальный алгоритм для вычисления f_1 использует последовательно полиномиальные алгоритмы для f (на входе x) и для f_2 (на входе $f(x)$).

4.2. Класс NP

Прежде всего заметим, что этот класс включает в себя только характеристические функции (напомним, что задачи, соответствующие таким функциям, состоят в проверке некоторого свойства входного слова).

[2)] Мы не объясняем, что это такое; нужный нам класс NP можно определить, не прибегая к недетерминированным вычислениям.

Теперь дадим неформальное описание этого класса задач. У нас появляется новый персонаж — Советник. От Исполнителя Советник отличается двумя чертами: он *интеллектуально всемогущ* и *пристрастен* (это означает, что Советник хочет, чтобы у рассматриваемого объекта было признано наличие исследуемого свойства, безотносительно к истинному положению дел). Последняя особенность не позволяет Исполнителю слепо опираться на мнение Советника: оно всегда одинаково. Исполнитель может задавать Советнику вопросы и действовать, исходя из полученных ответов. Каждый вопрос–ответ считается одним действием. Решение о значении функции принимает Исполнитель.

Замечание 1. В литературе по теории сложности Исполнитель (несколько более сильный — снабженный монеткой для подбрасывания) именуется Артуром, а Советник — Мерлином.

Функция (характеристическая) $f(x)$ принадлежит классу NP, если существует алгоритм для пары (Исполнитель, Советник), который всегда (при любых возможных вариантах диалога между Исполнителем и Советником) заканчивается за полиномиальное от длины входа время и результат работы которого удовлетворяет следующему условию: если $f(x) = 1$, то существует такой вариант диалога между Исполнителем и Советником, что результат равен 1; если же $f(x) = 0$, то при любом варианте диалога результат равен 0.

Замечание 2. Из данного выше неформального определения ясно, что $\mathrm{P} \subseteq \mathrm{NP}$ (Исполнитель может ничего не спрашивать). Является ли это включение строгим? Довольно интенсивные, хотя и безуспешные, попытки ответить на этот вопрос продолжаются уже почти 30 лет. С. Смейл включил проблему $\mathrm{P} \stackrel{?}{\neq} \mathrm{NP}$ в число трёх важнейших математических проблем следующего столетия (две другие — гипотеза Римана и гипотеза Пуанкаре), см. [10].

Прежде чем давать формальное определение класса NP, заметим следующее. Исполнитель работает вполне определённым образом, а Советник — всеведущ. Поэтому, посмотрев на вход, Советник может сразу сообщить Исполнителю весь их диалог, а Исполнитель — убедиться, что Советник не соврал; Исполнителю на это потребуется время, полиномиально зависящее от длины диалога.

Определение 5. *Функция f (со значениями в множестве $\{0,1\}$) принадлежит классу* NP, *если она представима в форме*

$$f(x) = \exists\, y\, \big((|y| < q(|x|)) \wedge R(x,y)\big),$$

где $q(\cdot)$ — полином, $R(\cdot,\cdot) \in \mathrm{P}$, а $|\cdot|$ — длина слова.

Здесь (и всюду далее) мы отождествляем логические значения «ложь» и «истина» с 0 и 1 соответственно.

В духе предыдущего неформального обсуждения это определение нужно понимать так: y — это сообщение Советника Исполнителю, а $R(\cdot,\cdot)$ — алгоритм проверки, который осуществляет Исполнитель.

Замечание 3. Приведем ещё несколько неформальных интерпретаций класса NP. Слово y в данном выше определении можно понимать как «подсказку» Исполнителю, воспользовавшись которой он может проверить выполнение NP-свойства. Другими словами, у NP-задачи есть ответ, который, быть может, трудно найти, но проверить правильность ответа — легко. Популярно также представление о слове y как о «доказательстве наличия свойства» (подразумевается, что изучение доказательства занимает полиномиальное от его длины время).

Лемма 1. *Пусть* $f_1 \propto f_2$. *Тогда*

а) $f_1 \notin \mathrm{P} \Rightarrow f_2 \notin \mathrm{P}$; б) $f_2 \in \mathrm{NP} \Rightarrow f_1 \in \mathrm{NP}$.

Доказательство. Пункт а) фактически доказан выше.

Докажем пункт б), привлекая неформальных персонажей из предыдущего обсуждения. Советник сообщает Исполнителю $f(x)$ (длина которого ограничена некоторым полиномом h от длины x, поскольку $f \in \mathrm{P}$) и слово y, которое убеждает Исполнителя в том, что $f_2(f(x)) = 1$. Исполнитель может проверить, что ему действительно сообщено $f(x)$.

Определение 6. *Функция* $f \in \mathrm{NP}$ *называется* NP-*полной, если любая функция из* NP *к ней сводится*[3)].

Если некоторую NP-полную функцию f можно вычислять за время $T(n)$, то любую функцию g из NP можно вычислять за время $T(n^c)$, где число c зависит от g, но не от входа.

NP-полные функции существуют, например, функция задающая предикат выполнимость для булевых формул:

$$SAT(x) = \begin{cases} 1, \text{ если } \exists\, t_1, \ldots, t_k : x(t_1, \ldots, t_k) = 1, \\ 0 \text{ в противном случае.} \end{cases}$$

В первой строчке предполагается, что x есть запись логической формулы с булевыми переменными $t_1, \ldots, t_k$ и пропозициональными связками $(\neg, \vee, \wedge)$.

Теорема 1 (Кук, Левин). 1) $SAT \in \mathrm{NP}$; 2) SAT — NP-*полна.*

Следствие. *Если* $SAT \in \mathrm{P}$, *то* $\mathrm{P} = \mathrm{NP}$.

[3)] Ниже будут использоваться аналогичные понятия полноты для других сложностных классов.

Эскиз доказательства теоремы Кука – Левина будет приведен в следующем разделе.

А пока заметим, что бóльшая часть доказательств NP-полноты использует полиномиальную сводимость и следующую лемму.

Лемма 2. *Если* $SAT \propto L$ *и* $L \in \mathrm{NP}$, *то* L — NP-*полная. И вообще, если* L_1 — NP-*полная*, $L_1 \propto L_2$ *и* $L_2 \in \mathrm{NP}$, *то* L_2 — NP-*полная.*

Доказательство. Достаточно проверить транзитивность сводимости: если $L_1 \propto L_2$, $L_2 \propto L_3$, то $L_1 \propto L_3$. Она следует из того, что композиция двух полиномиально вычислимых функций полиномиально вычислима.

5. Набросок доказательства теоремы Кука – Левина

1) Это утверждение почти очевидно. Советник сообщает Исполнителю значения переменных, входящих в формулу, при которых она истинна. Исполнитель справится с проверкой истинности полученного высказывания за полиномиальное время.

2) Пусть функция из NP, которую нужно свести к SAT, имеет вид $f(x) = \exists\, y\, \big((|y| < q(|x|)) \wedge R(x,y)\big)$.

Рассмотрим машину Тьюринга, вычисляющую $R(\cdot,\cdot)$ за полиномиальное время. Нам нужно записать в виде логической формулы условие того, что при некотором y (и заданном входе x), машина выдаёт результат 1. Для этого представим весь процесс вычисления, длящегося время $T = \mathrm{poly}(n)$ и использующего память $S = \mathrm{poly}(n)$, *таблицей вычисления* размера $T \times S$, показанной на рисунке 1.

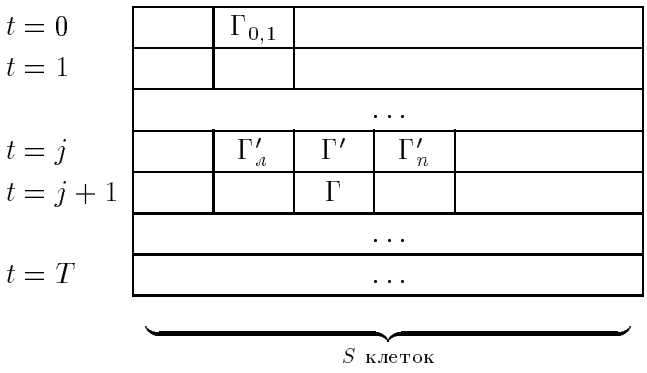


Рис. 1.

Строка с номером j таблицы задаёт состояние МТ после j тактов работы. Символы $\Gamma_{j,k}$, записанные в таблице, принадлежат алфавиту

$\mathcal{S}\times\{\varnothing\cup\mathcal{Q}\}$. Символ $\Gamma_{j,k}$ определяет пару (символ, записанный в k-й ячейке после j тактов работы; состояние управляющего устройства после j тактов работы, если головка находится над k-й ячейкой, в противном случае второй элемент пары — $\varnothing$). Для простоты также считаем, что если вычисление заканчивается при некотором входе за $T' < T$ тактов, то строки с номерами, бóльшими T', повторяют строку с номером T'.

Состояние каждой клетки таблицы можно закодировать конечным (не зависящим от n) числом булевых переменных. Имеются *локальные правила согласования*, т.е. состояние каждой клетки Γ в строке ниже нулевой однозначно определяется состояниями клеток в предыдущей строке, лежащих непосредственно над данной (Γ'), левее данной ($\Gamma'_л$) и правее данной ($\Gamma'_п$). Каждое такое условие можно записать в виде логической формулы от переменных, кодирующих состояния клеток, причем размер этой формулы от n также не зависит.

Еще нам нужно записать условие успешности вычисления (результат равен 1). Для этого заметим, что без ограничения общности можно считать, что состояния клеток таблицы кодируются так, что одна из кодирующих переменных равна 1 только в том случае, когда в ячейке записана 1. Тогда значение этой переменной для кода $\Gamma_{T,0}$ и будет результатом вычисления.

Определим формулу φ_x как конъюнкцию всех формул, в которые подставлены значения переменных, кодирующих вход $x\#y$, дополненный символами $\sqcup$ до длины $|x|+1+q(|x|)$. Значения, соответствующие x и $\#$, — константы, поэтому переменные, от которых зависит эта формула, отвечают y и кодам внутренних ячеек таблицы. Так что можно считать, что формула φ_x зависит от y и ещё от каких-то переменных, которые мы обозначим z.

Итак, мы сопоставили слову x формулу $\varphi_x(y,z)$, которая по построению обладает следующим свойством. Если выполняется $R(x,y)$, то найдется такой набор значений $z(x,y)$, при котором $\varphi_x(y,z(x,y))$ истинна (эти значения описывают работу МТ на входе $x\#y$). А если $R(x,y)$ не выполняется, то $\varphi_x(y,z)$ всегда ложна (поскольку по сути утверждает, что вычисление на входе (x,y) даёт ответ «да»). Таким образом, при $f(x)=1$ такая формула иногда (при некоторых значениях y) истинна, при $f(x)=0$ — всегда ложна.

6. Примеры NP-полных задач

Обширный список NP-полных задач содержится в книге Гэри и Джонсона [3]. Как правило, их NP-полнота доказывается с помощью сведéний. Приведём несколько примеров таких доказательств.

6.1. 3-КНФ

Эта задача задаётся предикатом

3-$SAT(x) = 1 \Longrightarrow$ x есть 3-КНФ, которая истинна при некоторых значениях переменных. 3-КНФ — это конъюнкция дизъюнкций, каждая из которых содержит три литерала, а литерал — это переменная или её отрицание.

3-$SAT(x) = 0 \Longrightarrow$ x есть 3-КНФ, которая ложна при всех значениях переменных.

3-$SAT(x)$ не определена во всех остальных случаях.

3-SAT также NP-полна. Это устанавливается сведением к ней SAT.

Теорема 2. $SAT \propto$ 3-SAT.

Доказательство. Рассмотрим вычисление истинности заданной формулы $\varphi(x_1, \ldots, x_n)$, использующей связки $(\neg, \vee, \wedge)$. Результаты промежуточных вычислений обозначим $y_1, \ldots, y_s$. Для каждой переменной y_k выполнено одно из трёх равенств

$$\begin{aligned} y_k &= u \vee v, \\ y_k &= u \wedge v, \\ y_k &= \neg v, \end{aligned} \tag{7}$$

где u, v либо переменные формулы, либо уже определённые вспомогательные переменные, т. е. $u, v \in \{x_1, \ldots, x_n, y_1, \ldots, y_{k-1}\}$.

Теперь запишем 3-КНФ, равносильную исходной формуле $\varphi(\cdot)$. В эту КНФ будут входить переменные $x_1, \ldots, x_n$ и $y_1, \ldots, y_s$. Построим вначале конъюнкцию K'' условий, означающих, что каждая из вспомогательных переменных y_k имеет значение, задаваемое формулой (7). Есть три типа таких условий и каждый можно записать в виде 3-КНФ:

$$\begin{aligned} \big(y \Leftrightarrow (x_1 \vee x_2)\big) &= (x_1 \vee x_2 \vee \neg y) \wedge (\neg x_1 \vee x_2 \vee y) \wedge (x_1 \vee \neg x_2 \vee y) \wedge \\ &\quad \wedge (\neg x_1 \vee \neg x_2 \vee y), \\ \big(y \Leftrightarrow (x_1 \wedge x_2)\big) &= (x_1 \vee x_2 \vee \neg y) \wedge (\neg x_1 \vee x_2 \vee \neg y) \wedge (x_1 \vee \neg x_2 \vee \neg y) \wedge \\ &\quad \wedge (\neg x_1 \vee \neg x_2 \vee y), \\ \big(y \Leftrightarrow \neg x\big) &= (x \vee y) \wedge (\neg x \vee \neg y). \end{aligned}$$

Подставляя эти 3-КНФ в K'', получим 3-КНФ K'. Искомая 3-КНФ имеет вид $K = K' \wedge y_s$. Действительно, истинность K равносильна утверждению: все присваивания выполнены правильно и в результате получилась 1 $(y_s = 1)$. Значит, если при каких-то значениях переменных x_i формула φ истинна, то 3-КНФ K выполнима, и наоборот.

6.2. Разрешимость системы уравнений в поле $\mathbb{F}_2$

Теперь докажем NP-полноту задачи из примера 3. Вспомним, что мы можем записывать многочлен двумя существенно различающимися по длине способами. Так что речь идет о двух, вообще говоря, разных вычислительных задачах. Однако они обе принадлежат классу NP. Это вполне очевидно — если Советник сообщает решение системы, то Исполнитель может проверить выполнение всех равенств при данных значениях переменных за полиномиальное время и в одном, и в другом случае.

Более того, обе эти задачи NP-полны. Для доказательства полноты сведем задачу выполнимости 3-КНФ к разрешимости системы вида (5). Запишем связки $\neg, \vee, \wedge$ в виде многочленов. Если считать, что истинностные значения — это 0 и 1, то для любого поля и любых $x, y \in \{0, 1\}$ выполнено

$$\begin{aligned} (\neg x) &= (1 - x), \\ (x \wedge y) &= xy, \\ (x \vee y) &= 1 - (1 - x)(1 - y). \end{aligned} \tag{8}$$

Поэтому выполнимость 3-КНФ $\bigwedge_{k=1}^{m} D_k$ равносильна разрешимости над полем $\mathbb{F}_2$ системы

$$A(D_k) + 1 = 0, \quad k = 1, \ldots, m, \tag{9}$$

где $A(D_k)$ обозначает многочлен, соответствующий дизъюнкции D_k при соответствии, задаваемом формулами (8). Поскольку мы использовали для сводимости многочлены степени 3, то полнота доказана для обеих кодировок: для многочленов степени 3 длины записей многочлена этими способами различаются не более чем кубически.

6.3. Целочисленное линейное программирование (ЦЛП)

Теперь разберем задачу из примера 2, т.е. разрешимость системы линейных диофантовых уравнений в неотрицательных числах.

Замечание 4. Название «линейное программирование» относится к задачам минимизации линейной функции на множестве решений системы линейных неравенств. Слово «целочисленное» указывает, что учитываются только те решения, для которых значения всех переменных — целые. С точностью до полиномиальных сводимостей задача разрешимости системы (4) эквивалентна задаче ЦЛП. Доказательство этого оставляется читателю в качестве упражнения.

Теорема 3. *Задача проверки разрешимости системы линейных уравнений в неотрицательных целых числах* NP*-полна.*

Как и в предыдущих случаях, нам необходимо доказать два утверждения: что эта задача принадлежит классу NP и что к ней сводятся все задачи из NP. Но теперь нетривиальны оба утверждения. Естественно пытаться доказывать принадлежность NP следующим образом: пусть Советник сообщит решение, а Исполнитель его проверит. Но тогда решение должно состоять из не слишком больших чисел, чтобы Исполнитель мог проверить выполнение равенств (4) за полиномиальное время.

Оказывается, что так оно и есть: из разрешимости системы (4) следует существование не слишком длинных решений. Опишем кратко идею доказательства.

Основная используемая оценка — это оценка величины определителя матрицы через длину её описания. Обозначим длину записи матрицы A (кодировка указана в примере 1) через s. Тогда

$$|\det A| \leqslant \prod_{i,j=1}^{n} (1 + |a_{ij}|) \leqslant 2^s. \tag{10}$$

Первое неравенство следует непосредственно из определения $\det A$, второе — из того, что запись числа a требует не менее $1+\log|a| \geqslant \log(1+|a|)$ битов.

Множество вещественных решений системы (4) является *полиэдром* — пересечением конечного числа полупространств. Хорошо известная теорема выпуклой геометрии утверждает, что любая точка полиэдра является выпуклой комбинацией его крайних точек и точек на его крайних лучах. Крайние точки полиэдра, задаваемого системой (4), являются решениями систем линейных уравнений вида

$$\begin{cases} Ax = b, \\ x_i = 0, \quad i \in S, \end{cases} \tag{11}$$

для каких-то подмножеств $S \subseteq \{1, \ldots, n\}$. Координаты этих точек по правилу Крамера являются отношениями миноров расширенной матрицы этой системы. В силу оценки (10) они не превосходят 2^{s+n^2+n} (в показателе написана максимально возможная длина описания минора расширенной матрицы).

Направляющие векторы крайних лучей — ненулевые (без ограничения общности, целочисленные) решения однородных систем вида

$$\begin{cases} Ax = 0, \\ x_i = 0, \quad i \in S, \end{cases} \tag{12}$$

поэтому можно считать, что для их координат выполняются те же неравенства.

Обозначим крайние точки полиэдра $x^{(1)}, \ldots, x^{(N)}$, направляющие векторы крайних лучей $y^{(1)}, \ldots, y^{(M)}$. Пусть у системы (4) есть целочисленное решение x. Тогда его можно записать в виде

$$x = \sum_{i=1}^{N} \lambda_i x^{(i)} + \sum_{j=1}^{M} \mu_j y^{(j)} = x^{(\lambda)} + \sum_{j=1}^{M} (\mu_j - \lfloor \mu_j \rfloor) y^{(j)} + y^{(\mu)}, \qquad (13)$$

где $\lambda_i, \mu_j \geqslant 0$, $\sum_{i=1}^{N} \lambda_i = 1$, все координаты вектора $x^{(\lambda)}$ ограничены 2^{s+n^2+n}, а вектор $y^{(\mu)}$ — целочисленный. Но тогда и вектор $x - y^{(\mu)}$ является целочисленным решением системы (4), а его координаты не превосходят $(M+1)2^{s+n^2+n}$. Заметим, что M заведомо не превосходит 2^n (а если вспомнить теорему Каратеодори, то $M \leqslant n$).

Итак, мы доказали, что для разрешимой в неотрицательных целых числах системы найдется и такое решение, длина записи которого $O(s^3)$ (мы грубо оценили n как s). Отсюда следует принадлежность этой задачи классу NP.

Для доказательства NP-полноты задачи разрешимости системы линейных уравнений в неотрицательных целых числах сведем к ней задачу 3-КНФ. Построим по 3-КНФ систему линейных уравнений в неотрицательных целых числах. Булевой переменной x_i из 3-КНФ сопоставим целочисленную неотрицательную переменную p_i, отрицанию переменной x_i — n_i, дизъюнкции D — переменную q_D. Каждой дизъюнкции $D = X_j \vee X_k \vee X_m$ (X_* — литералы) сопоставим также уравнение $P_j + P_k + P_m - q_D = 1$, в котором P_j, P_k, P_m — переменные, сопоставленные литералам дизъюнкции.

Искомая система содержит для всех i уравнения $p_i + n_i = 1$, а также все уравнения, сопоставленные дизъюнкциям из КНФ. Очевидно, что выполнимость 3-КНФ равносильна совместности такой системы.

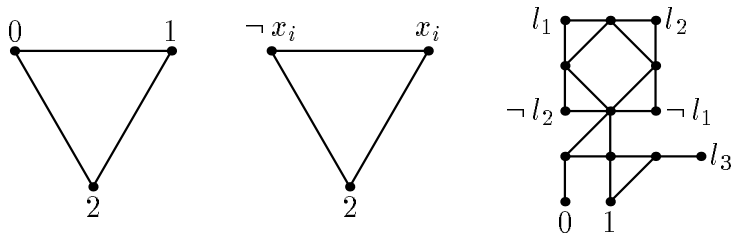
6.4. 3-раскраска

Дан граф. Спрашивается, можно ли раскрасить его вершины в три цвета так, чтобы концы каждого ребра были покрашены в разные цвета?

Будем считать, что граф задаётся матрицей смежности A. Строки и столбцы этой матрицы индексированы вершинами графа, $a_{ij} = 1$ если в графе есть ребро ij, в противном случае $a_{ij} = 0$.

Легко понять, что задача 3-раскраска принадлежит NP: Советник предъявит раскраску, а Исполнитель за линейное от длины описания графа время проверит, что она правильная.

Теорема 4. *Задача* 3-раскраска NP-*полна.*



константы а) переменная б) дизъюнкция в)

Рис. 2.

Доказательство. Сведем к этой задаче задачу 3-КНФ. Пусть есть 3-КНФ из m дизъюнкций, в которые входят n переменных. Граф, который сопоставляется этой КНФ, имеет $7m + 2n + 3$ вершин. Для описания структуры графа удобно пометить часть вершин. Во-первых, пометим три вершины числами 0, 1, 2. Во-вторых, пометим каждым литералом (переменной или её отрицанием) по одной вершине. Остальные $7m$ вершин разобьём на группы по 7, каждая группа соответствует одной из дизъюнкций.

Теперь опишем рёбра этого графа. Как показано на рис. 2а, вершины 0, 1 и 2 соединены между собой рёбрами. На рис. 2б показаны ещё n треугольников в этом графе. И, наконец, рис. 2в показывает, как соединены рёбрами вершины, соответствующие каждой дизъюнкции. На этом рисунке l_1, l_2, l_3 обозначают вершины, помеченные литералами, входящими в дизъюнкцию. Заметим, что некоторые рёбра мы перечислили по несколько раз.

Очевидно, что описанное выше построение можно выполнить за полиномиальное от n и m время. Докажем его корректность.

Рассмотрим, какие правильные раскраски в 3 цвета возможны для такого графа. Без ограничения общности можно считать, что вершины 0, 1 и 2 покрашены в цвета 0, 1 и 2 (из шести раскрасок, различающихся перестановками цветов, мы выбрали одну). Тогда вершины, помеченные x_i и $\neg x_i$, покрашены в цвета 0 и 1, причём их цвета должны быть противоположны (см. рис. 2б).

Прямым перебором вариантов можно проверить, что граф, изображённый на рис. 2в, удовлетворяет следующему свойству: если красить вершины, помеченные литералами, в цвета 0 или 1, а вершины, отмеченные отрицаниями литералов, — в противоположные цвета 1 или 0, то правильная раскраска остальных вершин этого графа в 3 цвета существует (и единственна!) тогда и только тогда, когда хотя бы одно из значений литералов отлично от 0.

Поэтому правильные 3-раскраски построенного графа, для которых вершины 0, 1, 2 покрашены в цвета 0, 1, 2 соответственно, находятся во взаимно однозначном соответствии с выполняющими наборами значений переменных исходной 3-КНФ.

Заметим, что проверить раскрашиваемость графа в 2 цвета просто. Нужно покрасить одну из вершин в какой-нибудь цвет, все смежные с этой вершины в противоположный и т. д. Если ещё не покрашенные вершины не соединены ни с одной из уже покрашенных, опять красим одну из них в произвольно выбранный цвет. Мы можем столкнуться с тем, что какую-то вершину нельзя покрасить ни в один цвет. Тогда граф нельзя правильно раскрасить в 2 цвета. Доказательство корректности этого (очевидно, полиномиального) алгоритма оставляется читателю в качестве легкого упражнения.

Знаменитая гипотеза четырёх красок утверждает, что любой планарный граф (т.е. граф, который можно нарисовать на плоскости без пересечений ребер) раскрашивается в 4 цвета. Легко построить примеры планарных графов, не раскрашиваемых в 3 цвета (скажем, полный граф на 4 вершинах, см. рис. 3).

Оказывается, что проверка раскрашиваемости планарного графа в 3 цвета NP-полна. Доказательство проводится полиномиальным сведением общей задачи 3-РАСКРАСКА к задаче 3-РАСКРАСКА ПЛАНАРНОГО ГРАФА. Идея сведения очень проста, но использует нетривиальную конструкцию, изображенную на рис. 4 (мы позаимствовали эту конструкцию из книги [3], в свою очередь Гэри и Джонсон приписывают её М. Дж. Фишеру).

Итак, нам нужно по произвольному графу G построить некоторый планарный граф, 3-раскрашиваемость которого равносильна 3-раскрашиваемости исходного графа. Нарисуем граф G на плоскости, допуская пересечения ребер, но не проводя ребра через вершины. Из нарисованного с пересечениями ребер графа G изготовим планарный граф по следующему рецепту. Вместо каждой точки пересечения ребер вклеим экземпляр графа H, изображенного на рис. 4, так, чтобы вершины, помеченные x, x', оказались на одном ребре, а вершины, помеченные y, y' — на другом. С полученным (уже планарным) графом проделаем ещё одну процедуру. Выбрав ребро uv исходного графа, будем двигаться от u к v и стягивать ребра типа xx', соединяющие вершины из идущих подряд вдоль нашего пути экземпляров графа H. Планарность при этом сохраняется. Стянем также ребро, соединяющее вершину u с первой из вершин графов H на нашем пути. (Если на ребре uv не было точек пересечения с другими ребрами, то не делаем ничего.) Повторив эту процедуру для всех ребер графа G, получим искомый граф $P(G)$. Заметим, что множество вершин $P(G)$ содержит по построению множество вершин G.

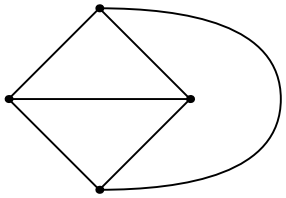


Рис. 3.

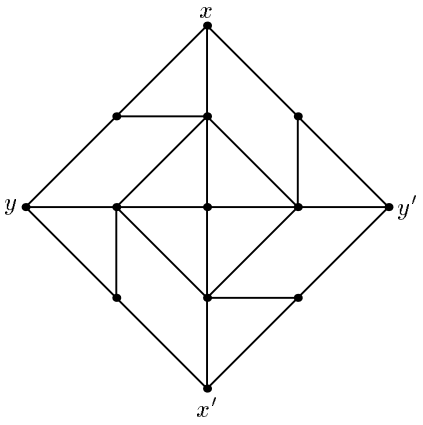


Рис. 4.

Полиномиальность такого сведения очевидна. Доказательство его корректности использует следующие два свойства графа H:

- при любой раскраске H в 3 цвета цвета вершин x и x', равно как и цвета y и y', совпадают;
- есть раскраски в три цвета, при которых вершины x и y покрашены одинаково, есть и такие, при которых они покрашены в разные цвета.

Читателю предоставляется самостоятельно проверить выполнение этих свойств и убедиться, что правильная 3-раскраска $P(G)$ порождает правильную 3-раскраску G (красим вершину в тот же цвет, в который она покрашена в $P(G)$) и наоборот (любая правильная 3-раскраска вершин G продолжается до правильной 3-раскраски $P(G)$).

7. Класс PSPACE

Как уже говорилось, в этот класс попадают те функции, которые могут быть вычислены на МТ, использующей память, ограниченную полиномом от длины входного слова. Этот класс включает в себя класс P (за время T мы сможем использовать память, не превосходящую T) и класс NP (диалог Советника с Исполнителем занимает полиномиальное время, поэтому Исполнитель, не ограниченный во времени, может перебрать по очереди все варианты записей такого диалога, используя для этого сравнительно небольшую — ограниченную полиномом от длины входа — память). Но класс PSPACE, по-видимому, гораздо шире чем NP. К сожалению, доказать это никому до сих пор не удалось.

Классу PSPACE, точнее говоря, характеристическим функциям, входящим в PSPACE, можно дать следующее неформальное описание. Представим несколько идеализированную модель судопроизводства. Слово x — описание некоторого дела, находящегося на рассмотрении суда, который должен вынести вердикт: виновен ли обвиняемый (значение характеристической функции равно 1). Судья — уже знакомый нам полиномиально ограниченный Исполнитель (он будет работать время, не превосходящее полинома от длины описания дела). Есть также Прокурор, настаивающий на виновности обвиняемого, и Адвокат, убеждающий судью в обратном. Оба они интеллектуально всемогущи и по очереди приводят свои аргументы. Правила ведения судебного разбирательства зафиксированы в Уголовно-Процессуальном Кодексе. Судья подводит итог разбирательства, основываясь на описании дела x, на состоявшейся дискуссии между Прокурором и Адвокатом и на УПК (т.е. по сути вычисляет значение некоторой полиномиально вычислимой функции, определяемой УПК, на входе, описывающем судебное разбирательство — слово x, текст первого выступления Прокурора, текст первого выступления Адвоката, текст второго выступления Прокурора и т.д.).

В таком экстравагантном контексте класс PSPACE определяется следующим образом: характеристическая функция f принадлежит PSPACE, если можно придумать такой УПК, что при $f(x) = 1$ у Прокурора есть стратегия ведения дискуссии, которая убеждает Судью в виновности обвиняемого при любых вариантах действий Адвоката; а при $f(x) = 0$ аналогичная стратегия есть у Адвоката.

Замечание 5. Обычно описанную выше модель излагают в более нейтральных терминах. Говорят об игре двух лиц, зависящей от входного слова, и существовании выигрышной стратегии у одного из игроков.

Теорема 5. *Стандартное и уголовно-процессуальное определения класса* PSPACE *равносильны.*

Доказательство. Покажем, что язык из PSPACE в смысле УПК принадлежит PSPACE в смысле стандартного определения. Пусть число выступлений сторон ограничено $p(|x|)$. Определим по индукции набор машин Тьюринга M_k для $k = 0, \ldots, p(|x|)$. Каждая M_k по заданному началу дискуссии $x, a_1, b_1, \ldots$ длины k определяет наличие убеждающей стратегии для Прокурора. Последней в этом ряду машине $M_{p(|x|)}$ нужно просто проимитировать работу Судьи и вычислить функцию УПК$(x, a_1, \ldots)$. Машина M_k перебирает все возможные варианты $(k+1)$-го выступления и консультируется с M_{k+1} по поводу окончательных результатов судебного разбирательства. Ее оценка перспектив разбирательства составляется очень просто: если текущее выступление за

Прокурором, то достаточно найти хотя бы один вариант выступления, после которого M_{k+1} гарантирует убеждающую стратегию для Прокурора. Если текущее выступление за Адвокатом, то после любого из возможных выступлений M_{k+1} должна обнаружить убеждающую стратегию для Прокурора. Машина M_0 определяет наличие убеждающей стратегии для Прокурора в самом начале процесса и для её работы нужно задействовать всю последовательность машин M_k. Но каждая из этих машин использует небольшую (полиномиально ограниченную) память, так что весь процесс потребует лишь полиномиально ограниченной памяти.

А теперь покажем обратное. Пусть есть машина M, вычисляющая некоторую характеристическую функцию f на полиномиальной памяти. Заметим прежде всего, что вычисление на памяти S бессмысленно проводить дольше, чем время $2^{O(S)}$ (все начнет повторяться после того, как мы исчерпаем все состояния нашей системы, а их не более чем $|\mathcal{A}|^S \cdot |\mathcal{Q}| \cdot S$, где $\mathcal{Q}, \mathcal{A}$ — соответственно множество состояний управляющего устройства и алфавит рассматриваемой МТ). Поэтому можно считать без ограничения общности, что время работы машины M ограничено 2^q, где $q = O(p(|x|))$.

Для простоты описания потребуем, чтобы после завершения вычисления МТ сохраняла без изменений достигнутое состояние.

Правила судебной дискуссии состоят в следующем. Прокурор утверждает, что на входном слове x машина выдаёт результат 1, а Адвокат подвергает это сомнению. В первом своём выступлении Прокурор обязан описать состояние машины M (строка, записанная на ленте, положение читающей головки, состояние управляющего устройства) после 2^{q-1} тактов работы. В ответном слове Адвокат указывает на один из промежутков: от начала до (2^{q-1})-го такта или от (2^{q-1})-го такта до конца. После этого Прокурор обязан описать состояние M в середине этого промежутка. Далее всё повторяется: Адвокат выбирает одну из половинок, Прокурор описывает состояние M в середине выбранной половинки и т. д.

Дискуссия заканчивается, когда длина промежутка становится равной 1. Судья подводит итог так: в течение процесса для обоих концов этого промежутка были описаны состояния M, если состояние правого конца получается из состояния левого конца за один такт работы M, то Судья склоняется к мнению Прокурора, в противном случае — к мнению Адвоката. Необходимые проверки займут у Судьи время, полиномиально ограниченное длиной входного слова.

Пусть $f(x) = 1$. Тогда убеждающая стратегия для Прокурора состоит в том, чтобы каждый раз сообщать истинное положение дел (напомним, что Прокурор интеллектуально всемогущ, так что он в состоянии промоделировать в уме работу машины M).

Пусть $f(x) = 0$. Тогда, что бы ни говорил Прокурор, на одном из промежутков (или на обоих) будет содержаться ошибка. Адвокат должен указывать каждый раз именно такой промежуток — это гарантирует ему успех.

В классе PSPACE существуют полные относительно полиномиальной сводимости задачи. Простейший вариант получается из приведенного выше доказательства.

Задача TQBF (Truth of Quantified Boolean Formula). Задаётся предикатом

$TQBF(x) \Leftrightarrow$ x есть истинная квантифицированная булева формула (QBF), т. е. формула вида

$$\mathsf{Q}_1 y_1 \ldots \mathsf{Q}_n y_n \varphi(y_1, \ldots, y_n),$$

где $y_i \in \{0, 1\}$, φ — некоторая логическая формула, а Q_i — либо $\forall$, либо $\exists$.

По определению кванторы действуют на формулы следующим естественным образом:

$$\forall\, x\, \psi(x_1, \ldots, x) \stackrel{\text{def}}{=} \psi(x_1, \ldots, 0) \wedge \psi(x_1, \ldots, 1), \tag{14}$$

$$\exists\, x\, \psi(x_1, \ldots, x) \stackrel{\text{def}}{=} \psi(x_1, \ldots, 0)) \vee \psi(x_1, \ldots, 1)). \tag{15}$$

Теорема 6. *Задача* TQBF PSPACE-*полна.*

Итог описанной выше дискуссии можно выразить в виде квантифицированной формулы, если записать условие «одно состояние МТ получается из другого за один такт» в виде логической формулы. Хотя в этой дискуссии выступления были длиннее чем в один бит, их нетрудно превратить в однобитовые, вставляя после каждого бита настоящего выступления одной из сторон фантомное выступление противоположной стороны («покашливание»). Формула φ от «покашливаний» не зависит.

8. Класс IP

Вернёмся к паре (Исполнитель, Советник). Работа этой пары позволяет решать задачи из класса NP. А изменится ли что-нибудь, если выдать Исполнителю генератор случайности (монетку для подбрасывания)? Класс функций, вычислимых парой (Исполнитель с монеткой, Советник) за полиномиальное время называется IP (более точное определение будет дано ниже). Справедлива следующая замечательная теорема.

Теорема 7. PSPACE = IP.

Подбрасывание монетки значительно улучшает эффективность советов! В остальной части этого раздела мы попробуем объяснить это неожиданное явление.

8.1. Дополнительные возможности: подбрасывание монетки и класс BPP

Для начала нужно понять, что изменится в определении алгоритма, если разрешить использование генератора случайности. Результат работы Исполнителя, использующего подбрасывания монетки, перестает быть однозначно определённым. Как тогда понимать утверждение «алгоритм (вероятностный) решает задачу»?

Естественно полагать, что вероятностный алгоритм решает задачу, если велика вероятность правильного ответа. Конечно, эта вероятность зависит от свойств генератора случайности. Мы будем считать, что генератор случайности производит последовательность независимых случайных битов (0 или 1 с равными вероятностями). Простейшая реальная модель такого генератора — подбрасывание монетки.

Если известна верхняя оценка времени работы алгоритма, то его можно преобразовать к следующему стандартному виду: сделаем достаточное количество подбрасываний монетки и запомним их результаты, составив таблицу случайных битов. После этого начнем действовать по алгоритму, заменяя подбрасывание монетки обращением к таблице случайных чисел, составленной на первом шаге. Время работы такой версии алгоритма имеет ту же (с точностью до мультипликативного множителя) верхнюю оценку. А вероятность получения ответа a для алгоритма в таком формате подсчитывается просто: это отношение количества тех таблиц случайных чисел, при использовании которых получается данный ответ a, к общему количеству таблиц, равному 2^r, где r — количество случайных битов.

Это замечание позволяет дать определение класса BPP — задач, решаемых вероятностными алгоритмами за полиномиальное время, — аналогично определению 5 класса NP.

Определение 7. *Функция f принадлежит классу* BPP, *если существуют такие полином $q(\cdot)$ и функция $R(\cdot,\cdot) \in$ P, что доля слов r длины $q(|x|)$, для которых выполнено $f(x) = R(x,r)$, больше* $2/3$.

Если в этом определении заменить число $2/3$ на любое фиксированное число, бóльшее $1/2$, класс BPP не изменится. Есть простой способ добиться вероятности, сколь угодно близкой к 1. Возьмём несколько одинаковых машин, запустим их все, а окончательным результатом будем считать мнение большинства. Если вероятность правильного ответа для

каждого экземпляра машины равна $c > 1/2$, то вероятность неправильного ответа после голосования n машин

$$\sum_{k=0}^{\lfloor n/2\rfloor}\binom{n}{k}c^k(1-c)^{n-k} < \sum_{k=0}^{\lfloor n/2\rfloor}2^n\left(c(1-c)\right)^{n/2}\left(\frac{1-c}{c}\right)^{n/2-k} <$$

$$< \lambda^n\sum_{k=0}^{\lfloor n/2\rfloor}\left(\frac{1-c}{c}\right)^{n/2-k} < \lambda^n\left(\frac{1-c}{c}\right)^{n/2-\lfloor n/2\rfloor}\frac{1}{1-(1-c)/c} =$$

$$= O(\lambda^n) \quad (16)$$

для подходящего λ ($2\sqrt{c(1-c)} < \lambda < 1$). Таким образом, голосование экспоненциально быстро уменьшает вероятность неправильного ответа.

8.2. Определение класса IP

Класс IP составляют задачи, для которых существуют «интерактивные доказательства правильности ответа». Другими словами, есть интеллектуально всемогущий и пристрастный Советник, к услугам которого разрешено прибегать полиномиально ограниченному вероятностному алгоритму, а задача принадлежит классу IP, если есть такой способ организовать работу пары (Исполнитель с монеткой, Советник), что вероятность правильного результата достаточно высока (больше 2/3).

Как и в предыдущих случаях, мы хотим привести работу пары наших персонажей к некоторому каноническому виду. Заметим, что теперь, в отличие от класса NP, Советник не знает заранее списка вопросов, которые ему будут заданы: эти вопросы определяются, помимо прочего, подбрасыванием монетки. Однако, как и в случае класса BPP, Исполнитель может составлять таблицы случайных битов и пользоваться ими.

Будем считать, что Советник видит результаты подбрасывания монетки. Поэтому со стороны Исполнителя было бы неосмотрительно составлять таблицу случайных битов на все время диалога с Советником. Однако он ничего не теряет в возможности контролировать Советника, если такая таблица составляется перед каждым вопросом. А Советник, глядя на таблицу, уже может понять, какой именно вопрос задаст ему Исполнитель, сообщить Исполнителю этот вопрос и свой ответ на него.

Поэтому работу пары (Исполнитель с монеткой, Советник) можно преобразовать (с незначительной потерей ресурсов) к следующему каноническому виду: Исполнитель составляет таблицу случайных битов, показывает её Советнику, тот говорит нечто в ответ и т. д. Количество таких раундов ограничено заранее заданным полиномом от длины входного слова. После завершения диалога с Советником, Исполнитель по записи этого диалога принимает решение. Вероятность правильного ответа

(доля диалогов, приводящих к правильному ответу) должна быть достаточно велика. Все эти неформальные соображения учтены в следующем определении, в котором f — характеристическая функция.

Определение 8. $f \in \mathrm{IP}$ *означает, что есть такие полиномиально вычислимая (характеристическая) функция* V *(Исполнитель), некоторая функция* P *(Советник) и полиномы* $q(\cdot)$ *(длина таблицы случайных чисел),* $s(\cdot)$ *(длина диалога), что* $|P(u)| = \mathrm{poly}(|u|)$ *(Советник даёт полиномиально ограниченные советы) и для каждого* x *доля тех двойных последовательностей*

$$\begin{array}{cccc} r_{11} & r_{12} & \dots & r_{1q(|x|)} \\ r_{21} & r_{22} & \dots & r_{2q(|x|)} \\ \dots & \dots & \dots & \dots \\ r_{s(|x|)1} & r_{s(|x|)2} & \dots & r_{s(|x|)q(|x|)}, \end{array}$$

для которых

$$f(x) = V(x, r_1, P(r_1), r_2, P(r_1, r_2), \dots, r_{s(|x|)}, P(r_1, r_2, \dots, r_{s(|x|)})),$$

больше $2/3$.

Мы использовали обозначение $r_k = (r_{k1}, r_{k2}, \dots, r_{kq(|x|)})$ и естественное соглашение: когда мы применяем функцию к последовательности аргументов, предполагается, что эта последовательность представлена в виде, аналогичном (1) (см. начало статьи).

Замечание 6. Работа Исполнителя в описанном выше формате похожа на работу Судьи из уголовно-процессуальной интерпретации класса PSPACE. Только теперь одна из спорящих сторон — генератор случайных чисел. Теорема 7 получает любопытную интерпретацию: анализ игры против сколь угодно умного противника с вычислительной точки зрения эквивалентен анализу (другой) игры против простейшего противника: генератора случайных чисел[4)].

8.3. IP $\subseteq$ PSPACE

Определение IP похоже на уголовно-процессуальное определение класса PSPACE. И доказательство IP $\subseteq$ PSPACE напоминает ту часть доказательства теоремы 5, в которой строится алгоритм определения выигрышной стратегии, использующий полиномиально ограниченную память.

Пусть $f(x) \in \mathrm{IP}$. Снова по индукции определяется набор машин Тьюринга M_k для $k = 0, \dots, s(|x|)$.

Каждая M_k по заданному началу диалога $x, r_1, p_1, \dots, r_k, p_k$ длины k между Исполнителем и Советником оценивает вероятность ответа 1 при

[4)] Автор благодарен А. Китаеву, обратившему его внимание на эту, известную специалистам по теории сложности, интерпретацию теоремы 7.

продолжении диалога. Последняя в этом ряду машина $M_{s(|x|)}$ имитирует работу Исполнителя, вычисляет функцию $V(x, r_1, p_1 \ldots)$ и сообщает в качестве ответа её значение. Машина M_k перебирает все возможные варианты $(k+1)$-го сообщения и консультируется с M_{k+1} по поводу окончательных результатов. Если слово за Советником, то оценка M_k — максимум оценок M_{k+1} по всем возможным вариантам сообщения Советника. Если слово за Исполнителем, то оценка M_k равна среднему арифметическому оценок M_{k+1} по всем r_k (это формула полной вероятности).

Алгоритм вычисления f на полиномиальной памяти запускает M_0 и выдаёт в качестве результата 1, если оценка M_0 больше $2/3$, и 0, если оценка M_0 меньше $2/3$.

8.4. PSPACE $\subseteq$ IP

Дадим набросок доказательства, подробно это доказательство изложено в книге Сипсера [9].

Достаточно доказать, что PSPACE-полная задача TQBF принадлежит IP.

Итак, пусть нужно проверить истинность высказывания

$$T_0 = \mathsf{Q}_1 x_1 \mathsf{Q}_2 x_2 \ldots \mathsf{Q}_m x_m \varphi(x_1, \ldots, x_m),$$

в котором $\varphi(\cdot)$ — некоторая логическая формула, $\mathsf{Q}_i \in \{\forall, \exists\}$, кванторы действуют на формулы по правилам (14)–(15).

Оценить истинность высказывания T_0 можно следующей рекурсивной процедурой. Обозначим через $T_j(x_1, x_2, \ldots, x_j)$ высказывание

$$\mathsf{Q}_{j+1} x_{j+1} \mathsf{Q}_{j+2} x_{j+2} \ldots \mathsf{Q}_m x_m \varphi(x_1, \ldots, x_j, x_{j+1}, \ldots, x_m).$$

Тогда $T_0 = T_1(0) *_1 T_1(1)$, где $*_1$ — связка, определяемая квантором Q_1. Найдем вначале $T_1(0)$, а затем $T_1(1)$, каждый раз вызывая рекурсивно саму описываемую процедуру (для определения $T_m(x_1, \ldots, x_m)$ достаточно вычислить значение формулы $\varphi(x_1, \ldots, x_m)$, так что рекурсия конечная) и вычислим $T_1(0) *_1 T_1(1)$.

Эта процедура требует вычисления всех 2^m возможных значений формулы $\varphi(\cdot)$, а потому занимает экспоненциально большое по сравнению с размером входа задачи время. Наглядно это вычисление можно изобразить в виде дерева, как показано на рис. 5а. В процессе вычисления мы получаем не только значение в корне, но и значения во всех промежуточных узлах дерева, количество которых экспоненциально велико.

Чем может помочь Советник в таком вычислении? Он, конечно, может сообщить значение T_0. Впрочем, поскольку Советник пристрастен, то в любом случае он скажет, что $T_0 = 1$. Попробуем проверить это сообщение и запросим значения $T_1(0)$ и $T_1(1)$ — должно выполняться соотношение $T_0 = T_1(0) *_1 T_1(1)$. Далее выберем случайно и равновероятно число

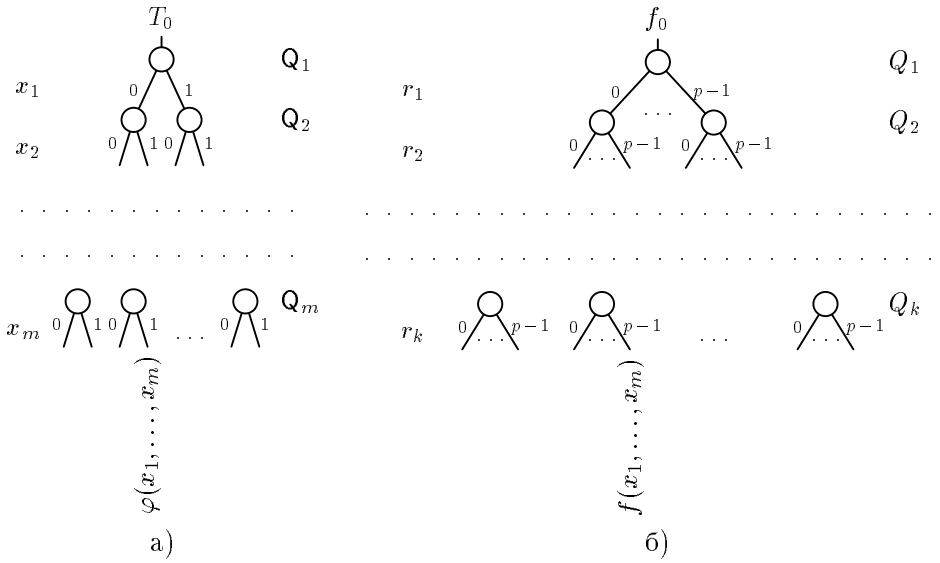


Рис. 5.

$r_1 \in \{0,1\}$, запросим у Советника значения $T_2(r_1,0)$ и $T_2(r_1,1)$, проверим $T_1(r_1) = T_2(r_1,0) *_2 T_2(r_1,1)$ и т. д. На последнем шаге уже без всякого Советника можно проверить, что

$$T_{m-1}(r_1,\ldots,r_{m-1}) = T_m(r_1,\ldots,r_{m-1},0) *_m T_m(r_1,\ldots,r_{m-1},1).$$

Вычисления будут длиться $O(m)+\Phi(n) = \mathrm{poly}(n)$ тактов, где $\Phi(n)$ — количество тактов, необходимых для вычисления значения логической формулы длины n при заданных значениях переменных. Они происходят вдоль одного из путей от корня к листьям в дереве на рис. 5а, выбираемого случайно и равновероятно.

С какой вероятностью Исполнитель принимает решение об истинности QBF? Если рассматриваемая формула истинна, то Советнику достаточно говорить истинные значения всех запрашиваемых величин, Исполнитель не увидит никакого противоречия и с вероятностью 1 признает формулу истинной. Что будет, если QBF ложна? Чтобы убедить Исполнителя в обратном, Советнику хотя бы раз придется солгать, сообщив неверное значение одной из пары запрашиваемых переменных. Эта ложь с вероятностью $1/2$ замечена не будет, что показывает непригодность описанной процедуры для надежного определения истинности QBF.

Как ни странно, есть способ исправить описанную выше процедуру. Если в исходном варианте из полного бинарного дерева перебора случайно выбирался один путь, и это ничего не дало, то в исправленной версии дерево станет шире (каждый раз будет выбор из p вариантов, где

$p = \Omega(n^4)$ — простое число) и глубже (глубина дерева была m, а в исправленной версии будет примерно m^2). Это дерево изображено на рис. 5б.

Чтобы построить такое разветвлённое дерево, будем считать истинностные значения 0 и 1 элементами поля $\mathbb{F}_p$ вычетов по модулю p. Любую логическую формулу $\varphi(x_1, x_2, \ldots, x_m)$ можно записать как многочлен $p(x_1, x_2, \ldots, x_m)$ над полем $\mathbb{F}_p$, используя выражения (8) на с. 97. Степень d этого многочлена не превосходит длины записи формулы $\varphi(x_1, x_2, \ldots, x_m)$, которая меньше n — размера входа задачи TQBF.

Кванторам сопоставим следующие операции с многочленами:

$$\forall \ \mapsto A_x f(x_1, \ldots, x) \stackrel{\text{def}}{=} f(x_1, \ldots, 0) f(x_1, \ldots, 1), \tag{17}$$

$$\exists \ \mapsto E_x f(x_1, \ldots, x) \stackrel{\text{def}}{=} 1 - (1 - f(x_1, \ldots, 0))(1 - f(x_1, \ldots, 1)). \tag{18}$$

Теперь число

$$p_0 = (Q_1)_{x_1} (Q_2)_{x_2} \ldots (Q_m)_{x_m} p(x_1, \ldots, x_m) \tag{19}$$

равняется истинностному значению формулы $\varphi(x_1, x_2, \ldots, x_m)$ (Q_i — операция, соответствующая квантору Q_i). Вычисление этого числа организовано в дерево, аналогичное изображенным на рис. 5. Степень ветвления у этого дерева равна p, а глубина — m.

Высказываниям $T_j(x_1, x_2, \ldots, x_j)$ при этом соответствуют многочлены

$$p_j(x_1, \ldots, x_j) = (Q_{j+1})_{x_{j+1}} (Q_{j+2})_{x_{j+2}} \ldots (Q_m)_{x_m} p(x_1, \ldots, x_j, x_{j+1}, \ldots, x_m).$$

Заметим, что операции A_x, E_x уменьшают число переменных на 1, но удваивают, вообще говоря, степень каждой из оставшихся переменных, так что степени p_j могут быть велики. Чтобы степени многочленов не росли чрезмерно при вычислениях, можно воспользоваться следующей операцией:

$$L_x f(x_1, \ldots, x) \stackrel{\text{def}}{=} x f(x_1, \ldots, 1) + (1 - x) f(x_1, \ldots, 0). \tag{20}$$

Многочлены f и $L_x f$ имеют одинаковое количество переменных, совпадают при $x \in \{0, 1\}$, а степень переменной x в $L_x f$ равна 1.

Итак, истинностное значение высказывания T_0 равно

$$p_0 = (Q_1)_{x_1} L_{x_1} (Q_2)_{x_2} L_{x_1} L_{x_2} \ldots (Q_m)_{x_m} L_{x_1} L_{x_2} \ldots L_{x_m} p(x_1, \ldots, x_m),$$

где Q_i определяется по входу задачи TQBF (так же, как в (19)). К многочлену $p(\cdot)$ применяются в заданном порядке $k = m + m(m+1)/2$ операций вида A_x, E_x или L_x. Пусть после применения первых $k - i$ операций получается многочлен $p_i(t_1, \ldots, t_j)$, $1 \leqslant i \leqslant k$. Поскольку операция L не меняет количества переменных в многочлене, число j не обязательно равно i.

Теперь опишем диалог между Исполнителем и Советником. Начинается он с того, что Советник сообщает значение p_0 (как и раньше, в самом начале он скажет, что $p_0 = 1$ независимо от его настоящего значения).

Затем Исполнитель спрашивает у Советника, чему равен многочлен $p_1(t)$. Получив коэффициенты этого многочлена, Исполнитель проверяет, что $p_0 = (S_1)_t p_1(t)$ (будем операцию, стоящую на i-м месте обозначать S_i). После этого Исполнитель случайно и равновероятно выбирает число $r_1 \in \mathbb{F}_p$ и применяет рекурсивно ту же процедуру для проверки равенства

$$p_1(r_1) = L_{x_1}(Q_2)_{x_2} L_{x_1} L_{x_2} \ldots (Q_m)_{x_m} L_{x_1} L_{x_2} \ldots L_{x_m} p(x_1, \ldots, x_m).$$

Конечность рекурсии обеспечивается тем, что значение многочлена $p(x_1, \ldots, x_m)$ Исполнитель вычисляет самостоятельно. Если все проверки дают положительный результат, Исполнитель выдаёт в качестве ответа 1, если хотя бы раз обнаружено неравенство — 0.

Теперь оценим вероятности ответа 1.

Если рассматриваемая QBF истинна, то Советнику опять достаточно говорить истинные значения всех запрашиваемых величин. А вот если QBF ложна, Советнику хотя бы раз придется солгать. Поскольку два многочлена степени $d = O(n)$ совпадают не более чем в d точках, то с вероятностью не меньшей $1 - d/p$ на следующем шаге будет проверяться ложное условие. По индукции получаем, что вероятность обнаружить ложь в описанном диалоге не меньше

$$\left(1 - \frac{d}{p}\right)^N,$$

где $N = O(n^2)$ — общее количество проверок. При $p = \Omega(n^4)$ эта вероятность будет близка к 1.

9. Заключение

Итак, помимо прямого способа доказывать вычислительную сложность задачи, есть косвенные — доказывать полноту задачи в подходящем сложностном классе. Мы привели два примера таких классов — NP и PSPACE. Если когда-нибудь в будущем удастся доказать, что включения $\mathrm{P} \subseteq \mathrm{NP}$ и/или $\mathrm{NP} \subseteq \mathrm{PSPACE}$ строгие, то, как следствие, для очень многих задач появятся доказательства их сложности.

Существует много других сложностных классов. Например, в уголовно-процессуальной модели вычисления можно ограничить число выступлений сторон некоторой абсолютной константой. Получится целая *иерархия* сложностных классов, включающая на одном из нижних уровней класс NP (единственное выступление Прокурора). Популярна гипотеза, что все включения в этой иерархии строгие.

Упомянём также особую модель вычислений — квантовые вычисления (см. [4]). Рассказывать о них мы не будем, заметим лишь, что они

содержат BPP и содержатся в PSPACE. Но приведем задачу, по вычислительной силе эквивалентную квантовым вычислениям.

Пример 5 (см. [8]). Оценка квадратичной суммы. *Дана*: (0,1)-*матрица* A *размера* $n\times n$, *на диагонали которой стоят единицы* ($a_{ii}=1$).

Спрашивается: *каков знак у суммы*

$$S=\sum_{Ax=0,x\in\{0,1\}^n}(-1)^{x^TBx}4^{\|x\|}3^{n-\|x\|},$$

если известно, что $|S|>5^n$?

В приведённой формуле матрица B получается из матрицы A заменой всех элементов на главной диагонали и выше нулями, $\|x\|$ — количество единиц в записи x.

Слова «если известно» означают, что на входах, не удовлетворяющих условию $|S|>5^n$, функция не определена, и алгоритм может работать на таких входах как угодно.

Этот пример замечательным образом иллюстрирует обсуждавшиеся нами идеи полноты и сведения. Если интересоваться только временем работы алгоритмов с точностью «до полинома», то вычислительные возможности квантовых компьютеров совпадают с возможностями вероятностных машин, работающих полиномиальное время и имеющих дополнительно доступ к устройству (оракулу), решающему задачу об оценке квадратичной суммы.

Список литературы

[1] *Кормен Т. Х., Лейсерсон Ч. Е., Райвест Р. Л.* Алгоритмы: построение и анализ / Пер. с англ. под ред. А. Шеня. М.: МЦНМО, 1999.

[2] *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов. М.: Мир, 1979.

[3] *Гэри М., Джонсон Д.* Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

[4] *Китаев А., Шень А., Вялый М.* Классические и квантовые вычисления. М.: МЦНМО, ЧеРо, 1999.

[5] *Манин Ю. И.* Вычислимое и невычислимое. М.: Советское радио, 1980.

[6] *Разборов А. А.* О сложности вычислений // Математическое Просвещение. Сер. 3, вып. 3. М.: МЦНМО:ЧеРо, 1999. С. 127–141.

[7] *Верещагин Н., Шень А.* Логические формулы и схемы // Математическое Просвещение. Сер. 3, вып. 4. М.: МЦНМО, 2000. С. 53–80.

[8] *Knill E., Laflamme R.* Quantum Computation and Quadratically Signed Weight Enumerators. `xxx.lanl.gov/quant-ph/9909094`

[9] *Sipser M.* Theory of computation. Boston, MA: PWS Publ. Co, 1997.

[10] *Smale S.* Problems for the next century // Math. Intelligencer, 1998. Vol. 20, no. 2. P. 7–15.

О проблемах вычислительной сложности

С. Смейл

Запись лекции, прочитанной в Высшем Колледже Математики Независимого Московского Университета 20 мая 1999 года.

Мы сейчас обсудим одну задачу, которая в элементарной форме иллюстрирует основные трудности теории вычислительной сложности. Для полинома $f \in \mathbb{Z}[t]$ определим число $\tau(f)$ следующим образом. Рассмотрим последовательность $(1, t, u_1, \ldots, u_m = f)$, в которой каждый последующий член получается из некоторых двух предшествующих: $u_k = u_i \circ u_j$, $i, j < k$; под операцией $\circ$ здесь подразумевается одна из трёх арифметических операций (сложение, вычитание, умножение). Инвариант $\tau(f)$ равен наименьшему возможному m.

Имеется следующая гипотеза Шуба – Смейла: *количество различных целых корней многочлена f не превосходит $\tau(f)^c$, где c — некоторая абсолютная константа.*

Пример. Последовательность $1, t, t^2, t^{2^2}, \ldots, t^{2^k}, t^{2^k} - 1$ показывает, что $\tau(t^{2^k} - 1) \leqslant k + 1$. Но при этом количество различных корней многочлена $t^{2^k} - 1$ равно 2^k. Поэтому для различных комплексных корней аналогичная гипотеза неверна.

Аналогичный пример можно построить с помощью многочленов Чебышева. Многочлены Чебышева вычисляются с помощью простой рекуррентной формулы. Они тоже дают пример многочленов высокой степени с малым τ. При этом все корни многочленов Чебышева вещественны и попарно различны. Для различных вещественных корней аналогичная гипотеза тоже неверна.

Теорема 1 (Шуб – Смейл). *Из гипотезы Шуба – Смейла следует, что* $\mathrm{P} \neq \mathrm{NP}/_{\mathbb{C}}$.

Теперь нужно объяснить, что означает $\mathrm{P} \neq \mathrm{NP}/_{\mathbb{C}}$.

Прежде всего отметим, что у алгебраистов нетривиальные проблемы обычно начинаются с диофантовых уравнений, соответствующих алгебраическим кривым, т. е. двум переменным. У нас проблемы начинаются уже в случае одной переменной.

Если забыть про $\mathbb{C}$, то проблема $\mathrm{P} \neq \mathrm{NP}$ — это одна из ключевых проблем компьютерной математики. Вместе с гипотезой Пуанкаре и гипотезой о нулях дзета-функции Римана она является одной из важнейших проблем математики — это подарок от computer science.

Рассмотрим многочлены $f_1(z_1, \ldots, z_n), \ldots, f_k(z_1, \ldots, z_n)$ над $\mathbb{C}$. Спрашивается, имеют ли эти многочлены общий нуль? Это — задача распознавания свойства: в качестве условия задаются многочлены $f_1, \ldots, f_k$ (точнее говоря, задаётся несколько комплексных чисел — коэффициентов многочленов), а результатом работы должен быть один из двух ответов: «да» (есть общий нуль) или «нет» (общего нуля нет).

Теорема Гильберта о нулях даёт следующий ответ: общего нуля не существует тогда и только тогда, когда существуют такие многочлены $g_1, \ldots, g_k$, что $\sum g_i f_i = 1$.

Теорема Гильберта о нулях — критерий, но не метод. Она не даёт никакого алгоритма. Но примерно 10 лет назад Браунвелл[1)] показал, что в теореме Гильберта о нулях можно считать, что

$$\deg g_i \leqslant \max(3, \max \deg f_i)^n,$$

причём этот результат неулучшаем.

Теорема Браунвелла даёт алгоритм: всё сводится к решению системы линейных уравнений для коэффициентов многочленов g_i.

Займёмся теперь вопросом о скорости этого алгоритма: сколько арифметических операций нужно выполнить, чтобы ответить на поставленный вопрос. Назовём *размером* входных данных количество коэффициентов многочленов f_i, а *временем* работы алгоритма назовём количество арифметических операций. Будем называть данный алгоритм *алгоритмом с полиномиальным временем*, если

$$\text{время} \leqslant (\text{размер})^C, \tag{1}$$

где C — некоторая константа.

Алгоритмы с полиномиальным временем — это как раз те алгоритмы, которые имеет смысл практически реализовывать на вычислительной машине. Если, скажем, время зависит от размера экспоненциально, то при увеличении размера входных данных время быстро выходит за разумные пределы. Алгоритм Браунвелла является алгоритмом с экспоненциальным временем. Экспоненциальная верхняя оценка для этого алгоритма легко выводится, например, из гауссова метода исключения для решения системы линейных уравнений.

[1)] Brownawell W. Bounds for the degrees in the Nullstellensatz // *Annals of Math.*, 1987. Vol. 126. P. 577–591.

Гипотеза такова: задача $HN/_{\mathbb{C}}$ (существует ли общий нуль системы полиномиальных уравнений над $\mathbb{C}$) трудноразрешима, т. е. не существует алгоритма с полиномиальным временем для решения этой задачи.

Здесь имеется в виду алгоритм не в смысле машины Тьюринга, а алгоритм над $\mathbb{C}$ в следующем смысле. Алгоритм — это ориентированный граф с одной вершиной, в которую не ведет ни одного ребра (*входом*). Граф может иметь циклы. Он задаёт работу вычислительной машины следующим образом. На вход подаётся бесконечная в обе стороны последовательность комплексных чисел $(\ldots, 0, z_1, \ldots, z_n, 0, \ldots)$, среди которых только $z_1, \ldots, z_n$ отличны от нуля, никаких ограничений на величину n не предполагается, так что такая модель вычислительной машины может работать со сколь угодно длинными последовательностями чисел. Вершины этого графа относятся к одному из трех типов:

- ▷ Выходы. Из них не ведет ни одного ребра. По достижении такой вершины работа заканчивается.
- ▷ Вычислительный узел. В вычислительный узел входит одно ребро и из него выходит тоже одно ребро. В вычислительном узле производится арифметическая операция с какими-то членами последовательности и один из членов последовательности заменяется на результат вычислений. Кроме того, можно все члены последовательности умножить на одно и то же число или произвести сдвиг последовательности.
- ▷ Узел ветвления. В узел ветвления входит одно ребро, а выходят из него два ребра, на которых стоят пометки «да» и «нет». В узле ветвления выясняется, верно ли что $z_i = 0$. Если $z_i = 0$, то мы идём дальше по ребру с пометкой «да», а если $z_i \neq 0$, то мы идём дальше по ребру с пометкой «нет». (Для вычислений над $\mathbb{R}$ вместо этого можно ввести проверку типа $x_i > 0$ или $x_i \geqslant 0$.)

На выходе алгоритма тоже получается последовательность чисел. В интересующем нас алгоритме $HN/_{\mathbb{C}}$ на выходе только один ненулевой элемент, который может принимать ровно два значения, соответствующие ответам «да» и «нет».

Такое определение алгоритма было дано Л. Блюм, С. Смейлом и М. Шубом в конце 80-ых годов. Странно, что раньше никто не додумался до этого совершенно естественного определения. Подробно ознакомиться с теорией таких алгоритмов можно по книге Blum L., Cucker F., Shub M., Smale S. Complexity and Real Computation. Springer Verlag, 1997.

С описанным выше алгоритмом естественным образом связана функция «входа – выхода». Она определена на некотором множестве входных

данных (например, машина не может производить деление на нуль, поэтому при некоторых входных данных она останавливается).

Размером входных данных назовем число n, а временем работы при данном входе — длину пути от входа к выходу (на разных входах эти пути могут быть различными). Алгоритмы с полиномиальным временем удовлетворяют неравенству (1) для некоторой константы C при всех входах. Класс таких алгоритмов обозначается $\mathrm{P}/_{\mathbb{C}}$.

После этого определения вопрос о том, существует ли полиномиальный алгоритм для задачи $HN/_{\mathbb{C}}$, приобретает строгий математический смысл. Заметим, что утверждение о том, что такого алгоритма не существует, в точности эквивалентно утверждению $\mathrm{P} \neq \mathrm{NP}/_{\mathbb{C}}$ (определение $\mathrm{NP}/_{\mathbb{C}}$ пока не давалось и на этой лекции не будет дано).

Вместо поля $\mathbb{C}$ можно взять произвольное поле K и определить вычислительную машину над произвольным полем. Например, поле $K = \mathbb{Z}_2$ соответствует определению алгоритма, принятому в логике и computer science.

Можно также поставить вопрос об общих нулях многочленов над $\mathbb{Z}_2$. Гипотеза о том, что не существует полиномиального алгоритма для решения этой задачи, эквивалентна гипотезе $\mathrm{P} \neq \mathrm{NP}$ в её классическом варианте.

Для числа $m \in \mathbb{Z}$ можно определить инвариант $\tau(m)$ по аналогии с инвариантом τ для многочленов. А именно, рассмотрим аналогичную последовательность $(1, m_1, \ldots, m_k = m)$ и определим $\tau(m)$ как минимальное возможное k. С помощью формулы Стирлинга можно доказать, что $\tau(m!) \leqslant (\ln m)^C$. Есть предположение, что верна и противоположная оценка такого же вида: $(\ln m)^{C'} \leqslant \tau(m!)$; эта проблема связана с разложением на простые множители.

На первый взгляд эти две проблемы (об инварианте τ для полиномов и для чисел) друг с другом не связаны.

Вернёмся к проблеме $\mathrm{P} \neq \mathrm{NP}/_K$. Мы не будем определять, что такое $\mathrm{NP}/_K$, вместо этого будем говорить об эквивалентной проблеме Гильберта о нулях над произвольным полем K: $HN/_K \notin \mathrm{P}/_K$. (Если поле не алгебраически замкнуто, то теорема Гильберта о нулях неверна, но задача об общих нулях системы многочленов имеет смысл над произвольным полем; здесь имеется в виду именно эта задача.)

В случае не алгебраически замкнутого поля доказано следующее утверждение.

Теорема 2. *Если поле K не алгебраически замкнуто и* $\operatorname{char} K = 0$, *то* $\mathrm{P} \neq \mathrm{NP}/_K$.

Для поля $\mathbb{Z}_2$, которое тоже не алгебраически замкнуто, вопрос остается открытым (характеристика этого поля отлична от нуля).

Вернёмся к алгебраически замкнутым полям. Для алгебраически замкнутого поля K ($\operatorname{char} K = 0$) проблема $\mathrm{P} \neq \mathrm{NP}/_K$ эквивалентна проблеме $\mathrm{P} \neq \mathrm{NP}/_{\mathbb{C}}$. Поэтому всё сводится к одному полю, например, полю $\mathbb{C}$ или полю $\overline{\mathbb{Q}}$ (так обозначается алгебраическое замыкание поля $\mathbb{Q}$). Это — один из основных результатов упомянутой выше книги. Доказательство использует понятие высоты алгебраического числа.

Представляется весьма правдоподобным, что $\mathrm{P}/_K = \mathrm{P}/_{\mathbb{F}_2}$ для любого конечного поля K. Но для полей конечной характеристики вопросов больше, чем ответов.

Рассмотрим вопрос об эквивалентности проблем над $\mathbb{C}$ и над $\bar{\mathbb{Q}}$. Одна из основных проблем при переходе от комплексных чисел к алгебраическим связана с тем, что нужно избавиться от комплексных констант, которые могут использоваться при вычислениях. Вообще говоря, они могли бы сильно упростить вычисления. Однако доказано, что такого упрощения не происходит.

В упомянутой выше книге не рассматривался вопрос о связи проблем $\mathrm{P} \neq \mathrm{NP}/_{\mathbb{Z}_2}$ и $\mathrm{P} \neq \mathrm{NP}/_{\mathbb{C}}$. Именно первая из них относится к классической computer science. В предисловии к этой книге Дик Карп высказал предположение, что эти проблемы никак друг с другом не связаны. Но уже после того как книга была написана, Смейл заметил следующее.

Напомним, что интерес к алгоритмам с полиномиальным временем связан с тем, что именно их можно эффективно реализовывать на компьютерах. Но сейчас используется ещё один важный класс алгоритмов — так называемые BPP-алгоритмы. В этих алгоритмах разрешается «подбрасывать монетку» и в зависимости от полученного результата производить те или иные вычисления. Требуется, чтобы правильный ответ получался в «квалифицированном большинстве» случаев[2)]. Тогда, повторив вычисления много раз, можно получить результат, который будет правильным с очень большой вероятностью. Например, если правильный результат получается с вероятностью $3/4$, то после 50 повторений вычислений вероятность ошибки будет равна единице, делённой на число атомов во Вселенной.

С математической точки зрения условие BPP накладывает меньше ограничений, чем условие P, но с практической точки зрения BPP-алгоритмы столь же хороши, как и P-алгоритмы.

Теорема 3 (Смейл). *Если* $\mathrm{BPP} \not\supseteq \mathrm{NP}$, *то* $\mathrm{P} \neq \mathrm{NP}/_{\mathbb{C}}$.

С точки зрения современной computer science $\mathrm{BPP} \not\supseteq \mathrm{NP}$ — это нечто очень похожее на $\mathrm{P} \neq \mathrm{NP}$.

[2)] Более формальное определение класса BPP см. в статье М. Вялого на с. 106. — *Прим. ред.*

По-новому о старом: фрагменты классической математики

Инверсии равносторонней гиперболы

А. Руинский

Равносторонняя гипербола (каноническое уравнение $x^2 - y^2 = a^2$) является симметричной линией, оси симметрии которой взаимно перпендикулярны. Ее инверсными образами являются некоторые известные линии.

Рассмотрим следующие определения и свойства, которыми мы будем пользоваться в статье.

Определение 1. Линии Φ_1 и Φ_2 будем называть инверсными, если существует инверсия, переводящая линию Φ_1 в линию, конгруэнтную Φ_2, и наоборот. Образ линии Φ при инверсии с центром O и степенью r^2 будем обозначать $I_r^O(\Phi)$.

Определение 2. Линию Φ будем называть инверсно-симметричной, если существует инверсия, переводящая линию Φ в себя. Центр такой инверсии будем называть инверсным центром линии.

Очевидно, что при любой степени инверсии инверсный образ линии относительно инверсного центра есть линия, гомотетичная Φ.

Свойство 1. Если две линии инверсны третьей, то они инверсны друг другу.

Свойство 2. Для того, чтобы линия Ψ была инверсно-симметричной, необходимо и достаточно, чтобы существовала симметричная линия Φ и окружность $O(r)$, центр которой не лежит на оси симметрии Φ, так, что $\Psi = I_r^O(\Phi)$. Центр инверсии линии Ψ суть $M = I_r^O(O')$, где O' — точка, симметричная O относительно оси симметрии линии Φ.

Математическое просвещение, сер. 3, вып. 4, 2000(120–126)

Важное замечание. Ось симметрии линии Φ, на которой не лежит центр O, может быть не единственной осью симметрии линии Φ. Свойство 2 утверждает, что *существует ось симметрии* Φ, не содержащая центр O. Это замечание важно, так как если Ψ и Φ — окружности, то их оси симметрии покрывают всю плоскость.

Формулы преобразования координат. Пусть $x^2 + y^2 = r^2$ — окружность инверсии и $I_r^O(x;y) = (\tilde{x};\tilde{y})$. Тогда

$$\tilde{x} = \frac{xr^2}{x^2+y^2}, \quad \tilde{y} = \frac{yr^2}{x^2+y^2}.$$

«Старые» координаты преобразуются в «новые» аналогичным образом.

1. Равносторонняя гипербола, лемниската Бернулли и улитка Паскаля

Теорема 1. *Инверсный образ равносторонней гиперболы относительно ее центра суть лемниската Бернулли.* (*См. рис.* 1.)

Доказательство. Напомним уравнение лемнискаты Бернулли:

$$(x^2+y^2)^2 - 2k^2(x^2-y^2) = 0.$$

Уравнение равносторонней гиперболы — $x^2 - y^2 = a^2$. Применяя формулы инверсии, получаем:

$$\frac{x^2r^4}{(x^2+y^2)^2} - \frac{y^2r^4}{(x^2+y^2)^2} = a^2 \quad \Longrightarrow \quad (x^2+y^2)^2 - \frac{r^4}{a^2}(x^2-y^2) = 0.$$

Если $r = a$, то уравнение лемнискаты еще более упрощается: $(x^2+y^2)^2 - a^2(x^2-y^2) = 0$.

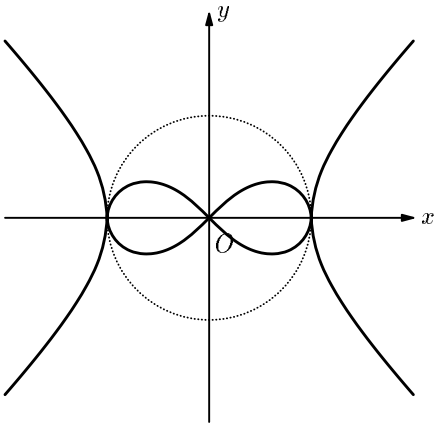


Рис. 1.

Теорема 2. *Инверсный образ равносторонней гиперболы относительно ее фокуса суть улитка Паскаля.* (*См. рис.* 2.)

Доказательство. Напомним уравнение улитки Паскаля:

$$(x^2+y^2-kx)^2-l^2(x^2+y^2)=0.$$

Фокусами равносторонней гиперболы $x^2-y^2=a^2$ являются точки $(-a\sqrt{2};0)$ и $(a\sqrt{2};0)$.

Рассмотрим инверсию с центром в левом фокусе $(-a\sqrt{2};0)$ и степенью $r^2=a^2$. Перенесем начало координат в центр инверсии: $(x-a\sqrt{2})^2-y^2=a^2$, т. е. $x^2-2\sqrt{2}ax+a^2-y^2=0$. Применяя формулы инверсии, получаем:

$$\frac{a^4(x^2-y^2)}{(x^2+y^2)^2}-2\sqrt{2}a\frac{a^2x}{x^2+y^2}+a^2=0 \quad\Longrightarrow$$
$$\Longrightarrow\quad (x^2+y^2)^2-2\sqrt{2}ax(x^2+y^2)+a^2(x^2-y^2)=0.$$

Выделим полный квадрат двух первых членов и получим:

$$(x^2+y^2)^2-2\sqrt{2}ax(x^2+y^2)+2a^2x^2-2a^2x^2+a^2(x^2-y^2)=0$$
$$\Downarrow$$
$$(x^2+y^2-\sqrt{2}ax)^2-a^2(x^2+y^2)=0.$$

Последнее уравнение определяет улитку Паскаля с $k=\sqrt{2}a$, $l=a$. Ясно, что $k=l\sqrt{2}$.

Теорема 3. *Улитка Паскаля при $k=l\sqrt{2}$ инверсна лемнискате Бернулли.*

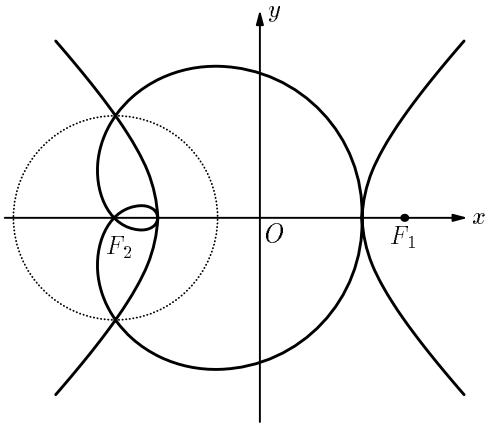


Рис. 2.

Доказательство. Так как улитка Паскаля при $k = l\sqrt{2}$ и лемниската Бернулли инверсны равносторонней гиперболе, то они инверсны друг другу (см. свойство 1).

Можно показать, что центр искомой инверсии является фокусом лемнискаты и одновременно центром окружности, конхоидой которой является улитка.

Теорема 4. *Улитка Паскаля при $k = l\sqrt{2}$ является инверсно-симметричной линией.*

Доказательство. Так как улитка Паскаля при $k = l\sqrt{2}$ является инверсным образом симметричной линии (гиперболы) и центр инверсии не лежит на оси симметрии (мнимая ось), то, по свойству 2, она — инверсно-симметричная линия. Инверсный центр улитки Паскаля суть инверсный образ фокуса F_1 относительно окружности, переводящей гиперболу в улитку, а степень искомой инверсии $|MF_2|^2$. (См. рис. 3.)

Замечание. Известно, что любая улитка инверсна некоторой конике, причем если $k = l$ (кардиоида), то улитка инверсна параболе (в этом случае центр инверсии лежит на оси симметрии и свойство 2 не может быть применено), а при всех других соотношениях между k и l, улитка Паскаля инверсна гиперболе или эллипсу. Так как в этом случае центр инверсии не лежит на оси симметрии (малая ось эллипса и мнимая ось гиперболы), то справедливо более общее свойство: *Любая улитка Паскаля, кроме кардиоиды, суть инверсно-симметричная линия.*

2. Произвольный инверсный образ равносторонней гиперболы

Теорема 5. *Любой инверсный образ равносторонней гиперболы, за исключением лемнискаты Бернулли, инверсно-симметричен. Если центр инверсии, преобразующей равностороннюю гиперболу, не принадлежит осям гиперболы, то получающаяся кривая имеет* ***два инверсных центра****.* (*См. рис.* 4а.)

Доказательство. Доказательство элементарно следует из свойства 2, применяемого относительно действительной и мнимой осей гиперболы.

Замечание 1. Очевидно, что аналогичное свойство выполняется для произвольных гиперболы и эллипса. У параболы любой несимметричный образ имеет один центр инверсии, а симметричный не имеет его вообще. (См. рис. 4б.)

Замечание 2. Очевидно, что аналогичные свойства верны для любой симметричной линии. Например, любой образ трехлепестковой розы,

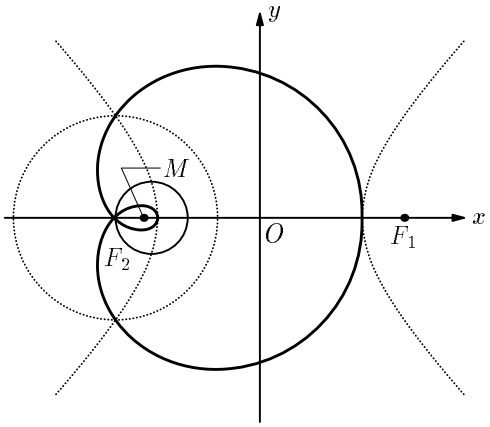


Рис. 3.

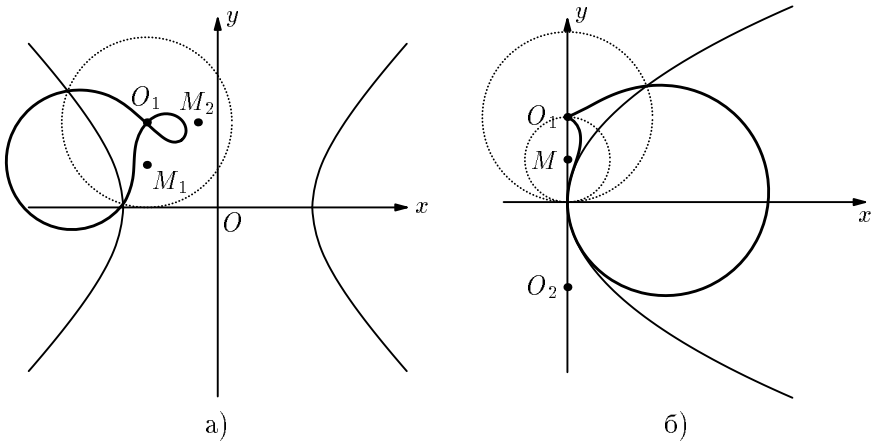


Рис. 4. *Несимметричный образ а) гиперболы; б) параболы.*

кроме образа относительно ее центра, имеет минимум два и максимум три центра инверсии. Образ астроиды может иметь три или четыре таких центра. У образов синусоиды или циклоиды есть бесконечно много центров инверсии.

3. Равносторонняя гипербола и строфоиды

Уравнение строфоиды в декартовой системе координат:

$$(x^2+y^2)\cdot(Ax+By)+aA(x^2-y^2)+2aBxy=0,$$

где $Ax+By=0$ — уравнение ведущей прямой (рис. 5б), a — параметр. Очевидно, что в случае $B=0$ получим $x(x^2+y^2)+a(x^2-y^2)=0$, т.е. уравнение прямой строфоиды (рис. 5а). Если $B\neq 0$, то $k=-\dfrac{A}{B}$ — угловой коэффициент ведущей прямой $(y=kx)$ и уравнение наклонной строфоиды приобретает вид:

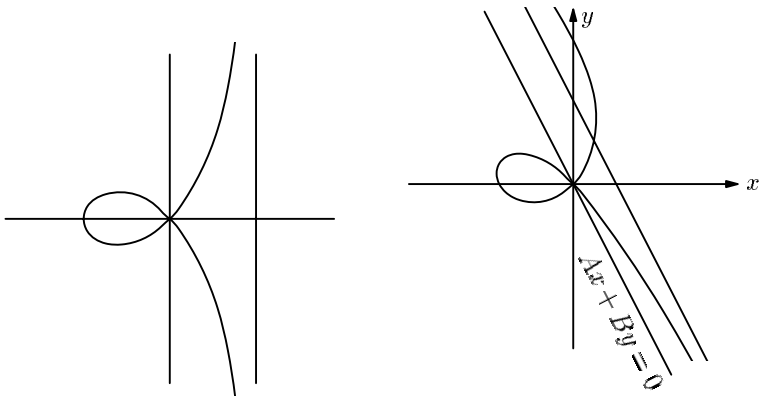
$$(x^2+y^2)(kx-y)+ka(x^2-y^2)-2axy=0.$$

Уравнение наклонной строфоиды всегда приводимо к виду:

$$(x^2+y^2)(mx-y)+b(x^2-y^2)=0,$$

в котором отсутствует член, содержащий xy.

Теорема 6. *Инверсный образ равносторонней гиперболы относительно любой окружности, центр которой лежит на этой гиперболе, суть строфоида. Если центр окружности инверсии — вершина гиперболы, то строфоида — прямая. Во всех остальных случаях строфоида — наклонная.*



а) б)

Рис. 5.

Доказательство. Пусть точка $(x_1; y_1)$ лежит на гиперболе $x^2 - y^2 = a^2$. Тогда $x_1^2 - y_1^2 = a^2$. Перенеся начало координат в точку $(x_1; y_1)$, получим:

$$(x + x_1)^2 - (y + y_1)^2 = a^2 \quad \Longrightarrow \quad x^2 + 2x_1x - y^2 - 2y_1y = 0.$$

Применим формулы инверсии:

$$\frac{r^4(x^2 - y^2)}{(x^2 + y^2)^2} + 2x_1r^2\frac{x}{x^2 + y^2} - 2y_1r^2\frac{y}{x^2 + y^2} = 0.$$

Если $y_1 = 0$, а $x_1 = \pm a$, то уравнение определяет прямую строфоиду: $x(x^2 + y^2) \pm \dfrac{r^2}{2a}(x^2 - y^2) = 0$. Если $y_1 \neq 0$, то после несложных преобразований получим:

$$(x^2 + y^2)\left(\frac{x_1}{y_1}x - y\right) + \frac{r^2}{2y_1}(x^2 - y^2) = 0.$$

Последнее уравнение определяет наклонную строфоиду, для которой $m = \dfrac{x_1}{y_1}$, $b = \dfrac{r^2}{2y_1}$. Очевидно, что ведущая прямая строфоиды совпадает с касательной гиперболы в центре инверсии.

Замечание. Доказанная теорема устанавливает ряд инверсных свойств прямой и наклонной строфоид. Прямая строфоида инверсно-симметрична относительно одной окружности, так как центр инверсии, переводящей в нее равностороннюю гиперболу, лежит на действительной оси гиперболы и не лежит на мнимой. Этот центр суть полюс строфоиды, что элементарно доказывается на основании ее геометрического определения. Наклонная строфоида инверсно-симметрична относительно двух окружностей. Все эти утверждения следуют из теоремы 5. Ясно, что и прямая, и наклонная строфоиды инверсны лемнискате Бернулли, улитке Паскаля, друг другу и всем другим образам равносторонней гиперболы.

В заключение приведем еще одну любопытную теорему, касающуюся прямой и наклонной строфоид.

Теорема 7. *На любой линии, инверсной равносторонней гиперболе, лежит одна и только одна точка, являющаяся центром инверсий, переводящих данную линию в равностороннюю гиперболу. Все остальные инверсии, центры которых лежат на линии, переводят последнюю в строфоиды (прямые или наклонные).*

Из этой теоремы следует, что центр инверсии любого образа равносторонней гиперболы, кроме строфоид, не принадлежит этому образу. Понятно, что аналогичные строфоидам классы линий существуют в инверсных семействах других линий.

Числа Фибоначчи и простота числа $2^{127}-1$

А. Н. Рудаков

Эта статья основана на материалах лекции, прочитанной студентам Высшего Колледжа Математики Независимого Московского Университета 3 апреля 1999 года.

1. Введение

Число $M = 2^{127} - 1$ долгое время было в списке рекордов, оно с 1877 г. по 1951 г. являлось самым большим известным простым числом. Простота $2^{127} - 1$ была установлена Э.Лукасом (É.Lucas). Им был найден замечательный способ доказательства простоты, потребовавший для $M = 2^{127} - 1$ около ста часов вычислений (без компьютера!), но никаких делений на меньшие простые числа[1)]. Я собираюсь изложить математическую суть алгоритма Лукаса, обсудив заодно некоторые изящные результаты из конечной арифметики. Сами вычисления мы проводить не будем.

Мне лично этот сюжет кажется очень хорошим примером того, что для построения хорошего алгоритма нужна хорошая теория. Впрочем, существуют изложения результата Лукаса, привлекающие значительно меньше «теории», чем моё изложение здесь (см. [2] и [1]).

Подробное историческое исследование работ Э.Лукаса и нахождения простых чисел см. в [3].

2. Числа Фибоначчи и основная теорема

Как известно, последовательность чисел Фибоначчи получается следующим образом: мы определяем $u_1 = 1$, $u_2 = 1$ и находим каждое следующее число по формуле $u_{n+1} = u_n + u_{n-1}$. У чисел Фибоначчи

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$$

немало замечательных свойств. Например, сначала идут два нечётных числа, потом чётное, а потом опять два нечётных и т. д. Это легко увидеть,

[1)] Про алгоритмы в теории чисел, в том числе про алгоритмы проверки простоты числа, можно прочесть в статье *НестеренкоЮ. В.* Алгоритмические проблемы теории чисел // Математическое просвещение, 1998. Сер. 3, вып. 2. С. 87–114.

если рассматривать числа Фибоначчи по модулю 2. Если мы знаем u_{n-1} и u_n по модулю 2, то u_{n+1} будет их «суммой по модулю 2». Следовательно, мы имеем последовательность:

$$\begin{array}{lcccl} u_3 & \equiv & 1+1 & \equiv & 0 \pmod 2 \\ u_4 & \equiv & 0+1 & \equiv & 1 \pmod 2 \\ u_5 & \equiv & 1+0 & \equiv & 1 \pmod 2 \\ \dots & & \dots & & \dots \end{array}$$

или $1, 1, 0, 1, 1, 0, 1, 1, 0, \dots$ Это и означает, что каждое третье число чётно, а числа перед ним и после него нечётны и т. д.

Можно заметить и что каждое пятое число делится на 5. Для этого надо только вычислить числа Фибоначчи по модулю 5. Это будет последовательность чисел

$$1, 1, 2, 3, 0, 3, 3, 6, 9 \equiv -1, 0, -1, -1, -2, -3, 0, -3, -3, \dots$$

После 20-го члена всё начнёт повторяться, и регулярно, через четыре места на пятом идут нули.

Задача 1. Покажите, что каждое четвёртое число Фибоначчи делится на 3.

Задача 2. Покажите, что если m делит u_k, то m делит u_{2k}, u_{3k}, u_{4k}, ...

Можно получить также формулу для чисел Фибоначчи. Она хорошо известна, но позвольте мне напомнить, как мы рассуждаем. Если мы отвлечёмся от «начальных данных», $u_1 = 1$, $u_2 = 1$, а рассмотрим только уравнение перехода

$$x_{n+1} = x_n + x_{n-1}, \tag{1}$$

то, конечно, есть много последовательностей, удовлетворяющих этому уравнению. Одна из них, называемая иногда *числами Лукаса*, это:

$$v_1 = 1,\ v_2 = 3,\ v_3 = 4,\ \dots,\ v_{n+1} = v_n + v_{n-1}.$$

Есть и другие последовательности, при этом если $\{a_n\}$ и $\{b_n\}$ — две такие последовательности, то можно построить третью, взяв их линейную комбинацию с некоторыми коэффициентами, например, $c_n = 2a_n + 3b_n$. Тут стоят коэффициенты 2 и 3, но они могут быть любыми. В частности, если

$$\alpha = \frac{1+\sqrt{5}}{2} \text{ и } \beta = \frac{1-\sqrt{5}}{2},$$

т.е. α и β — корни уравнения $x^2 = x + 1$, то последовательности $a_n = \alpha^n$ и $b_n = \beta^n$ удовлетворяют уравнению перехода (1), а значит, и любая их линейная комбинация обладает этим свойством. Так как $\alpha + \beta = 1$,

$\alpha^2+\beta^2=3$, то сумма этих последовательностей даёт числа Лукаса

$$\alpha^n+\beta^n=v_n. \tag{2}$$

Для чисел Фибоначчи надо более искусно подобрать коэффициенты. В результате получится

$$u_n=\frac{\alpha^n-\beta^n}{\alpha-\beta}. \tag{3}$$

В частности, из этого следует, что $u_{2n}=u_n\cdot v_n$.

Мне бы хотелось сейчас сформулировать нашу основную теорему, которая есть по существу теорема Лукаса (1876), хотя она не была сформулирована им в такой форме. Современное изложение исторических деталей есть в [3].

Теорема 1. *Пусть q — простое число вида $4k+3$ и $M=2^q-1$. Тогда M простое если и только если $v_{(M+1)/2}\equiv 0 \pmod M$.*

Этот результат является основой алгоритма, позволяющего установить простоту числа $2^{127}-1$, однако надо ещё добавить «быстрый» способ вычисления $v_{(M+1)/2}$. Мы это обсудим позже.

3. Комплексные числа в конечной арифметике

Давайте немножко изменим способ выражения: вместо того чтобы говорить «a сравнимо с b по модулю m, $a\equiv b \pmod m$», будем говорить «a равно b в „арифметике по модулю m“, $a=_{(m)} b$». Формально это ничего не меняет, чуть-чуть другие слова, но можно начать представлять себе, что есть некие числа «арифметики по модулю m», которые просто обозначаются целыми числами, а сами по себе есть нечто другое. Например, 6 и -1 это два обозначения для одного и того же числа «арифметики по модулю 7».

При таком подходе почти сразу возникает вопрос, а нельзя ли расширить область чисел, рассмотрев, например, «комплексные числа». Ведь комплексные числа — это пары действительных, а пары можно рассматривать и здесь. Давайте рассмотрим «комплексные числа по модулю 7». Определим такое комплексное число z как пару $z=(a,b)$, где a и b — «числа по модулю 7». Сложение задаётся обычным образом:

$$(a_1,b_1)+(a_2,b_2)=(a_1+a_2,\,b_1+b_2);$$

умножение тоже:

$$(a_1,b_1)\cdot(a_2,b_2)=(a_1a_2-b_1b_2,\,a_1b_2+a_2b_1).$$

Довольно просто убедиться, что это хорошее определение: есть нуль, единица, ассоциативность, коммутативность... Можно вычислить и

обратный элемент: если $z = (a, b)$, то

$$z^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right).$$

Однако может оказаться, что $a^2 + b^2 =_{(7)} 0$ и обратный элемент не определён.

Так как 7 — очень небольшое число, можно сделать явную проверку. Всевозможные элементы по модулю 7 легко выписываются, это:

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6.$$

Квадратами будут 0, 1, 4, 2, и всё! Суммы двух квадратов получаются такие:

$$0,\ 1,\ 4,\ 2;\ \ 1,\ 2,\ 5,\ 3;\ \ 4,\ 5,\ 3,\ 6;\ \ 2,\ 3,\ 6,\ 4.$$

Т. е. 0 встречается только один раз как $0 = 0^2 + 0^2$, все остальные суммы ненулевые. Значит, у ненулевого комплексного числа есть обратный элемент. Получилась хорошая арифметика со всеми четырьмя операциями, или то, что иначе называют полем, а точнее, квадратичным расширением простого поля из 7 элементов.

Кстати, 7 нельзя заменить на 5, поскольку $1^2 + 2^2 =_{(5)} 0$ в арифметике по модулю 5. Проблема, собственно, в том, какие числа в арифметике по модулю p надо считать отрицательными.

Вспомним, для построения обычных комплексных чисел мы берём отрицательное число -1, для которого не существует квадратного корня, и «добавляем» этот квадратный корень формально, т. е. пишем $z = a + bi$, где $i^2 = -1$. Далее правила операций возникают сами собой, из раскрытия скобок:

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i,$$
$$(a_1 + b_1 i) \cdot (a_2 + b_2 i) = (a_1 a_2 + b_1 b_2(-1)) + (a_1 b_2 + a_2 b_1)i.$$

Можно взять и другое отрицательное число, например -2, и рассмотреть комплексные числа в виде $z = a + bj$, где $j^2 = -2$. Получится всё то же самое, в частности, операции тоже возникают сами собой, из раскрытия скобок:

$$(a_1 + b_1 j) + (a_2 + b_2 j) = (a_1 + a_2) + (b_1 + b_2)j,$$
$$(a_1 + b_1 j) \cdot (a_2 + b_2 j) = (a_1 a_2 + b_1 b_2(-2)) + (a_1 b_2 + a_2 b_1)j.$$

Отличие возникает только в одном месте, где приходится считать j^2. Формулой для обратного элемента будет

$$(a + bj)^{-1} = \frac{a}{a^2 + 2b^2} + \frac{-b}{a^2 + 2b^2}j,$$

и так как $a^2 + 2b^2 \neq 0$ как только $(a, b) \neq (0, 0)$, то никаких проблем не возникает.

Задача 3. Проверьте, что можно построить квадратичное расширение простого поля из 5 элементов, рассматривая числа $a+bj$, где $j^2=-2$. Все четыре действия арифметики будут корректно определены.

Давайте будем использовать такое определение: скажем, что элемент a в «арифметике по модулю p», где p — простое число, является отрицательным, если уравнение $x^2 =_{(p)} a$ не имеет решений, и положительным в противном случае (если при этом $a \neq_{(p)} 0$). Например, по модулю 5 числа 1 и 4 положительные, а 2 и 3 — отрицательные. Так как $-1 =_{(5)} 4$, то число -1 тоже положительное, так уж получается. Зато по модулю 7 числа 1, 2, 4 положительные, а -1, -2 и -4, или 6, 5 и 3, отрицательные. То, что нам естественно назвать «знаком элемента», исторически называется символом Лежандра $\left(\frac{a}{p}\right)$. По определению

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{если } a \text{ положительно по модулю } p, \\ -1, & \text{если } a \text{ отрицательно по модулю } p, \\ 0, & \text{если } a =_{(p)} 0. \end{cases}$$

Можно проверить, что для нечётного простого числа p ровно половина (т.е. $\frac{p-1}{2}$) ненулевых чисел по модулю p положительна и ровно половина отрицательна и что произведение двух отрицательных всегда положительно.

Задача 4. Докажите, что если $\left(\frac{a}{p}\right) = -1$ и $\left(\frac{b}{p}\right) = -1$, то $\left(\frac{ab}{p}\right) = +1$.

Задача 5. Проверьте, что если t отрицательно по модулю p, то числа $a+bj$, где $j^2=t$, определяют квадратичное расширение простого поля из p элементов (где все четыре действия арифметики корректно определены).

Главное приложение вышесказанного для нас в следующем. Пусть p — простое число и число 5 отрицательно по модулю p. Тогда числа $\alpha = \frac{1+\sqrt{5}}{2}$ и $\beta = \frac{1-\sqrt{5}}{2}$ определены как комплексные числа по модулю p (как элементы квадратичного расширения) и формулы (2) и (3) для чисел Лукаса и Фибоначчи сохраняют смысл в комплексных числах по модулю p.

4. Комплексное сопряжение для чисел по модулю p

Существенной составляющей структуры обычных комплексных чисел является операция комплексного сопряжения: если $z=a+bi$, то $\bar{z}=a-bi$. Мы знаем, что сопряжённое суммы есть сумма сопряжённых и то же для

произведения:

$$\overline{(z_1 + z_2)} = \bar{z}_1 + \bar{z}_2, \quad \overline{(z_1 \cdot z_2)} = \bar{z}_1 \cdot \bar{z}_2.$$

Отсюда легко заключить, что если α есть комплексный корень уравнения с действительными коэффициентами:

$$x^2 + ax + b = 0,$$

то $\bar{\alpha}$ тоже будет корнем этого уравнения.

Мы можем определить сопряжение и в квадратичном расширении поля из p элементов формулой

$$\overline{(a + bj)} \stackrel{\text{def}}{=} a - bj.$$

Ясно, что сопряжённое суммы есть сумма сопряжённых, сопряжённое произведения есть произведение сопряжённых. Кроме того, имеет место следующая замечательная формула.

Пусть p — простое число и t отрицательно по модулю p, т. е. $\left(\frac{t}{p}\right) = -1$. Построим комплексные числа как числа вида $a + bj$, где a и b рассматриваются по модулю p и $j^2 = t$.

Предложение 1. *В этих условиях если $z = a + bj$ и $\bar{z} = a - bj$, то*

$$\bar{z} = z^p. \tag{4}$$

Отсюда следует, что $z^{p+1} = z\bar{z} = a^2 - tb^2$, т. е. $(p+1)$-я степень «комплексного» числа обязательно будет «действительным» числом.

Для доказательства формулы (4) давайте вспомним, что для наших чисел

$$(x + y)^p =_{(p)} x^p + y^p.$$

Это следует из того, что коэффициенты бинома Ньютона, $\binom{p}{i} = \frac{p!}{i!(p-i)!}$, являются целыми числами, делящимися на p при $0 < i < p$. Тогда мы можем написать

$$(a + bj)^p =_{(p)} a^p + b^p j^p.$$

Используя малую теорему Ферма, мы заключаем, что $a^p =_{(p)} a$, $b^p =_{(p)} b$. Остаётся вычислить j^p. Конечно,

$$j^p = j^{p-1} \cdot j = t^{(p-1)/2} \cdot j.$$

Нам нужно показать, что для отрицательного элемента t выполняется равенство $t^{(p-1)/2} =_{(p)} -1$. Отметим, что число $\frac{p-1}{2}$ целое, и если s является положительным элементом, то $s = a^2$ и

$$s^{(p-1)/2} =_{(p)} a^{p-1} =_{(p)} 1,$$

где последнее равенство следует из теоремы Ферма. Тем самым положительные элементы предоставляют нам $\frac{p-1}{2}$ корней полиномиального уравнения

$$x^{(p-1)/2} = 1$$

в поле «элементов по модулю p». Полиномиальное уравнение, по теореме Безу, не может иметь больше корней, чем его степень, и тем самым для отрицательного элемента t имеем

$$t^{(p-1)/2} \neq_{(p)} 1.$$

В то же время $t^{p-1} =_{(p)} 1$, и так как

$$t^{p-1} - 1 =_{(p)} \left(t^{(p-1)/2} - 1\right)\left(t^{(p-1)/2} + 1\right),$$

то остаётся единственная возможность: $t^{(p-1)/2} =_{(p)} -1$. Это завершает доказательство формулы (4).

Следствие. *Пусть p простое и 5 отрицательно по модулю p. Тогда для $\alpha = \frac{1+\sqrt{5}}{2}$ и $\beta = \frac{1-\sqrt{5}}{2}$ имеем:*

1) $\alpha^p =_{(p)} \beta$, $\beta^p =_{(p)} \alpha$;

2) $\alpha^{p+1} =_{(p)} \beta^{p+1} =_{(p)} \alpha \cdot \beta =_{(p)} -1$.

Мы можем применить этот результат к числам Фибоначчи и Лукаса. В этих условиях получаем:

$$u_{p+1} = \frac{\alpha^{p+1} - \beta^{p+1}}{\alpha - \beta} \equiv 0 \pmod{p};$$

$$v_p = \alpha^p + \beta^p \equiv \alpha + \beta \equiv 1 \pmod{p}.$$

Чтобы пользоваться этими сравнениями, нам надо уметь определять, для каких p число «5» будет положительным и для каких отрицательным по модулю p. Сейчас мы попробуем в этом разобраться.

5. Квадратный корень из 5 по модулю p

Свойство, которое я хочу сейчас сформулировать, легко следует из более общих и довольно глубоких результатов о символе Лежандра, которые объединяются под названием квадратичного закона взаимности[2)]. Нам нужен только частный случай этого общего закона, обнаруженного Эйлером и Лежандром, доказанного Гауссом и являющегося одной из жемчужин «элементарной» теории чисел.

[2)] См. статью В. В. Прасолова, сс. 140–144. — *Прим. ред.*

Предложение 2.

$$\left(\frac{5}{p}\right) = \begin{cases} +1, & \text{если } p \equiv \pm 1 \pmod 5, \\ -1, & \text{если } p \equiv \pm 2 \pmod 5. \end{cases}$$

Сначала две общих леммы.

Лемма (Лежандр).

$$a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod p.$$

Фактически это значит, что $(p-1)/2$-я степень a по модулю p равна $+1$ для положительных a и -1 для отрицательных a. Это мы разобрали в предыдущем пункте.

Заметим, что любое ненулевое число по модулю p равно с точностью до знака одному из чисел $1, 2, \ldots, \frac{p-1}{2}$. Если обозначить через $\mathcal{P}$ множество этих чисел:

$$\mathcal{P} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\},$$

то для любого ненулевого x по модулю p либо $x \in \mathcal{P}$, либо $-x \in \mathcal{P}$. Фиксируем p и некоторое $a \neq_{(p)} 0$.

Лемма (Гаусс). *Пусть для* $k = 1, 2, \ldots, \frac{p-1}{2}$ *число* ε_k *равно* $+1$ *или* -1 *и выбрано так, что* $a \cdot k \cdot \varepsilon_k \in \mathcal{P}$ *по модулю* p. *Тогда*

$$\left(\frac{a}{p}\right) = \prod_{k=1}^{(p-1)/2} \varepsilon_k.$$

Действительно, во-первых заметим, что если числа k' и k'' различны, то произведения $a \cdot k' \cdot \varepsilon_{k'}$ и $a \cdot k'' \cdot \varepsilon_{k''}$ тоже будут различны. Они могли бы совпадать только если $a \cdot k' =_{(p)} a \cdot k''$ или $a \cdot k' =_{(p)} -a \cdot k''$, но и первое и второе невозможно. Значит, когда k пробегает всё множество $\mathcal{P}$, то и произведение $a \cdot k \cdot \varepsilon_k$ пробегает всё $\mathcal{P}$. Пусть K есть произведение всех элементов из $\mathcal{P}$. Мы имеем:

$$K = \prod_{k=1}^{(p-1)/2} a \cdot k \cdot \varepsilon_k =_{(p)} a^{(p-1)/2} \cdot K \cdot \prod_{k=1}^{(p-1)/2} \varepsilon_k.$$

Сокращая на K, получаем, что $1 =_{(p)} a^{(p-1)/2} \cdot \prod_{k=1}^{(p-1)/2} \varepsilon_k$, что с учётом леммы Лежандра доказывает лемму Гаусса.

Замечание. Можно сказать, что мы здесь моделируем одно из известных доказательств малой теоремы Ферма.

Теперь мы можем обратиться к предложению 2. У нас будет $a=5$. Для нечётного p

$$p \equiv \pm 1 \pmod 5 \iff p = 10n+1 \text{ или } p = 10n+9,$$

$$p \equiv \pm 2 \pmod 5 \iff p = 10n+3 \text{ или } p = 10n+7.$$

Давайте применим лемму Гаусса для $p=10n+1$. Здесь $\frac{p-1}{2} = 5n$, и нам нужны $k = 1, 2, \ldots, 5n$.

k	$5k$	ε_k
$1, 2, \ldots, n$	$5, 10, \ldots, 5n$	$+1$
$n+1, \ldots, 2n$	$5n+1, \ldots, 10n$	-1
$2n+1, \ldots, 3n$	$(10n+1)+4, \ldots, (10n+1)+5(n-1)+4$	$+1$
$3n+1, \ldots, 4n$		-1
$4n+1, \ldots, 5n$		$+1$

Тем самым -1 встречается $2n$ раз и $\prod \varepsilon_k = +1$. Т.е. если $p=10n+1$, то $\left(\dfrac{5}{p}\right) = +1$.

Для случая $p=10n+3$ можно рассуждать совершенно аналогично. Здесь $\frac{p-1}{2} = 5n+1$.

k	$5k$	ε_k
$1, 2, \ldots, n$		$+1$
$n+1, \ldots, 2n$		-1
$2n+1, \ldots, 3n$		$+1$
$3n+1, \ldots, 4n$		-1
$4n+1$	$20n+5 = (10n+3)+(10n+2)$	-1
$4n+2, \ldots, 5n+1$		$+1$

В результате мы получаем на один элемент -1 больше, всего $2n+1$ минус единиц, а значит, $\left(\dfrac{5}{p}\right) = -1$ в этом случае. Мы предоставляем читателям самостоятельно проверить два оставшихся случая и будем считать предложение 2 доказанным.

6. Доказательство основной теоремы

Возвращаясь к доказательству основной теоремы, сформулированной в конце раздела 2, заметим прежде всего, что мы можем вычислить значение $M \pmod 5$. Мы знаем, что $2^4 \equiv 1 \pmod 5$ и что

$$M = 2^q - 1 = 2^{4k+3} - 1 \equiv 2^3 - 1 \equiv 2 \pmod 5.$$

Запомним это: в условиях теоремы $M \equiv 2 \pmod 5$.

Предположим теперь, что M — простое число. Тогда $\left(\frac{5}{M}\right) = -1$ и мы можем применить предложение 1 и следствие из пункта 4. В частности,

$$\alpha^{M+1} \equiv \beta^{M+1} \equiv -1 \pmod{M},$$

а значит, $v_{M+1} \equiv -2 \pmod{M}$.

Пусть $N = 2^{q-1} = \frac{M+1}{2}$, т. е. $M + 1 = 2N$. Заметим, что

$$(v_N)^2 = (\alpha^N + \beta^N)^2 = \alpha^{2N} + \beta^{2N} + 2(\alpha\beta)^N = v_{2N} + 2 \cdot (-1)^N. \qquad (5)$$

В нашем случае N чётно, значит,

$$(v_N)^2 = v_{2N} + 2 \equiv -2 + 2 \equiv 0 \pmod{M}.$$

Тем самым мы получили утверждение теоремы в этом случае.

Обратно, пусть известно, что $v_N \equiv 0 \pmod{M}$. Надо доказать, что число M простое. Во всяком случае, мы можем утверждать (поскольку $M \equiv 2 \pmod 5$), что не все простые делители p числа M имеют вид $p \equiv \pm 1 \pmod 5$; найдётся простой делитель p числа M, для которого $p \equiv \pm 2 \pmod 5$, и тем самым $\left(\frac{5}{p}\right) = -1$, поэтому число 5 отрицательно по модулю p и мы можем использовать результаты пункта 4. В частности, $\alpha^{p+1} =_{(p)} \beta^{p+1} =_{(p)} -1$. В то же время p делит M, значит,

$$v_N = \alpha^N + \beta^N =_{(p)} 0.$$

Пусть $\varepsilon = \alpha/\beta$. Тогда мы получим, с одной стороны,

$$\varepsilon^N =_{(p)} -1, \qquad (6)$$

а с другой стороны, $\varepsilon^{p+1} =_{(p)} 1$.

Из равенства (6) следует, что $\varepsilon^{2N} = \varepsilon^{2^q} =_{(p)} +1$.

Лемма. *Пусть* $\varepsilon^a =_{(p)} 1$ *и* $\varepsilon^b =_{(p)} 1$. *Используя деление с остатком, запишем* $a =_{(p)} bc + r$. *Тогда* $\varepsilon^r =_{(p)} 1$.

Действительно, $1 =_{(p)} \varepsilon^a =_{(p)} (\varepsilon^b)^c \varepsilon^r =_{(p)} 1 \cdot \varepsilon^r =_{(p)} \varepsilon^r$.

Повторяя это рассуждение, получим, что $\varepsilon^d = 1$, где d — наибольший общий делитель для a и b. В нашем случае это означает, что

$$\varepsilon^d =_{(p)} 1, \text{ где } d = \text{НОД}(2^q, p+1).$$

Теперь либо $p + 1 = 2^q$, т. е. $p = M$ и M — простое число, либо $p + 1 < 2^q$. Во втором случае $d = 2^s$, где $s < q$. Тогда d делит $N = 2^{q-1}$, значит, $\varepsilon^N = (\varepsilon^d)^{N/d} =_{(p)} 1$, что противоречит равенству (6). Теорема 1 доказана.

Таким образом, простота числа $M = 2^q - 1$ зависит от значения числа $v_{2^{q-1}}$ по модулю M.

Замечательным образом мы можем использовать формулу (5) для вычисления чисел v_{2^i}. Обозначим $r_i = v_{2^i}$. Тогда $r_0 = v_1 = 1$. Теперь из формулы (5) имеем: $r_1 = r_0^2 + 2 = 3$ (здесь N нечётно). При $i \geqslant 1$ мы применяем формулу (5) с чётным N:

$$r_{i+1} = r_i^2 - 2, \quad r_1 = 3.$$

И наш основной результат принимает следующий вид.

Теорема 2. *Если q — простое число вида $4k+3$, то число $M = 2^q - 1$ простое если и только если $r_{q-1} \equiv 0 \pmod{M}$.*

7. Организация вычислений. Примеры

Вычисление r_i удобно производить в двоичной записи: $r_1 = 11$ (в двоичной системе).

Таким образом, $r_2 = 111$, т.е. 7 в десятичной системе.

Для r_2 получаем:

$$\begin{array}{rcccc}
 & & 1 & 1 & \\
 & \times & 1 & 1 & \\
\hline
 & & 1 & 1 & \\
+ & 1 & 1 & & \\
\hline
 & - & 1 & 0 & \\
\hline
r_2 = & 1 & 1 & 1 &
\end{array}$$

Для r_3:

$$\begin{array}{rccccccc}
 & & & & 1 & 1 & 1 & \\
 & \times & & & 1 & 1 & 1 & \\
\hline
 & & & & 1 & 1 & 1 & \\
 & & & 1 & 1 & 1 & & \\
 & & 1 & 1 & 1 & & & \\
\hline
 & - & & & & 1 & 0 & \\
\hline
r_3 = & 1 & 0 & 1 & 1 & 1 & 1 &
\end{array}$$

Итак, $r_3 = 101111$, т.е. 47 в десятичной системе.

Здесь мы уже видим один случай нашей теоремы: при $q = 3$, $M = 7$ — простое, и как раз $r_2 = 7 \equiv 0 \pmod{7}$.

Следующим q будет $q = 7$, $M = 2^7 - 1 = 127$. Конечно, можно использовать обычные деления для анализа простоты числа 127, но посмотрим, как работает алгоритм.

Нам надо посчитать r_4, r_5 и $r_6 \pmod{127}$. Приятно заметить, что мы можем производить редукцию по модулю 127 уже в процессе вычислений, и она соответствует «сдвигу двоичной записи» на 7 единиц:

$$2^7 \equiv 1 \pmod{2^7-1}, \text{ значит, } 2^{7+k} \equiv 2^k \pmod{2^7-1}.$$

Тем самым r_4 по модулю 127 можно считать следующим образом:

$$\begin{array}{rcccc:ccccccc}
 & & & & & & 1 & 0 & 1 & 1 & 1 & 1 \\
 & & & & & 1 & 0 & 1 & 1 & 1 & 1 & \\
+ & & & & 1 & 0 & 1 & 1 & 1 & 1 & & \\
 & & & 1 & 0 & 1 & 1 & 1 & 1 & & & \\
1 & 0 & 1 & 1 & & 1 & 1 & & & & & \\
\hline
- & & & & & & & & & & 1 & 0
\end{array}$$

После переноса получаем

$$\begin{array}{c:ccccccc}
 & 1 & 0 & 1 & 1 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & \mathbf{1} \\
1 & 1 & 1 & 1 & 0 & \mathbf{1} & \mathbf{0} \\
1 & 1 & 0 & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\
\hline
- & & & & & 1 & 0
\end{array}$$

Теперь мы должны считать «циклически» — перенося любую вылезающую влево за 7 разрядов единичку направо. Получаем:

$$\begin{array}{rccccccc}
 & & 1 & 0 & 1 & 1 & 0 & 1 \\
 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\
+ & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\
 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\
\hline
 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
 & & 1 & & 1 & 1 & 1 & 1 \\
 & & & & & & & 1 \\
\hline
 & 1 & & 1 & 1 & 1 & 1 & 1 \\
 & 1 & & 1 & & & & \\
\hline
 & 0 & 1 & 1 & 0 & 0 & 0 & 0
\end{array}$$

Таким образом, $r_4 \equiv 0110000 \pmod{127}$.

Теперь для r_5:

$$\begin{array}{rccccccc}
+ & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
\hline
 & 0 & 0 & 1 & 0 & 0 & 0 & 0
\end{array}$$

То есть $r_5 \equiv 2^4 \pmod{127}$. Теперь $r_6 \equiv 2^8 - 2 \equiv 2 - 2 \equiv 0 \pmod{127}$. Тем самым 127 — простое число.

Аналогичным образом было посчитано, что число $M = 2^{127} - 1$ простое. Только тут надо было осуществлять циклические сложения двоичных чисел длины 127. Как объясняет Вильямс [3], Лукас сделал себе шахматную доску и записывал числа по линиям этой доски, расставляя ладьи на местах единиц и оставляя пустыми клетки нулей. Циклические сложения можно тогда осуществлять как «игру», следуя нескольким простым правилам. Потребовалось примерно 100 часов такой игры, чтобы вычислить r_{127} по модулю $2^{127} - 1$.

Список литературы

[1] *Bruce J. W.* A really trivial proof of the Lucas–Lehmer test // Amer. Math. Monthly, 1993. Vol. 100. P. 370–371.

[2] *Rosen M. I.* A proof of the Lucas–Lehmer test // Amer. Math. Monthly, 1988. Vol. 95. P. 855–856.

[3] *Williams H. C.* Édouard Lucas and primality testing. Canadian Math. Soc. Monographs, vol. 22. Wiley–Interscience Publications, 1998.

Доказательство квадратичного закона взаимности по Золотарёву

В. В. Прасолов

Квадратичный закон взаимности выражает связь между следующими двумя свойствами простых чисел p и q:

- ▷ число p сравнимо с некоторым квадратом целого числа по модулю q,
- ▷ число q сравнимо с некоторым квадратом целого числа по модулю p.

Первым эту связь обнаружил Эйлер и высказал соответствующую гипотезу, которую в некоторых частных случаях доказал Лежандр, а первое полное доказательство получил Гаусс. Сейчас известно много разных доказательств квадратичного закона взаимности. Одно из наиболее простых доказательств предложил в 1872 г. известный русский математик Егор Иванович Золотарёв[1)]. Его статья [12] опубликована по-французски. Идея Золотарёва обсуждалась довольно часто, но только в работах иностранных авторов (см. список литературы в конце статьи).

Для полноты мы докажем китайскую теорему об остатках, но следующие более элементарные сведения о сравнениях предполагаются известными:

- ▷ если числа m и n взаимно просты, то для любого целого числа a разрешимо сравнение $mx \equiv a \pmod{n}$,
- ▷ если p — простое, то для любого целого числа $a \not\equiv 0 \pmod{p}$ формула $x \bmod p \mapsto ax \bmod p$ задаёт перестановку множества $\{1, 2, \ldots, p-1\}$.

Несложно показать, что если p — простое число, то $a^p \equiv a \pmod{p}$ (*малая теорема Ферма*). Действительно, интересен лишь случай, когда $a \not\equiv 0 \pmod{p}$. В этом случае формула $x \bmod p \mapsto ax \bmod p$ задаёт перестановку множества $\{1, 2, \ldots, p-1\}$. Следовательно,

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv a \cdot (2a) \cdot \ldots \cdot (p-1)a \equiv a^{p-1}\bigl(1 \cdot 2 \cdot \ldots \cdot (p-1)\bigr) \pmod{p}.$$

После сокращения получаем $1 \equiv a^{p-1} \pmod{p}$.

[1)] Золотарёв (1847–1878) прожил только 31 год, но и за это короткое время он уже успел написать ряд работ первостепенной важности. 26 июня 1878 г. Золотарёв поехал на поезде на дачу к знакомым. На промежуточной станции он вышел из вагона и, когда поезд тронулся, попал под паровоз. Его извлекли из-под колес со смятой ступней и переломанной выше колена ногой. Он скончался после 12 дней тяжелых страданий.

Доказательство малой теоремы Ферма достаточно хорошо известно, но мы сочли нужным его напомнить, потому что оно имеет много общего с основной идеей Золотарёва.

1. Китайская теорема об остатках

Теорема 1. *Пусть числа $m_1, \ldots, m_k$ попарно взаимно простые и $m = m_1 \cdot \ldots \cdot m_k$. Тогда для любых целых чисел $a_1, \ldots, a_k$ система сравнений $x \equiv a_i \pmod{m_i}$, $i = 1, \ldots, k$, имеет решение, причём если x_1 и x_2 — два решения, то $x_1 - x_2$ делится на m.*

Доказательство. Положим $n_i = m/m_i$. Число n_i является произведением чисел, взаимно простых с m_i, поэтому $(n_i, m_i) = 1$. В таком случае можно выбрать целые числа r_i и s_i так, что $r_i m_i + s_i n_i = 1$. Положим $e_i = s_i n_i$ и $x = a_1 e_1 + \cdots + a_k e_k$. Ясно, что $e_i \equiv 1 \pmod{m_i}$ и $e_i \equiv 0 \pmod{m_j}$ при $j \neq i$, поэтому $x \equiv a_i \pmod{m_i}$, $i = 1, \ldots, k$.

Если x_1 и x_2 — решения рассматриваемой системы сравнений, то $x_1 - x_2 \equiv 0 \pmod{m_i}$, $i = 1, \ldots, k$. Числа $m_1, \ldots, m_k$ попарно взаимно простые, поэтому $x_1 - x_2$ делится на m.

2. Квадратичные вычеты и невычеты

Пусть p — простое число. Число a, не делящееся на p, называют *квадратичным вычетом* по модулю p, если $x^2 \equiv a \pmod{p}$ для некоторого целого числа x; в противном случае число a называют *квадратичным невычетом*.

Для простого числа p *символ Лежандра* $\left(\dfrac{a}{p}\right)$ определяется следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \text{ делится на } p, \\ 1, & \text{если } a \text{ — квадратичный вычет}, \\ -1, & \text{если } a \text{ — квадратичный невычет}. \end{cases}$$

Символ Лежандра мы иногда будем обозначать (a/p).

Теорема 2 (Лежандр). *Пусть p — нечётное простое число. Тогда*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Доказательство. Пусть $\mathbb{F}_p$ — поле вычетов по модулю p, обозначим $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$. Рассмотрим отображение $\mathbb{F}_p^* \to \mathbb{F}_p^*$, заданное формулой $x \mapsto x^2$. Прообраз каждого элемента либо пуст, либо состоит из двух элементов x и $-x$, поэтому образ состоит из $(p-1)/2$ элементов. С другой стороны, если $a = x^2$, то $a^{(p-1)/2} = x^{p-1} = 1$, поэтому все элементы образа

являются корнями уравнения $X^{(p-1)/2}=1$, которое не может иметь более $(p-1)/2$ корней. Остаётся заметить, что все элементы $\mathbb{F}_p^*$ являются корнями уравнения $X^{p-1}=1$, поэтому невычеты являются корнями уравнения $X^{(p-1)/2}=-1$.

Следствие 1. $\left(\dfrac{ab}{p}\right)=\left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$.

Следствие 2.

$$\left(\frac{-1}{p}\right)=\begin{cases}1 & \text{при } p=4k+1,\\ -1 & \text{при } p=4k+3.\end{cases}$$

Обобщением символа Лежандра является *символ Якоби*, который обозначается точно так же и определяется следующим образом. Пусть $m=p_1\cdot\ldots\cdot p_k$, где $p_1,\ldots,p_k$ нечётные простые числа (не обязательно различные). Тогда

$$\left(\frac{a}{m}\right)=\left(\frac{a}{p_1}\right)\cdot\ldots\cdot\left(\frac{a}{p_k}\right).$$

Пример. $\left(\dfrac{2}{15}\right)=\left(\dfrac{2}{3}\right)\left(\dfrac{2}{5}\right)=(-1)(-1)=1$, *но* $2\not\equiv x^2 \pmod{15}$.

Золотарёв предложил следующую интерпретацию символа Лежандра, которую затем Фробениус [4] перенёс и на символ Якоби.

Теорема 3 (Золотарёв – Фробениус). *Пусть m — нечётное число, a — число, взаимно простое с m, и $\pi_{a,m}: i\mapsto ai \bmod m$ — подстановка на множестве остатков от деления на m. Тогда* $\operatorname{sgn}\pi_{a,m}=(a/m)$, *где* $\operatorname{sgn}\pi_{a,m}$ — *знак подстановки* $\pi_{a,m}$.

Доказательство. Рассмотрим многочлен

$$A(x_1,\ldots,x_m)=\prod_{1\leqslant i<j\leqslant m}(x_i-x_j).$$

Под действием чётной подстановки многочлен A не изменяется, а под действием нечётной подстановки он изменяет знак. Поэтому знак любой подстановки σ равен отношению $A(x_{\sigma(1)},\ldots,x_{\sigma(m)})$ к $A(x_1,\ldots,x_m)$. Положим $x_1=1,\ldots,x_m=m$. Тогда

$$\begin{aligned}\operatorname{sgn}\pi_{a,m} &= \prod_{1\leqslant i<j\leqslant m}\frac{\pi_{a,m}(i)-\pi_{a,m}(j)}{i-j}\equiv\prod_{1\leqslant i<j\leqslant m}\frac{ai-aj}{i-j}\equiv\\ &\equiv \prod_{1\leqslant i<j\leqslant m}a\equiv a^{m(m-1)/2}\pmod m.\end{aligned}$$

Учитывая, что $a^m\equiv a \pmod m$, получаем

$$\operatorname{sgn}\pi_{a,m}\equiv a^{(m-1)/2}\equiv(a/m)\pmod m.$$

3. Квадратичный закон взаимности

Теорема 4 (квадратичный закон взаимности). *Пусть m и n — нечётные взаимно простые числа. Тогда*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

Доказательство. [11] Пусть $P = \{0, 1, \ldots, mn-1\}$ и $\overline{P} = \{\,(a,b) \mid 0 \leqslant a < m,\ 0 \leqslant b < n\}$. Согласно китайской теореме об остатках отображение $c \mapsto \bar{c} = (c \bmod m, c \bmod n)$ является взаимно однозначным отображением P на $\overline{P}$.

Рассмотрим отображения $\mu, \nu\colon \overline{P} \to \overline{P}$, заданные формулами $\mu(a,b) = \overline{a+mb}$ и $\nu(a,b) = \overline{na+b}$. Ясно, что $\mu(a,b) = (a,\ a+mb \bmod n)$, поэтому отображение μ переставляет элементы вида (a_0, b), где a_0 фиксировано. Следовательно, μ — подстановка множества $\overline{P}$ и $\operatorname{sgn}\mu = \left(\frac{m}{n}\right)^m = \left(\frac{m}{n}\right)$. Аналогично $\operatorname{sgn}\nu = \left(\frac{n}{m}\right)$.

Рассмотрим теперь на множестве P подстановку $\nu^{-1}\mu\colon na+b \mapsto a+mb$. Знак этой подстановки равен $(-1)^k$, где k — количество пар элементов множества $\overline{P}$, для которых выполняются неравенства $na+b > na'+b'$ и $a+mb < a'+mb'$. По условию $|b-b'| < n$ и $|a-a'| < m$, поэтому приходим к следующим неравенствам: $a > a'$ и $b < b'$. Таким образом, $k = \binom{n}{2}\binom{m}{2} = \frac{m-1}{2}\cdot\frac{n-1}{2}$. В итоге получаем

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \operatorname{sgn}\mu\operatorname{sgn}\nu = \operatorname{sgn}\nu^{-1}\mu = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

Следствие. *Пусть m — нечётное число. Тогда*

$$\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}.$$

Доказательство. При $m = 3$ требуемое равенство легко проверяется. Предположим, что $m \geqslant 3$ — нечётное натуральное число, для которого выполняется требуемое равенство. Тогда

$$\begin{aligned}\left(\frac{2}{m+2}\right) &= \left(\frac{-1}{m+2}\right)\left(\frac{m}{m+2}\right) = (-1)^{\frac{m+1}{2}}(-1)^{\frac{m-1}{2}\cdot\frac{m+1}{2}}\left(\frac{m+2}{m}\right) = \\ &= (-1)^{\frac{m+1}{2}}\left(\frac{2}{m}\right) = (-1)^{\frac{m+1}{2}}(-1)^{\frac{m^2-1}{8}} = (-1)^{\frac{(m+2)^2-1}{8}}.\end{aligned}$$

Отметим, что как правило в учебниках по теории чисел сначала доказывают равенство $\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}$, а уже затем доказывают квадратичный закон взаимности. Но это равенство не требует отдельного доказательства, оно следует из квадратичного закона взаимности.

Список литературы

[1] *Brenner J. L.* Zolotarev's theorem on the Legendre symbol // Pacific J. Math., 1973. Vol. 45. P. 413–414.

[2] *Cartier P.* Sur unegénéralization des symboles de Legendre–Jacobi // L'Ens. Math., 1970. Vol. 16. P. 31–48.

[3] *Dressler R. E., Shult E. E.* A simple proof of the Zolotareff–Frobenius theorem // Proc. Amer. Math. Soc., 1975. Vol. 54. P. 53–54.

[4] *Frobenius G.* Über das quadratische Reziprozitätsgesetz, I. S.-B. Preuss. Akad. Wiss., Berlin, 1914, P. 335–349.

[5] *Lehmer D. H.* The characters of linear permutations // Linear and Multilinear Algebra, 1976. Vol. 4. P. 1–16.

[6] *Lerch M.* Sur un thórème arithmetique de Zolotarev // Česka Acad., Bull. Int. Cl. Math., 1986. Vol. 3. P. 34–37.

[7] *Morton P.* A generalization of Zolotarev's theorem // Amer. Math. Monthly, 1979. Vol. 86. P. 374–376.

[8] *Riesz M.* Sur le lemme de Zolotareff et sur la loi de réciprocité des restes quadratiques // Math. Scand., 1953. Vol. 1. P. 159–169.

[9] *Rousseau G.* Exterior algebras and the quadratic reciprocity law // L'Ens. Math., 1990. Vol. 36. P. 303–308.

[10] *Rousseau G.* On the quadratic reciprocity law // J. Austral. Math. Soc. (Series A), 1991. Vol. 51. P. 423–425.

[11] *Rousseau G.* On the Jacobi symbol // J. Number Theory, 1994. Vol. 48. P. 109–111.

[12] *Zolotareff G.* Nouvelle démonstration de la loi de réciprocité de Legendre // Nouv. Ann. Math. (2), 1872. Vol. 11. P. 354–362.

Два замечательных предела

Ю. И. Любич

1. Введение

По давно установившейся традиции «первым замечательным пределом» называют

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

а «второй замечательный предел» — это

$$\lim_{x\to 0}(1+x)^{\frac{1}{x}}. \tag{2}$$

Второй замечательный предел замечателен не только тем, что он существует, но и тем, что его величина — это знаменитое *неперово число* $e = 2{,}71828\ldots$ (названное так в честь Джона Непера (1550-1617), который изобрел логарифмы[1)]). Что касается первого замечательного предела, то, как известно, он *равен единице, но при условии, что угол x измеряется в радианах*. А это значит, что и он связан с другим не менее замечательным числом — *архимедовым числом* π (π — отношение длины любой окружности к ее диаметру, одно и то же для всех окружностей по соображениям подобия). Эта величина встречалась в древних текстах намного раньше Архимеда (287 – 212 до н.э.), но ее приближенное значение $\frac{22}{7} = 3{,}142\ldots$, найденное Архимедом, долгое время оставалось непревзойденным по точности (напомним, что $\pi = 3{,}1415\ldots$), не говоря уже о том, что π регулярно появлялось у Архимеда в его обширных вычислениях площадей и объемов. (Эти вычисления представляют собой прототип современного интегрального исчисления.)

Как изменится величина первого замечательного предела, если изменить угловой масштаб, т.е. произвести *скейлинг*, как любят сейчас говорить физики и некоторые математики? Если, например, угол α

[1)] Обозначение e было введено Эйлером в 1736 г. Название «неперово число» не вполне оправдано: Непер при построении таблиц логарифмов, опубликованных в 1614 г., в качестве основания использовал число $0{,}9999999^{10000000}$, очень близкое к числу $1/e$, но не равное ему. — *Прим. ред.*

измеряется в градусах, то $\alpha = 180x/\pi$, где x — радианная мера угла, и тогда

$$\lim_{\alpha\to 0}\frac{\sin\alpha}{\alpha} = \frac{\pi}{180}\lim_{x\to 0}\frac{\sin x}{x} = \frac{\pi}{180}. \tag{3}$$

Если же, вообще, в некотором масштабе $\alpha = kx$, где k — постоянный положительный коэффициент, то

$$\lim_{\alpha\to 0}\frac{\sin\alpha}{\alpha} = \frac{1}{k}. \tag{4}$$

Формальное несоответствие между (3) и (4) бросается в глаза читателю, твердо помнящему теорему единственности предела. Но объясняется оно тем, что, изменяя угловой масштаб, мы продолжаем считать синус функцией угла как геометрической фигуры независимо от выбора масштаба. Такова традиция в элементарной геометрии, где синус острого угла в прямоугольном треугольнике определяется как отношение соответствующего катета к гипотенузе (одно и то же для всех таких треугольников с данным углом — по соображениям подобия). Однако отношение синуса к самому углу лишено смысла, пока не выбран угловой масштаб. В математическом анализе, в отличие от элементарной геометрии, синус рассматривается как функция числового аргумента — радианной меры угла. Стандартное доказательство существования первого замечательного предела (и его равенства единице) основано на геометрическом неравенстве $\sin x < x < \operatorname{tg} x$, справедливом именно в этом масштабе. Тем самым, это доказательство нуждается в достаточно сложном понятии длины окружности[2)]. (Отметим, что общее понятие длины кривой, по существу, относится к интегральному исчислению). Оказывается, идея скейлинга (это понятие обсуждается далее) приводит к совсем другому доказательству, хотя и более длинному, но более элементарному в том смысле, что оно не зависит от понятия длины кривой. Угловой масштаб в этом доказательстве остается произвольным, величина предела зависит от выбора масштаба (см. (4)). На этом пути радиан можно определить как тот масштаб, для которого первый замечательный предел равен единице. А тогда и число π можно *определить* поновому, а именно, как удвоенную радианную меру прямого угла. Если теперь определить длину окружности обычным образом (или применить к этому случаю общее определение длины кривой и соответствующую формулу интегрального исчисления) то, конечно, длина окружности радиуса R окажется равной $2\pi R$ и, вообще, длина дуги окружности с центральным углом x радиан окажется равной $l = xR$. В конечном счете, мы приходим к обычной формуле для радианной меры угла: $x = l/R$.

[2)] Это замечание, послужившее автору толчком к написанию настоящей статьи, принадлежит Адаму Эпштейну из Университета штата Нью-Йорк.

В частности, радиан, определенный выше, оказывается обычным радианом, т. е. углом, для которого длина соответствующей дуги окружности равна радиусу.

Весь этот план реализуется ниже и, более того, скейлинговый подход распространяется на второй замечательный предел, точнее, на эквивалентную ситуацию, связанную с величиной

$$l(a) = \lim_{x \to 0} \frac{a^x - 1}{x} \quad (a > 1). \tag{5}$$

В этом контексте число e определяется как то значение a, для которого $l(a) = 1$. Оказывается, что величина $a^{1/l(a)}$ не зависит от a и равна e. Это легко следует из (5), если известно, что $l(a) \neq 0$, однако доказательство последнего неравенства не вполне тривиально. В заключение мы рассматриваем показательную функцию e^z комплексного переменного z, в результате чего происходит естественное объединение первого и второго замечательного предела.

2. Скейлинг и выпуклые функции

Будем говорить, что функция f, заданная на некотором интервале $(0, \varepsilon)$ вещественной оси, *подчиняется скейлингу*, если она удовлетворяет неравенству

$$f(\lambda x) \leqslant \lambda f(x) \quad (0 < x < \varepsilon,\ 0 < \lambda < 1). \tag{6}$$

Для пояснения геометрического смысла неравенства (6) рассмотрим в плоскости с декартовыми координатами $(x; y)$ множество $\mathcal{E}_f$ тех точек, для которых $y \geqslant f(x)$. Оно называется *надграфиком* функции f. Неравенство (6) выполняется, если и только если все преобразования подобия $(x; y) \mapsto (\lambda x; \lambda y)$ $(0 < \lambda < 1)$ отображают надграфик в себя (т. е. если $(x; y) \in \mathcal{E}_f$, то $(\lambda x; \lambda y) \in \mathcal{E}_f$ при всех $0 < \lambda < 1$).

Для нас класс функций, подчиняющихся скейлингу, важен потому, что имеет место

Теорема. *Если на некотором интервале $(0, \varepsilon)$ функция f подчиняется скейлингу, то при $x \to 0$ отношение $f(x)/x$ стремится к некоторому пределу или к $-\infty$.*

Доказательство. Пусть $0 < t < x < \varepsilon$. Полагая в (6) $\lambda = t/x$ получаем

$$\frac{f(t)}{t} \leqslant \frac{f(x)}{x}, \tag{7}$$

и требуемое утверждение вытекает из теоремы о пределе монотонной функции.

Замечание 1. Если $f(x)$ задана также и при $x = 0$ и непрерывна в этой точке, то (6) в пределе при $\lambda \to 0$ дает $f(0) \leqslant 0$. Если при этом $f(0) < 0$, то $f(x)/x \to -\infty$ при $x \to 0$. Однако $f(x)/x$ может стремиться к $-\infty$ и в случае $f(0) = 0$.

Пример. *$f(x) = -\sqrt{x}$ подчиняется скейлингу, $f(0) = 0$, но $f(x)/x \to -\infty$.*

Замечание 2. Из (7), в свою очередь, следует неравенство

$$\frac{f(t)}{t} \leqslant \frac{f(x) - f(t)}{x - t} \quad (0 < t < x < \varepsilon), \tag{8}$$

которое также будет полезно в дальнейшем.

В приложениях предыдущей теоремы к двум замечательным пределам мы будем устанавливать неравенство (6), пользуясь некоторым более сильным свойством, а именно, — выпуклостью.

Функция f на некотором промежутке I вещественной оси называется *выпуклой*, если выполняется неравенство

$$f((1-\lambda)x_1 + \lambda x_2) \leqslant (1-\lambda)f(x_1) + \lambda f(x_2) \quad (0 < \lambda < 1) \tag{9}$$

при всех $x_1, x_2 \in I$. Такова, например, функция $f(x) = ax^2 + bx + c$ при любых $a \geqslant 0$, b, c (в частности, любая линейная функция выпукла).

Сумма двух выпуклых функций выпукла. В частности, сумма любой выпуклой и любой линейной функции выпукла.

Если функция f выпукла на $[0, \varepsilon]$ и $f(0) = 0$, то она подчиняется скейлингу на $(0, \varepsilon)$, ибо (6) следует из (9) при $x_1 = 0$, $x_2 = x$. Таким образом, *теорема о существовании предела $f(x)/x$ верна для выпуклых функций f таких, что $f(0) = 0$.*

Геометрический смысл выпуклости функции f состоит в выпуклости ее надграфика $\mathcal{E}_f$. (Напомним, что множество M в плоскости называется *выпуклым*, если для каждой пары точек A, B из M отрезок AB целиком принадлежит M).

Следующее предложение существенно облегчает проверку выпуклости конкретных функций.

Лемма. *Если неравенство (9) выполняется при $\lambda = \frac{1}{2}$, т. е.*

$$f\left(\frac{x_1 + x_2}{2}\right) \leqslant \frac{f(x_1) + f(x_2)}{2} \quad (x_1, x_2 \in I), \tag{10}$$

и если функция f непрерывна, то она выпукла.

Доказательство. Неравенство (10) означает, что для любых двух точек A, B из надграфика $\mathcal{E}_f$ середина C отрезка AB также принадлежит $\mathcal{E}_f$. Повторяя это рассуждение, получаем, что середины C_1, C_2 отрезков AC и CB принадлежат $\mathcal{E}_f$ и т. д. Полученные таким путем точки

$C, C_1, C_2, \ldots$ (*двоично-рациональные точки* отрезка AB) располагаются на отрезке AB всюду плотно, т. е. в любой близости от любой точки отрезка есть двоично-рациональная точка. По непрерывности функции f все точки отрезка AB принадлежат $\mathcal{E}_f$. Действительно, если некоторая точка отрезка AB не лежит в $\mathcal{E}_f$, то в ней выполняется неравенство $y < f(x)$. Тогда оно выполняется и во всех достаточно близких точках, т. е. они также не лежат в $\mathcal{E}_f$.

3. Первый замечательный предел

Будем рассматривать $\sin x$ как функцию числового значения угла при каком-нибудь выбранном масштабе. Числовое значение прямого угла обозначим через d.

Очевидно, при $x_1, x_2 \in [0, d]$

$$\sin \frac{x_1 + x_2}{2} = \frac{\sin x_1 + \sin x_2}{2 \cos \frac{x_1 - x_2}{2}} \geqslant \frac{\sin x_1 + \sin x_2}{2}. \tag{11}$$

Мы видим, что функция $-\sin x$ на $[0, d]$ удовлетворяет неравенству (10). По лемме она окажется выпуклой, если мы докажем ее непрерывность. Тогда станет применимой и теорема о пределе $f(x)/x$. Тем самым, мы установим существование первого замечательного предела, если только сумеем исключить возможность стремления $\sin x/x$ к $+\infty$ при $x \to 0$. (Условие $x > 0$ несущественно, так как $\sin x/x$ — четная функция).

а) *Функция* $\sin x$ *непрерывна.* Действительно,

$$\sin(x + h) - \sin x = 2 \sin \frac{h}{2} \cos\left(x + \frac{h}{2}\right). \tag{12}$$

Поэтому достаточно доказать, что

$$\lim_{t \to 0} (\sin t) = 0 \tag{13}$$

(непрерывность в нуле). При этом, очевидно, можно ограничиться значениями $t > 0$. Но, как видно из того же неравенства (12), $\sin t$ является возрастающей функцией при $0 \leqslant t \leqslant d$. Поэтому существует $\sigma = \lim\limits_{t \to +0} (\sin t) \geqslant 0$. Из формулы удвоения (тоже скейлинг!), записанной в виде

$$\sin 2t = 2 \sin t \sqrt{1 - \sin^2 t} \tag{14}$$

при $t \to +0$ получаем

$$\sigma = 2\sigma \sqrt{1 - \sigma^2} \tag{15}$$

и, если $\sigma \neq 0$, то $2\sqrt{1 - \sigma^2} = 1$, откуда $\sigma = \dfrac{\sqrt{3}}{2}$ — противоречие.

б) *Отношение* $\sin x/x$ *ограничено.* Действительно, в силу (8), примененного к функции $-\sin x$, имеем

$$\frac{\sin(t+2x)-\sin t}{2x} \leqslant \frac{\sin t}{t} \quad \left(0 < t \leqslant d,\ 0 < x \leqslant \frac{d-t}{2}\right),$$

откуда

$$\frac{\sin x}{x}\cos(t+x) \leqslant \frac{\sin t}{t}.$$

Но

$$\cos(t+x) > \cos\frac{t+d}{2}$$

и, следовательно,

$$\frac{\sin x}{x} \leqslant \frac{\sin t}{t\cos\dfrac{t+d}{2}} \quad \left(0 < x < \frac{d-t}{2}\right).$$

Существование первого замечательного предела доказано.

4. Второй замечательный предел

Как уже говорилось во введении, мы рассмотрим вопрос о существовании предела

$$l(a) = \lim_{x\to 0}\frac{a^x-1}{x} \tag{16}$$

при $a > 1$. Последнее условие несколько упрощает дальнейший анализ, но само по себе несущественно.

Неравенство между средним геометрическим и средним арифметическим

$$\sqrt{uv} \leqslant \frac{u+v}{2} \quad (u, v \geqslant 0) \tag{17}$$

при подстановке $u = a^{x_1}$, $v = a^{x_2}$ превращается в

$$a^{\frac{x_1+x_2}{2}} \leqslant \frac{a^{x_1}+a^{x_2}}{2}. \tag{18}$$

По лемме это влечет выпуклость функции a^x (а, значит, и функции $a^x - 1$) на всей вещественной оси, если уже известно, что эта функция непрерывна. Но тогда и существование предела $l(a)$ будет обеспечено, ибо, во-первых, $(a^x-1)/x > 0$ при $x > 0$ (так что стремление к $-\infty$ исключено) и, во-вторых, если $x < 0$, скажем $x = -t$, $t > 0$, то

$$\lim_{x\to -0}\frac{a^x-1}{x} = \lim_{t\to +0} a^{-t}\,\frac{a^t-1}{t} = l(a). \tag{19}$$

Для доказательства непрерывности функции a^x заметим, что

$$a^{x+h} - a^x = a^x(a^h - 1) \tag{20}$$

(ср. (12)). Поэтому достаточно доказать, что

$$\lim_{h\to 0} a^h = 1 \tag{21}$$

(непрерывность в нуле, ср. (13)). При этом можно считать $h > 0$, так как $a^{-h} = (a^h)^{-1}$.

Из формулы (20) видно, что функция a^x — возрастающая. Поэтому существует $\tau = \lim\limits_{h\to+0} a^h \geqslant 1$. Из формулы удвоения

$$a^{2h} = (a^h)^2 \tag{22}$$

следует $\tau^2 = \tau$, т. е. $\tau = 1$.

Докажем, что $l(a) > 0$ при всех $a > 1$. С этой целью применим неравенство (8) к $f(x) = a^x - 1$ и затем заменим t на x, а x на $x + h$ $(h > 0)$. Получим

$$\frac{a^x - 1}{x} \leqslant \frac{a^{x+h} - a^x}{h} \quad (x > 0, h > 0) \tag{23}$$

Отсюда

$$\frac{a^h - 1}{h} \geqslant \frac{1 - a^{-x}}{x} \quad (x > 0, h > 0), \tag{24}$$

что при $h \to +0$ дает

$$l(a) \geqslant \frac{1 - a^{-x}}{x} > 0. \tag{25}$$

Если теперь заменить в (16) x на $x/l(a)$, то получится

$$\lim_{x\to 0} \frac{e^x - 1}{x} = 1, \tag{26}$$

где

$$e = a^{1/l(a)}. \tag{27}$$

На первый взгляд, введенное таким путем число e зависит от a. В действительности же оно постоянно. Для доказательства заметим, что (26) означает, что $l(e) = 1$. Но, с другой стороны, из соотношения

$$\frac{(ab)^x - 1}{x} = \frac{a^x - 1}{x} b^x + \frac{b^x - 1}{x} \tag{28}$$

при $x \to 0$ следует

$$l(ab) = l(a) + l(b) > l(a) \quad (a, b > 1), \tag{29}$$

т. е. функция l — возрастающая. Поэтому каждое свое значение она принимает лишь в одной точке. В частности, значение 1 она принимает лишь в одной точке, а эта точка и есть e.

Теперь можно вычислить $l(a)$. Логарифмируя (27) по основанию e (соответствующие логарифмы называются *натуральными* и обозначаются

через «ln»), получаем $1 = \ln a/l(a)$, откуда

$$l(a) = \ln a. \tag{30}$$

(С этой точки зрения равенство (29) становится совершенно понятным, но в нашем контексте (30) логически следует за (29)). Таким образом, окончательно

$$\lim_{x\to 0} \frac{a^x - 1}{x} = \ln a. \tag{31}$$

Мы доказали это при $a > 1$, но легко видеть, что это верно и при $0 < a \leqslant \leqslant 1$.

Сделаем теперь в (26) замену переменной: $e^x - 1 = t$. Условия $x \to 0$ и $t \to 0$ эквивалентны. Поэтому (26) можно переписать в виде

$$\lim_{x\to 0} \frac{t}{\ln(1+t)} = 1,$$

откуда

$$\lim_{t\to 0} \ln(1+t)^{1/t} = 1$$

и, следовательно,

$$\lim_{t\to 0} (1+t)^{1/t} = e, \tag{32}$$

т. е. мы получили второй замечательный предел.

Уместно подчеркнуть, что все экспоненты a^x $(a > 0)$ получаются из стандартной e^x скейлингом,

$$a^x = e^{x \ln a}, \tag{33}$$

т. е. выбор основания e можно рассматривать как функцию масштаба измерения, но уже не углов, а логарифмов чисел. Замечательно, что этому тоже можно придать геометрический смысл, но в *неевклидовой* геометрии Лобачевского (открытой им в 20-х годах прошлого века).

Отметим еще, что равенство (31) можно переписать в виде

$$\lim_{x\to 0} \frac{e^{kx} - 1}{x} = k, \tag{34}$$

аналогичном (4).

5. Объединение в комплексной плоскости

Читателю уже ясна глубокая аналогия между двумя замечательными пределами. Нет ли здесь прямой связи? Прямая связь, действительно, есть, она была установлена Иоганном Бернулли (1667–1748) и прочно вошла в математику после Эйлера (1707–1783). Устанавливается она равенством

$$e^{ix} = \cos x + i \sin x, \tag{35}$$

которое формально должно рассматриваться как *определение* экспоненты e^{ix}. Это определение оказывается в высшей степени мотивированным и целесообразным. Действительно, рассмотрим, принимая (35), выражение

$$\frac{e^{ix}-1}{x}=\frac{\cos x-1}{x}+i\frac{\sin x}{x}=-\frac{x}{2}\left(\frac{\sin\frac{x}{2}}{\frac{x}{2}}\right)^2+i\frac{\sin x}{x}. \tag{36}$$

Устремляя x к нулю и используя первый замечательный предел, получаем

$$\lim_{x\to 0}\frac{e^{ix}-1}{x}=i. \tag{37}$$

Заменяя здесь x на kx с любым вещественным $k\neq 0$, получаем

$$\lim_{x\to 0}\frac{e^{ikx}-1}{x}=ik. \tag{38}$$

Равенство (34) оказалось верным не только для вещественных, но и для мнимых значений k !

Естественным завершением изложенного хода мысли является рассмотрение экспоненты e^z с любым комплексным $z=x+iy$. Экстраполируя теорему сложения

$$e^{x_1+x_2}=e^{x_1}e^{x_2} \tag{39}$$

на рассматриваемую ситуацию, мы должны принять *по определению*, что

$$e^z=e^{x+iy}=e^x(\cos x+i\sin y). \tag{40}$$

(После этого теорема сложения может быть доказана для любых комплексных показателей. Тем самым, происходит объединение двух «вещественных» теорем сложения: для экспоненты и для тригонометрических функций.) И теперь мы должны спросить себя, сохраняется ли равенство (26) в комплексной плоскости, т.е. верно ли, что

$$\lim_{z\to 0}\frac{e^z-1}{z}=1?$$

(Определение предела в комплексном анализе формально такое же, как в вещественном). Ответ утвердителен, для доказательства нужно использовать оба замечательных предела. Мы предоставляем читателю сделать это во всех деталях.

В этом пункте мы вплотную подошли к началам сразу нескольких важных математических теорий: комплексного анализа, неевклидовой геометрии, теории групп и т.д., но это уже, как говорится, another story (другая история).

Наш семинар: математические сюжеты

Теория препятствий для начинающих*

Д. Реповш А. Скопенков

I should say it meant something simple
and obvious, but then I am no philosopher!

I. Murdoch *The sea, the sea*

Введение

Теория препятствий является важной частью алгебраической топологии и имеет многочисленные применения в других областях математики. А раз так, основные идеи этой теории наверняка можно доступно изложить человеку, не имеющему специальных познаний в топологии. К сожалению, изучение теории препятствий по существующей литературе возможно только после длительного освоения немотивированных абстрактных понятий и теорий. Настоящая же статья, напротив, посвящена изложению идей теории препятствий на простейших частных случаях. Она предназначена в первую очередь для читателей, не владеющих топологией, но мы смеем надеяться, что она будет интересна и специалистам.

В школьных (в частности, олимпиадных) задачах *невозможность* реализовать некоторую конструкцию часто доказывается путем построения

*Работа Д. Реповша частично поддержана исследовательским грантом Министерства Науки и Технологии Республики Словения No. J1-0885-0101-98. Работа А. Скопенкова частично поддержана грантом Российского Фонда Фундаментальных Исследований №96-01-00009.

алгебраического *препятствия*, или *инварианта* (например, из соображений четности). Точно так же *неэквивалентность* конструкций часто доказывается путем построения алгебраического *инварианта*, их различающего (этот инвариант является *препятствием* к эквивалентности). Многие непохожие друг на друга задачи топологии аналогичным образом естественно приводят к похожим друг на друга *препятствиям*. В настоящей статье этот процесс продемонстрирован на примере наиболее наглядных топологических задач.

Для чтения статьи (кроме §3.C,D) достаточно геометрической интуиции (используемые начальные понятия теории графов приведены в конце введения, а используемое в §3 понятие двумерного многообразия там кратко объясняется). В частности, все необходимые алгебраические объекты (со страшными названиями группы когомологий, препятствия и характеристические классы) естественно возникают и строго *определяются* в процессе доказательства теорем. Мы также приводим результат вычисления препятствий, дающий интересные геометрические следствия (само вычисление остается читателю в качестве задачи, кроме вычислений в §3.C,D, за которыми мы отсылаем читателя к [5]). Подчеркнем, что мы не требуем от читателя знакомства с алгебраическим понятием группы, в тексте можно воспринимать это слово как синоним слова «множество».

Часть материала сформулирована в виде задач, обозначаемых жирными числами. Читатель также может рассматривать восполнение деталей *набросков доказательств* как материал для самостоятельной работы. Следует подчеркнуть, что задачи не используются в остальном тексте. В некоторых задачах могут встретиться незнакомые вам термины; такие задачи следует просто игнорировать. Отметим также, что для решения задач достаточно понимания их формулировок и *не требуется* никаких дополнительных понятий и теорий.

Параграфы статьи независимы друг от друга (ссылки между ними посвящены исключительно сравнению материала). Они расположены примерно в порядке возрастания сложности. В каждом параграфе приводится краткая история вопроса. Конкретные ссылки даются только по (к сожалению, относительно малоизвестному) материалу §2.

Для читателя, уже знакомого с алгебраической топологией, отметим, что мы не используем стандартную терминологию теории препятствий там, где мы считаем, что она неудобна для начинающего. Приведем здесь для сравнения эту терминологию. Расстановки элементов группы G на i-симплексах полиэдра K называются *i-мерными коцепями на K с коэффициентами в G* (у нас они называются просто *расстановками*). Группа таких расстановок обычно обозначается $C^i(K,G)$. Множество $\delta C^{i-1}(K,G)$ всех кограниц образует подгруппу группы $C^i(K,G)$, обозначаемую

$B^i(K,G)$. Когда $G=\mathbb{Z}_2$, мы пропускаем коэффициенты в обозначениях коцепей, коциклов, когранич и (ко)гомологий.

* * * * * *

Напомним используемые начальные понятия теории графов. Грубо говоря, граф можно понимать как конечное множество точек (его «вершины»), некоторые пары которых выделены («соединены ребрами»). Мы примем следующее формальное определение. *Разбиением* (представляющим граф) назовем конечное множество точек (на плоскости), некоторые пары которых соединены ломаными; эти точки называются *вершинами* разбиения, а ломаные — его *ребрами*; ребра могут пересекаться, но точки пересечения (кроме двух концов ребра) не могут быть вершинами. Разбиения G_1 и G_2 называются *изоморфными*, если существует взаимно однозначное отображение f множества вершин разбиения G_1 на множество вершин разбиения G_2, удовлетворяющее условию: вершины $A,B\in G_1$ соединены ребром в том и только в том случае, если $f(A),f(B)\in G_2$ соединены ребром. Разбиения G_1 и G_2 называются *гомеоморфными*, если G_1 можно получить из G_2 операциями *подразделения ребра* (рис. 0.1) и

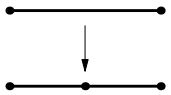


Рис. 0.1.

обратными. *Графом* называется класс эквивалентности разбиения (по отношению гомеоморфности). Разбиение (элемент класса эквивалентности) называется разбиением или триангуляцией соответствующего графа (допуская вольность речи, иногда конкретное разбиение называют графом). Через S^1 обозначается граф, гомеоморфный окружности. Грубо говоря, *подграф* данного графа — это его часть (точное определение приведите сами). Граф называется *деревом*, если он связен и не содержит подграфа, гомеоморфного S^1. *Степенью* вершины называется число выходящих из нее ребер. Количества вершин, ребер и компонент связности графа K обозначаются V, E и C, соответственно.

§1. В направлении Хопфа

Для подмножества (например, графа) $K\subset\mathbb{R}^2$ определим понятие *ветра* (или непрерывного отображения в окружность). Ветер $f\colon K\to S^1$ сопоставляет каждой точке $x\in K$ единичный вектор $f(x)$ (точку на окружности). Вектор $f(x)$ должен непрерывно зависеть от x. Два ветра $f_0,f_1\colon K\to S^1$ называются *гомотопными* (обозначение: $f_0\simeq f_1$), если существует семейство $f_t\colon K\to S^1$ ветров, непрерывно зависящее от

параметра $t \in [0,1]$. Для графа $K \subset \mathbb{R}^2$ обозначим через $[K, S^1]$ множество ветров $K \to S^1$ с точностью до гомотопии. В этом параграфе решается задача нахождения множества $[K, S^1]$ (а в виде задач в конце параграфа предлагаются ее обобщения на другие случаи).

Теорема Хопфа о гомотопической классификации отображений n-полиэдра в S^n (т.е. «многомерных ветров») была доказана Хайнцем Хопфом около 1930 г. («по заказу» Павла Сергеевича Александрова). Идея приводимого ниже доказательства теоремы Хопфа принадлежит Сэмюэлю Эйленбергу и Сондерсу Маклейну (около 1940 г.). Задача о гомотопической классификации произвольных отображений — одна из основных в алгебраической топологии. Дальнейшее развитие теорема Хопфа получила в работах Нормана Стинрода (1941 г.), Льва Семеновича Понтрягина (1942 г.) и Михаила Михайловича Постникова (около 1950 г.).

1. Для любого дерева существует ровно один ветер с точностью до гомотопии.

Степенью $\deg f$ ветра $f\colon S^1 \to S^1$ называется число оборотов вектора $f(x)$ (вокруг своего неподвижного начала) при однократном обходе точкой x окружности S^1 против часовой стрелки.

Основная теорема топологии. *Отображение* $\deg\colon [S^1, S^1] \to \mathbb{Z}$ *является биекцией.*

Мы не приводим доказательства (интуитивно очевидной) инъективности в Основной теореме топологии.

2. a) Докажите сюръективность в Основной теореме топологии.

b) Выведите из Основной теоремы топологии Основную теорему алгебры.

3. a) Пусть K — несвязное объединение или букет k окружностей (рис. 1.1). Фиксируем произвольно направление на каждой из этих окружностей. Для ветра $f\colon K \to S^1$ поставим на каждой из этих окружностей степень сужения ветра f на эту окружность. Полученную расстановку k целых чисел обозначим $\deg f$. Тогда $\deg\colon [K, S^1] \to \mathbb{Z}^k$ — биекция.

b) Множество $[K, S^1]$ не меняется при стягивании ребра.

c) $[K, S^1] = \mathbb{Z}^{E-V+C}$.

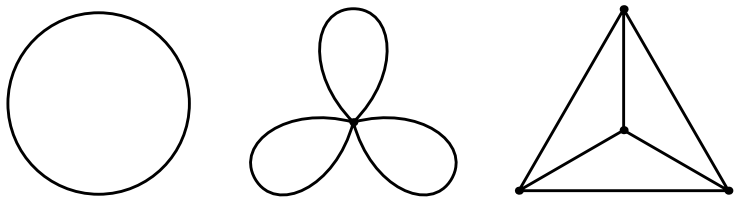


Рис. 1.1.

Хопф доказывал свою теорему при помощи обобщения метода задач 3b, 3c. Приведем другое доказательство, развивающее идею задачи 3a и следующее общему методу теории препятствий.

Теорема Хопфа. *Для графа K отображение* $\deg\colon [K,S^1]\to H^1(K,\mathbb{Z})$ *является биекцией.*

Вычисление. $H^1(K,\mathbb{Z})\cong\mathbb{Z}^{E-V+C}$.

Определение $H^1(K,\mathbb{Z})$, deg *и доказательство.* Знакомство с этим доказательством рекомендуем начать со случая $K=K_4$ (рис. 1.1). Фиксируем произвольный единичный вектор v. Произвольный ветер $K\to S^1$ гомотопен *клеточному* ветру, т. е. ветру, для которого в каждой вершине графа K стоит вектор v. Поэтому достаточно классифицировать клеточные ветры $K\to S^1$ с точностью до гомотопии, все отображения (ветры) которой не обязательно клеточны.

Фиксируем произвольно направление на каждом ребре графа K. Возьмем клеточный ветер $f\colon K\to S^1$. Поставим на каждом ребре $e\subset K$ с началом n и концом k число оборотов вектора $f(x)$ при обходе точкой x ребра e от n к k. Полученную расстановку обозначим $\gamma(f)$. Множество всех расстановок целых чисел на ребрах графа K обозначим через $\mathbb{Z}^E$. Расстановки можно складывать: для этого просто складываются числа, стоящие на каждом ребре (такое сложение называется *покомпонентным*). Если $f,g\colon K\to S^1$ — такие клеточные ветры, что $\gamma(f)=\gamma(g)$, то по Основной теореме топологии $f\simeq g$.

Обратное неверно, как показывает пример следующей гомотопии (см. рис. 1.2). Для вершины a графа K изменим ветер f так, чтобы вектор в a сделал один оборот против часовой стрелки, ветер в маленькой окрестности вершины a «потянулся» за вектором в a, а вне этой маленькой окрестности ветер не менялся. В результате получим ветер $g\colon K\to S^1$, гомотопный ветру f. Понятно, что $\gamma(f)-\gamma(g)$ есть расстановка ±1 (в зависимости от ориентации) на ребрах, содержащих вершину a, и 0 на всех остальных ребрах. Эта расстановка называется *элементарной кограницей вершины a* и обозначается δa.

В окрестностях вершин $a_1,\dots,a_k$ сделаем описанную выше гомотопию ветра f, поворачивая векторы в этих вершинах на $n_1,\dots,n_k$ оборотов, соответственно. Эту гомотопию можно задать расстановкой чисел $n_1,\dots,n_k$ в вершинах $a_1,\dots,a_k$, соответственно (и нулей в остальных вершинах). Обозначим полученную расстановку через Γ, а полученный ветер через f_Γ. Множество всех расстановок целых чисел на вершинах графа K с операцией покомпонентного сложения обозначим через $\mathbb{Z}^V$. Каждой вершине a отвечает «характеристическая» расстановка $a\in\mathbb{Z}^V$ единицы в вершине a и нуля в остальных вершинах. Определим отображение

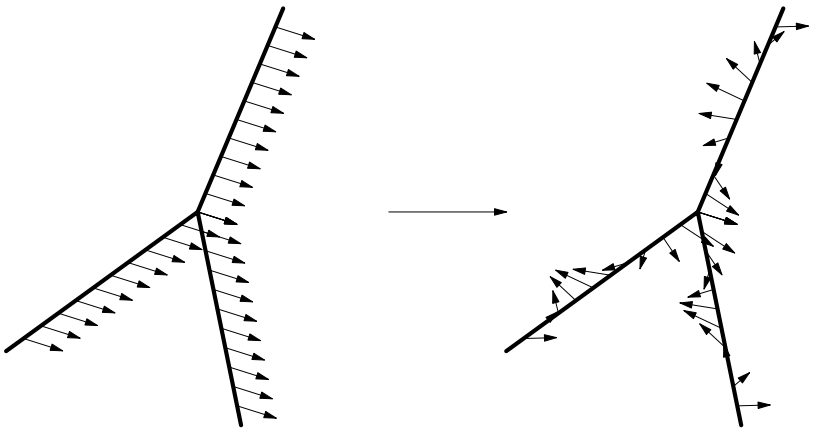


Рис. 1.2.

$\delta\colon \mathbb{Z}^V \to \mathbb{Z}^E$ формулой $\delta(n_1a_1 + \ldots + n_ka_k) = n_1\delta a_1 + \ldots + n_k\delta a_k$. Тогда $\gamma(f) - \gamma(f_\Gamma) = \delta\Gamma$.

Назовем расстановки $\gamma_1, \gamma_2 \in \mathbb{Z}^E$ *когомологичными*, если $\gamma_1 - \gamma_2 = \delta\Gamma$ для некоторого $\Gamma \in \mathbb{Z}^V$. Группа $H^1(K, \mathbb{Z}) = \mathbb{Z}^E/\delta(\mathbb{Z}^V)$ расстановок с точностью до когомологичности называется *одномерной группой когомологий графа K с коэффициентами в $\mathbb{Z}$*. Обозначим $\deg f = [\gamma(f)] \in \in H^1(K, \mathbb{Z})$.

Теперь рассмотрим гомотопию $f_t\colon K \to S^1$ между клеточными ветрами f_0, f_1. Поставим на каждой вершине a число оборотов вектора $f_t(a)$ при изменении t от 0 до 1. Полученную расстановку обозначим $\Gamma(\{f_t\})$. Легко проверить, что $\gamma(f_0) - \gamma(f_1) = \delta\Gamma(\{f_t\})$. Значит, $\deg f_1 = \deg f_0$. Поэтому отображение $\deg\colon [K, S^1] \to H^1(K, \mathbb{Z})$ корректно определено. Если $\deg f = \deg g$, то $\gamma(f) - \gamma(g) = \delta\Gamma$ для некоторого $\Gamma \in \mathbb{Z}^E$, значит $f \simeq f_\Gamma \simeq g$. Поэтому отображение deg инъективно. Доказательство его сюръективности оставляем читателю в качестве задачи. □

Заметим, что построенное отображение $\deg\colon [K, S^1] \to H^1(K, \mathbb{Z})$ зависит от выбора направлений на ребрах графа K. Для ветра f класс $\deg f$ является *препятствием* к гомотопности ветра f ветру с постоянным направлением.

4. a) Группа $H^1(K, \mathbb{Z})$ зависит только от топологического типа графа K, т. е. одномерные группы когомологий гомеоморфных графов изоморфны.

b) Отображение $\deg\colon [K, S^1] \to H^1(K, \mathbb{Z})$ является изоморфизмом групп (S^1 является группой, поэтому $[K, S^1]$ является группой).

5. a) Используя $[S^1, \mathbb{RP}^2] \cong \mathbb{Z}_2$, найдите $[K, \mathbb{RP}^2]$ для графа K, т. е. определите одномерную группу когомологий $H^1(K)$ с $\mathbb{Z}_2$-коэффициентами и биекцию $\deg\colon [K, \mathbb{RP}^2] \to \to H^1(K)$.

b) Для графа K с эквивариантной инволюцией найдите множество $[K, S^1]_{eq}$ эквивариантных (т. е. перестановочных с данной инволюцией на K и антиподальной инволюцией на S^1) отображений $K \to S^1$ с точностью до эквивариантной гомотопии.

6. a) Отображение $\partial D^2 \to S^1$ гомотопно отображению в точку (т. е. имеет степень ноль) тогда и только тогда, когда оно продолжается на D^2.

b) Используя $[S^2, S^1] \cong 0$, найдите $[K, S^1]$ для поверхности K, т. е. определите одномерную группу когомологий $H^1(K, \mathbb{Z})$ с $\mathbb{Z}$-коэффициентами и биекцию $\deg\colon [K, S^1] \cong H^1(K, \mathbb{Z})$.

c) Найдите $H^1(K, \mathbb{Z})$ для связного 2-многообразия K с триангуляцией T, имеющей V, E и F вершин, ребер и граней, соответственно (см. определение в начале §3).

d) Конечный n-полиэдр можно представлять себе как объединение некоторого количества граней размерностей не более n в разбиении пространства $\mathbb{R}^m$ на единичные кубы. Используя $[S^i, S^1] \cong 0$ для $i \geqslant 2$, найдите $[K, S^1]$ для конечного n-полиэдра K, т. е. определите одномерную группу когомологий $H^1(K, \mathbb{Z})$ с $\mathbb{Z}$-коэффициентами и биекцию $\deg\colon [K, S^1] \cong H^1(K, \mathbb{Z})$.

7. a) (n-мерная теорема Хопфа) Используя $[S^i, S^n] \cong 0$ для $i < n$ и $[S^n, S^n] \cong \mathbb{Z}$, найдите $[K, S^n]$ для конечного n-полиэдра K, т. е. определите n-мерную группу когомологий $H^n(K, \mathbb{Z})$ с $\mathbb{Z}$-коэффициентами и биекцию $\deg\colon [K, S^n] \cong H^n(K, \mathbb{Z})$.

b) Для конечного полиэдра K определите n-мерную группу когомологий $H^n(K, \mathbb{Z})$ с $\mathbb{Z}$-коэффициентами так, чтобы отображение $\deg\colon [K, S^n] \to H^n(K, \mathbb{Z})$ было по-прежнему корректно определено.

c) Если $\dim K = n + 1$, то $\deg\colon [K, S^n] \to H^n(K, \mathbb{Z})$ сюръективно.

8. a) Попытайтесь обобщить ваши вычисления множества $[K, \mathbb{RP}^2]$ на 2-полиэдр K и найдите такой 2-полиэдр K, что $[K, \mathbb{RP}^2] \ncong H^1(K)$.

b) Используя $[S^1, \mathbb{RP}^{n+2}] \cong \mathbb{Z}_2$ и $[S^i, \mathbb{RP}^{n+2}] \cong 0$ для $i = 2, 3, \ldots, n$, докажите $[K, \mathbb{RP}^{n+2}] \cong H^1(K)$ для n-полиэдра K.

c) Используя $[S^2, \mathbb{CP}^n] \cong \mathbb{Z}$ и $[S^i, \mathbb{CP}^n] \cong 0$ для $i = 1, 3, 4, \ldots, n$, докажите $[K, \mathbb{CP}^n] \cong H^2(K, \mathbb{Z})$ для n-полиэдра K.

9. (Теорема Стинрода для $n = 2$) Напомним, что $[S^3, S^2] \cong \mathbb{Z}$.

a) Для 3-полиэдра K и класса $\gamma \in H^2(K, \mathbb{Z})$ постройте биекцию $\deg^{-1} \gamma \to H^3(K, \mathbb{Z})$. Получится биекция $[K, S^2] \cong H^2(K, \mathbb{Z}) \times H^3(K, \mathbb{Z})$.

b) Для 4-полиэдра K и отображения $f\colon K^{(3)} \to S^2$ постройте препятствие $\mathrm{Sq}^2(\deg f)$ из $H^4(K, \mathbb{Z})$ к продолжению отображения $f\colon K^{(3)} \to S^2$ на все K. Получится отображение Sq^2, для которого последовательность $[K, S^2] \xrightarrow{\deg} H^2(K, \mathbb{Z}) \xrightarrow{\mathrm{Sq}^2} H^4(K, \mathbb{Z})$ точна.

c) Для коцикла $a \in Z^2(K, \mathbb{Z})$ элемент $\mathrm{Sq}^2[a]$ представляется коциклом $b \in Z^4(K, \mathbb{Z})$, определенным по формуле $b(\sigma_{01234}) = a(\sigma_{012})a(\sigma_{234})$.

d) Пусть K — четырехмерное многообразие и класс $a \in H^2(K, \mathbb{Z})$ двойственен по Пуанкаре классу $Da \in H_2(K, \mathbb{Z})$, представляющемуся погружением $h\colon N \to K$ 2-многообразия N. Тогда $\mathrm{Sq}^2 a$ есть сумма точек (со знаком) в $h(N) \cap h'(N)$, где h' — погружение, близкое к h.

10. (Теорема Стинрода) Пусть $\rho_2\colon H^n(K, \mathbb{Z}) \to H^n(K)$ — приведение по модулю 2. Напомним, что $[S^{n+1}, S^n] \cong \mathbb{Z}_2$ для $n \geqslant 3$.

a) Для $n \geqslant 3$, $(n+2)$-полиэдра K и отображения $f\colon K^{(n+1)} \to S^n$ постройте препятствие $\mathrm{Sq}^2 \rho_2(\deg f) \in H^{n+2}(K)$ к продолжению отображения $f\colon K^{(n+1)} \to S^n$ на все K. Получится отображение Sq^2, для которого последовательность $[K, S^n] \xrightarrow{\deg} \to H^n(K, \mathbb{Z}) \xrightarrow{\mathrm{Sq}^2 \circ \rho_2} H^{n+2}(K)$ точна.

b) Для $n \geqslant 3$, $(n+1)$-полиэдра K и элемента $\gamma \in H^n(K,\mathbb{Z})$ постройте биекцию $\deg^{-1}\gamma \to H^{n+1}(K)/\operatorname{Sq}^2\rho_2 H^{n-1}(K,\mathbb{Z})$. Получится биекция $[K,S^n] \cong H^n(K,\mathbb{Z}) \times$ $\times H^{n+1}(K)/\operatorname{Sq}^2\rho_2 H^{n-1}(K,\mathbb{Z})$.

11. Напомним, что для любого n существует (бесконечный) полиэдр $K(\mathbb{Z},n)$, такой что $[S^n,K(\mathbb{Z},n)] \cong \mathbb{Z}$ и $[S^i,K(\mathbb{Z},n)] \cong 0$ для любого $i \neq n$. Например, $K(\mathbb{Z},1) \cong S^1$ и $K(\mathbb{Z},2) \cong \mathbb{CP}^\infty$.

a) $H^n(K,\mathbb{Z}) \cong [K,K(\mathbb{Z},n)]$ для любого полиэдра K.

b) Если $\alpha \in H^2(K,\mathbb{Z})$, то $f_{\operatorname{Sq}^2\alpha} = f_1 \circ f_\alpha$, где $1 \in H^4(\mathbb{CP}^3,\mathbb{Z}) \cong H_2(\mathbb{CP}^3,\mathbb{Z}) \cong$ $\cong \mathbb{Z}$ — образующая и отображения $f_{\operatorname{Sq}^2\alpha}\colon K \to K(\mathbb{Z},4)$, $f_1\colon \mathbb{CP}^3 \to K(\mathbb{Z},4)$ и $f_\alpha\colon K \to$ $\to \mathbb{CP}^3$ соответствуют классам $\operatorname{Sq}^2\alpha, 1$ и α при изоморфизмах $H^4(K,\mathbb{Z}) \cong [K,K(\mathbb{Z},4)]$, $H^4(\mathbb{CP}^3,\mathbb{Z}) \cong [\mathbb{CP}^3,K(\mathbb{Z},4)]$ и $H^2(K,\mathbb{Z}) \cong [K,\mathbb{CP}^3]$.

§2. В направлении Ван Кампена

Понятие препятствия, по-видимому, впервые возникло именно у Ван Кампена при решении проблемы о вложимости n-мерных полиэдров в $\mathbb{R}^{2n}$ [6], [4], [9, §2], [11, §2], [12, §2]. Но показать основную идею гораздо проще на проблемах аппроксимируемости пути вложениями и планарности графов [14], [9, §9], [3, §4], [10, §1], [1, §4]. Этим проблемам (аккуратно сформулированным ниже) и посвящен настоящий параграф.

1. a) Охотник прошел по лесной дорожке в форме окружности диаметром 1 км, сделав два оборота. Он вел на поводке длиной 1 м собаку, которая в конце движения вернулась в исходную точку. Тогда собака обязательно пересекала свой след (в некоторый момент времени, отличный от конечного).

Приведем другую формулировку этой задачи (эквивалентность доказана в [8]). Рассмотрим две полянки (т. е. два круга), соединенных двумя тропинками (т. е. полосками) a и b, как на рис. 2.1. Собака бегала по полянкам и тропинкам и вернулась в исходную точку. Каждый раз, когда собака перебегала с полянки на тропинку, она записывала обозначение этой тропинки. Если получилась запись $abab$, то собака обязательно пересекала свой след (в некоторый момент времени, отличный от конечного).

b) Верно ли a) без предположения о том, что собака в конце движения вернулась в исходную точку?

c) Докажите a) для случая, когда охотник сделал *три* оборота.

d) Для какого числа оборотов в a) собака обязательно пересекала свой след?

Путь $\varphi\colon I \to \mathbb{R}^2$ на плоскости называется *аппроксимируемым вложениями*, если существует сколь угодно близкий к нему путь без самопересечений, т. е. для любого $\varepsilon > 0$ существует такой несамопересекающийся путь (т. е. вложение) $f\colon I \to \mathbb{R}^2$, что расстояние между точками $f(x)$ и $\varphi(x)$ меньше ε для любой точки $x \in I$. Аналогично определяется аппроксимируемость вложениями *цикла* $\varphi\colon S^1 \to \mathbb{R}^2$. Пусть I — граф с вершинами $a_0,a_1,\ldots,a_n$ и ребрами $a_0a_1,\ldots,a_{n-1}a_n$. Путь $\varphi\colon I \to \mathbb{R}^2$ называется *симплициальным*, если $\varphi(a_j) \notin \varphi(a_{i-1}a_i)$ для любых $i,j = 1,\ldots,n$ и сужение $\varphi|_{[a_{i-1},a_i]}$ линейно для любого $i = 1,\ldots,n$. Все встречающиеся нам пути будут симплициальными (с разными n).

Строгая формулировка задачи 1a) такова: композиция $\varphi\colon S^1 \to S^1 \subset \subset \mathbb{R}^2$ двукратной намотки и стандартного включения не аппроксимируется вложениями. Чтобы объяснить идею построения препятствия Ван Кампена, приведем наброски двух решений задачи 1a). Назовем путь собаки *незатейливым*, если во время движения по тропинкам она не пересекала свои следы. Для незатейливого пути f поставим на каждой полянке 0, если точки входа собаки на полянку и ее выхода с полянки располагаются как на рис. 2.2a, и 1 в противном случае (рис 2.2b). Пусть $v(f)$ будет суммой по модулю 2 этих двух чисел. Для пути f на рис. 2.1 $v(f) = 1$. Ясно, что $v(f)$ зависит только от расположения отрезков пути собаки на тропинках. При изменении такого расположения на одной тропинке число на каждой полянке изменится, поэтому $v(f)$ не изменится. Так как от любого расположения отрезков пути на тропинках можно перейти к любому другому указанными операциями, то $v(f) = 1$ для *любого* незатейливого пути f. Поэтому собака обязательно пересекала свой след.

Теперь приведем другое решение. Возьмем любой цикл общего положения $f\colon S^1 \to \mathbb{R}^2$, близкий к композиции $\varphi\colon S^1 \to S^1 \subset \mathbb{R}^2$ двукратной намотки и стандартного включения. Для любых двух ребер i, j пересечение $f(i) \cap f(j)$ состоит из конечного числа точек. Пусть $v(f)$ будет суммой по модулю 2 чисел $|f(i) \cap f(j)|$ по всем неупорядоченным парам $\{i, j\}$ несмежных ребер графа S^1. Для цикла f_0, показанного на рис. 2.3, $v(f_0) = 1$. Если в процессе непрерывного изменения f_t, $t \in [0, 1]$, движется только внутренность ребра $e \subset S^1$, то $v(f_0) - v(f_1)$ равно числу точек пересечения цикла $f_0(e) \cup f_1(e)$ с путем $f_0(S^1 - \bar{e})$ (где $\bar{e}$ — объединение ребра e и двух соседних с ним). Так как путь $f_0(S^1 - \bar{e})$ можно замкнуть, не добавляя новых пересечений с $f_0(e) \cup f_1(e)$, то $v(f_0) - v(f_1) = 0$. Это интуитивно очевидное утверждение следует из формулы Эйлера; другое доказательство см. в [2]. Любой цикл $f_1\colon S^1 \to \mathbb{R}^2$ общего положения, близкий к

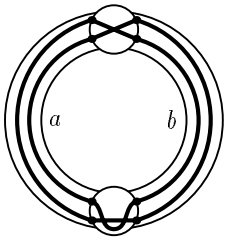


Рис. 2.1.

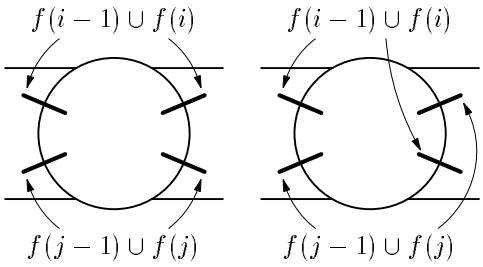


Рис. 2.2.

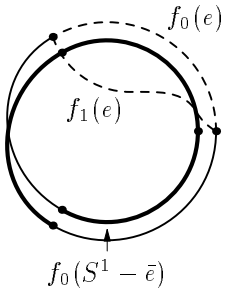


Рис. 2.3.

φ, может быть преобразован к f_0 последовательностью нескольких изотопий плоскости $\mathbb{R}^2$ и нескольких гомотопий, описанных выше. Значит, $v(f) = 1$ для *любого* цикла $f\colon S^1 \to \mathbb{R}^2$, близкого к φ. Следовательно, φ не аппроксимируется вложениями.

2. a) Если образом $\varphi(I)$ пути $\varphi\colon I \to \mathbb{R}^2$ является отрезок или окружность, то этот путь аппроксимируем вложениями.

b) Пути и циклы на рис. 2.4 не аппроксимируемы вложениями (для наглядности мы рисуем не только сам путь f, а близкий к нему путь φ общего положения). Указание: если не получается, используйте нижеследующую теорему или задачу 4a).

c) Эйлеров путь или цикл на плоскости аппроксимируем вложениями тогда и только тогда, когда он не имеет трансверсальных самопересечений (рис. 2.4a).

d) Город N состоит из нескольких площадей (кругов), соединенных непересекающимися дорогами (прямолинейными отрезками). Известно, что существует маршрут, проходящий по каждой дороге ровно один раз (этот маршрут может проходить по площадям несколько раз). Докажите, что существует *несамопересекающийся* маршрут, проходящий по каждой дороге ровно один раз. (Иными словами, в любом нарисованном на плоскости без самопересечений эйлеровом графе существует эйлеров цикл, аппроксимируемый вложениями.)

Теорема. *Симплициальный путь $\varphi\colon I \to \mathbb{R}^2$ аппроксимируем вложениями тогда и только тогда, когда препятствие Ван Кампена $v(\varphi) \in H_0(\Delta) \cong H^2(I^*_\varphi)$ нулевое.*

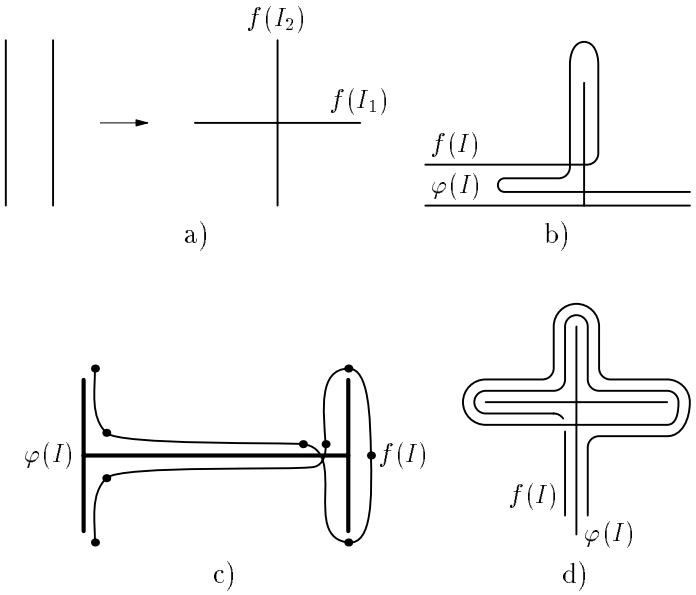


Рис. 2.4.

Определение $H_0(\Delta)$, $H^2(I^*_\varphi)$, $v(\varphi)$ *и доказательство необходимости.* Знакомство с этим доказательством рекомендуем начать с отображений φ и f с рис. 2.4c). Обозначим ребро $a_{i-1}a_i$ графа I числом i.

Построение препятствия Ван Кампена $v(\varphi) \in H_0(\Delta)$ является обобщением первого решения задачи 1a. Для симплициального пути $\varphi\colon I \to \mathbb{R}^2$ построим его *сингулярный граф* Δ (рис. 2.5 на с. 165 для пути на рис. 2.4c). Вершины графа Δ — такие пары (a_i, a_j) вершин графа I, что $\varphi(a_i) = \varphi(a_j)$ и $i - j > 1$. Вершины (a_i, a_j) и $(a_{i\pm1}, a_{j\pm1})$ соединены ребром в графе Δ, если они принадлежат ему (знаки $\pm$ выбираются независимо).

Рассмотрим произвольный незатейливый путь f. В вершине (a_i, a_j) графа Δ поставим число 0, если точки входа пути f на полянку $\varphi(a_i) = \varphi(a_j)$ и точки ее выхода с этой полянки располагаются как на рис. 2.2a, и 1 в противном случае (рис. 2.2b). Полученную расстановку обозначим через $\nu(f)$. Поставим на каждой компоненте связности графа Δ, не содержащей точек (a_i, a_{i+2}), сумму (по модулю 2) чисел в вершинах этой компоненты. Множество всех расстановок нулей и единиц на компонентах графа Δ обозначим через $H_0(\Delta)$. Полученную расстановку $v(\varphi) \in H_0(\Delta)$ назовем *препятствием Ван Кампена (с коэффициентами в* $\mathbb{Z}_2$) к аппроксимируемости пути φ вложениями.

Ясно, что $\nu(f) = 0$ тогда и только тогда, когда путь f можно так изменить на полянках, чтобы он стал несамопересекающимся. Ясно также, что $\nu(f)$ зависит только от расположения отрезков пути на тропинках. При изменении такого расположения на одной тропинке e для любых двух ребер i и j графа I таких, что $\varphi(i) = \varphi(j) = e$, изменятся числа в вершинах (a_i, a_j) и (a_{i+1}, a_{j+1}) (или (a_i, a_{j+1}) и (a_{i+1}, a_j)) графа Δ. Поэтому $v(\varphi)$ не изменится. Так как от любого расположения отрезков пути на тропинках можно перейти к любому другому указанными операциями, то $v(\varphi)$ не зависит от f. Значит, если $v(\varphi) \neq 0$, то путь φ не аппроксимируется вложениями.

Построение препятствия Ван Кампена $v(\varphi) \in H^2(I^*_\varphi)$ является обобщением второго решения задачи 1a. Это построение более сложно, чем предыдущее, но именно оно может быть обобщено до настоящего препятствия Ван Кампена (к вложимости графов в плоскость). Обозначим через I^* верхнюю «наддиагональ» таблицы $n \times n$, т. е. объединение клеток $i \times j$ с $i < j-1$, отвечающих парам несоседних ребер графа I (рис. 2.5). Для любого пути $f\colon I \to \mathbb{R}^2$ общего положения, достаточно близкого к φ, и любых двух несоседних ребер i, j пересечение $f(i) \cap f(j)$ состоит из конечного числа точек. Поставим в клетке $i \times j \in I^*$ число $|f(i) \cap f(j)| \mod 2$. Полученную расстановку назовем *препятствующей* и обозначим через $\nu(f)$: если путь f несамопересекающийся, то $\nu(f) = 0$. Множество расстановок нулей и единиц в клетках «наддиагонали» I^* (в нем $2^{(n-1)(n-2)/2}$ элементов) обозначается через $C^2(I^*)$. Расстановки можно складывать:

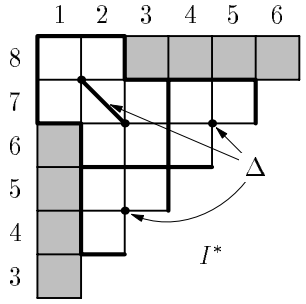


Рис. 2.5.

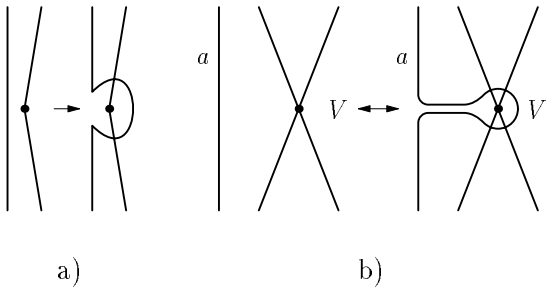


Рис. 2.6.

для этого просто складываются числа, стоящие на каждом ребре (такое сложение называется *покомпонентным*). Покрасим в черный цвет клетки $i \times j$ таблицы I^*, для которых $\varphi(i) \cap \varphi(j) = \varnothing$. Так как путь f близок к φ, то $\nu(f) = 0$ в черных клетках. Обозначим через $C^2_\varphi(I^*)$ подмножество множества $C^2(I^*)$, состоящее из расстановок с нулями в черных клетках. Итак, $\nu(f) \in C^2_\varphi(I^*)$.

При *преобразовании Райдемайстера* пути f на рис. 2.6а расстановка $\nu(f)$ изменяется ровно в двух соседних клетках $i \times j$ и $i \times (j+1)$ (или $j \times i$ и $(j+1) \times i$). Если одна из этих двух клеток не лежит в I^*, то число в ней не стоит и не меняется. Расстановка 1 в клетках таблицы I^*, соседних с ребром e, и 0 в остальных клетках таблицы I^* называется *элементарной кограницей ребра e таблицы I^** и обозначается δe.

Сделаем указанное преобразование Райдемайстера для ребер $e_1, \ldots, e_k$ таблицы I^*. Эту операцию можно задавать расстановкой единиц на ребрах $e_1, \ldots, e_k$ (и нулей на остальных ребрах). Обозначим полученную расстановку через N, а полученный путь через f_N. Множество расстановок нулей и единиц на ребрах таблицы I^* (в нем 2^{n^2-n-2} элементов) с операцией покомпонентного сложения обозначается через $C^1(I^*)$. Каждому ребру e отвечает «характеристическая» расстановка $e \in C^1_\varphi(I^*)$ единицы на ребре e и нуля на остальных ребрах. Определим отображение $\delta\colon C^1(I^*) \to C^2(I^*)$ формулой $\delta(e_1 + \ldots + e_k) = \delta e_1 + \ldots + \delta e_k$. Тогда $\nu(f) - \nu(f_N) = \delta N$.

Покрасим в черный цвет ребра $i \times a_j$ и $a_j \times i$ таблицы I^*, для которых $\varphi(a_j) \notin \varphi(i)$ (таким образом, граница черной клетки состоит из черных ребер, но могут быть и другие черные ребра). Обозначим через $C^1_\varphi(I^*)$ подмножество множества $C^1(I^*)$, состоящее из расстановок с нулями на черных ребрах. Так как f близко к φ, то указанное преобразование Райдемайстера возможно лишь при $N \in C^1_\varphi(I^*)$. Ясно, что $\delta C^1_\varphi(I^*) \subset C^2_\varphi(I^*)$.

Назовем расстановки $\nu_1, \nu_2 \in C^1_\varphi(I^*)$ *когомологичными*, если $\nu_1 - \nu_2 = \delta N$ для некоторого $N \in C^1_\varphi(I^*)$. Группа $H^2_\varphi(I^*) = C^2_\varphi(I^*)/\delta(C^1_\varphi(I^*))$ расстановок с точностью до когомологичности называется *двумерной группой когомологий (с коэффициентами в $\mathbb{Z}_2$) пространства I^* относительно его черного подпространства. Препятствие Ван Кампена (с коэффициентами в $\mathbb{Z}_2$)* определяется как $v(\varphi) = [\nu(f)] \in H^2_\varphi(I^*)$.

Чтобы доказать корректность этого определения, т. е. независимость $v(\varphi)$ от выбора пути f, рассмотрим пути $f_0, f_1 \colon I \to \mathbb{R}^2$ общего положения, близкие к φ. Возьмем произвольную гомотопию $f_t \colon I \to \mathbb{R}^2$, $t \in [0,1]$ общего положения, близкую к φ. На каждом ребре $i \times a_j$ или $a_j \times i$ таблицы I^* поставим число (по модулю 2) моментов времени t, для которых $f_t(a_j) \in f_t(i)$ (это число конечно по соображениям общего положения). Полученную расстановку нулей и единиц на ребрах таблицы I^* обозначим через $N(\{f_t\})$. Так как $f_t(x)$ близко к $\varphi(x)$, то из $\varphi(a_j) \notin \varphi(i)$ вытекает $f_t(a_j) \notin f_t(i)$. Поэтому $N(\{f_t\}) \in C^1_\varphi(I^*)$. Легко проверить, что $\nu(f_0) - \nu(f_1) = \delta N(\{f_t\})$. Поэтому $v(\varphi)$ не зависит от f. Ясно, что $v(\varphi)$ является препятствием к аппроксимируемости пути φ вложениями.

Доказательство изоморфизма $H_0(\Delta) \cong H^2(I^*_\varphi)$ (он называется изоморфизмом Пуанкаре) и того, что два построенных препятствия Ван Кампена переходят друг в друга при этом изоморфизме, оставляем читателю в качестве задачи (решите сначала задачу 3). □

Конструкция препятствия Ван Кампена $v(\varphi) \in H_0(\Delta)$ и доказательство достаточности в теореме (которого мы здесь не приводим) были получены слушателем курса, по материалам которого написана настоящая статья [15].

Обозначим через $I^{*\varphi}$ объединение черных клеток и ребер. Стандартными обозначениями групп $C^k_\varphi(I^*, \cdot)$ и $H^2_\varphi(I^*, \cdot)$ являются $C^k(I^*, I^{*\varphi}, \cdot)$ и $H^2(I^*, I^{*\varphi}, \cdot)$, соответственно.

3. (Вычисление) a) $H^2_\varphi(I^*) \cong \mathbb{Z}_2^k$, где k — число кусков таблицы I^*, ограниченных черными ребрами и содержащих хотя бы одну белую клетку.

b) Для каждого куска из a) сосчитаем сумму стоящих в нем чисел расстановки $\nu(f)$. Тогда $v(\varphi)$ есть набор из k таких сумм.

4. a) Если симплициальный путь $\varphi \colon I \to \mathbb{R}^2$ аппроксимируем вложениями, то

(R) для любого непрерывного движения точек x и y по отрезку I, в процессе которого $\varphi(x) \neq \varphi(y)$, а в конце которого точки x и y возвращаются каждая в свое исходное положение (т. е. для любого непрерывного отображения $S^1 \to \{(x,y) \in I \times I \mid \varphi(x) \neq \varphi(y)\}$), число оборотов вектора от $\varphi(x)$ к $\varphi(y)$ в процессе этого движения равно нулю.

b) То же верно для цикла $\varphi \colon S^1 \to \mathbb{R}^2$ и для отображения $\varphi \colon K \to \mathbb{R}^2$ произвольного графа K.

c) Трехкратная намотка $\varphi \colon S^1 \to S^1 \subset \mathbb{R}^2$ не аппроксимируется вложениями, хотя для нее выполнено условие (R).

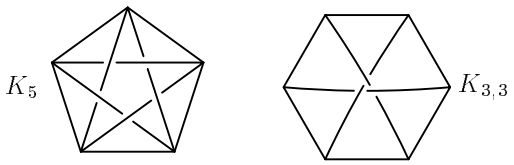


Рис. 2.7.

d) В каждой точке (x, y) на ребре таблицы I^* поставим вектор с направлением от $f(x)$ к $f(y)$. Тогда в каждой клетке таблицы I^* стоит число «четность числа оборотов вектора при обходе по ее границе».

e) Рассмотрим более слабую форму (r) условия (R): число оборотов четно. Тогда $(r) \Leftrightarrow (v(\varphi) = 0)$. Таким образом, препятствие Ван Кампена является частным случаем препятствий, рассмотренных в §1, т.к. таблицу I^* можно рассматривать как двумерный полиэдр, а клетки $i \times j$ как его двумерные клетки.

5. Постройте препятствие Ван Кампена $V(\varphi)$ с $\mathbb{Z}$-коэффициентами и докажите для него аналог задач 3 и 4.

6. Постройте аналог препятствий $v(\varphi)$ и $V(\varphi)$ для аппроксимируемости циклов вложениями. Докажите их неполноту (даже для отображений, образами которых являются триоды).

Теорема. *Следующие условия равносильны для конечного графа* K:

(P) K *планарен* (*т. е. у него существует разбиение, ребра которого попарно не пересекаются*),

(K) K *не содержит подграфов, гомеоморфных графам* K_5 (*полный граф с 5 вершинами*) *и* $K_{3,3}$ (*домики и колодцы*) (*рис.* 2.7),

(v) *препятствие Ван Кампена* $v(K) \in H^2(K^*)$ *нулевое.*

Условие (K) проще, чем (v), но не обобщается на высшие размерности.

Набросок определения $H^2(K^*)$, $v(K)$ *и доказательства.* Чтобы объяснить идею построения препятствия Ван Кампена, докажем непланарность графа K_5. Возьмем любое отображение общего положения $f\colon K_5 \to \to \mathbb{R}^2$. Для любых двух ребер σ, τ пересечение $f(\sigma) \cap f(\tau)$ состоит из конечного числа точек. Пусть $v(f)$ будет суммой по модулю 2 чисел $|f(\sigma) \cap f(\tau)|$ по всем неупорядоченным парам $\{\sigma, \tau\}$ несмежных ребер графа K_5. Для отображения f, показанного на рис. 2.7, $v(f) = 1$. Для каждого ребра графа K_5 с вершинами a, b граф $K_5 - \{a, b\}$, полученный удалением из K_5 вершин a, b и внутренностей ребер, выходящих из a, b, есть окружность (это то самое свойство графа K_5, которое необходимо для доказательства). Поэтому аналогично второму решению задачи 1а $v(f)$ не зависит от f. Значит, $v(f) = 1$ для *любого* отображения $f\colon K_5 \to \mathbb{R}^2$. Следовательно, K_5 не планарен. Непланарность графа $K_{3,3}$ доказывается аналогично. Итак, $(P) \Rightarrow (K)$ доказано.

Докажем теперь $(P) \Rightarrow (v)$. Зафиксируем триангуляцию T графа K. Для любого отображения $f\colon K \to \mathbb{R}^2$ общего положения и любых двух несмежных ребер σ, τ из K пересечение $f(\sigma) \cap f(\tau)$ состоит из конечного числа точек. Пусть $\nu(f)_{\sigma\tau} = |f(\sigma) \cap f(\tau)| \mod 2$. Тогда $\nu(f) \in C^2(K^*)$, где $C^2(K^*)$ есть множество расстановок 0 и 1 на неупорядоченных парах непересекающихся ребер графа K с операцией покомпонентного сложения.

При движении Райдемайстера на рис. 2.6b к $\nu(f)$ добавляется расстановка единицы на паре $\alpha \times \beta$ для $a \in \alpha$ и нуля на остальных парах. Эту расстановку назовем *элементарной кограницей* $\delta(a \times \beta)$ неупорядоченной пары $\{a, \beta\}$. Группа расстановок нулей и единиц на парах $\{v, \beta\}$ с операцией покомпонентного сложения обозначается через $C^1(K^*)$. Итак, $N(\{f_t\}) \in C^1(K^*)$. Определим отображение $\delta\colon C^1(K^*) \to C^2(K^*)$, отношение когомологичности на $C^2(K^*)$, *двумерную группу когомологий* $H^2(K^*) = C^2(K^*)/\delta(C^1(K^*))$ и *препятствие Ван Кампена* $v(K) = [\nu(f)] \in H^2(K^*)$, как и в доказательстве предыдущей теоремы.

Для заданных отображений $f_0, f_1\colon K \to \mathbb{R}^2$ общего положения рассмотрим произвольную гомотопию $f_t\colon K \to \mathbb{R}^2$ общего положения. На каждой паре $\{a, \beta\}$ поставим число (по модулю 2) моментов t, для которых $f_t(a) \in f_t(\beta)$. Полученную расстановку нулей и единиц на парах $\{v, \beta\}$ обозначим через $N(\{f_t\})$ (заметим, что в [11, §2] расстановка $N(\{f_t\})$ определена неправильно). Легко проверить, что $\nu(f_0) - \nu(f_1) = \delta N(\{f_t\})$. Значит, $v(K)$ не зависит от f, и поэтому является препятствием к вложимости графа K в плоскость.

Импликация $(K) \Rightarrow (P)$ была доказана Казимиром Куратовским в 1930 г. (см. простое доказательство в [7]). Доказательство импликации $(v) \Rightarrow (K)$ оставляем читателю в качестве задачи. Прямое доказательство импликаций $(v) \Rightarrow (P)$ и $(K) \Rightarrow (v)$ см. в [13]. □

7. a) Постройте препятствие Ван Кампена $V(K)$ с целыми коэффициентами.

b) Постройте препятствие Ван Кампена $v(K)$ к вложимости n-полиэдра K в $\mathbb{R}^{2n}$ и докажите, что n-остов $(2n+2)$-симплекса не вложим в $\mathbb{R}^{2n}$.

§3. В направлении Штифеля и Уитни

Напомним определение утолщения и двумерного многообразия, используемые в этом параграфе. Для графа K рассмотрим объединение дисков, число которых равно числу вершин графа K. На каждом таком диске введем ориентацию (или, что то же самое, вложим эти диски в плоскость с фиксированной ориентацией). Тогда граничные окружности дисков тоже будут ориентированы. На каждой такой граничной окружности отметим непересекающиеся отрезки, отвечающие выходящим из соответствующей вершины ребрам. Для каждого ребра графа K соеди-

ним (не обязательно в плоскости) соответствующие ему два отрезка ленточкой. Эта ленточка называется *перекрученной*, если стрелки на двух ее противоположных концах, лежащих в дисках, совпадают. Ленточка называется *неперекрученной*, если эти стрелки противоположны. Пусть N — объединение построенных дисков и ленточек. Топологическая пара (N, K), состоящая из N и графа K, естественно вложенного в N, называется *утолщением* графа K. Иногда для краткости мы будем называть утолщением поверхность N. Два утолщения одного графа K *эквивалентны*, если можно изменить ориентации на их дисках так, чтобы

1) ленточки в двух утолщениях, соответствующие одному и тому же ребру графа K, были бы одновременно перекручены или нет, и

2) для любой вершины графа K непересекающиеся отрезки на граничной окружности соответствующего диска идут в одинаковом (ориентированном) порядке.

Заклеив все граничные окружности утолщения дисками, получим *замкнутое 2-многообразие*. Утолщение называется *триангуляцией* соответствующего 2-многообразия, если каждая граничная окружность этого утолщения проходит ровно по трем ленточкам, ровно по трем дискам и при этом каждую ленточку и каждый диск пересекает ровно по одному отрезку. Каждое замкнутое ориентируемое связное 2-многообразие эквивалентно (мы не уточняем, в каком смысле) сфере с g ручками. Здесь g — некоторое число, однозначно определяемое по поверхности и называемое ее *родом*.

A. Ориентируемость

Утолщение называется *ориентируемым*, если оно эквивалентно утолщению, не имеющему перекрученных ленточек. Замкнутое 2-многообразие, полученное из некоторой триангуляции, называется *ориентируемым*, если эта триангуляция ориентируема. При помощи перехода к двойственному клеточному разбиению доказывается, что это определение равносильно стандартному: можно ввести ориентацию на всех 2-симплексах триангуляции (в обычном смысле), так что ориентации соседних 2-симплексов согласованы. Ориентируемость не зависит от триангуляции (кто не хочет этого доказывать, может считать, что ниже везде рассматриваются 2-многообразия с фиксированной триангуляцией).

1. Утолщение окружности на рис. 3.1 (лист Мёбиуса) неориентируемо.

2. Гомеоморфные графы имеют одинаковое количество (ориентируемых) утолщений с точностью до эквивалентности.

3. Сколько (ориентируемых) утолщений с точностью до эквивалентности у
a) окружности, b) триода, c) креста, d) n-ода, e) восьмерки, f) буквы Θ?

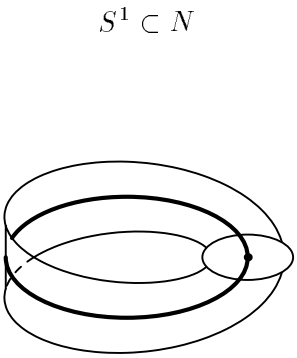
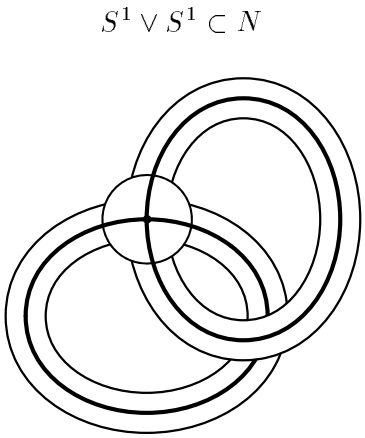


Рис. 3.1.



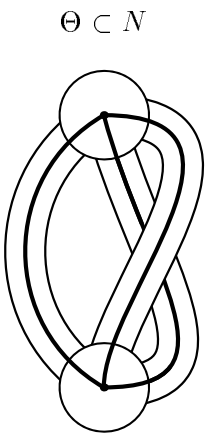


Рис. 3.2.

Проиллюстрируем метод теории препятствий на примере получения критерия ориентируемости утолщения. Этот критерий является по сути лишь переформулировкой определения ориентируемости на алгебраический язык. Кроме того, существует более простой критерий ориентируемости (задача 5). Поэтому приводимый критерий ориентируемости утолщения важен не сам по себе, а именно как иллюстрация метода теории препятствий. Идея доказательства этого критерия нужна при классификации утолщений (задачи 8 и 9).

Теорема. *Утолщение (N,K) (или двумерное многообразие N) ориентируемо тогда и только тогда, когда его первый класс Штифеля – Уитни $w_1(N,K) \in H^1(K)$ (или $w_1(N) \in H^1(N)$) нулевой.*

Вычисление. $H^1(K) \cong \mathbb{Z}_2^{E-V+C}$ ($H^1(N) = \mathbb{Z}_2^{2g} = \mathbb{Z}_2^{2-\chi}$, *где g и χ — род и эйлерова характеристика поверхности N, соответственно*).

Определение $H^1(K)$, $w_1(N,K)$, $H^1(N)$, $w_1(N)$, $H^1(N)$ и доказательство. Рассмотрим сначала случай утолщений. Возьмем набор ориентаций o на дисках данного утолщения N. На каждом ребре графа K поставим 1, если соответствующая ленточка перекручена, и 0 в противном случае. Полученную расстановку назовем *препятствующей* и обозначим $\omega(o)$: если $\omega(o) = 0$, то утолщение N ориентируемо. Конечно, $\omega(o)$ зависит также от утолщения (N,K), но мы не указываем это в обозначениях. Множество всех расстановок нулей и единиц на ребрах графа K с операцией покомпонентного сложения обозначим через $\mathbb{Z}_2^E$. Расстановки можно складывать: для этого просто складываются числа, стоящие на каждом ребре (такое сложение называется *покомпонентным*).

Различие между наборами ориентаций o и o' можно измерять (и задавать) так. На каждой вершине графа K поставим 0, если ориентации соответствующего диска в o и в o' совпадают, и 1 в противном случае. Полученную расстановку назовем *различающей* и обозначим $d(o,o')$: если $d(o,o')=0$, то $o=o'$ (и наоборот). Группу всех расстановок 0 и 1 на вершинах графа K с операцией покомпонентного сложения обозначим через $\mathbb{Z}_2^V$.

Если $\omega(o)\neq 0$, то o не определяет ориентации утолщения, но еще не все потеряно: можно попытаться изменить o, так чтобы препятствующая расстановка стала нулевой. Выясним, как $\omega(o)$ зависит от o. При изменении ориентации одного диска, соответствующего вершине a, к $w(o)$ прибавляется расстановка 1 на ребрах, выходящих из a, и 0 на всех остальных ребрах. Эта расстановка называется *элементарной кограницей вершины* a и обозначается δa. Каждой вершине a отвечает «характеристическая» расстановка $a\in\mathbb{Z}_2^V$ единицы в вершине a и нуля в остальных вершинах. Определим отображение $\delta\colon \mathbb{Z}_2^V\to\mathbb{Z}_2^E$ формулой $\delta(a_1+\ldots+a_k)=\delta a_1+\ldots+\delta a_k$. Тогда $\omega(o)-\omega(o')=\delta d(o,o')$.

Назовем расстановки $\omega_1,\omega_2\in\mathbb{Z}_2^E$ *когомологичными*, если $\omega_1-\omega_2=\delta\Omega$ для некоторого $\Omega\in\mathbb{Z}_2^V$. Группа $H^1(K)=\mathbb{Z}_2^E/\delta(\mathbb{Z}_2^V)$ расстановок с точностью до когомологичности называется *одномерной группой когомологий графа K с коэффициентами в $\mathbb{Z}_2$*. Из формулы $\omega(o)-\omega(o')=\delta d(o,o')$ следует, что *первый класс Штифеля – Уитни* $w_1(N,K)=[\omega(o)]\in H^1(K)$ не зависит от o. Значит, $w_1(N,K)$ является препятствием к ориентируемости утолщения (N,K). Так как $d(o,o')$ может принимать *любое* значение из группы $\delta(\mathbb{Z}_2^V)$, то в случае $\omega(o)\in\delta(\mathbb{Z}_2^V)$ можно так изменить o на o', чтобы получилось $\omega(o')=0$. Значит, $w_1(N)$ является *полным* препятствием к ориентируемости утолщения N.

Критерий ориентируемости многообразий получается аналогично. В этом случае для препятствующей расстановки $w(o)$ сумма чисел на трех ребрах, образующих границу некоторого приклеенного диска, равна нулю. Расстановки с таким условием образуют подгруппу *одномерных коциклов* $Z^1(N)<\mathbb{Z}_2^E$. Проверяется, что $\delta(\mathbb{Z}_2^V)\subset Z^1(N)$. *Первый класс Штифеля – Уитни* $w_1(N)=[\omega(o)]$ получается лежащим в *одномерной группе когомологий* 2-многообразия N (с коэффициентами в $\mathbb{Z}_2$) $H^1(N)=$ $=Z^1(N)/\delta(\mathbb{Z}_2^V)$. □

Для многообразия N класс $[\omega(o)]\in C^1(N)/\delta(\mathbb{Z}_2^V)\cong H^1(K)$ также является (полным) препятствием к ориентируемости, но он лежит в группе $H^1(K)$, которая слишком велика и топологически не инвариантна, т.е. зависит от графа K, а не от многообразия N.

4. Группа $H^1(K)$ зависит только от топологического типа графа K, т. е. одномерные группы когомологий гомеоморфных графов изоморфны.

5. Следующие условия на утолщение (N, K) равносильны ориентируемости:

H) *первый класс Штифеля – Уитни* $w_1^*(N,K)\colon H_1(K) \to \mathbb{Z}_2$ нулевой,

M) (N, K) не содержит подутолщения, гомеоморфного изображенному на рис. 3.1 листу Мёбиуса.

Здесь $H_1(K)$ — множество подграфов графа K, у которых степень каждой вершины четна (или, что то же самое, множество таких расстановок 0 и 1 на ребрах графа K, что для любой вершины a число 1 на ребрах, выходящих из вершины a, четно). Операция симметрической разности (или, что то же самое, покомпонентной суммы по модулю 2) превращает это множество в абелеву группу и в линейное пространство над $\mathbb{Z}_2$. Для любого подграфа $g \in H_1(K)$ сумма $\omega(o)\cdot g$ значений $\omega(o)$ по всем ребрам подграфа g не зависит от набора ориентаций o. Поэтому формула $w_1^*(N,K)(g) = \omega(o)\cdot g$ корректно задает линейную функцию $w_1^*(N,K)\colon H_1(K) \to \mathbb{Z}_2$. Утолщения (N, K) и (N', K') *гомеоморфны*, если от одного можно перейти к другому операциями одновременного подразделения ребра графа и соответствующей ленточки утолщения или обратными. Если L — подграф графа K, то утолщение N графа K содержит утолщение графа L, называемое *подутолщением* утолщения N. Указание к доказательству H$\Leftrightarrow$M: несамопересекающиеся циклы образуют базис в линейном пространстве $H_1(K)$ над $\mathbb{Z}_2$.

6. a) $H_1(K) \cong \mathbb{Z}_2^{E-V+C} \cong H^1(K)$.

b) Отображение $\varphi\colon H^1(K) \to (H_1(K))^*$, заданное формулой $\varphi[\nu](h) = \nu\cdot h$ корректно определено, является изоморфизмом и переводит w_1 в w_1^* (см. задачу 5).

7. Для графа K обозначим через $ST^2(K)$ ($T^2(K)$) множество ориентируемых (всех) утолщений (N, K) с точностью до эквивалентности. Для связного *специального* (т. е. имеющего только вершины степени 3) графа $|ST^2(K)| = 2^{V-1}$ и $|T^2(K)| = 2^E$ (это неверно без предположения о специальности — см. задачу 3).

8. Для связного графа K (не гомеоморфного точке, окружности или отрезку) с V вершинами степеней $k_1, \ldots, k_V$ a) $|ST^2(K)| = \frac{1}{2}(k_1-1)!\cdot\ldots\cdot(k_V-1)!$.

b) первый класс Штифеля – Уитни определяет инвариант $w_1\colon T^2(K) \to H^1(K)$.

c) $|T^2(K)| = 2^{E-V}(k_1-1)!\ldots(k_V-1)!$, где $E = \frac{1}{2}(k_1+\ldots+k_V)$.

9. Для графа K рассмотрим объединение трехмерных шаров, число которых равно V. На каждом таком шаре введем ориентацию (или, что то же самое, вложим эти шары в пространство с фиксированной ориентацией). Тогда граничные сферы дисков тоже будут ориентированы. На каждой такой граничной сфере отметим непересекающиеся двумерные диски, отвечающие выходящим из соответствующей вершины ребрам. Для каждого ребра графа K соединим (не обязательно в трехмерном пространстве) соответствующие ему два диска трубкой. Эта трубка называется *перекрученной*, если ориентации на двух ее противоположных основаниях, лежащих в шарах, совпадают. Трубка называется *неперекрученной*, если эти ориентации противоположны. Пусть N — объединение построенных шаров и трубок. Топологическая пара (N, K), состоящая из N и графа K, естественно вложенного в N, называется *3-утолщением* графа K. Два 3-утолщения графа K *эквивалентны*, если можно изменить ориентации на их дисках так, чтобы трубки в двух утолщениях, соответствующие одному и тому же ребру графа K, были бы одновременно перекручены или нет. Обозначим через $T^3(K)$ множество 3-утолщений графа K с точностью до эквивалентности. Тогда $w_1\colon T^3(K) \to H^1(K)$ является взаимно однозначным отображением на.

10. Какие из утолщений задач 3e, 3f вложимы в плоскость?

11. Понятие утолщения возникло при исследовании вложимости графа в плоскость и в поверхности (ср. §2). Действительно, когда граф вложен в плоскость (или в поверх-

ность), легко выбрать окрестность этого графа, являющуюся его утолщением. Если дано отображение общего положения графа K в плоскость, то аналогично можно построить ориентируемое утолщение графа K, соответствующее этому отображению. Так как любой граф имеет конечное число утолщений (задача 8), то вопрос о вложимости графов в плоскость сводится к вопросу о вложимости ориентируемых утолщений в плоскость.

Следующие условия на утолщение (N, K) равносильны:

P) N вложимо в плоскость,

E) $V - E + S = 2$, где V и E — количества вершин и ребер графа K, а S — число граничных окружностей утолщения N,

S) (N, K) не содержит подутолщений, гомеоморфных изображенным на рис. 3.2.

12. Сформулируйте и решите аналоги задачи 11 для вложений в поверхности (аналог критерия S — только для специальных графов и вложений в тор и лист Мёбиуса).

B. Построение единичных касательных векторных полей

Те, кто не знают, что такое n-мерное многообразие, могут считать, что $n = 2$. *Единичным касательным векторным полем* на подмножестве K гладкого многообразия N называется непрерывное семейство единичных касательных к N векторов в точках подмножества K, гладко зависящих от точки $x \in K$. Исследование векторных полей было начато Анри Пуанкаре в качественной теории дифференциальных уравнений. В этом параграфе, следуя идеям Хайнца Хопфа, мы построим препятствие к существованию единичного ($\Leftrightarrow$ ненулевого) касательного векторного поля на данном гладком замкнутом многообразии. Слово «поле» будет означать «единичное касательное векторное поле».

Теорема Эйлера – Пуанкаре. *Среди сфер с ручками только тор имеет единичное касательное векторное поле.*

Набросок доказательства. Построение поля на торе оставляем читателю в качестве упражнения. Докажем, что на сфере S^2 не существует поля (случай сфер с $g \geqslant 2$ ручками рассматривается аналогично). Рассмотрим на сфере граф S^1 с двумя вершинами (рис. 3.3). Построим поле на множестве S^0 этих двух вершин. Очевидно, что это можно сделать, причем однозначно (с точностью до непрерывной деформации в классе единичных касательных векторных полей). Поэтому существование поля на S^2 равносильно продолжимости построенного поля с S^0 на S^2. Малую окрестность каждого из двух ребер графа S^1 можно рассматривать как часть плоскости. Поэтому поле на S^0 продолжается до поля на S^1 (действительно, поле на ребре есть то же самое, что отображение ребра в окружность: каждому вектору сопоставляется точка на окружности с направлением этого вектора; любое отображение границы отрезка в окружность продолжатся на отрезок). Заметим, что такое продолжение неоднозначно. Обозначим полученное поле на S^1 через v. Малую окрестность каждой из

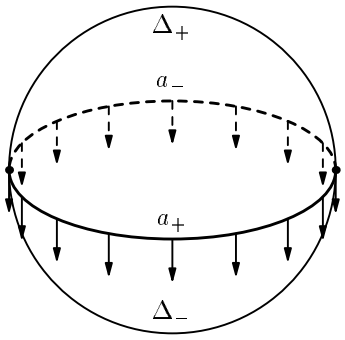


Рис. 3.3.

двух полусфер, на которые данная окружность разбивает сферу, можно рассматривать как часть плоскости. Аналогично рассуждая о продолжении поля с границы $\partial\Delta$ полусферы Δ на саму полусферу Δ, приходим к задаче о продолжении отображения $\partial\Delta \to S^1$ на Δ. Последнее продолжение возможно тогда и только тогда, когда степень $\varepsilon_\Delta(v)$ отображения $\partial\Delta \to S^1$ равна нулю. Положим $e(v) = \varepsilon_{\Delta_+}(v) + \varepsilon_{\Delta_-}(v)$. Ясно, что для поля v', определенного на *всей* сфере, $e(v') = 0$. Для поля v, изображенного на рис. 3.3, $e(v) = 1 + 1 = 2$ (разберитесь, почему не $1 - 1 = 0$!). Различие между полями v и v' на S^1, совпадающими на S^0, можно измерять (и задавать) парой чисел (d_+, d_-): число $d_\pm$ равно числу оборотов вектора при движении от начала ребра $a_\pm$ к его концу (при этом берется вектор первого поля) и обратно (при этом берется вектор второго поля). Ясно, что $\varepsilon_{\Delta_\pm}(v') = \varepsilon_{\Delta_\pm}(v) \pm d_+ \pm d_-$. Поэтому $e(v) = e(v')$ — противоречие. □

Теорема Хопфа. *На ориентируемом n-многообразии N существует единичное касательное векторное поле тогда и только тогда, когда класс Эйлера $e(N) \in H^n(N, \mathbb{Z})$ нулевой.*

Вычисление. *Если N связно и имеет непустой край, то $H^n(N, \mathbb{Z}) \cong$ $\cong 0$ и $e(N) = 0$. Если N связно и замкнуто, то $H^n(N, \mathbb{Z}) \cong \mathbb{Z}$ и $e(N) =$ $= \chi = 2 - 2g$, где χ и g — эйлерова характеристика и род многообразия N (второе равенство имеет смысл и справедливо только для $n = 2$). Далее, $e(N^{2k+1}) = 0$ и $e(S^{2k}) = 2$.*

Определение $H^n(N, \mathbb{Z})$, $e(N)$ и доказательство. Рассмотрим только случай $n = 2$ (общий случай рассматривается аналогично). Возьмем некоторую триангуляцию T многообразия N. Построим поле на множестве T^0 ее вершин. Очевидно, что это можно сделать, причем однозначно (с точностью до непрерывной деформации в классе единичных касательных векторных полей). Поэтому существование поля на N равносильно продолжимости построенного поля с T^0 на N.

Теперь продолжим построенное поле с T^0 на объединение T^1 ребер триангуляции T. Любое ребро триангуляции имеет малую окрестность, диффеоморфную плоскости. Поэтому поле на подмножестве этой окрестности (или, что то же самое, на подмножестве плоскости) отождествляется с отображением этой части (в данном случае, ребра) в окружность: каждому вектору сопоставляется точка на окружности с направлением этого вектора. Любое отображение границы отрезка в окружность продолжатся на отрезок, поэтому построенное поле можно продолжить с T^0 на T^1. Заметим, что такое продолжение неоднозначно.

Пусть теперь на T^1 задано поле v. Попробуем продолжить его на N. Аналогично рассуждая о продолжении поля с границы $\partial\Delta$ грани Δ на саму грань Δ, приходим к задаче о продолжении отображения $\partial\Delta \to S^1$ на Δ. Последнее продолжение возможно тогда и только тогда, когда степень отображения $\partial\Delta \to S^1$ равна нулю. Выберем ориентацию на многообразии N и окружности S^1. Поставим на каждой грани триангуляции T степень указанного отображения $\partial\Delta \to S^1$. Полученную расстановку целых чисел на гранях триангуляции T назовем *препятствующей* и обозначим через $\varepsilon(v)$: поле v продолжается на N тогда и только тогда, когда $\varepsilon(v) = 0$. Группу всех расстановок целых чисел на гранях триангуляции T с операцией покомпонентного сложения обозначим через $\mathbb{Z}^F$, где F — количество граней триангуляции T.

Различие между полями v и v' на T^1, совпадающими на T^0, можно измерять (и задавать) так. На каждом ребре триангуляции T поставим число поворотов вектора при движении от начала ребра e к его концу (при этом берется вектор первого поля) и обратно (при этом берется вектор второго поля). Полученную расстановку назовем *различающей* и обозначим $d(v, v')$: если $d(v, v') = 0$, то поле v можно непрерывно продеформировать в классе единичных касательных векторных полей в поле v' (обратное также справедливо). Группу всех расстановок целых чисел на ребрах триангуляции T с операцией покомпонентного сложения обозначим через $\mathbb{Z}^E$, где E — количество ребер триангуляции T.

Если $\varepsilon(v) \neq 0$, то v не продолжается на T^2, но еще не все потеряно: можно попытаться изменить поле v на T^1, так чтобы препятствующая коцепь стала равной нулю. Для этого выясним, как $\varepsilon(v)$ зависит от v. При изменении поля на одном ребре e «на один оборот» к $\varepsilon(v)$ прибавляется расстановка $+1$ и -1 на двух примыкающих к e гранях (выбор знака определяется ориентациями) и 0 на всех остальных гранях. Эта расстановка называется *элементарной кограницей ребра* e и обозначается δe. Каждому ребру e отвечает «характеристическая» расстановка $e \in \mathbb{Z}^E$ единицы на ребре e и нуля на остальных ребрах. Определим отображение $\delta\colon \mathbb{Z}^E \to \mathbb{Z}^F$ формулой $\delta(n_1 a_1 + \ldots + n_k a_k) = n_1 \delta a_1 + \ldots + n_k \delta a_k$. Тогда $\varepsilon(v) - \varepsilon(v') = \delta d(v, v')$.

Назовем расстановки $\varepsilon_1, \varepsilon_2 \in \mathbb{Z}^F$ *когомологичными*, если $\varepsilon_1 - \varepsilon_2 = \delta\Omega$ для некоторого $\Omega \in \mathbb{Z}^E$. Группа $H^2(N, \mathbb{Z}) = \mathbb{Z}^F/\delta(\mathbb{Z}^E)$ расстановок с точностью до когомологичности называется *двумерной группой когомологий поверхности N с коэффициентами в $\mathbb{Z}$*. Из формулы $\varepsilon(v) - \varepsilon(v') = \delta d(v, v')$ следует, что *класс Эйлера* $e(N) = [\varepsilon(v)] \in H^2(N, \mathbb{Z})$ не зависит от v. Значит, $e(N)$ является препятствием к существованию поля на N. Независимость класса Эйлера от T мы оставляем читателю в качестве задачи. Так как $d(v, v')$ может принимать *любое* значение из группы $\delta(\mathbb{Z}^E)$, то в случае $\varepsilon(v) \in \delta(\mathbb{Z}^E)$ можно изменить v на v', чтобы получилось $\varepsilon(v') = 0$. Это доказывает часть «тогда». □

13. Определите *n-й класс Штифеля – Уитни* $w_n(N) \in H^n(N)$ как полное препятствие к построению единичного касательного векторного поля на неориентируемом n-многообразии N. Вычислите его для $n = 2$.

C. Построение ортонормированных систем векторных полей

Ученик Хопфа Эдуард Штифель рассмотрел задачу о построении *пары, тройки* и т. д. *ортонормированных* касательных векторных полей на данном многообразии (ввиду каноничности процесса ортогонализации Грама – Шмидта ортонормированность можно заменить на линейную независимость). Развивая идеи Хопфа, около 1934 г. он пришел к определению характеристических классов (окончательная формализация была завершена Норманом Стинродом). Любопытно, что Штифель начал с частного случая ориентируемых 3-многообразий и пытался построить пример такого многообразия, на котором не существует пары ($\Leftrightarrow$ тройки) ортонормированных касательных векторных полей. Затем, используя свою теорию, он доказал, что такого многообразия нет. Позже было проделано много других конкретных вычислений, дающих интересные следствия (например, несуществование алгебр с делением на $\mathbb{R}^n$ для $n \neq 2^k$).

Через $\mathbb{Z}_{(i)}$ обозначим группу $\mathbb{Z}$ для четного i и $\mathbb{Z}_2$ для нечетного i.

Теорема Штифеля. *На 3-многообразии N существует пара ортонормированных касательных векторных полей тогда и только тогда, когда второй класс Штифеля – Уитни $w_2(N) \in H^2(N)$ нулевой.*

Вычисление. *$w_2(N) = 0$ для ориентируемого 3-многообразия N.*

Набросок определения $w_2(N)$, $H^2(N)$ и доказательства. Триангулируем N. Построим пару векторных полей на нульмерном остове. Для продолжения пары полей на ребро покроем его одной картой, тогда каждой паре векторов в точке x на этом ребре сопоставится пара векторов в $\mathbb{R}^3$, а всему симплексу отображение ребра в $V_{3,2}$ (пространство ортонормированных 2-реперов в $\mathbb{R}^3$). Из связности пространства $V_{3,2}$ следует, что

построенная пара векторных полей продолжается на 1-остов. Отображение границы $\partial\Delta$ грани Δ в $V_{3,2}$ ставит ему в соответствие элемент из $\pi_1(V_{3,2}) \cong \mathbb{Z}_2$. Таким образом, заданию пары w ортонормированных векторных полей на 1-остове соответствует препятствующая расстановка $\varepsilon(w)$ нулей и единиц на гранях. В нашем случае для препятствующей расстановки $\varepsilon(w)$ сумма чисел на гранях любого 3-симплекса равна нулю. Расстановки с таким условием образуют подгруппу *двумерных коциклов* $Z^2(T) < \mathbb{Z}_2^F$. Далее аналогично предыдущему определяется отображение $\delta\colon \mathbb{Z}_2^E \to \mathbb{Z}_2^F$ и доказывается, что $\delta(\mathbb{Z}_2^E) \subset Z^2(T)$ и что *второй класс Штифеля – Уитни* $w_2(N) = [\varepsilon(w)] \in H^2(N) = Z^2(T)/\delta(\mathbb{Z}_2^E)$ равен нулю тогда и только тогда, когда w можно продолжить на 2-остов. Пары w ортонормированных векторных полей на 2-остове всегда можно продолжить на все многообразие N, поскольку $\pi_2(V_{3,2}) = \pi_2(SO_3) = \pi_2(\mathbb{RP}^3) = \pi_2(S^3) = 0$. □

Теорема. *Если на n-многообразии N существует k ортонормированных касательных векторных полей ($1 < k < n$), то $(n-k+1)$-й класс Штифеля – Уитни*

$$W_{n-k+1}(N) \in H^{n-k+1}(N, \mathbb{Z}_{(n-k)})$$

является нулевым.

Пример вычисления. $w_i(\mathbb{RP}^n) = C_n^i \mod 2$, *где* $w_i(N) \in H^i(N, \mathbb{Z}_2)$ — *приведение по модулю* 2 *препятствия* $W_i(N)$ (*которое легче вычисляется*).

Набросок определения $H^{n-k+1}(N, \mathbb{Z}_{(n-k)})$, $W_{n-k+1}(N)$ *и доказательства.* Аналогично предыдущему, из соотношений $\pi_i(V_{nk}) = 0$ для $i < n-k$, следует, что k полей беспрепятственно строятся на $(n-k)$-остове. Поскольку $\pi_{n-k}(V_{nk}) = \mathbb{Z}_{(n-k)}$ для $1 < k < n$, то при продолжении поля на $(n-k+1)$-остов появляется препятствие $W_{n-k+1} \in H^{n-k+1}(N, \mathbb{Z}_{(n-k)})$ (которое уже не является полным). □

14. a) Определите описанным выше способом w_1 и покажите, что это определение совпадает с полученным в §3.A.

b) В 1942 г. Лев Семенович Понтрягин придумал новые характеристические классы. Владимир Абрамович Рохлин показал, что эти классы естественно появляются при построении системы касательных векторных полей, некоторые фиксированные подсистемы которой имеют ранг, не меньший заданного ранга для каждой из этих фиксированных подсистем (обобщение задачи Штифеля). В дальнейшем оказалось, что классы, рассмотренные Понтрягиным, зависимы (мы не уточняем, в каком смысле) между собой и с классами Штифеля – Уитни. Поэтому среди всех этих классов выделены *классы Понтрягина*, образующие «максимальную независимую систему».

Определите j-й класс Понтрягина $p_j(N) \in H^{4j}(N, \mathbb{Z})$ как препятствие к построению системы из $n - 2j + 2$ векторов, имеющей ранг не менее $n - 2j + 1$ в каждой точке.

D. Погрузимость и вложимость многообразий

Гладкое отображение $f\colon N \to \mathbb{R}^m$ гладкого многообразия N называется *погружением*, если $df(x) \neq 0$ для любой точки $x \in N$. Погружение $f\colon N \to \mathbb{R}^m$ называется *вложением*, если оно инъективно. По соображениям общего положения, любое n-многообразие вкладывается в $\mathbb{R}^{2n+1}$ и погружается в $\mathbb{R}^{2n}$. В 1935 г. Хопф рассказал о результатах Штифеля на Международной топологической конференции в Москве. Там выяснилось, что Хасслер Уитни около 1934 г. тоже естественно пришел к определению характеристических классов, изучая вложимость и погрузимость n-многообразий в $\mathbb{R}^m$ с $m < 2n+1$ и $m < 2n$, соответственно. Используя свою теорию, Уитни доказал вложимость n-многообразий в $\mathbb{R}^{2n}$, их погрузимость в $\mathbb{R}^{2n-1}$, а также невложимость и непогрузимость некоторых проективных пространств. Позже было проделано много других конкретных вычислений, дающих интересные следствия.

Теорема Уитни. *Если n-многообразие N погрузимо в $\mathbb{R}^m$, то $(m-n+1)$-й нормальный класс Штифеля – Уитни*

$$\bar{W}_{m-n+1}(N) \in H^{m-n+1}(N, \mathbb{Z}_{(m-n)})$$

является нулевым.

Примеры вычислений. $\sum_{i=0}^{k} C_n^{k-i} \bar{w}_i(\mathbb{R}\mathbb{P}^n) = 0$, *где* $k > 1$ *и* $\bar{w}_i(N) \in H^i(N, \mathbb{Z}_2)$ *— приведение по модулю 2 препятствия* $\bar{W}_i(N)$. *Если q меньше количества единиц в двоичной записи числа n, то* $\bar{w}_{n-q}(N) = 0$.

Набросок определения $H^{m-n+1}(N, \mathbb{Z}_{(m-n)})$, $\bar{W}_{m-n+1}(N)$ *и доказательства.* Если N погрузимо в $\mathbb{R}^{2n-1}$, то для композиции $N \to \mathbb{R}^{2n-1} \subset \mathbb{R}^{2n}$ погружения и включения существует единичное *нормальное* векторное поле. Аналогично теореме Хопфа можно определить *нормальный класс Эйлера* $\bar{e}(N, f) \in H^n(N, \mathbb{Z})$ как препятствие к построению единичного нормального векторного поля для погружения $f\colon N \to \mathbb{R}^{2n}$. Итак, если N погружается в $\mathbb{R}^{2n-1}$, то $\bar{e}(N, f) = 0$ для *некоторого* отображения f, а именно, для композиции $f\colon N \to \mathbb{R}^{2n-1} \subset \mathbb{R}^{2n}$ (см., впрочем, задачу 16а). Аналогично для композиции $f\colon N \to \mathbb{R}^{2n-1} \to \mathbb{R}^M$ погружения и включения равно нулю $\mathbb{Z}_2$-препятствие к построению $M-2n+1$ ортонормированных нормальных векторных полей, называемое *n-м нормальным классом Штифеля – Уитни* $\bar{w}_n(N, f) \in H^n(N)$. Аналогично, если N погрузимо в $\mathbb{R}^m$, то для композиции $f\colon N \to \mathbb{R}^m \to \mathbb{R}^M$ погружения и включения равно нулю препятствие к построению $M-m$ линейно независимых нормальных векторных полей, называемое *$(m-n+1)$-м нормальным классом Штифеля – Уитни* $\bar{W}_{m-n+1}(N, f) \in H^{m-n+1}(N, \mathbb{Z}_{(m-n)})$. Осталось доказать независимость $\bar{W}_{m-n+1}(N, f)$ от f. Класс $\bar{W}_{m-n+1}(N, f)$ сохраняется

при композиции $f\colon N \to \mathbb{R}^M$ с включением $\mathbb{R}^M \subset \mathbb{R}^{M'}$, поскольку гомоморфизм включения $\pi_{m-n}(V_{M-n,M-m}) \to \pi_{m-n}(V_{M'-n,M'-m})$ является изоморфизмом при $M \geqslant m+2$. Возьмем теперь два разных погружения $f, g\colon N \to \mathbb{R}^m$. Так как $\tau \oplus \nu_f = \tau \oplus \nu_g = m$, то $\nu_f \oplus m = \nu_g \oplus m$, и $\bar{W}_{m-n+1}(N, f) = \bar{W}_{m-n+1}(N, g)$. □

Заметим, что доказательство леммы 1 на с. 178 [5] неполно: доказано, что классы Штифеля – Уитни стабильно эквивалентных расслоений одновременно равны нулю, а не то, что они совпадают. В доказательстве теоремы Уитни фактически строится препятствие к существованию такого расслоения ν над N, что $\nu \oplus \tau = m$. На этой идее основана формулировка теоремы Смейла – Хирша о классификации погружений.

15. Аналогично нормальным классам Штифеля – Уитни *нормальные классы Понтрягина* препятствуют погрузимости: если ориентируемое n-многообразие N погрузимо в $\mathbb{R}^m$, то *k-й нормальный класс Понтрягина* $\bar{p}^k(N) \in H^{4k}(N, \mathbb{Z})$ нулевой для $2k > m - n$.

16. Пусть $f, f'\colon N \to \mathbb{R}^m$ — два погружения n-многообразия N, находящиеся в общем положении.

a) Если N ориентируемо и $m = 2n$, то $f(N) \cap f'(N)$ есть конечное число точек со знаками, сумма которых равна 0 и равна $\bar{e}(N, f)$.

b) Если f, f' — вложения, то $f^{-1}(f(N) \cap f'(N))$ есть подмногообразие многообразия N, гомологический класс которого равен 0 и двойственен по Пуанкаре к $\bar{w}_{m-n}(N)$.

c) Тогда $f^{-1}(f(N) \cap f'(N))$ и $\Sigma(f) = \mathrm{Cl}\{x \in N : |f^{-1}(f(x))| \geqslant 2\}$ есть погруженные подмногообразия многообразия N, причем гомологический класс первого равен 0, а второго — двойственен по Пуанкаре к $\bar{w}_{m-n}(N)$ (и не зависит от f).

17. a) Если n-многообразие N вложимо в $\mathbb{R}^m$, то $\bar{w}_{m-n}(N) = 0$.

b) Если к тому же N ориентируемо и $m - n$ четно, то $\bar{p}_{(m-n)/2}(N) = 0$ (см. задачу 14b).

Благодарности

Эта статья основана на спецсеминарах, которые второй автор вел в 1994–1999 гг. на мехмате МГУ и в июле 1999 года в Кировской Летней Математической Школе. Авторы благодарны А.Б.Сосинскому, М.Н.Вялому и В.В.Ященко за большой труд по редактированию рукописи, С.М.Гусейн-Заде за замечания, В.Курлину и Р.Садыкову за предоставление записей некоторых лекций, М.Скопенкову за обсуждения по §2.

Список литературы

[1] *Akhmetiev P., Repovs D., Skopenkov A.* Obstructions to approximating maps of n-surfaces in $\mathbb{R}^{2n}$ by embeddings // Topol. Appl. To appear.

[2] *Болтянский В. Г. и Ефремович В. А.* Наглядная топология. М.: Наука, 1982.

[3] *Cavicchioli A., Repovš D., Skopenkov A. B.* Open problems on graphs, arising from geometric topology // Topol. Appl., 1998. Vol. 84. P. 207–226.

[4] *Freedman M. H., Krushkal V. S., Teichner P.* Van Kampen's embedding obstruction is incomplete for 2-complexes in $\mathbb{R}^4$ // Math. Res. Letters, 1994. Vol. 1. P. 167–176.

[5] *Фоменко А. Т., Фукс Д. Б.* Курс гомотопической топологии. М.: Наука, 1989.

[6] *van Kampen E. R.* Komplexe in Euclidische Raumen // Abb. Math. Sem. Hamburg, 1932. Vol. 9. S. 72–78. Berichtigung dazu, s. 152–153.

[7] *Makarychev Yu.* A short proof of Kuratowski's graph planarity criterion // J. of Graph Theory, 1997. Vol. 25. P. 129–131.

[8] *Minc P.* Embedding simplicial arcs into the plane // Topol. Proc., 1997.

[9] *Repovš D., Skopenkov A. B.* Embeddability and isotopy of polyhedra in Euclidean spaces // Труды Матем. Инст. РАН, 1996. Т. 212. С. 173–188.

[10] *Repovš D., Skopenkov A. B.* A deleted product criterion for approximability of a map by embeddings // Topol. Appl., 1998. Vol 87. P. 1–19.

[11] *Реповш Д., Скопенков А.* Новые результаты о вложимости полиэдров и многообразий в евклидовы пространства // УМН, 1999. Т. 54, №6. С. 61–109.

[12] *Реповш Д., Скопенков А.* Кольца Борромео и препятствия к вложимости // Труды Матем. Инст. РАН, 1999. Т. 225. С. 331–338.

[13] *Sarkaria K. S.* A one-dimensional Whitney trick and Kuratowski's graph planarity criterion // Israel J. Math., 1991. Vol 73. P. 79–89.

[14] *Siekluckі K.* Realization of mappings // Fund. Math., 1969. Vol. 65. P. 325–343.

[15] *Skopenkov M.* A criterion for approximability by embeddings of PL maps $S^1 \to \mathbb{R}^2$. Preprint, 1999.

Задача об объеме симметризации выпуклого множества

Р. Н. Карасёв

Симметризацией выпуклого множества называется множество, составленное из середин отрезков, соединяющих точки множества и центрально-симметричного ему. В 1985 году английские математики Роджерс и Шепард доказали, что объем симметризации выпуклого компакта в n-мерном пространстве не превосходит $2^{-n}\binom{2n}{n}$ объема исходного компакта. В статье доказывается этот результат при $n = 3$ и обсуждаются некоторые вопросы и идеи, возникающие в процессе доказательства.

1. Формулировка основного результата

Пусть A и B — множества (фигуры) в трехмерном пространстве. *Суммой Минковского* этих множеств называется множество

$$A + B = \{a + b : a \in A, b \in B\}.$$

Оно состоит из объединения всех точек, образованных сдвигами множества A на векторы из B (или наоборот). Определим операцию умножения фигуры на число. Пусть A — множество, λ — число. Тогда по определению

$$\lambda A = \{\lambda a : a \in A\}.$$

Это образ фигуры при гомотетии с коэффициентом λ и центром в начале координат.

Множество, составленное из середин отрезков, один из концов которых лежит на исходной фигуре, а второй — на фигуре, ей центрально-симметричной, называется *симметризацией (по Минковскому)* исходной фигуры. Легко понять, что симметризация фигуры X — это множество $\frac{1}{2}X - \frac{1}{2}X$; заметим, что оно всегда центрально-симметрично и выпукло, если X выпукло.

Обозначим объем множества X через $|X|$. Целью работы является доказательство следующего неравенства:

Теорема 1 (Роджерс – Шепард). *Пусть X — выпуклый компакт в $\mathbb{R}^3$. Тогда*

$$|X - X| \leqslant 20|X|, \tag{1}$$

причем для правильного симплекса достигается равенство.

Поскольку $|\lambda X| = |\lambda|^3|X|$, то для объема симметризации

$$|\frac{1}{2}X - \frac{1}{2}X| \leqslant \frac{5}{2}|X|. \tag{2}$$

Случай равенства в (2) составляет содержание следующей задачи, предложенной на Всероссийской олимпиаде школьников по математике в 1998 году:

Задача 1 (А. Я. Канель). *Даны два центрально-симметрично расположенных правильных тетраэдра с ребром $\sqrt{2}$ — T_1 и T_2. Найдите объем фигуры, состоящей из середин отрезков с концами в T_1 и T_2 соответственно.*

Решение этой задачи в общих чертах таково. Заметим, что искомая фигура Φ при параллельных переносах одного из тетраэдров также подвергается параллельному переносу, что не влияет на ее объем. Тогда можно разместить оба тетраэдра в единичном кубе так, что каждый будет своими вершинами упираться в четыре вершины куба. С помощью несложных векторных равенств можно показать, что Φ выпукла и является выпуклой оболочкой середин ребер куба. Тем самым Φ есть кубооктаэдр, объем которого легко вычисляется и равен $5/6$, что составляет $5/2$ от объема тетраэдра.

Для пространства произвольной размерности n теорема 1 верна в следующей формулировке:

$$|X - X| \leqslant \binom{2n}{n}|X|.$$

Доказательство общего случая можно найти в [1]. Обобщение приводимого ниже доказательства на случай произвольной размерности требует доказательства оценки для *смешанных объемов*, которая в многомерном случае все еще остается гипотезой (см. [2, гл. 4, §7] и [3]).

2. Смешанные объемы

Лемма 1. *Функция $|A+tB|$ при $t \geqslant 0$ является многочленом третьей степени $c_0 + c_1t + c_2t^2 + c_3t^3$ для любых двух выпуклых множеств A и B.*

Вместо доказательства леммы рассмотрим в качестве иллюстрации такой пример: A — некоторый многогранник, а B — единичный шар. В

этом случае множество $A + \varepsilon B$ является ε-окрестностью многогранника (т.е. множеством точек, удаленных от A не более, чем на ε). Можно описать это множество так: это сам многогранник, слои толщиной ε на гранях многогранника (это в точности точки, для которых ближайшая точка многогранника лежит на грани), цилиндрические сектора на ребрах многогранника (для этих точек ближайшие точки — на ребрах), и куски шаров радиуса ε, ограниченные выходящими из вершин многогранными углами (это множество точек, ближайшими к которым являются вершины многогранника). Строение $A + \varepsilon B$ сразу дает формулу:

$$|A + \varepsilon B| = |A| + c_1\varepsilon + c_2\varepsilon^2 + \frac{4}{3}\pi\varepsilon^3.$$

Здесь c_1 — площадь поверхности A (на самом деле *площадь* поверхности некоторой фигуры Φ *по Минковскому* определяется равенством $S(\Phi) = \frac{d}{d\varepsilon}|\Phi + \varepsilon B|$ при $\varepsilon = 0$).

Коэффициент c_2 равен $\sum \frac{1}{2} l_i(\pi - \alpha_i)$, где l_i — длина i-го ребра, α_i — двугранный угол при этом ребре, сумма берется по всем ребрам. Отметим, что если мы нарисуем фиктивное ребро на грани многогранника, то оно внесет нулевой вклад в сумму, так как двугранный угол при нем будет равен π.

Коэффициент c_3 при ε^3 равен $(4/3)\pi$, так как при больших ε этот коэффициент играет главную роль в выражении, а $A + \varepsilon B$ — это почти шар εB, объем которого и есть $\frac{4}{3}\pi\varepsilon^3$.

Обратим внимание на то, что даже если A не является многогранником, то $|A+\varepsilon B|$ тем не менее является многочленом. В самом деле, можно найти многогранники, сколь угодно близкие к A. Объемы сумм Минковского для таких многогранников (многочлены) будут приближаться к $|A+\varepsilon B|$. Теперь достаточно проделать небольшое упражнение по анализу и понять, что если функция сколь угодно близко приближается многочленом фиксированной степени, то она сама многочлен той же или меньшей степени.

Аналогичное рассуждение показывает, что коэффициенты c_i близки для близких друг к другу многогранников, что не так уж очевидно при выражении этих коэффициентов через площади поверхностей и длины ребер.

Заметим также, что если A — гладкая выпуклая фигура, а не многогранник, то c_3 — это интеграл от гауссовой кривизны (по поверхности фигуры), а c_2 — интеграл от средней кривизны. Величины c_k иногда называют *функционалами Минковского.*

Понятие *смешанного объема* (см. [4]) возникает при рассмотрении сумм нескольких множеств. Приведем соответствующее определение.

Рассмотрим для n выпуклых компактов (т. е. ограниченных и замкнутых множеств) X_i в n-мерном пространстве объем суммы Минковского $t_1X_1+t_2X_2+\ldots+t_nX_n$, $t_i \geqslant 0$. Утверждается, что это многочлен степени n от переменных t_i, поэтому его можно записать в виде:

$$|t_1X_1 + t_2X_2 + \ldots + t_nX_n| = \sum_{1\leqslant i_j\leqslant n} V(X_{i_1}, X_{i_2}, \ldots, X_{i_n})t_{i_1}t_{i_2}\ldots t_{i_n},$$

где коэффициенты при равных одночленах полагаем равными. Эти коэффициенты $V(X_{i_1}, \ldots, X_{i_n})$ и называются *смешанными объемами*.

Аналогично суммам двух множеств, существование смешанных объемов легче доказать для случая, когда X_i — многогранники. В этом случае объем суммы Минковского допускает явное (но довольно неудобное) выражение через объемы граней разных размерностей. Для произвольных выпуклых компактов это утверждение также будет верным, так как любой выпуклый компакт приближается многогранниками, а операция разности и функция объема в определенном смысле непрерывны. Поэтому объемы сумм Минковского компактов и приближающих многогранников будут мало различаться.

По определению смешанные объемы не зависят от перестановки своих аргументов и обладают некоторыми другими интересными свойствами, например, полилинейностью по своим аргументам. Еще одно важное свойство смешанных объемов — монотонность:

$$V(X_1, X_2, \ldots, X_n) \leqslant V(Y_1, Y_2, \ldots, Y_n) \tag{3}$$

при условии, что $X_i \subseteq Y_i$. Его можно доказать, рассматривая изменение смешанного объема при замене только одного из X_i бóльшим подмножеством. Чтобы доказать монотонность для многогранников, рассмотрим замену в смешанном объеме первого аргумента X_1 на Y_1 ($X_1 \subseteq Y_1$). Рассматривая строение $t_1X_1 + \ldots + t_nX_n$, можно увидеть, что в выражении для объема этого множества линейный по t_1 член — это сумма площадей граней $t_2X_2 + \ldots + t_nX_n$, умноженных на расстояние между началом координат (которое считается расположенным внутри X_1) и плоскостью, опорной к X_1 и параллельной данной грани (сравните со случаем двух множеств, одно из которых — единичный шар, его роль выполняет X_1). При замене X_1 бóльшим множеством расстояние от начала координат до опорной к X_1 плоскости в данном направлении увеличится, а значит, увеличится и смешанный объем.

Возвращаясь к сумме двух выпуклых множеств, можно написать

$$|A + tB| = \sum \binom{n}{k} V(\underbrace{A, \ldots, A}_{n-k}, \underbrace{B, \ldots, B}_{k})t^k.$$

Смешанные объемы с повторяющимися аргументами в дальнейшем

будем обозначать $V(A, n-k; B, k)$. Для сумм двух множеств монотонность смешанного объема приводит к не такому уж тривиальному факту: при замене A на множество, в нем содержащееся, коэффициенты многочлена $|A + tB|$ уменьшаются.

3. Доказательство теоремы (1)

Обозначим для выпуклого множества X

$$X^* = -X = \{-x : x \in X\}.$$

Нас интересует значение многочлена $|X+tX^*|$ при $t = 1$, поэтому нужно оценить сверху его коэффициенты, которые мы обозначили через c_i.

Так как $|X + tX^*| = |tX + X^*|$, то $c_0 = c_3 = |X|$ и $c_1 = c_2$. Значит, теорема 1 равносильна оценке:

Лемма 2. *В приведенных выше обозначениях* $c_1 = c_2 \leqslant 9|X|$.

Доказательство леммы 2 использует следующую лемму, которую мы сформулируем для множества X в $\mathbb{R}^n$ при произвольном n.

Лемма 3. *Для произвольного множества X в n-мерном пространстве множество X^* можно поместить в X, уменьшив X^* в n раз.*

Доказательство. Рассмотрим симплекс S (в трехмерном случае просто тетраэдр) наибольшего объема, который можно поместить в X, пусть его вершины — это $p_0, p_1, \ldots, p_n$. Ясно, что точки p_i лежат на поверхности X. Проведем через каждую p_i плоскость α_i, параллельную плоскости, проходящей через остальные p_j. Если хотя бы одна точка $p \in X$ лежит по другую сторону от α_i по сравнению с p_j $(j \neq i)$, то, заменив p_i на p, можно увеличить объем симплекса S. Значит, все плоскости α_i — опорные и X содержится в симплексе, ограниченном плоскостями α_i. Легко видеть, что этот симплекс подобен S с коэффициентом $-n$, значит, $S \supset X \supset -\frac{1}{n}X^*$.

Доказательство леммы 2. Оценка

$$c_1 = c_2 = 3V(X, X, X^*) = 3 \cdot 3V(X, X, \tfrac{1}{3}X^*) \leqslant 9V(X, X, X) = 9|X|$$

следует из монотонности входящих в нее смешанных объемов. Монотонность в данном случае доказывается аналогично доказательству (3).

Как и выше, достаточно рассмотреть случай многогранников. Заметим, что

$$V(A, A, B) = \frac{1}{3}\frac{d}{dt}|A + tB|\,\Big|_{t=0}.$$

Член первого порядка в $|A + tB|$ есть сумма по всем граням A произведений площади грани на расстояние между плоскостями, параллельными

этой грани, одна из которых проходит через фиксированную точку внутри B, а другая — опорная к B с той же стороны, где находится соответствующая грань A. Расстояние между такими плоскостями уменьшится, если B заменить на содержащееся в нем множество, а значит, вся сумма также уменьшится.

4. Замечания и дополнения

1. Метод, использующий лемму 3, допускает обобщение на многомерный случай, приводя к оценке

$$c_i \leqslant n^{\min\{i,n-i\}} \binom{n}{k},$$

которая приведена в [5]. Правда, для симплекса в n-мерном пространстве эти коэффициенты, видимо, имеют меньшие значения. Есть гипотеза, что $c_i \leqslant \binom{n}{i}^2 |X|$ (см. [4]), т.е. случай симплекса является экстремальным. В терминах смешанных объемов

$$V(X, i; X^*, n-i) \leqslant \binom{n}{i} |X|$$

и тогда, в силу равенства

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n},$$

суммированием получается следующее соотношение

$$|X + X^*| \leqslant \binom{2n}{n} |X|.$$

К сожалению, провести доказательство для $n > 3$ пока не удается, так как полученная нами оценка и оценка в гипотезе совпадают только при $i = 1, n-1$.

Было бы интересно также получить оценки сверху для смешанных объемов, в которых фигурируют два или более выпуклых тела, в отличие от случая X и X^*.

2. Изучая выражение $|A+\varepsilon B|$, где A — параллелепипед, а B — единичный шар, можно решить следующую интересную задачу (Турнир Городов 1998 года):

Задача 2 (А.Шень). *Можно ли поместить параллелепипед с бóльшим периметром в параллелепипед с меньшим периметром?* (*Периметр — сумма длин ребер.*)

Ответ на вопрос этой задачи отрицателен, так как сумма двугранных углов при параллельных ребрах параллелепипеда равна 2π и, следователь-

но, коэффициент c_2 равен $\pi/4$, умноженному на периметр. В самом деле, предположим противное. Учитывая

$$|A_1 + \varepsilon B| \leqslant |A_2 + \varepsilon B| \qquad (A_1 + \varepsilon B \subseteq A_2 + \varepsilon B)$$

и равенство коэффициентов c_3 в этих выражениях, легко выводим, что первый периметр не более второго.

Еще одно, более идейное, решение этой задачи получается применением монотонности смешанных объемов.

3. Есть много других интересных вопросов о суммах Минковского. Например, характеризация множеств, являющихся суммами Минковского отрезков. Если два отрезка на плоскости не параллельны, то их сумма Минковского — параллелограмм. Если три отрезка в $\mathbb{R}^3$ некомпланарны, то их сумма Минковского — параллелепипед. Однако, если взять больше отрезков (для определенности будем рассматривать трехмерное пространство), то получаются менее тривиальные примеры. Оказывается, что многогранник является суммой Минковского отрезков, или *зоноэдром*, если все его грани имеют центр симметрии (это нетрудно доказать). Иначе можно сказать, что зоноэдры — это проекции многомерных параллелотопов. Это также в точности те многогранники, которые можно разрезать на параллелепипеды. Если рассматривать произвольные выпуклые фигуры, то те из них, которые можно сколь угодно приблизить зоноэдрами, называются *зоноидами*. В качестве упражнения можно ответить на вопрос: какими свойствами характеризуются зоноиды среди остальных выпуклых фигур?

Список литературы

[1] *Rogers C. A., Shephard G. C.* Some extremal problems for convex bodies // Mathematika, 1985. Vol. 5. No 2. P. 93–102.

[2] *Бураго Д. М., Залгаллер И. А.* Геометрические неравенства. Ленинград: Наука, 1980.

[3] *Makai E.* Research problem // Period. Math. Hung., 1974. Vol. 5. No 4. P. 352–354.

[4] *Minkowsky H.* Theorie der konvexer Körper, insbesondere Begründing ihres Oberflächenbegriffs. Ges. Abh., 2. Leipzig — Berlin, 1911, S. 131–229.

[5] *Bonnesen T., Fenchel W.* Theorie der konvexen Körper. Berlin, 1934.

Что такое преобразование Фурье?

М. Кельберт

1. Ряды Фурье и дискретное преобразование Фурье

Метод преобразования Фурье играет исключительно важную роль в математической физике: Норберт Винер считал его одним из важнейших достижений человечества (см. книгу Н. Винера «Я — математик»).

С помощью преобразования Фурье можно исследовать химическое строение отдаленных планет (спектральный анализ сигналов радиотелескопов), исследовать функциональные системы человеческого организма (спектральный анализ кардиограмм, энцефалограмм) и т. д.

Много книг написано о создателе этого метода — французском математике Жане Батисте Жозефе Фурье (см., например, [2]). В них рассказывается, в частности, о его путешествии, вместе с другими учеными, в Египет, в составе знаменитой экспедиции Наполеона. Во время этого путешествия он не только занимался математикой, но и с успехом участвовал в расшифровке египетских иероглифов. На обратном пути во Францию Фурье и его коллеги, которые везли с собой археологические находки, были захвачены англичанами. Следуя благородному духу той эпохи, англичане высадили ученых на безопасный берег (в 1801 году Фурье вернулся во Францию на английском бриге "Good Design"), а впоследствии вернули во Францию захваченные ими драгоценные древние рукописи[1)].

Мы начнем обзор открытого Фурье метода с так называемых *рядов Фурье*. Выражения вида

$$a_0 + a_1 \cos x + b_1 \sin x + \ldots + a_n \cos nx + b_n \sin nx$$

называются *тригонометрическими полиномами* (степени n). Оказывается, что любая непрерывная (и не только непрерывная) функция на $(-\pi, \pi)$ может быть аппроксимирована с наперед заданной точностью тригонометрическими полиномами с подходящими коэффициентами $a_0, \ldots, a_n$, $b_1, \ldots, b_n$.

Это утверждение можно проиллюстрировать, сравнивая графики функций $y = x$, $y = |x|$, $y = x^2$ с графиками тригонометрических

[1)] Французы «благородной» эпохи возвращать захваченные рукописи египтянам не стали. — *Прим. ред.*

полиномов, аппроксимирующих эти функции (см. рис. 1):

$$y = 2\sin x - \sin 2x + \frac{2}{3}\sin 3x - \frac{1}{2}\sin 4x + \frac{2}{5}\sin 5x - \frac{1}{3}\sin 6x + \frac{2}{7}\sin 7x,$$

$$y = \frac{\pi}{2} - \frac{4}{\pi}\cos x - \frac{4}{9\pi}\cos 3x,$$

$$y = \frac{\pi^2}{3} - 4\cos x + \cos 2x - \frac{4}{9}\cos 3x + \frac{1}{4}\cos 4x - \frac{4}{25}\cos 5x$$

(догадайтесь, почему в первом случае появляются только синусы, а в остальных только косинусы). Интересно заметить, что для приближения функций $y = |x|$ и $y = x^2$ с удовлетворительной точностью требуется меньше гармоник, чем в случае функции $y = x$.

Линейные комбинации функций вида $\sin\frac{kx}{T}$ и $\cos\frac{kx}{T}$, также называемые тригонометрическими полиномами, имеют период $2\pi T$. Поэтому можно так переформулировать наше утверждение: *любая периодическая функция может быть аппроксимирована тригонометрическими полиномами.*

Этот факт, обнаруженный Фурье в ходе его исследований по распространению тепла, имеет важное значение для физики. Действительно, функции синус и косинус описывают простейшие волны, называемые *монохроматическими*, т.е. волны фиксированной длины (или фиксированной частоты, если рассматривать x как время). Поскольку любую периодическую функцию можно интерпретировать как профиль некоторой волны, открытие Фурье можно выразить следующим образом: любая волна может быть представлена как суперпозиция (сумма) монохроматических волн.

Из школьного курса физики вы, вероятно, знакомы с изящной демонстрацией этого факта в опыте со стеклянной призмой. На призму направляется пучок белого света, который представляет из себя смесь электромагнитных волн различных частот. С другой стороны призмы можно увидеть несколько лучей света различных цветов от фиолетового до красного. Каждый из этих лучей соответствует электромагнитным колебаниям определенной частоты, т.е. может рассматриваться как монохроматическая волна. Итак, этот опыт экспериментально доказывает разложимость падающего пучка на монохроматические волны. Физик назовет коэффициенты этого разложения *амплитудами монохроматических волн*, а математик назовет их *коэффициентами Фурье.*

Именно коэффициенты Фурье стоят в тригонометрических полиномах, графики которых приведены на рис. 1.

Как найти эти коэффициенты? Рассуждение Фурье [1], которое с современной точки зрения нельзя назвать строгим, состоит в следующем.

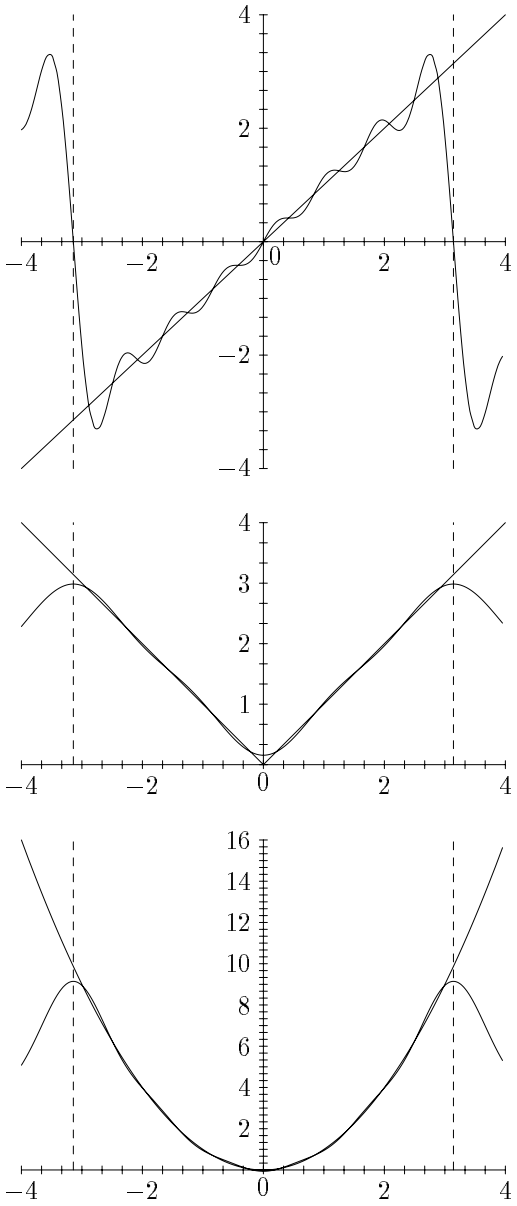


Рис. 1.

Пусть функция $f(x)$, имеющая период $2\pi T$, представлена рядом Фурье

$$f(x) = \frac{1}{2}a_0 + \sum_{n=1}^{\infty} a_n \cos\frac{nx}{T} + b_n \sin\frac{nx}{T}. \tag{1}$$

Для тригонометрических функций выполняются соотношения

$$\int_{-\pi T}^{\pi T} \cos\frac{nt}{T}\sin\frac{mt}{T}\,dt = 0, \quad \int_{-\pi T}^{\pi T} \cos\frac{nt}{T}\cos\frac{mt}{T}\,dt = \int_{-\pi T}^{\pi T} \sin\frac{nt}{T}\sin\frac{mt}{T}\,dt = \delta_{n,m}\pi T, \tag{2}$$

где $\delta_{n,n} = 1$, $\delta_{n,m} = 0$ при $n \neq m$. Поэтому, если формально умножить равенство (1) на $\cos\frac{mx}{T}$ или $\sin\frac{mx}{T}$ и почленно проинтегрировать от $-\pi T$ до πT, «лишние» гармоники исчезнут и получится формула для коэффициентов

$$a_m = \frac{1}{\pi T}\int_{-\pi T}^{\pi T} f(t)\cos\frac{mt}{T}\,dt, \qquad b_m = \frac{1}{\pi T}\int_{-\pi T}^{\pi T} f(t)\sin\frac{mt}{T}\,dt. \tag{3}$$

Заметим, что в силу формулы Эйлера $e^{ix} = \cos x + i\sin x$ любой тригонометрический полином может быть записан в следующем виде

$$c_{-n}e^{-inx} + \ldots + c_{-1}e^{-ix} + c_0 + c_1 e^{ix} + \ldots + c_n e^{inx},$$

где $c_k = \frac{1}{2}(a_k + ib_k)$, $k > 0$, $c_0 = a_0$, $c_k = \frac{1}{2}(a_k - ib_k)$, $k < 0$. Поэтому формулы (1) и (3) можно переписать в более удобном виде (полагая $T = 1$)

$$f(x) = \sum_{k=-\infty}^{\infty} c_k e^{ikx}, \quad c_k = (2\pi)^{-1}\int_{-\pi}^{\pi} f(x)e^{-ikx}dx. \tag{4}$$

Если более внимательно приглядеться к опыту с призмой, то можно заметить, что получается «непрерывный спектр», а не дискретный набор лучей. Для описания таких разложений имеется *интегральная формула Фурье*. Ее можно получить, подставляя выражения (3) в формулу (1) и переходя формально к пределу $T \to \infty$

$$f(x) = \frac{1}{\pi}\int_0^{\infty} du \int_{-\infty}^{\infty} f(t)\cos u(x-t)\,dt = \int_0^{\infty}[a(u)\cos xu + b(u)\sin xu]\,du, \tag{5}$$

где

$$a(u) = \frac{1}{\pi}\int_{-\infty}^{\infty} f(t)\cos ut\,dt, \quad b(u) = \frac{1}{\pi}\int_{-\infty}^{\infty} f(t)\sin ut\,dt.$$

Теория рядов Фурье и непрерывного преобразования Фурье достаточно сложна и преподносит немало неожиданностей. Однако не обязательно владеть этой теорией в полном объеме для того, чтобы успешно использовать преобразование Фурье (или, как говорят математики, гармонический анализ) для решения практических задач. Дело в том, что экспериментальные данные, которые обрабатываются на компьютерах, обычно представляются в виде конечной (быть может, очень длинной) последовательности чисел. В этом случае применяется дискретное преобразование Фурье, с которым работать гораздо легче. Мы начнем с определения дискретного преобразования Фурье и обсудим его связь с проблемой сжатия (редукции) данных.

Что такое дискретный аналог ряда Фурье? Периодические функции с периодом 2π можно рассматривать как функции на окружности единичного радиуса. Пусть $z = e^{2\pi i/m}$. Дискретным аналогом этой окружности служит набор точек $z^j = e^{2\pi ij/m}$, $(j = 1, \dots, m)$, а периодической функции — периодическая последовательность $(y_1, y_2, \dots)$, $y_k = y_{k+m}$. Назовем *дискретным преобразованием Фурье* последовательности $\bar{y} = (y_1, \dots, y_m)$ следующую (вообще говоря, комплексную) последовательность

$$c_j = \sum_{k=1}^{m} y_k z^{kj}, \quad j = 1, \dots, m. \tag{6}$$

Любая такая последовательность может быть легко восстановлена с помощью формулы обращения Фурье

$$y_k = m^{-1} \sum_{j=1}^{m} c_j z^{-kj}, \tag{7}$$

где c_j, $j = 1, \dots, m$, — коэффициенты Фурье, определенные выше.

Иными словами, исходная последовательность чисел $\bar{y}$ (которую можно периодически продолжить в обе стороны) представляется в виде ряда по «элементарным гармоникам» $e^{-2\pi ij/m}$ с коэффициентами c_j. Равенства (6) и (7) являются дискретными аналогами соотношений (4).

Приведем примеры дискретного преобразования Фурье при малых значениях m:

($m = 2$) $c_1 = y_2 - y_1, c_2 = y_1 + y_2$;

($m = 3$) $c_1 = y_3 - \frac{1}{2}(y_2 + y_1) + i\frac{\sqrt{3}}{2}(y_1 - y_2)$,

$c_2 = y_3 - \frac{1}{2}(y_2 + y_1) - i\frac{\sqrt{3}}{2}(y_1 - y_2)$, $\quad c_3 = y_1 + y_2 + y_3$;

($m = 4$) $c_1 = y_4 - y_2 + i(y_1 - y_3)$, $\quad c_2 = y_2 - y_1 - y_3 + y_4$,

$c_3 = y_4 - y_2 + i(y_1 - y_3)$, $\quad c_4 = y_1 + y_2 + y_3 + y_4$.

Проверьте, что и в общем случае $c_m = y_1 + y_2 + \ldots + y_m$.

Задача 1. Докажите, что для альтернирующего дискретного сигнала $y_k = (-1)^k$, $1 \leqslant k \leqslant m$, и четного m выполнено $c_{m/2} = m$, $c_k = 0$, $k \neq m/2$.

Задача 2. Докажите формулу обращения.

Подсказка. Проверьте, что, как и в случае рядов Фурье, «лишние» гармоники исчезнут при суммировании.

Можно сказать, что формула обращения задает представление последовательности в виде тригонометрического полинома, в то время как формула, определяющая преобразование Фурье, дает коэффициенты этого полинома.

Во многих приложениях объем необходимой числовой информации слишком велик даже для современных мощных компьютеров. В этом случае возникает проблема *сжатия данных* (т.е. сокращения числового массива таким образом, чтобы можно было воспроизвести исходные данные с достаточной точностью). Приближение функций с помощью тригонометрических полиномов часто оказывается полезным при решении этой проблемы.

Предположим, что значения $y_1 = f(x_1), \ldots, y_m = f(x_m)$ функции $f(x)$, явное аналитическое выражение для которой не известно, измеряются в некотором эксперименте и по данным $y_1, \ldots, y_m$ нам удалось численно оценить коэффициенты Фурье функции $f(x)$.

Часто оказывается, что функция

$$\hat{f}(x) = a_0 + a_1 \cos x + b_1 \sin x + \ldots + a_n \cos nx + b_n \sin nx$$

хорошо приближает функцию $f(x)$, даже когда число элементарных гармоник n значительно меньше объема данных m. В этом случае достаточно запомнить в памяти компьютера только коэффициенты Фурье вместо исходного объема данных.

Поскольку значения функции $y_i = f(x_i)$ известны экспериментатору лишь в отдельных точках x_i, $i = 1, \ldots, m$, коэффициенты Фурье функции $f(x)$ должны определяться по этой последовательности. Аналогичная ситуация возникает при вычислениях на компьютерах, если аналитическое выражение для функции $f(x)$ недоступно или является достаточно сложным.

Поэтому в дальнейшем мы будем интересоваться не коэффициентами Фурье непрерывных функций, а коэффициентами Фурье конечных последовательностей $\bar{y} = (y_1, \ldots, y_m)$. Эффективная процедура их вычисления имеет большое практическое значение. Она называется *быстрым преобразованием Фурье* (*БПФ*).

2. Китайская теорема об остатках

Любое натуральное число, не превосходящее $M = \prod_{j=1}^{k} m_j$, где числа m_j — попарно взаимно простые, может быть единственным образом восстановлено, если известны остатки от деления этого числа на m_j, $j = 1, \ldots, k$.

Эта теорема была открыта в древнем Китае в первом столетии нашей эры, ее обычно называют *китайской теоремой об остатках* или *теоремой Сон-Ши*.

Для доказательства этой теоремы нам потребуются некоторые факты из элементарной теории чисел (в частности, из теории остатков).

Упражнение. Найдите остаток от деления числа 62^{50} на 5.

Мы опустим некоторые определения, относящиеся к элементарной теории чисел. Их можно найти в любом учебнике (например, [3]). Нам потребуется также следующая теорема, доказательство которой советуем придумать, вспомнить или прочитать в учебнике.

Теорема 1. *Пусть M и m — взаимно простые числа. Тогда существуют целые числа N и n такие, что $NM + nm = 1$.*

Сформулируем теперь китайскую теорему об остатках. Поскольку эта теорема имеет ключевое значение для нас, приведем ее доказательство.

Теорема 2. *Пусть $M = \prod_{j=1}^{k} m_j$ — произведение попарно взаимно простых чисел. Тогда для любых c_j, $0 \leqslant c_j < m_j$, существует единственное решение следующей системы сравнений*

$$c \equiv c_j \pmod{m_j}, \quad j = 1, \ldots, k, \tag{8}$$

такое что $0 \leqslant c < M$.

Доказательство. Прежде всего докажем единственность решения. Пусть c и c' два различных решения (8), не превосходящих M. Тогда

$$c = Q_j m_j + c_j, \qquad c' = Q'_j m_j + c_j, \quad j = 1, \ldots, k.$$

Число $c - c' = (Q_j - Q'_j) m_j$ делится без остатка на любое m_j, а, значит, и на $M = \prod_{j=1}^{k} m_j$, поскольку числа m_j не имеют общих делителей. С другой стороны, $0 \leqslant c, c' < M$, т.е. $-M < c - c' < M$. Поэтому $c - c' = 0$.

Для доказательства существования решения используем теорему 1. Положим $M_j = \dfrac{M}{m_j}$ и найдем такие N_j и n_j, что $M_j N_j + m_j n_j = 1$. Покажем, что

$$c = \sum_{r=1}^{k} c_r N_r M_r \mod M \tag{9}$$

и есть решение системы (8). Действительно, для каждого $j = 1, \ldots, k$

$$c = \sum_{r=1}^{k} c_r N_r M_r \equiv c_j N_j M_j \pmod{m_j},$$

поскольку M_r делится без остатка на m_j (при всех $r \neq j$). А так как $M_j N_j + m_j n_j = 1$, то $M_j N_j = 1 \pmod{m_j}$ и потому $c = c_j \pmod{m_j}$. Это завершает доказательство теоремы. □

Упражнения. 1. Пусть $m_1 = 3, m_2 = 4, m_3 = 5$. Найдите такое число, не превосходящее 59, что его остатки при делении на 3, 4 и 5 равны $c_1 = 2$, $c_2 = 1$ и $c_3 = 2$, соответственно.

2. Разобьем двоичную запись некоторого числа $A = (\ldots a_1 a_0)_2$ на блоки длины k. Обозначим $A_j = a_{(j-1)k} + 2a_{(j-1)k+1} + \ldots + 2^{k-1} a_{jk-1}$. Например,

$$47 = 101111, \quad k = 3, \quad A_1 = 1 + 2 + 4, \quad A_2 = 1 + 4.$$

Докажите, что остатки от деления числа A на $2^k - 1$ и на $2^k + 1$ такие же, как у чисел $A_1 + A_2 + \ldots$ и $A_1 - A_2 + \ldots$, соответственно. В приведенном выше примере

$$47 \equiv (7 + 5) \equiv 5 \pmod{7}, \qquad 47 \equiv (7 - 5) \equiv 2 \pmod{9}.$$

3. Пусть заданы остатки $u_1, \ldots, u_k$ от деления некоторого числа на попарно взаимно простые числа $m_1, \ldots, m_k$. То число, которое может быть восстановлено по китайской теореме об остатках, будем обозначать $\langle u_1, \ldots, u_k \rangle$ или $\langle (u_1)_{m_1}, \ldots, (u_k)_{m_k} \rangle$. Докажите следующие равенства

а) $\langle u_1, \ldots, u_k \rangle \pm \langle v_1, \ldots, v_k \rangle = \langle u_1 \pm v_1, \ldots, u_k \pm v_k \rangle$,

б) $\langle u_1, \ldots, u_k \rangle \langle v_1, \ldots, v_k \rangle = \langle u_1 v_1, \ldots, u_k v_k \rangle$
(здесь произведение чисел понимается по модулю $M = m_1 \cdot \ldots \cdot m_k$).

Читатель может сейчас спросить: почему эти факты интересны и как они связаны с преобразованием Фурье? Оказывается, что китайская теорема об остатках дает способ быстрого вычисления коэффициентов Фурье.

3. Быстрое преобразование Фурье

Для прямого вычисления преобразования Фурье по формуле (6) нужно осуществить порядка m^2 операций умножения и порядка m^2 операций сложения. Это много или мало? Будем рассуждать в терминах времени вычисления для компьютеров. Перемножение двух чисел на персональном компьютере среднего быстродействия занимает 10^{-5} секунд. Для последовательности данных длины порядка $n = 10^4$ (что типично, например,

для геофизических приложений) получаем, что вычисление преобразования Фурье занимает порядка 20 минут. Это очень долго для одной последовательности данных.

Для многих типов компьютеров время, нужное для перемножения чисел, гораздо больше времени, требуемого для сложения чисел. Поэтому мы будем стараться уменьшить именно количество умножений, не обращая внимания на количество сложений.

Как сократить число умножений? Вспомним, как нас учили делать это в начальной школе: для того, чтобы вычислить $23 \cdot 37 + 29 \cdot 37$ мы запишем это число в виде $(23+29)\cdot 37$. Тогда вместо двух умножений нам достаточно выполнить одно.

Внимательный читатель мог заметить, что многие из чисел z^{kj}, $j,k = 1,\dots,m$, появляющиеся в (6), в действительности совпадают. Используем этот факт для того, чтобы сократить число умножений. Китайская теорема об остатках может в этом существенно помочь.

Предположим, что число m записывается в виде $m = m_1 m_2$, где m_1 и m_2 — взаимно простые числа.

Пусть k_1 и k_2 — остатки от деления индекса k, появляющегося в (6), на m_1 и m_2, соответственно. Аналогично формуле (9), число k можно представить в виде $k = k_1 M_2 m_2 + k_2 M_1 m_1$, где M_1 и M_2 единственным образом определяются из соотношений $m_1 M_1 + m_2 M_2 \equiv 1 \pmod m$, $0 < M_1, M_2 < m$.

Теперь представим преобразование Фурье, т. е. сумму в правой части (6), как двойную сумму по индексам k_1 и k_2, пробегающим значения от 0 до $m_1 - 1$ и $m_2 - 1$, соответственно. Пусть также j_1 — остаток от деления $M_2 j$ на m_1, а j_2 — остаток от деления $M_1 j$ на m_2.

Заметим, что $j = m_2 j_1 + m_1 j_2 \pmod m$. Для доказательства достаточно просуммировать равенства $M_2 j = m_1 p + j_1$, $M_1 j = m_2 q + j_2$, умноженные на m_2 и m_1 соответственно. Здесь p и q неотрицательные целые числа.

Далее, введем обозначения $\beta = z^{M_2 m_2^2}$, $\gamma = z^{M_1 m_1^2}$ и заметим, что $z^{m_1 m_2} = 1$. Если теперь вынести общие множители из внутренней суммы по индексу j_2, то получится следующий результат

$$c_{j_1,j_2} = \sum_{k_1=0}^{m_1-1} \beta^{j_1 k_1} \sum_{k_2=0}^{m_2-1} \gamma^{j_2 k_2} \Gamma(k_1,k_2), \tag{10}$$

где $c_{j_1,j_2} = c_{j_1 m_2 + j_2 m_1}$, $\Gamma(k_1,k_2) = y_{k_1 M_2 m_2 + k_2 M_1 m_1}$.

Заметим, что имеется лишь m_1 весов $\beta^{j_1 k_1}$ и m_2 весов $\gamma^{j_2 k_2}$, которые хранятся в памяти компьютера. Поэтому для вычисления одной внутренней суммы по формуле (10) требуется выполнить m_2 умножений, а для

вычисления всех m_1 внутренних сумм при $k_1 = 0, \ldots, m_1 - 1$ требуется выполнить $m = m_1 m_2$ умножений. После этого остается умножить эти внутренние суммы на m_1 весов $\beta^{j_1 k_1}$, так что всего требуется $m_1 m$ умножений. Все остальные операции в формуле (10) являются сложениями.

Итак, если число m не является простым, мы можем вычислить преобразование Фурье за $\leqslant m^{3/2}$ умножений[2)]. Если мы сможем разложить m_1 и m_2 на произведение взаимно простых чисел, число умножений сократится еще более. Разумеется, некоторые трудности возникают из-за порядка вычисления коэффициентов a_j, но их можно преодолеть, затрачивая относительно небольшое дополнительное время.

Проиллюстрируем правило перенумерации индексов следующим примером. Пусть $m = m_1 \times m_2 = 3 \times 7$. Ясно, что $1 \times 7 + 19 \times 3 = 64 \equiv 1 \pmod{21}$. Поэтому $M_1 = 1$, $M_2 = 19$. Представим исходную последовательность чисел $a_0, \ldots, a_{20}$ в виде таблицы $a(k_1, k_2)$: в клетку (k_1, k_2), $k_1 = 0, 1, 2$, $k_2 = 0, 1, \ldots, 6$, ставим элемент с индексом $k = 7k_1 + 15k_2 \pmod{21}$, поскольку $19 \times 3 \equiv 15 \pmod{21}$. Получаем расстановку индексов на входе:

$$\begin{array}{ccccccc} 0 & 15 & 9 & 3 & 18 & 12 & 6 \\ 7 & 1 & 16 & 10 & 4 & 19 & 13 \\ 14 & 8 & 2 & 17 & 11 & 5 & 20. \end{array}$$

В клетке (k_1, k_2), $k_1 = 0, 1, 2$, $k_2 = 0, 1, \ldots, 6$, выходной таблицы стоит элемент с индексом $j_1 \equiv 19j \equiv j \pmod 3$, $j_2 \equiv j \pmod 7$. Получаем расстановку индексов на выходе:

$$\begin{array}{ccccccc} 0 & 3 & 6 & 9 & 13 & 15 & 18 \\ 7 & 10 & 13 & 16 & 19 & 1 & 4 \\ 14 & 17 & 20 & 2 & 5 & 8 & 11. \end{array}$$

В действительности, описанный выше алгоритм, называемый алгоритмом Гуда – Томаса, был первым (1960–63) алгоритмом быстрого вычисления дискретного преобразования Фурье, хотя приоритет обычно приписывается Кули – Тьюки (1965). Причина этого в том, что алгоритм Кули – Тьюки был широко разрекламирован и использует более простой метод упорядочения коэффициентов.

В заключение опишем алгоритм Кули – Тьюки. При фиксированных m_1 и m_2 (здесь m_1 и m_2 могут иметь общие простые множители) введем

[2)] При $m = 2^n$ есть алгоритм вычисления дискретного преобразования Фурье, использующий $O(m \log m)$ умножений, который также называется быстрым преобразованием Фурье. Об этом алгоритме и его применении к задаче быстрого умножения чисел можно прочитать в книгах Кнут Д. Искусство программирования на ЭВМ. В 3 т. Т. 2. М.: Мир, 1977, Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М.: Мир, 1979. — *Прим. ред.*

индексы j_1, j_2, k_1, k_2 с помощью соотношений $j = m_2 j_1 + j_2$, $k = m_1 k_2 + k_1$, где $j_1, k_1 = 0, 1, \ldots, m_1 - 1$ и $j_2, k_2 = 0, 1, \ldots, m_2 - 1$. Переходя к суммированию по k_1, k_2 в (6) так же, как и в первом из описанных выше алгоритмов, получим равенство

$$a_j \equiv a_{j_1,j_2} = \sum_{k_1=0}^{m_1-1} z^{jk_1} \sum_{k_2=0}^{m_2-1} \gamma^{k_2 j_2} y_{k_1,k_2},$$

где $\gamma = z^{m_1}$, $y_{k_1,k_2} = y_{m_1 k_2 + k_1}$, $a_j = a_{m_2 j_1 + j_2}$. Подробнее об алгоритмах БПФ можно прочитать в книгах [4], [5], [6], [7], [8].

4. Обработка изображений

Понятие дискретного преобразования Фурье естественно обобщается на двумерный случай, когда данные образуют не последовательность чисел, а двумерный массив $y(k,l)$, $1 \leqslant k \leqslant K$, $1 \leqslant l \leqslant L$. Преобразование Фурье этого массива (матрицы) образует новый массив, элементы которого имеют следующий вид

$$V(j,m) = \sum_{k=1}^{K} \sum_{l=1}^{L} z_1^{kj} z_2^{lm} y(k,l), \tag{11}$$

где $z_1 = e^{2\pi i/K}$, $z_2 = e^{2\pi i/L}$.

Двумерное преобразование Фурье — это не просто математическая абстракция, оно полезно во многих прикладных задачах, включая обработку изображений. Под *изображением* мы понимает двумерную таблицу, элементы которой отвечают уровням яркости фотографии в точке с декартовыми координатами (kh, lh), где h — размер элементарной ячейки (разрешение) изображения. Эта простая модель изображения вполне удовлетворительна при анализе фотографий поверхности Земли и других планет, сделанных из космоса.

Преобразование Фурье позволяет значительно сократить количество информации, которое необходимо использовать для восстановления изображения. Обычно достаточно запомнить лишь несколько первых гармоник (коэффициентов Фурье), чтобы воспроизвести изображение с приемлемой точностью при помощи обратного преобразования Фурье

$$\hat{y}(k,l) = \frac{1}{m^2} \sum_{j=1}^{\hat{j}} \sum_{m=1}^{\hat{m}} z_1^{-kj} z_2^{-lm} V(j,m).$$

Шляпка над y указывает на то, что $\hat{y}(k,l)$ только приблизительно совпадает с $y(k,l)$ в случае, когда $\hat{j} < K, \hat{m} < L$.

Оказывается, что во многих практических ситуациях точность такой аппроксимации является достаточно хорошей, даже когда K, L зна-

чительно больше, чем $\hat{j}$, $\hat{m}$. В качестве примера обсудим использование преобразования Фурье для сжатия информации при исследовании формы морской поверхности. Воспользуемся идеализированной моделью, предполагая, что уровень контрастности в любой точке пропорционален высоте морской волны. Предположим также, что длина волны равна p в некотором направлении и q в перпендикулярном к нему направлении, это означает, что

$$y(k,l) = A\cos\frac{2\pi k}{p}\cos\frac{2\pi l}{q},$$

где A — амплитуда волны. Легко проверить, что $V(j,m) = A$, если $j = \frac{K}{p}, m = \frac{L}{q}$, и нулю во всех остальных случаях (для простоты мы предположим, что $\frac{K}{p}, \frac{L}{q}$ — целые числа). Таким образом, для восстановления этого изображения достаточно знать только три числа $(p, q, V(\frac{K}{p}, \frac{L}{q}))$.

В случае произвольного массива $y(k,l)$ отбрасывание членов с большими значениями k и l в сумме (11) приводит к более сглаженному изображению, чем первоначальное. Это скорее положительное свойство, поскольку мелкомасштабные флуктуации обычно вызваны шумом и их удаление при обработке приводит к улучшению качества изображения.

Американский исследователь Роналд Брайсвелл использовал двумерное преобразование Фурье для анализа источников радиоволн на поверхности Солнца по радиоастрономическим данным. Построенные им карты солнечной активности были высоко оценены специалистами НАСА, которые использовали их для обеспечения безопасности астронавтов, принимавших участие в лунных полетах.

5. Покрытия целочисленного тора

Алгоритмы быстрого вычисления многомерного преобразования Фурье интересовали исследователей с середины 70-х годов (см., например, [9] в случае простого $n = p$). В 1988 году инженер Исидор Гертнер (он получил образование в Каунасе, Литва, и теперь работает в США) придумал новый метод быстрого вычисления многомерного преобразования Фурье ([10]). Мы поясним его идею в случае двумерного массива данных $n \times n$. Этот массив можно периодически продолжить на всю решетку $\mathbb{Z}^2$ и рассматривать как двумерный дискретный тор. Метод Гертнера требует вычисления N одномерных преобразований Фурье, где N равно минимальному числу линий

$$L_{m,r} = \{(k,l) : km + lr \equiv 0 \pmod{n}\},$$

покрывающих квадрат

$$T_n = \{(k,l) : k = 0, \dots, n-1,\ l = 0, \dots, n-1\}.$$

Переменные m, r, определяющие «линию», пробегают значения $0, 1, \dots, n-1$.

Слово *линия* записано в кавычках потому, что в действительности каждая «линия» $L_{m,r}$ на (k,l)-плоскости представляет из себя семейство параллельных линий $km + lr = 0, km + lr = n$, $km + lr = 2n, \dots$

Утверждение «линии покрывают квадрат» означает, что (i) все линии проходят через начало координат $(0,0)$ и (ii) любая другая точка с целочисленными координатами (рассматриваемая как точка двумерного тора) принадлежит в точности одной линии.

Обозначим через $v(n)$ минимальное число линий $L_{m,r}$, $(m,r) \in T_n$, покрывающих T_n. Ключевая идея метода Гертнера состоит в так называемом *дискретном преобразовании Радона*. Этот метод безусловно заслуживает отдельной статьи, поэтому мы ограничимся лишь следующей задачей.

Задача 3*. Попробуйте разработать алгоритм быстрого двумерного преобразования Фурье.

Подсказка. Рассмотрим семейство параллельных линий, перпендикулярных линии $L_{m,r}$. Просуммируем элементы таблицы вдоль каждой такой перпендикулярной линии и затем вычислим одномерное преобразование Фурье полученных сумм. Выполним эту процедуру для каждой из $v(n)$ линий покрытия.

Интересно явно вычислить число $v(n)$ минимально необходимых одномерных преобразований Фурье. Следующая теорема относится к покрытию n-мерного тора.

Теорема 3. *Если $n = p$ — простое число, то $v(p) = p+1$, и искомое покрытие состоит из следующих линий:*

$$k \equiv 0 \pmod p, \quad k + l \equiv 0 \pmod p, \quad k + 2l \equiv 0 \pmod p, \dots,$$
$$k + (p-1)l \equiv 0 \pmod p, \quad l \equiv 0 \pmod p.$$

Упражнение. Проиллюстрируйте это утверждение рисунком при $n = 5$. Проверьте, что указанные линии действительно покрывают все точки квадрата T_5.

Подсказка. Линия $L_{1,2}$ проходит через точки $(1,2), (2,4), (3,1), (4,3)$; а линия $L_{1,3}$ проходит через точки $(1,3)$, $(2,1)$, $(3,4)$, $(4,2)$; остальное очевидно.

Доказательство теоремы 3. Вначале проверим, что $v(p) \geqslant p+1$. Из определения линии $L_{m,r}$ вытекает, что она не может покрывать более,

чем p точек квадрата T_p, потому что для любого фиксированного k такое l, что $km + lr \equiv 0 \pmod p$ находится единственным образом. Если бы существовало два решения, скажем, l_1 и l_2, то $(l_1 - l_2)r \equiv 0 \pmod p$. Поскольку p — простое число, то это равенство влечет $l_1 = l_2$.

Кроме того, каждая линия $L_{m,r}$ содержит $(0,0)$. Поскольку квадрат T_p содержит p^2 точек, очевидным образом справедливо следующее неравенство

$$v(p) \geqslant \frac{p^2 + p - 1}{p}, \quad \text{т. е. } v(p) \geqslant p + 1.$$

Покажем теперь, что каждая точка (k', l') квадрата T_p принадлежит по крайней мере одной линии $L_{1,r}$, $r = 0, 1, \ldots, p-1$ или $L_{0,1}$. Действительно, предположим, что (k', l') не принадлежит $L_{0,1}$. Числа k', $k'+l'$, $\ldots$, $k' + (p-1)l'$ имеют различные остатки при делении на p (проверьте это), а поскольку их количество в точности равно p, одно из них должно делиться на p без остатка. Это означает, что (k', l') принадлежит одной из линий $L_{1,r}$, что завершает доказательство. □

Задача 4. Предположим, что p простое число и $k \geqslant 1$. Докажите, что

$$v(p^k) = (p+1)p^{k-1}.$$

Задача 5. Пусть p_1, p_2 — два различных простых числа. Тогда

$$v(p_1 p_2) = p_1 p_2 + p_1 + p_2 + 1.$$

Задача 6. Найдите семейство 12 линий, покрывающих квадрат T_6. Докажите, что число линий в этом семействе не может быть уменьшено.

Отметим, что традиционные методы быстрого вычисления двумерного преобразования Фурье массива $n \times n$ требуют $2n$ вычислений одномерного преобразования Фурье. Таким образом, метод Гертнера примерно вдвое сокращает число операций, когда $n = p$ — простое число. В 1991 г. М. Кельберт и А. Мазель нашли $v_d(n)$ для любого n и массивов любой размерности d (см. [11]).

Приведем эту формулу. Разложим n в произведение $n = p_1^{k_1} p_2^{k_2} \ldots p_l^{k_l}$, где $p_1, \ldots, p_l$ — простые числа. Тогда

$$v_d(n) = n^{d-1} \prod_{i=1}^{l} \left(1 + \frac{1}{p_i} + \ldots + \frac{1}{p_i^{d-1}}\right). \tag{12}$$

Проверьте, что при $d = 2$ эта формула содержит результат теоремы 3 и задач 4 и 5.

Из формулы (12) видно, что при дискретизации изображения выгодно выбрать в качестве n простое число, а не степень двойки, как это обычно

делается в приложениях. Например, в двумерном случае, при $n = 32$, 33 и $n = 35$ нужно использовать одномерное преобразование Фурье 48 раз, а при $n = 31$ только 32 раза.

В размерностях $d > 2$ разница оказывается более существенной. Например, при $d = 3$ и $n = 31$ одномерное преобразование Фурье нужно использовать 993 раза, а при $n = 32$, 33, 35 — 1792, 1729 и 1767 раз, соответственно.

Список литературы

[1] *Fourier J. B. J.* The Analytical Theory of Heat. Cambridge Univ. Press, 1878.

[2] *Grattan-Guinness I.* Joseph Fourier, 1768-1830: a survey of his life and work, based on a critical edition of his monograph on the propagation of heat. Cambridge: MIT Press, 1972.

[3] *Хассе Г.* Лекции по теории чисел. М.: Иностранная литература, 1953.

[4] *Blahut R. E.* Digital Transmission of Information. Reading, MA: Addison-Wesley, 1990.

[5] *Blahut R. E.* Fast Algorithms for Digital Signal Processing. Reading, MA.: Addison-Wesley, 1985.

[6] *Nussbaumer H. J.* Fast Fourier Transform and Convolution Algorithms. Berlin: Springer-Verlag, 1981.

[7] *Brigham E. O.* The Fast Fourier Transform and its Applications. London: Prentice Hall Intern., 1988.

[8] *McClellan J. H., Rader C. M.* Number Theory in Digital Signal Processing. London: Prentice Hall Intern., 1979.

[9] *Auslander L., Feig E., Winograd S.* New algorithm for multi-dimensional discrete Fourier transform // IEEE Trans. ASSP, 1983. Vol. 31. No 2. P. 388–403.

[10] *Gertner I.* New efficient algorithm to compute the two-dimensional discrete Fourier transform // IEEE Trans. ASSP, 1988. Vol. 36. No 7. P. 1036–1050.

[11] *Кельберт М., Мазель А.* Быстрое вычисление многомерного дискретного преобразования Фурье // Проблемы передачи информации, 1991. Т. 27. №2. С. 107–110.

Нам пишут...

Мы получаем различные материалы не только от читателей нашей страны, но и от живущих за её пределами. Приятно констатировать, что «Математическое просвещение» пользуется успехом у читателей, и у них возникает желание через наш альманах поделиться своими знаниями и своим опытом. В этом номере мы помещаем две небольшие заметки наших зарубежных коллег.

В заметке Л. С. Гурина предлагается способ вычисления числа π, не опирающийся на теорию рядов и не требующий вычислений с радикалами. Автор считает, что этот способ может быть использован в преподавании.

Об одном элементарном способе вычисления числа π

Л. С. Гурин

Исходя из тождества $\frac{\pi}{4} = \operatorname{arctg} 1 = N\alpha + \beta$, задавшись числом $\alpha = \operatorname{arctg} t$, $0 < t < 1$, проводим итеративную процедуру:

$$t_1 = \operatorname{tg} 2\alpha = \frac{2t}{1-t^2}, \quad t_i = \operatorname{tg} 2^i\alpha = \frac{2t_{i-1}}{1-t_{i-1}^2}, \quad i = 2, \ldots, m,$$

где m находим из условия $t_m < 1$, $t_{m+1} > 1$. Представим число $N = N(t)$ в виде: $N = \sum_{k=1}^{m+1} a_k 2^{m+1-k}$. Из определения числа m ясно, что $a_1 = 1$. Обозначим $N_i = \sum_{k=1}^{i} a_k 2^{m+1-k}$. Тогда значения a_i находятся последовательно. Если известны $a_1, \ldots, a_i$, то

$$a_{i+1} = \begin{cases} 1, & \operatorname{tg}(N_i + 2^{m-i})\alpha \leqslant 1, \\ 0, & \operatorname{tg}(N_i + 2^{m-i})\alpha > 1. \end{cases}$$

Наконец, полагаем $\beta = \beta(t) = \operatorname{arctg} \frac{1 - \operatorname{tg} N\alpha}{1 + \operatorname{tg} N\alpha}$. Равенство $\pi = 4(N(t)\alpha + \beta(t))$ даёт возможность вычислить π с любой точностью, которая при заданном t зависит от точности определения величин $\operatorname{arctg} x$ при $x = t$ и $x = \beta(t)$.

Ныне число π сосчитано со многими миллионами десятичных знаков, но это требует привлечения современных средств математического анализа. Состояние вопроса отлично представлено в сборнике Berggen L., Borwein L., Borwein P., PI, A Sourse Book. NY, Springer-Verlag, Inc., 1997.

Тождества Ньютона и математическая индукция

З. Б. Райхштейн

Пусть многочлен $f(x) = x^n + s_1 x^{n-1} + \ldots + s_{n-1}x + s_n$ имеет корни $x_1, \ldots, x_n$. Тогда

$$s_r = (-1)^r \sum_{i_1 < \ldots < i_r} x_{i_1} \cdot \ldots \cdot x_{i_r} .$$

Каждый многочлен s_r симметрический и однородный степени r. Всякий симметрический многочлен от $x_1, \ldots, x_n$ можно однозначно представить как многочлен от $s_1, \ldots, s_n$, так что эти многочлены образуют базис в кольце всех симметрических многочленов. Многочлены $-s_1, s_2, \ldots, (-1)^n s_n$ называются *элементарными симметрическими многочленами.*

Суммы степеней

$$p_r(x_1, \ldots, x_n) = x_1^r + \ldots + x_n^r , \quad (r = 1, 2, \ldots)$$

тоже образуют базис в пространстве всех симметрических многочленов, если коэффициенты многочленов — рациональные, действительные или комплексные числа.

Тождества Ньютона можно рассматривать как формулы перехода между этими двумя базисами. Если мы положим $s_{n+1} = s_{n+2} = \ldots = 0$, то для любых натуральных чисел n и d

$$p_d + s_1 p_{d-1} + \ldots + s_{d-1} p_1 + d s_d = 0. \qquad (1)$$

Заметим, что эти тождества справедливы для многочленов с коэффициентами в любом поле, хотя суммы степеней не всегда образуют базис в кольце симметрических многочленов.

Впервые тождества (1) были опубликованы Ньютоном в книге *Arithmetica universalis*, вышедшей в свет в 1707 году. (Для $d \leqslant 4$ они были известны уже Жирарду в начале XVII века.)

Известно много доказательств тождеств Ньютона[3]. Мы приведём ещё одно, которое годится для любого поля коэффициентов.

Обозначим многочлен, стоящий в левой части (1), через $F_n^{(d)}$ и докажем $F_n^{(d)} = 0$ индукцией по $m = n - d$.

База индукции будет состоять в доказательстве $F_n^{(d)} = 0$ для любого

[3] См., например, *Meed D. G.* Newton's indentities // American Math. Monthly, 1992. Vol. 99, no. 8. P. 749–751; *Zeidelberg D.* A combinatorial proof of Newton's identities // Discrete Math., 1984. Vol. 49, no. 3. P. 319. (Или *Макдональд И.* Симметрические функции и многочлены Холла. М.: Мир, 1985; Прасолов В. В. Многочлены. М.: МЦНМО, 1999. — *Прим. ред.*)

$m = n - d \leqslant 0$. По определению $s_1, \ldots, s_n$, данному выше,

$$\begin{aligned} f(x_1) &= x_1^n + s_1 x_1^{n-1} + \ldots + s_n = 0, \\ &\vdots \\ f(x_n) &= x_n^n + s_1 x_n^{n-1} + \ldots + s_n = 0. \end{aligned} \tag{2}$$

Складывая эти уравнения, получаем

$$p_n + s_1 p_{n-1} + \ldots + s_{n-1} p_1 + n s_n = 0,$$

т.е. $F_n^{(n)} = 0$. Аналогично, если мы подставим выражения (2) в формулу

$$x_1^{d-n} f(x_1) + \ldots + x_n^{d-n} f(x_n) = 0,$$

то получим $F_n^{(d)} = 0$ для всех $d \geqslant n$ (проверьте!).

Теперь докажем, что $F_n^{(d)} = 0$ при $m = n - d \geqslant 1$. Предположение индукции состоит в том, что $F_{n'}^{(d')} = 0$ при $n' - d' \leqslant m - 1$. Заметим, что из определения s_r и p_r следует

$$F_n^{(d)}(x_1, \ldots, x_{n-1}, 0) = F_{n-1}^{(d)}(x_1, \ldots, x_{n-1}).$$

(Проверьте!) По предположению индукции $F_{n-1}^{(d)}(x_1, \ldots, x_{n-1}) = 0$. Другими словами, $F_n^{(d)}$ делится на x_n, а так как $F_n^{(d)}$ — симметрический многочлен, то и на $x_1, \ldots, x_{n-1}$. Итак, $F_n^{(d)}$ делится на $s_n = x_1 \cdot \ldots \cdot x_n$. Но степень $F_n^{(d)}$ меньше степени s_n. Поэтому $F_n^{(d)} = 0$, что и требовалось доказать.

Уточнения

К сожалению, в моей статье «О разбиении множеств на части меньшего диаметра» в вып.3 «Математического просвещения» обнаружилась ошибка. Лемма 4 (на с. 182) неверна: диаметр d каждой из четырёх частей, на которые правильный вписанный тетраэдр разбивает шар, не равен длине ребра этого тетраэдра (d больше стороны правильного треугольника, вписанного в шар).

Таким образом, неверно и мое утверждение, что найдено новое доказательство гипотезы Борсука в трёхмерном пространстве.

М. Л. Гервер

Задача Герко о чемпионах

М. Н. Вялый

Все пункты этой задачи решаются по индукции, причем сложность рассуждений резко растет.

Начнем с решения пункта а). База индукции очевидна: один победитель единственного соревнования из двоих — это уже половина.

Пусть есть пример 2^n спортсменов, упорядоченных по силе в n видах спорта так, что среди них 2^{n-1} возможных победителей, обозначим такой пример C_n.

Опишем пример C_{n+1} из 2^{n+1} спортсменов, упорядоченных по силе в $(n+1)$-м виде спорта так, что среди них 2^n возможных победителей. Разделим спортсменов на две равные группы A и A'. Будем считать, что в видах спорта с 2-го по $(n+1)$-й спортсмены в каждой из групп упорядочены как в примере C_n, в 1-м виде спорта любой из A' сильнее любого из A, а в остальных видах — наоборот.

Если первым провести соревнование по 1-му виду спорта, то останется группа A', если любое другое — останется группа A. Учитывая, что в примере C_n есть 2^{n-1} возможных победителей, получаем $2^{n-1}+2^{n-1}=2^n$ возможных победителей в примере C_{n+1}.

б) Укажем для каждого вида спорта спортсмена, который при любом порядке проведения соревнований выбывает в этом виде или раньше (независимо от того, каким по очереди проводится этот вид спорта). Построение индуктивное.

Для 1-го вида соревнований — это самый слабый в 1-м виде.

Пусть уже построено множество $A_k=\{a_1,\ldots,a_k\}$ спортсменов такое, что a_i выбывает в i-м виде спорта или раньше.

Из спортсменов, не входящих в множество A_k, выберем самого слабого в $(k+1)$-м виде спорта, обозначим его через a_{k+1}. Докажем, что a_{k+1} выбывает в $(k+1)$-м виде спорта или раньше при любом порядке соревнований. Пусть $(k+1)$-й вид спорта проходит r-м по порядку, а из множества A_k за первые $r-1$ соревнований выбыло w человек. В r-м соревновании выбывает 2^{n-r} человек. Поэтому a_{k+1} проходит в следующий тур только при выполнении условия $2^{n-r}\leqslant k-w$. Но после $(k+1)$-го вида спорта должны пройти соревнования по не менее чем $k-w$ видам спорта с номерами из множества $\{1,\ldots,k\}$. Поэтому $k-w\leqslant n-r<2^{n-r}$. Таким образом, a_{k+1} выбывает в $(k+1)$-виде спорта или раньше.

в) Обратим внимание на то, что в конструкции, описанной в пункте а), есть произвол в выборе соревнования, отбирающего группу A. Оказывается, что *максимальное число возможных победителей из* 2^n

спортсменов, соревнующихся в ***каких-то*** n *видах спорта из* $(n+1)$*-го возможного, равно* $2^n - 1$.

Прежде чем доказывать это утверждение, поясним коротко, как использовать его для решения пункта в). База индукции по-прежнему очевидна. Для индуктивного перехода повторим рассуждение пункта а) и заметим, что из группы A' победителями можно сделать $2^n - n$ человек, а из A — $2^n - 1$ человек. Итого получаем $2^n - n + 2^n - 1 = 2^{n+1} - (n+1)$ возможных победителей.

Нужную оценку для числа возможных победителей в соревнованиях по n видам спорта из $(n+1)$-го возможного мы получим, доказав более сильное утверждение: *существует такой пример* E_n *из* 2^n *спортсменов, упорядоченных в* $(n+1)$*-м виде спорта, что выбором* n *видов спорта и порядка их проведения можно сделать победителями* $2^n - 1$ *участников, а единственному исключительному участнику (будем называть его* ***аутсайдером****) можно обеспечить выход в финал.*

База при $n = 1$ очевидна (два соревнования, в каждом из которых спортсмены упорядочены одинаково).

Индуктивный переход. Строим пример E_{n+1}, исходя из существования примера E_n. Опять разделим 2^{n+1} спортсменов на равные группы B и B'. Будем считать, что в 1-виде спорта любой из B' сильнее любого из B, в остальных видах — наоборот, а в видах со 2-го по $(n+2)$-й спортсмены внутри B и B' упорядочены, как в примере E_n. Дополнительно предположим, что аутсайдер в B — самый сильный среди B в 1-м виде спорта.

Проводя первым 1-й вид спорта, получим $2^n - 1$ возможных победителей из B', причем при некотором порядке проведения соревнований аутсайдер из B' выйдет в финал (индуктивное предположение).

Если вообще не проводить соревнования по 1-му виду спорта, то в первом соревновании выбывают все из B', а далее проводится $n - 1$ соревнование. По индуктивному предположению выбором вида спорта для первого соревнования и порядка проведения соревнований по остальным видам спорта можно сделать победителями $2^n - 1$ спортсменов из B.

Осталось объяснить, как сделать победителем аутсайдера в B. Для этого *первым проводим тот вид соревнований, который является последним при порядке соревнований, обеспечивающем выход аутсайдера в финал.* После этого останутся только спортсмены из B. Далее проводим соревнования в таком порядке, который обеспечивает выход аутсайдера из B в финал, а завершаем — 1-м видом спорта. В нем аутсайдер побеждает.

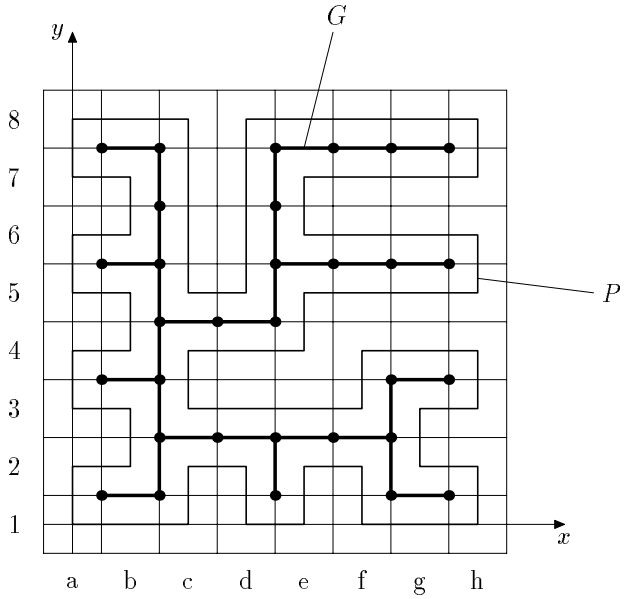
Задача Шаповалова о ладье

П. А. Кожевников

Достаточно доказать, что число, например, горизонтальных ходов ладьи при делении на 4 даёт в остатке 2.

Пусть траектория центра ладьи ограничивает многоугольник P (мы считаем, что центр ладьи всегда ставится точно в центр клетки). Та часть разметки шахматной доски на поля, которая находится целиком внутри P, образует некоторый граф G (см. рис.), вершины этого графа — узлы шахматной разметки. Нетрудно понять, что G — дерево. Введём систему координат с началом в центре поля a1 шахматной доски и осями, параллельными горизонталям и вертикалям доски. Тогда все вершины P имеют целочисленные координаты, а стороны параллельны осям. Установим следующий общий факт.

Лемма. *Пусть P — многоугольник с вершинами в целых точках со сторонами, параллельными осям, такой что соответствующий граф G (получаемый соединением центров соседних клеточек P: любой такой многоугольник можно вырезать из клетчатой бумаги) является деревом. Далее, пусть A — число целых точек на границе P, у которых абсцисса чётная, B — число целых точек на границе P, у которых абсцисса нечётная. Тогда сумма длин горизонтальных сторон P сравнима с $A - B + 2$ по модулю 4.*



Доказательство проведём индукцией по площади P. База ($S_P = 1$, P состоит из одной клетки) тривиальна. Переход осуществляем, отрезая от P клеточку, соответствующую листу дерева G (у всякого дерева, конечно же, есть лист). Клеточка может примыкать к P либо по горизонтальному отрезку, либо по вертикальному отрезку. В первом случае сумма длин горизонтальных сторон P не изменяется, в то же время $A - B$ тоже не изменяется. Во втором случае и сумма длин, и $A - B$ изменяются на 2.

Для многоугольника P, ограниченного траекторией центра ладьи, $A = 32$, $B = 32$, следовательно число горизонтальных ходов сравнимо с $A - B + 2 = 2$ по модулю 4.

Задача о двухцветном графе

И. Межиров

Условие задачи. Предположим, что каждая вершина графа может находиться в одном из двух состояний. Для каждой вершины графа A дана операция PA, которая меняет состояния вершины A и всех ее соседей. Доказать, что найдется композиция этих операций, меняющая состояния всех вершин.

Решение. Проведем доказательство по индукции. Для графа из 1 вершины утверждение тривиально. Пусть утверждение верно для всех графов из n вершин. Докажем, что оно верно для всех графов из $(n+1)$-ой вершины. Пусть дан какой-нибудь граф из $(n+1)$-ой вершины. Выберем в нем произвольную вершину A. Если исключить A из графа, то останется подграф исходного графа, имеющий n вершин. По предположению индукции существует композиция операций P, изменяющая состояние всех вершин этого подграфа. Обозначим одну из таких композиций через RA. Введем это обозначение для всех A, т. е. введем операцию R, применимую к любой вершине. Если хотя бы одна операция RA изменяет состояние A, то она изменяет состояние всех вершин графа. В этом случае доказательство шага индукции закончено. Теперь разберем случай, когда все RA не изменяют состояние A. Польза от рассмотрения операции R в оставшемся случае заключается в том, что ее действие не зависит от ребер графа. Для разбора оставшегося случая достаточно найти операцию, изменяющую состояния всех вершин, кроме четного их числа. В самом деле, пусть операция T меняет состояния всех вершин, кроме вершин $A_1, A_2, \ldots, A_{2k}$. Тогда операция

$$T \circ RA_1 \circ RA_2 \circ \cdots \circ RA_{2k}$$

меняет состояние всех вершин, поскольку состояние вершин A_i меняется нечетным количеством операций R, а состояние всех остальных вершин меняется T и четным числом операций R. Теперь, если в графе четное число вершин, то будем считать, что T ничего не меняет. Если в графе нечетное число вершин, то найдется вершина B, имеющая четное число соседей, так как количество пар (вершина, выходящее из нее ребро) четно. Тогда положим $T = PB$ и T будет менять состояния нечетного числа вершин, т. е. всех, кроме четного числа. Доказательство закончено.

Аналогичным рассуждением доказывается следующее более общее утверждение.

Задача о включении лампочек. Пусть дано конечное число лампочек и набор переключателей, каждый из которых переключает какие-то из лампочек. Вначале лампочки не горят. Необходимое и достаточное условие для того, чтобы можно было их все включить: *для любого*

подмножества из нечётного числа лампочек можно найти набор переключателей, меняющий состояние нечётного числа лампочек из этого подмножества (что этот набор делает с остальными лампочками, неважно).

Комментарий от редакции

Эта задача дает прекрасный пример использования линейной двойственности в комбинаторике. Перескажем задачу о включении лампочек на языке линейной алгебры. Рассмотрим пространство над $\mathbb{F}_2$ со скалярным произведением, ортогональный базис которого $\{e_1, \ldots, e_n\}$ индексирован лампочками (будем складывать лампочки по модулю 2). Каждому переключателю s_i, $1 \leqslant i \leqslant m$ сопоставим сумму тех лампочек, которые он переключает. Тогда включение всех лампочек равносильно условию

$$e_1 + \ldots + e_n = \sum_{j \in J} s_j,$$

которое можно равносильным образом переписать так:

$$e_1 + \ldots + e_n \in \mathbb{F}_2(s_1, \ldots, s_m) \Leftrightarrow (e_1 + \ldots + e_n)^\perp \supset \mathbb{F}_2(s_1, \ldots, s_m)^\perp \Leftrightarrow$$
$$\Leftrightarrow \mathbb{F}_2^m \setminus (e_1 + \ldots + e_n)^\perp \subset \mathbb{F}_2^n \setminus \mathbb{F}_2(s_1, \ldots, s_m)^\perp.$$

В левое множество входят в точности нечетные подмножества лампочек, в правое — те наборы, в которых можно переключить нечетное число лампочек.

Задачный раздел

В этом разделе вниманию читателей предлагается подборка задач разной степени сложности, в основном трудных. Некоторые из этих задач (не обязательно самые сложные!) требуют знания «неэлементарной» математики — анализа, линейной алгебры и т. п.

Составителям этой подборки кажется, что предлагаемые ниже задачи окажутся интересными как для сильных школьников, интересующихся математикой, так и для студентов-математиков.

Мы обращаемся с просьбой ко всем читателям, имеющим свои собственные подборки таких задач, присылать их в редакцию. И, разумеется, мы с удовольствием будем публиковать свежие авторские задачи. Ждем ваших писем (как с вновь предлагаемыми задачами, так и с решениями опубликованных задач).

В скобках после условия задачи приводится фамилия автора (уточнения со стороны читателей приветствуются). Если автор задачи нам неизвестен, то в скобках указывается «фольклор».

1. Дано 109-значное число, в десятичной записи которого нет нулей. Докажите, что в его десятичной записи либо некоторая группа соседних цифр повторится 10 раз подряд, либо найдутся записи 10 различных 100-значных чисел. *(А. Я. Белов)*

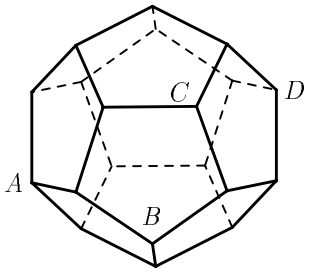
2. Между пунктами A и B расстояние 60 км. Поезд делает остановку в пункте A и через час — в пункте B. Докажите, что в некоторый момент времени его ускорение не меньше чем 240 $км/ч^2$. *(В. М. Тихомиров)*

3. Имеется граф G и его автоморфизм $f\colon G \to G$ порядка 2: если $x \in G$, то $f(f(x)) = x$ (напомним, что автоморфизм графа сохраняет смежность вершин). Примерами могут служить графы правильных центрально-симметричных многогранников или правильные решетки на евклидовой и гиперболической плоскостях; есть и много других примеров.

   В каждой вершине графа написано вещественное число. Любые два соседних числа (т. е. стоящих в концах одного ребра графа) отличаются меньше чем на 1. Докажите, что найдется пара вершин $(x, f(x))$, числа в которых также отличаются меньше чем на 1. *(Г. А. Гальперин)*

4. Несколько школьников играют в пинг-понг «на вылет». Они установили очередь, вначале играют первые двое, а затем победитель играет со следующим из очереди. На другой день ребята играют по той же системе, но порядок в очереди изменен на противоположный (т. е. очередь идет от последнего к первому). Докажите, что найдется пара игроков, которые встречались и в первый день, и во второй.
(*Б. Р. Френкин*)

5. Найдите угол между диагоналями AB и CD правильного додекаэдра.
(*С. Анисов*)



6. а) Двое флатландцев спускаются к морю с высочайшей вершины Флатландии «Пик Кипа» — один по левому склону, другой по правому. Гора нигде не опускается ниже уровня моря, а ее поверхность — график кусочно-линейной непрерывной функции. Флатландцы «непрерывно» двигаются, так что зависимость координат флатландца от времени — непрерывная функция, на скорость ограничений нет.

   Могут ли флатландцы достичь моря, все время находясь на одинаковой высоте над уровнем моря?

   б) Верно ли аналогичное утверждение для нескольких гор равной высоты, с каждой из которых спускается пара флатландцев (все они должны все время находиться на одинаковой высоте)?

   в) Пусть поверхность горы есть график дифференцируемой функции. Верно ли утверждение пункта а)?
(*Н. Н. Константинов*)

7. К данной параболе проведены три касательные. Докажите, что окружность, описанная около образованного ими треугольника, проходит через фокус параболы.
(*А. Заславский*)

8. Решите функциональное уравнение для непрерывных вещественных функций вещественного переменного:

$$F(x+y) = A(x) + B(x)C(y).$$

(*А. Я. Канель-Белов, Б. Р. Френкин*)

9. M — компакт в метрическом пространстве, $A\colon M \to M$ — отображение компакта в себя, не уменьшающее расстояние. Докажите, что A — изометрия (т.е. сохраняет расстояния).
(*Г. А. Гальперин*)

10. Известно, что ранг коммутатора $[AB] = AB - BA$ двух матриц равен единице. Докажите, что матрицы A и B имеют общий собственный вектор. (*фольклор*)

11. На некоторых клетках бесконечной доски стоят фишки (не более одной на каждой клетке), некоторые клетки пустые. Назовем расстановку *почти полной*, если найдется такое число C, что можно сдвинуть каждую фишку на расстояние, не превышающее C (иногда нулевое) так, чтобы пустых клеток не осталось. Назовем расстановку *не слишком пустой*, если найдется такое число D, что количество пустых клеток в любом квадрате не превосходит DP, где P — периметр квадрата. Докажите, что почти полные расстановки — это в точности не слишком пустые. (*А. Я. Белов*)

12. а) С многочленами от двух переменных можно делать следующие операции вывода. Пусть есть или уже выведены многочлены P_1, P_2. Тогда выводятся следующие многочлены:

$$\lambda P_1,\ \lambda \in \mathbb{R}; \qquad P_1 + P_2; \qquad P_1(R(x), R(y)),$$

где R — произвольный многочлен от одной переменной.

а) Верно ли, что любая система многочленов выводится из конечной подсистемы?

б) Тот же вопрос для многочленов с целыми коэффициентами, которые можно умножать только на целые числа. (*В. Шпехт*)

Решения задач из предыдущих выпусков

В этом номере мы помещаем решения избранных задач, опубликованных в предыдущих выпусках «Математического просвещения». В дальнейшем мы рассчитываем опубликовать все решения.

Далее номер задачи $K.L$ означает, что это L-я задача из K-го выпуска. В скобках указано, кому принадлежит приводимое решение задачи.

1.3. Условие. Может ли сумма чисел вида $a\sin(k\pi/n)$, где a — рациональное число, k, n — целые, равняться $\sqrt{1997}$?

Решение. Ответ: «может». Более того, то же самое верно для любого числа $\sqrt{a}$, $a \in \mathbb{Q}$. Докажем это утверждение для $\sqrt{2l+1}$, где l — целое.

Выражение $T_n(t) = \cos(n \arccos t)$ есть многочлен (многочлен Чебышёва), степень которого равна n, старший коэффициент равен 2^{n-1}, а при нечетном $n = 2l+1$ многочлен Чебышёва нечетен и его коэффициент при первой степени равен $(-1)^l(2l+1)$. Все эти факты легко получаются из рекуррентного соотношения

$$T_{n+1}(t) = 2tT_n(t) - T_{n-1}(t),$$

проверяемого непосредственно из определения $T_n(t)$.

Многочлен $T_{2l+1}(t)/t$ — четный и имеет нули $\pm\cos\frac{(2k+1)\pi}{2(2l+1)}$, $0 \leqslant k < l$. Отсюда следует, что

$$\prod_{k=0}^{l-1} \cos\frac{(2k+1)\pi}{2(2l+1)} = \frac{\sqrt{2l+1}}{2^l},$$

и остается представить это произведение в виде требуемой суммы, пользуясь обычными тригонометрическими формулами.

Пример: $T_5(t)/t = 16t^4 - 20t^2 + 5 = 16\bigl(x^2 - \cos^2\frac{\pi}{10}\bigr)\bigl(x^2 - \cos^2\frac{3\pi}{10}\bigr)$, поэтому $\cos\frac{\pi}{10}\cos\frac{3\pi}{10} = \frac{\sqrt{5}}{4}$, откуда и получаем требуемое представление

$$\sin\frac{\pi}{10} + \sin\frac{3\pi}{10} = \frac{\sqrt{5}}{2}.$$

(*В. М. Тихомиров*)

1.7. Условие. Пусть функция непрерывно дифференцируема на отрезке $[0,1]$,

$$f(0)=f(1)=0, \qquad \int\limits_0^1 \bigl(f'(t)\bigr)^2\,dt \leqslant 1.$$

Изобразите на координатной плоскости множество точек, через которые может проходить график функции $y=f(x)$.

Решение. Искомое множество является внутренностью круга $y^2 + (x-1/2)^2 \leqslant 1/4$.

Действительно, зафиксировав точку ξ, $0<\xi<1$, найдем верхнюю и нижнюю грани тех чисел η, для которых $\eta=f(\xi)$, где f — из описанного в условии задачи класса. Обозначим $\hat u(x)=\sqrt{\dfrac{1-\xi}{\xi}}\chi_{[0,\xi]}(x)-\sqrt{\dfrac{\xi}{1-\xi}}\chi_{[\xi,1]}(x)$, где χ_A — характеристическая функция множества A:

$$\chi_A=\begin{cases}1, & \text{если } x\in A,\\ 0, & \text{если } x\notin A.\end{cases}$$

Как легко понять, функция

$$\hat f(x)=\int\limits_0^x \hat u(z)\,dz$$

кусочно-линейная, равна 0 в точках 0 и 1 и имеет излом в точке $\sqrt{\xi(1-\xi)}$. Подберем числа $\hat\lambda$ и $\hat\mu$ так, чтобы функция

$$a(x)u+\frac{\hat\lambda u^2}{2},$$

где $a(x)=-\chi_{[0,\xi]}(x)+\hat\mu$, достигала своего минимума в точке $\hat u(x)$; $\hat\lambda$ и $\hat\mu$ легко вычисляются, но нам их значения не понадобятся, важно лишь, что $\hat\lambda>0$. Используя условия задачи, получаем цепочку неравенств:

$$-f(\xi)+\frac{\hat\lambda}{2}\overset{\int f'^2\leqslant 1,\ \int f'=0}{\geqslant}\int\limits_0^1\left((-\chi_{[0,\xi]}(x)+\hat\mu)f'(x)+\frac{\hat\lambda f'(x)^2}{2}\right)dx\geqslant$$

$$\geqslant\int\limits_0^1\left((-\chi_{[0,\xi]}(x)+\hat\mu)\hat u(x)+\frac{\hat\lambda\hat u(x)^2}{2}\right)dx=-\hat f(\xi)+\frac{\hat\lambda}{2},$$

откуда $f(\xi)\leqslant\sqrt{\xi((1-\xi)}$ и равенство достигается лишь для функции $\hat f(x)$, которая не непрерывно дифференцируема. Из симметрии $|f(\xi)|\leqslant\sqrt{\xi((1-\xi)}$. А если $|\eta|<\sqrt{\xi((1-\xi)}$, точку (ξ,η) можно получить как $(\xi,f(\xi))$, где f — непрерывно дифференцируема. (*В. М. Тихомиров*)

1.8. Условие. а) Может ли семейство подмножеств натурального ряда быть несчетным, если для любых двух подмножеств из этого семейства одно строго содержится в другом?

б) Тот же вопрос, если пересечение любых двух множеств в семействе конечно.

Решение. В обоих пунктах ответ: «может». Рассмотрим семейства множеств $M_\alpha = \bigcup_n (n^2, n^2 + \lfloor \alpha n \rfloor)$ и $N_\alpha = \bigcup_n n^2 + \lfloor \alpha n \rfloor$, где $0 < \alpha < 1$. Ясно, что при $0 < \alpha < \beta$ имеет место строгое включение $M_\alpha \subset M_\beta$ и, кроме того, при всех достаточно больших n число вида $n^2 + \lfloor \alpha n \rfloor$ не совпадает с числом вида $m^2 + \lfloor \beta m \rfloor$. Поэтому семейство M_α служит примером к п. а), а семейство N_α — к п. б). *(А. Я. Белов)*

1.10. Условие. Функция, заданная на всей вещественной прямой, бесконечно дифференцируема. В каждой точке некоторая производная (номер производной может зависеть от точки) равна нулю. Докажите, что эта функция — многочлен.

Решение. Обозначим рассматриваемую функцию через f. Для каждого многочлена p построим замкнутые множества

$$M'_p = \{x \mid f(x) = p(x)\},$$
$$M_p = M'_p \setminus \{x \mid x \text{ изолированная точка } M'_p\}$$

и докажем, что для какого-то p выполнено $M_p = \mathbb{R}$.

Покажем, что $M_{p_1} \cap M_{p_2} = \varnothing$ при $p_1 \neq p_2$. Каждая точка множества M_p по построению является предельной, а ряд Тейлора f в предельной точке $x_0 \in M_p$ однозначно восстанавливается по значениям функции на $M_p \setminus \{x_0\}$. Действительно, предположим обратное. Пусть для некоторых двух функций $f_1, f_2 \in C^\infty$ с несовпадающими в x_0 рядами Тейлора при $x_n \to x_0$ ($x_k \neq x_0$, $k > 0$) выполнено $f_1(x_n) = f_2(x_n)$. Тогда функция $g = f_1 - f_2$ обращается в 0 на $\{x_n\}$ (сколь угодно близко от x_0), а ее ряд Тейлора — ненулевой. Применяя формулу Тейлора для первого ненулевого члена ряда Тейлора функции g, приходим к противоречию.

Обозначим $N = \mathbb{R} \setminus \cup_p M_p$. Это открытое множество. Докажем, что N пусто, после чего из связности $\mathbb{R}$ заключим, что ровно одно M_p непусто (что и требуется доказать).

Итак, предположим, что N непусто. Обозначим через $F^{(n)}$ множество нулей n-й производной f. Построим систему вложенных интервалов Δ_i индуктивно. Выберем произвольно интервал $\Delta_0 \subset N$, а каждый интервал Δ_{n+1} выберем в открытом непустом множестве $\Delta_n \setminus F^{(n+1)}$ (если $\Delta_n \subset F^{(n+1)}$, то f совпадает с многочленом на Δ_n). Нетрудно видеть, что в точках $\cap_{n=0}^\infty \Delta_n$ все производные f отличны от 0. Пришли к противоречию. *(Д. Ю. Бураго)*

2.1. Условие. Дана возрастающая функция $f(x)$ такая, что $f(0) > 0$, $f(1) < 1$. Докажите, что существует такое x, что $f(x) = x$ и, кроме того, x — точка непрерывности функции f.

Решение. Пусть точка x_0 удовлетворяет следующим условиям:

▷ Сколь угодно близко слева от x_0 есть такая точка x, что $f(x) > x$.

▷ Сколь угодно близко справа от x_0 есть такая точка x, что $f(x) < x$.

Тогда из монотонности функции f следует равенство $f(x_0) = x_0$. Покажем непрерывность f в точке x_0. В силу симметрии достаточно это проверить для непрерывности слева.

Пусть последовательность $x_n \to x_0$ сходится слева к точке x_0 и пусть значения $f(x_n)$ отличаются от $f(x_0) = x_0$ не менее, чем на $\varepsilon > 0$. В этом случае $f(x_n) < x_0 - \varepsilon$. Поскольку $x_n \to x_0$ слева, то в силу монотонности f неравенство $f(x) < x_0 - \varepsilon$ выполняется для всех $x < x_0$.

Но если $x_0 - x < \varepsilon$ и при этом $f(x) < x_0 - \varepsilon$, то $f(x) < x$. Следовательно, $f(x) < x$ в некоторой левой окрестности точки x_0. Получили противоречие с выбором точки x_0.

Итак, непрерывность f в точке x_0 доказана.

Остается показать существование такой точки x_0. Поскольку $f(0) > 0$ и $f(1) < 1$, то в качестве x_0 можно взять $\sup\{x | \forall\, t < x\ f(t) \geqslant t\}$.

(*А. Я. Белов*)

2.3. Условие. Пусть $a_0 = a$, $a_{n+1} = a^{a_n}$, q — произвольное натуральное число, большее 1. Докажите, что последовательность остатков от деления a_n на q стабилизируется (т.е. все остатки, начиная с некоторого, равны).

Решение. Воспользуемся следующим фактом: остатки от деления чисел вида a^n на q периодичны с периодом $q_1 < q$. Тогда при достаточно больших n остаток от деления числа n на q_1 однозначно определяет остаток от деления числа a^n на q.

Будем решать задачу индукцией по q. Можно считать, что при всех $q' < q$ остатки последовательности a_n по модулю q' при всех достаточно больших n стабилизируются. Но тогда стабилизируются и остатки последовательности $a_{n+1} = a^{a_n}$ при делении на q. А последовательность a_{n+1} получается из последовательности a_n сдвигом. (*А. Я. Белов*)

2.4. Условие. Можно ли числа от 1 до 2^{1000} раскрасить в два цвета так, чтобы не существовало арифметических прогрессий длины 2000, составленных из чисел одного цвета?

Решение. Ответ: искомая раскраска существует.

Покажем, что отлична от нуля вероятность того, что в случайно и равновероятно выбранной раскраске нет арифметической прогрессии длины 2000.

Оценим количество прогрессий длины 2000. Каждая такая прогрессия задается первыми двумя членами $i_1 < i_2$, причем не все такие пары задают прогрессию. Поэтому количество прогрессий строго меньше числа пар — т.е. числа $2^{1000}(2^{1000}-1)/2 < 2^{1999}$.

С другой стороны, вероятность того, что данная прогрессия раскрашена одинаково, равна $2/2^{2000} = 2^{-1999}$.

И сумма таких вероятностей по всем прогрессиям меньше 1. Таким образом, искомая раскраска существует.

Замечание. От вероятностей в таком рассуждении легко избавиться. Для этого нужно говорить о покрытиях подходящим образом подобранных множеств. (*А. Я. Белов*)

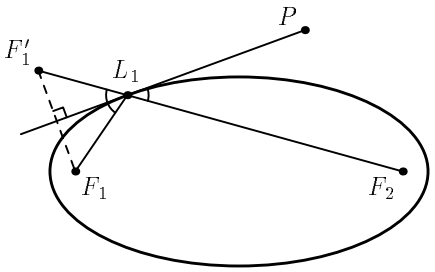
2.5. Условие. Дано выпуклое тело в пространстве. Докажите, что можно отметить 4 точки на его поверхности так, чтобы касательная (т.е. опорная плоскость) в каждой отмеченной точке была параллельна плоскости, проходящей через остальные три.

Решение. Расположим 4 точки A, B, C, D в вершинах тетраэдра максимального объема, вписанного в данное тело. Если плоскость, проходящая через D и параллельная (ABC), содержит внутреннюю точку тела, то на поверхности тела можно найти точку D', расстояние от которой до плоскости (ABC) больше расстояния от точки D до этой плоскости. Получили противоречие с максимальностью объема тетраэдра $ABCD$.

Осталось показать существование тетраэдра максимального объема, вписанного в данное тело. Прежде всего, ограничены координаты вершин, а также ограничены объемы вписанных тетраэдров (объемом самого тела). Обозначим через v точную верхнюю грань таких объемов. Рассмотрим последовательность тетраэдров, вписанных в исходное тело, объемы которых стремятся к v. Координаты вершин тетраэдров задают точку 12-мерного пространства. Извлечем из последовательности таких точек сходящуюся подпоследовательность стандартным образом: рассмотрим подпоследовательность, у которой сходятся первые координаты, из нее извлечем подпоследовательность тетраэдров со сходящимися вторыми координатами и т. д. Предельной точке соответствует тетраэдр максимального объема v, вписанный в данное тело. (*А. Я. Белов*)

2.6. Условие. Из произвольной точки P вне эллипса проведены два касательных к эллипсу луча l_1 и l_2. Кроме того, из P проведены лучи s_1 и s_2 через фокусы эллипса. Докажите, что угол между l_1 и s_1 равен углу между l_2 и s_2.

Решение. Пусть PL_1, PL_2 — касательные к эллипсу, F_1, F_2 — его фокусы, F_1', F_2' — точки, симметричные F_1, F_2 относительно прямых PL_1,



PL_2. Тогда из свойств эллипса получаем (см. рис.):

$$F_1'F_2 = F_1L_1 + F_2L_1 = F_1L_2 + F_2L_2 = F_1F_2'.$$

Следовательно, треугольники $PF_1'F_2$ и PF_1F_2' равны по трем сторонам и, значит, равны углы $F_1'PF_2$ и F_1PF_2', что равносильно утверждению задачи.

(*А. Заславский*)

3.1. Условие. A, B, C — произвольные матрицы размера 2×2. Докажите тождество Холла: $[[A,B]^2, C] = 0$. (Через $[A,B] \stackrel{\text{def}}{=} AB - BA$ обозначается *коммутатор*).

Решение. Поскольку $\operatorname{tr}(AB) = \operatorname{tr}(BA)$, след коммутатора $[A,B] = AB - BA$ равен нулю. С другой стороны, след матрицы есть сумма ее собственных значений, а собственных значений у матрицы второго порядка два. Поэтому собственные значения матрицы $[A,B]$ — нули или противоположные числа. Если они равны нулю, то и матрица $[A,B]^2 = 0$. Если они ненулевые противоположные числа, то матрица $[A,B]$ диагонализуема и ее квадрат $[A,B]^2$ есть скалярная матрица, т.е. матрица вида $\begin{pmatrix} \lambda^2 & 0 \\ 0 & \lambda^2 \end{pmatrix}$. Такая матрица лежит в центре (т.е. коммутирует со всеми матрицами). Поэтому в алгебре матриц второго порядка выполняется тождество $[[A,B]^2, C] = 0$.

(*А. Я. Белов*)

3.2. Условие. Пусть $|\varepsilon_i| < 1$ и произведение $\prod(1-\varepsilon_i)$ сходится. Верно ли, что сходится ряд $\sum \varepsilon_i$?

Решение. Ответ: не обязательно.

Положим $\varepsilon_{2n} = -\delta_n$, $\varepsilon_{2n+1} = \delta_n + \cdots + \delta_n^k + \ldots$, где $\delta_n \to 0$. Тогда $(1+\varepsilon_{2n})(1+\varepsilon_{2n+1}) = 1$, поэтому произведение $\prod_n(1+\varepsilon_{2n})$ сходится и равно единице.

С другой стороны,

$$\sum_m \varepsilon_m = \sum_n -\delta_n + \delta_n + \ldots + \delta_n^k + \ldots = \sum_n \frac{\delta_n^2}{1-\delta_n}.$$

Для завершения конструкции достаточно выбрать δ_n так, чтобы ряд $\sum \delta_n^2$ расходился. Например, можно положить $\delta_n = n^{-1/2}$, тогда

$$\varepsilon_k = \begin{cases} -\dfrac{1}{\sqrt{n}}, & \text{если } k = 2n, \\ \dfrac{1}{\sqrt{n}-1}, & \text{если } k = 2n+1. \end{cases}$$

(*А. Я. Белов*)

3.4. Условие. а) Пусть $p > 3$ – простое число. Докажите, что на торической шахматной доске размера $p \times p$ можно расставить p ферзей так, чтобы они не били друг друга.

б) Назовем *магараджей* фигуру, которая из клетки $(0,0)$ за один ход может попасть в клетки $(0, \pm k)$, $(\pm k, 0)$, $(\pm k, \pm k)$, $(\pm k, \pm 2k)$, $(\pm 2k, \pm k)$ (k — целое положительное число). Ответьте на вопрос пункта а) для магарадж и при $p > 7$.

Решение. Занумеруем вертикальные ряды (координата X) и горизонтальные ряды (координата Y) с помощью остатков от деления на p. Будем рассматривать шахматную доску как плоскость над $\mathbb{Z}_p$.

а) Расположим ферзей в точках с координатами $(x, 2x)$. Легко видеть, что они не бьют друг друга. Ферзь бьет вдоль линий $x = \text{const}$, $y = \text{const}$, $\pm x \pm y = \text{const}$. При $p > 3$ направления этих линий отличаются от направлений прямой $y = 2x$, а две прямые либо совпадают по направлению, либо пересекаются в одной точке. (Ибо система из двух линейных сравнений по простому модулю с непропорциональными левыми частями имеет единственное решение.) Если же $p = 3$, то $2 = -1$ в $\mathbb{Z}_p$, направление прямой $y = 2x$ совпадает с линией боя ферзя и расположить трех ферзей не удается. Итак, даже на торической доске $p \times p$, где p — простое, можно поставить p ферзей так, чтобы они не били друг друга. А. К. Толпыго заметил любопытный факт: на торической шахматной доске 15×15 нельзя расставить 15 ферзей так, чтобы они не били друг друга.

б) Решение аналогично, только магараджи ставятся вдоль прямой $y = 3x$ (ходом «длинного коня»). При $p = 7$ это направление совпадает с направлением прямой $x = -2y$, ибо $-1/2 = 3$ в $\mathbb{Z}_7$. При бóльших p направление прямой $y = 3x$ не совпадает с направлением боя магараджи $ax + by = \text{const}$, $|a|, |b| \leqslant 2$.

Аналогичным образом можно при всех достаточно больших p расположить p не бьющих друг друга k-монстров на торической доске порядка p. Мы называем *k-монстром* фигуру, которая бьет по направлениям прямых $ax + by = const$, где $|a|, |b| \leqslant k$. Возникает вопрос: верно ли это для всех достаточно больших досок (не только простого порядка)?

(*А. Я. Белов*)

3.5. Условие. Дан произвольный многочлен с комплексными коэффициентами. Докажите, что корни его производной лежат внутри выпуклой оболочки корней самого многочлена.

Решение. Это известный результат Гаусса. См. Gauss, Opera omnia, т. 3, с. 112, Göttingen, Ges. d. Wiss., 1886; т. 8, с. 32, 1900; можно также обратиться к книге Полиа Г., Сеге Г. Задачи и теоремы из анализа. М.: Наука, 1978. С. 115, 300; оттуда мы и позаимствовали ссылку на оригинальный текст Гаусса.