

МАТЕМАТИЧЕСКОЕ ПРОСВЕЩЕНИЕ

Третья серия

ВЫПУСК 16

Москва
Издательство МЦНМО
2012

УДК 51.009

ББК 22.1

М34

Редакционная коллегия

| | | |
|--------------------|--------------------|-------------------|
| Бугаенко В. О. | Винберг Э. Б. | Вялый М. Н. |
| Гальперин Г. А. | Глейзер Г. Д. | Гусейн-Заде С. М. |
| Дориченко С. А. | Егоров А. А. | Ильяшенко Ю. С. |
| Канель-Белов А. Я. | Константинов Н. Н. | Прасолов В. В. |
| Розов Н. Х. | Сосинский А. Б. | Тихомиров В. М. |
| Френкин Б. Р. | Яценко И. В. | |

ГЛАВНЫЙ РЕДАКТОР: Э. Б. Винберг ОТВ. СЕКРЕТАРЬ: М. Н. Вялый

АДРЕС РЕДАКЦИИ:

119002, Москва, Б. Власьевский пер., д. 11, к. 301

(с пометкой «Математическое просвещение»)

EMAIL: matpros@mccme.ru WEB-PAGE: www.mccme.ru/free-books

М34 **Математическое просвещение.** Третья серия, вып. 16. —

М.: МЦНМО, 2012. — 240 с.

ISBN 978-5-94057-988-5

В сборниках серии «Математическое просвещение» публикуются материалы о проблемах современной математики, изложенные на доступном для широкой аудитории уровне, заметки по истории математики, обсуждаются проблемы математического образования.

УДК 51.009

ББК 22.1

ISBN 978-5-94057-988-5

© МЦНМО, 2012.

СОДЕРЖАНИЕ

Математический мир

| | |
|---|---|
| В. М. Тихомиров <i>Вспоминая братьев Ягломов</i> | 5 |
|---|---|

Наш семинар: математические сюжеты

| | |
|---|-----|
| С. В. Дужин <i>Перечисление деревьев</i> | 14 |
| М. Скопенков, В. Смыкалов, А. Устинов <i>Случайные блуждания и электрические цепи</i> | 25 |
| А. Б. Скопенков <i>Еще одно доказательство «из Книги»: теорема Менгера</i> | 48 |
| Э. Э. Лернер, Э. Ю. Лернер <i>Биективное доказательство дискретного закона арксинуса</i> | 50 |
| А. В. Акопян, Г. А. Кабатянский, О. Р. Мусин <i>Контактные числа, коды и сферические многочлены</i> | 57 |
| М. Н. Вялый, В. А. Гурвич <i>Ультраметрики, деревья, потоки и узкие места</i> | 75 |
| Д. А. Байгушев <i>Об асимптотике эргодических перестановок Арнольда</i> | 89 |
| В. О. Мантуров <i>Четырехвалентные графы с крестовой структурой. Вложения в двумерные поверхности</i> | 94 |
| Д. П. Ильютко <i>Матрицы пересечений эйлеровых циклов 4-валентных графов с крестовой структурой</i> | 105 |
| А. М. Райгородский <i>Задача Эрдёша – Гинзбурга – Зива и ее окрестности</i> | 132 |
| Е. А. Горин <i>Задача часовщика</i> | 145 |
| В. И. Войтицкий <i>Дробная форма натурального числа и ее применение в задачах на циклические перестановки цифр</i> | 151 |
| П. А. Кожевников <i>Еще раз о точке Фейербаха</i> | 165 |
| А. Д. Медных <i>О формуле Брахмагупты в геометрии Лобачевского</i> | 172 |

Преподавание математики

| | |
|---|-----|
| А. Гасников, Е. Черноусова, Т. Нагапетян, О. Федько <i>Стохастический анализ в задачах</i> | 181 |
|---|-----|

Конкурсы и олимпиады

| | |
|--|-----|
| И. В. Аржанцев, В. И. Богачёв, А. И. Гарбер, А. А. Заславский, В. Ю. Протасов, А. Б. Скопенков <i>Студенческие олимпиады мехмата МГУ 2010 – 2011 гг.</i> | 214 |
|--|-----|

Нам пишут

| | |
|---|-----|
| А. Б. Скопенков <i>Отклик на статью В. О. Мантурова</i> | 228 |
| <i>Отклики на задачный раздел «Математического просвещения»</i> | 229 |

Задачный раздел

| | |
|---|-----|
| <i>Условия задач</i> | 230 |
| <i>Решения задач из предыдущих выпусков</i> | 233 |

Математический мир

Вспоминая братьев Ягломов

В. М. Тихомиров

6 марта 1921 года в Харькове в семье инженера родились братья-близнецы — Акива и Исаак (а близкие звали их Кика и Ися). Братья были совершенно неразличимы и очень дружны.

Когда мальчикам исполнилось шесть лет, семья переехала в Москву. Интерес к математике у братьев обнаружился очень рано. Еще в ранние школьные годы братья вместе с отцом начали решать задачи из журнала «Математика в школе». В 1935/36 учебном году они стали заниматься в математических кружках при МГУ и слушать лекции для школьников, которые читали мехматские профессора. Вскоре оба они стали заниматься в кружке Давида Оскаровича (Додика) Шклярского, человека, влюбленно-го в математику и энтузиаста занятий со школьниками. Среди участников кружка был Андрей Сахаров, с которым у братьев завязалась дружба.

Шклярскому суждено было совершить переворот во всем кружково-олимпийском движении: вместо докладов он стал предлагать участникам своего кружка интересные задачи для решения. В 1938 году такой стиль работы привел к триумфу: все первые премии были взяты участниками кружка Шклярского. Ими стали Владимир Волынский, Александр Кронрод и братья Ягломы. Премии победителям вручал Андрей Николаевич Колмогоров.

Окончив школу в том же году, братья поступают в Московский университет: Кика на физический факультет, а Ися на механико-математический. При этом они договорились, что оба будут учиться одновременно на обоих факультетах. Оба они учились прекрасно: в 1940 году в «Правде» была помещена фотография шести юношей с подписью: «Студенты физического факультета Московского государственного университета, досрочно закончившие зимнюю экзаменационную сессию на „отлично“», среди них был Акива Яглом. Братья очень активно включились в культурную жизнь

Москвы — театральную, музыкальную и художественную и обрели очень широкий круг знакомых. К лету 1941 года оба они окончили три курса и физфака и мехмата (тогда никаких специальных разрешений не требовалось: со своей физфаковской зачеткой Кика приходил на мехмат сдавать экзамены, и преподаватели проставляли оценку ему в зачетку, то же происходило и с Исей).

Началась война. Братья Ягломы не были призваны в армию из-за сильной близорукости. Они продолжали учиться сначала в МГУ, а затем в Свердловском университете (в Свердловск вместе с Народным комиссариатом черной металлургии, где работал отец, эвакуировалась семья Ягломов). В Свердловске братья дважды имели контакты с А. Н. Колмогоровым, и он ознакомил их с теорией турбулентности, которой активно занимался в то время. Летом 1942 года братья Ягломы закончили Свердловский университет (в военные годы во многих высших учебных заведениях четвертый курс был последним). По рекомендации А. Н. Колмогорова оба брата поступили на работу в Главную геофизическую обсерваторию, эвакуированную из Ленинграда в Свердловск.

В 1943 году Колмогоров предложил Акиве Моисеевичу поступить к нему в аспирантуру в Математический институт им. В. А. Стеклова. Тот с радостью согласился. Колмогоров прислал А. М. Яглому вызов в Москву, и с осени того года А. М. был зачислен в аспирантуру МИАН. Одновременно началось его сотрудничество на кафедре теории вероятностей МГУ, возглавляемой Колмогоровым.

Исаак Моисеевич по окончании университета в Свердловске, поступил в аспирантуру МГУ, который тогда переехал в Свердловск. Учебой И. М. в аспирантуре руководил заведующий кафедрой дифференциальной геометрии МГУ Вениамин Федорович Каган, и геометрия стала основной профессией Исаака Моисеевича. В 1945 году Исаак Моисеевич защитил в МГУ кандидатскую диссертацию.

В ту пору у братьев был только один пиджак, который принадлежал Акиве Моисеевичу. Для выступления с докладом по диссертации Исаак Моисеевич позаимствовал пиджак у своего брата, а по окончании доклада вернул пиджак Кике. Защита прошла успешно, но когда объявили результат, Вениамин Федорович бросился поздравлять, разумеется, Акиву Моисеевича, который был в пиджаке!

Акива Моисеевич ожидал, что Колмогоров даст ему какую-нибудь тему по теории турбулентности, но тот предложил ему развить на примере броуновского движения результаты своей работы по обратимости стохастических законов природы. А. М. Яглом в течение года справился с поставленной задачей, но на предложение Колмогорова организовать защиту и окончить аспирантуру, попросил не реализовывать этот план, ибо хотел в течение двух оставшихся лет аспирантуры заниматься проблемами теоретической физики. В итоге защита диссертации у Акивы Моисеевича

состоялась на год позже брата. Диссертация была озаглавлена так: «О статистической обратимости брауновского движения».

Братьям предстояло выбрать место работы. И здесь их творческие пути разошлись. А. М. наиболее привлекало предложение И. Е. Тамма и В. Л. Гинзбурга поступить на работу в ФИАН, но он отказался от этого предложения, узнав, что придется заниматься проблемами, связанными с атомным оружием. Из нескольких других возможностей Акива Моисеевич выбрал возглавляемую Колмогоровым лабораторию атмосферной турбулентности Института теоретической геофизики АН СССР. В Лаборатории атмосферной турбулентности Акива Моисеевич проработал 45 лет (сначала в ИТГ, потом в ГЕОФИАНЕ, наконец, в Институте физики атмосферы). С начала шестидесятых годов А. М. Яглом возглавил в ИФА Лабораторию атмосферной турбулентности.

Основным делом Исаака Моисеевича Яглома стало математическое просвещение. Много сил он уделял также переводческой деятельности.

Служебная карьера Исаака Моисеевича сложилась не столь успешно, как у его брата: места работы ему пришлось менять много раз.

После защиты кандидатской диссертации Исаак Моисеевич работал в математической редакции Издательства иностранной литературы. С 1948 г. И. М. работал на мехмате МГУ и в 1949 г. получил звание доцента, но во время кампании, известной как «борьба с космополитизмом», был уволен (вместе с И. М. Гельфандом, И. С. Градштейном и другими). После этого он работал в Орехово-Зуевском педагогическом институте, а затем в Московском государственном педагогическом институте.

Большинству математиков И. М. Яглом известен своими популярными книгами по геометрии и другим областям математики. Он создал серию «Библиотека математического кружка», где были изданы многие книги, в частности, книги Д. О. Шклярского, Н. Н. Ченцова и И. М. Яглома «Избранные задачи и теоремы элементарной математики» (первый том — «Арифметика и алгебра», второй — «Геометрия» (планиметрия), третий — «Геометрия» (стереометрия)).

Включение фамилии Шклярского в число авторов требует комментария.

Шклярский добровольцем ушел на фронт. Некоторые студенты-добровольцы были делегированы ЦК ВЛКСМ в Бригаду особого назначения при НКВД СССР. Возглавлял бригаду Судоплатов. В этой бригаде были Николай Кузнецов, Дмитрий Медведев (бывший командиром отряда), Николай Королёв (бывший адъютантом Медведева), были еще некоторые спортсмены. Дмитрий Медведев был впоследствии командиром партизанского отряда, действовавшего в Западной Украине. Ему принадлежит книга «Это было под Ровно», где он описывает героические дела своего отряда, и в частности, подвиги Николая Кузнецова — легендарного советского разведчика. Николай Королев был выдающимся советским боксером-тяжеловесом, имя которого в предвоенные и первые послевоенные годы знали все.

Додика Шклярского в бригаде очень любили. Он был застенчивый, молчаливый, всегда занимался математикой. Как-то раз глубокой ночью один из членов бригады, оставивший воспоминания, проснулся и увидел Шклярского, который сидел на нарах в турецкой позе и что-то писал при свете свечи. На вопрос: «Что ты пишешь?» он сказал: «Не мешай мне, пожалуйста. . . » Это была математика, а что он мог ответить об этом человеке, который ею никогда не занимался?

16 октября 1941 года (это был один из самых трагических дней в истории Москвы) перед отправкой на фронт отряд ночевал на Бронной, в школе. Додик жил до войны в Васильевском переулке, рядом с Белорусским вокзалом. Командир отпустил москвичей домой. Додик пошел, полагая, что Москву возьмут немцы, желая спрятать свои рукописи. Он зашел в свой дом и спрятал их. С войны Д. О. Шклярский не вернулся. Часть его рукописей сохранилась и была опубликована после войны в «Успехах математических наук». Одна из них была посвящена задачам, которые давались школьникам на математическом кружке. В память о своем учителе И. М. Яглом включил Д. О. Шклярского в число авторов двухтомника «Избранные задачи и теоремы элементарной математики». Эта книга несколько раз переиздавалась.

Назову еще несколько книг и брошюр И. М. Яглома. Многие из них украшали и украшают библиотеки тех, кому дорога наша наука.

В. Г. Болтянский, И. М. Яглом. Выпуклые фигуры. 1951. 343 с.

И. М. Яглом, А. М. Яглом. Неэлементарные задачи в элементарном изложении. 1954. 544 с.

И. М. Яглом. Принцип относительности Галилея и неевклидова геометрия. 1969. 304 с.

Н. Н. Ченцов, Д. О. Шклярский, И. М. Яглом. Геометрические неравенства и задачи на максимум и минимум. 1970. 336 с.

Н. Н. Ченцов, Д. О. Шклярский, И. М. Яглом. Геометрические оценки и задачи из комбинаторной геометрии. 1974. 384 с.

И. М. Яглом. Комплексные числа и их применение в геометрии. 1963. 192 с.

И. М. Яглом. Проблема тринадцати шаров. 1975. 84 с.

И. М. Яглом, А. М. Яглом. Вероятность и информация. 1973. 512 с.

Я. Б. Зельдович, И. М. Яглом. Высшая математика для начинающих физиков и техников. 1982. 512 с.

Л. И. Головина, И. М. Яглом. Индукция в геометрии. 1961. 100 с.

И. М. Яглом. Необыкновенная алгебра. 1968. 72 с.

И. М. Яглом. Современная культура и компьютеры. 1990. 48 с.

И. М. Яглом. Геометрия точек и геометрия прямых. 1968. 49 с.

И. М. Яглом. Элементарная геометрия прежде и теперь. 1972. 47 с.

И. М. Яглом. Математика и реальный мир. 1978. 64 с.

И. М. Яглом. Герман Вейль. 1967. 47 с.

И. М. Яглом. Феликс Клейн и Софус Ли. 1977. 64 с.

Многие из этих книг были переведены на иностранные языки.

Из других популярных книг И. М. Яглома отметим «Принцип относительности Галилея и неевклидова геометрия» (вышла в английском переводе), «Идеи и методы аффинной и проективной геометрии» (совместно с В. Г. Ашкинуде), «Индукция в геометрии» (совместно с Л. И. Головиной, вышла в английском и немецком переводах), «Комплексные числа и их применение к геометрии» (вышла во французском и английском переводах), «Новые направления в математике» (вышла в Москве на французском языке), «Необыкновенная алгебра» (вышла в английском переводе), «Конечная алгебра, конечная геометрия и коды», а также популярные научные биографии математиков «Герман Вейль», «Феликс Клейн и Софус Ли», которая потом вышла в расширенном английском переводе. В нескольких изданиях на русском, французском, немецком и чешском языках вышла книга И. М. и А. М. Ягломов «Вероятность и информация».

Исаак Моисеевич Яглом был удостоен Европейской премии Cortina Ullis, выдаваемой раз в два года за вклад в популяризации какой-то одной науки. Премия за популяризацию математики впервые была присуждена в сентябре 1989 г. и была поделена между И. Ягломом (за книгу “Felix Klein and Sophus Lie. Evolution of the idea of Symmetry in the 19th century”, Birkhäuser, Boston – Bazel, 1983) и М. Кацем (за книгу “Enigmas of Chance. An autobiography”, Harper and Row, N. Y., 1985). К сожалению, обоих авторов в тот момент уже не было в живых.

В шестидесятые годы в комиссии, возглавляемой А. Н. Колмогоровым, И. М. Яглом принял деятельное участие в разработке программы школьного курса геометрии. В 1968 году Исаак Моисеевич подписал письмо в защиту А. С. Есенина-Вольпина и был уволен из Педагогического института. После этого он работал в вечернем Металлургическом институте в Москве. Затем ему удалось устроиться в Ярославский университет. Продолжая жить в Москве, каждый месяц Исаак Моисеевич на какое-то время переезжал в Ярославль, где читал лекции, вел семинары, занимался с учениками. Однажды его попросили выступить с докладом на некоем семинаре общего философского направления. Исаак Моисеевич выбрал волновавшую тогда его тему об устройстве человеческого мозга. Незадолго до того Нобелевская премия была присуждена за открытие разных функций двух полушарий человеческого мозга. Среди прочего Исаак Моисеевич сказал, что люди одинаково владеющие правой и левой рукой обладают нередко особыми способностями и в обоих полушариях. И в качестве примера привел своего друга Андрея Дмитриевича Сахарова. Тот был в это время сослан в Нижний Новгород и подвергался «всенародному осуждению». Выступление на этом семинаре стоило Исааку Моисеевичу места в Ярославском университете. После этого у него не было возможности преподавать. Он работал в последние годы Академии педагогических наук.

Интересы И. М. Яглома выходили далеко за пределы математики. Он был человеком широкой души, всегда готовым прийти на помощь тем, кто в ней нуждался.

Исаак Моисеевич был истинным знатоком истории, литературы, театра, живописи. В его квартире висели картины Модильяни, Фалька и других художников.

Большая творческая, педагогическая и общественная деятельность, частые увольнения, трудности с работой и изданием книг в Москве, болезнь жены и сына подорвали здоровье Исаака Моисеевича, и 17 мая 1988 г. он скончался.

Творческая судьба Акивы Моисеевича Яглома сложилась весьма успешно. В начале своего творческого пути Акива Моисеевич с одной стороны развивал тематику А. Н. Колмогорова по теории случайных процессов, а с другой, сотрудничая с И. М. Гельфандом, занимался проблемами теоретической физики, связанными с теорией представлений и с континуальными интегралами. И почти сразу же он начал свои исследования по статистической гидродинамике. Первый цикл его работ включает публикации по теории марковских цепей, ветвящихся процессов, стохастической обратимости броуновского движения и статьи по экстраполяции и фильтрации случайных процессов, где А. М. значительно развил пионерские работы Колмогорова конца тридцатых, начала сороковых годов. Некоторые итоги его начальной деятельности по этой проблематике были подведены в его статье «Введение в теорию случайных функций», опубликованной в 1952 году в «Успехах математических наук», занимающей 165 страниц. В 1962 году она была дважды издана в США, как отдельная книга, так как ничего подобного там тогда еще не издавалось. В работах, совместных с И. М. Гельфандом и А. Н. Колмогоровым, развивалась теория информации. В 1955 году А. М. защищает докторскую диссертацию под названием «Теория корреляции непрерывных процессов и полей с приложениями к задачам статистической экстраполяции временных рядов и к теории турбулентности».

В 1956 году в Москве состоялся Третий Всесоюзный математический съезд. В трудах съезда помещены три доклада А. М. Яглома: «Количество информации и энтропия для непрерывных распределений» (с И. М. Гельфандом и А. Н. Колмогоровым), «Континуальные интегралы» (с И. М. Гельфандом и Р. А. Минлосом) и «Микроструктура развитой турбулентности» (с А. М. Обуховым). В пятидесятые годы начинается цикл его популяризаторских публикаций, среди которых вышедшая в 1957 году замечательная книга «Вероятность и информация», написанная с И. М. Ягломом. В дальнейшем А. М. исследовал теоретические и прикладные проблемы турбулентности и геофизической гидродинамики.

Среди работ начального периода прежде всего надо отметить его работу 1948 года по теории однородной и изотропной турбулентности в вязкой сжимаемой жидкости и работу 1949 года о поле ускорений в турбулентном потоке. Существенным результатом последней работы явилось обнаружение того, что частотный спектр лагранжевых ускорений жидкой частицы в турбулентном потоке является постоянной величиной, связанной со скоростью диссипации кинетической энергии турбулентности, т.е. это «белый шум» в инерционном интервале развитой турбулентности. Впоследствии это позволило связать представления теории турбулентности Колмогорова – Обухова с результатами теории броуновского движения. В другой работе того же года было выведено динамическое уравнение для поля температур пассивной примеси, что явилось вторым точным результатом в теории турбулентности после колмогоровского динамического уравнения для поля скоростей (его знаменитого закона «четырёх пятых»). В 1965 году вышла первая часть монографии А. С. Мони́на и А. М. Яглома «Статистическая гидродинамика»; в 1967 году вышла ее вторая часть. В 1971 и 1975 годах оба тома вышли в английском переводе в издательстве MIT Press, расширенные и дополненные материалами, появившимися к тому времени. В конце 70-х годов книга была издана в четырех томах на японском языке. Эта книга заслуженно считается энциклопедией по данной тематике.

Потребности приложений теории турбулентности к проблемам гидродинамики атмосферы стимулировали обобщение и дальнейшее развитие теории случайных процессов и полей. Его работы способствовали созданию математического аппарата, необходимого для превращения статистической гидродинамики в строгую физико-математическую дисциплину. Им были детально изучены процессы со стационарными приращениями произвольного порядка, статистически однородные и изотропные, а также локально изотропные скалярные и векторные случайные поля. Для каждого из этих классов дан и проанализирован общий вид соответствующих корреляционных функций, а также получены спектральные представления как корреляционных и структурных функций, так и самих процессов и полей и исследованы свойства их спектральных характеристик.

В своей работе А. М. Яглом умел связывать теоретические исследования с результатами, полученными авторами экспериментальных работ. Этим, в частности, объясняется его интерес к проблемам статистического оценивания. При этом высокий уровень математической строгости исследований сочетается с изложением полученных результатов в форме, доступной прикладнику. В своих работах Акива Моисеевич использовал колоссальный объем литературы: списки литературы в его статьях и книгах

обычно содержат максимально возможное количество литературных ссылок, причем значительная часть относится к приложениям и содержит экспериментальные результаты. Именно поэтому его статьи, обзоры и монографии уже давно стали настольными книгами для специалистов всего мира, работающих в самых различных областях науки: метеорологии, океанологии, гидрологии, радиотехнике и др.

Всего в списке научных трудов А. М. Яглома свыше 150 статей и семь книг.

Следует отдельно сказать о его уникальной двухтомной монографии, написанной им уже давно, но не потерявшей своего значения. К сожалению, специалисты в России с ней не знакомы, так как ему не удалось издать ее тогда в СССР. Она и сейчас заслуживает издания в русском переводе.

Наконец, нельзя не сказать о выдающемся педагогическом таланте Акивы Моисеевича. Он в течение ряда лет был профессором кафедры теории вероятностей МГУ. Его лекции и доклады на различных научных конференциях были всегда содержательны и интересны.

В 1992 году Яглом переехал в США. Это было вызвано во многом семейными причинами. В Америке он стал работать в Массачусетском технологическом институте. В 1988 году А. М. Яглом получил премию Американского физического общества имени Отто Лапорта, а в 2007 году Европейский союз наук о Земле присудил ему медаль Л. Ф. Ричардсона. Ему должны были вручить эту медаль в апреле 2008 года.

Работая в МИТ, А. М. получил грант на написание труда по развитию статистической гидродинамики за последние тридцать с лишним лет, прошедших за годы, после выхода в свет английского издания его монографии с А. С. Мониним. Он поставил перед собой цель описать то необозримое море литературы, которое родилось в развитие четырех крохотных заметок в ДАН СССР, опубликованных его учителем А. Н. Колмогоровым в 1941 и 1942 годах. Он хорошо понимал, что эта цель неосуществима. Отвечая как-то на вопрос о том, когда он собирается закончить свою работу, Акива Моисеевич напомнил, что некогда в Америке проходил шумный процесс, на котором преступнику был вынесен приговор в три пожизненных срока плюс еще тридцать лет. «Вот этого мне бы, возможно хватило», — с улыбкой заключил он.

Акива Моисеевич Яглом был интересным и глубоким человеком, прекрасным собеседником, любил путешествия, особенно в горах. Он был теснейшим, сокровенным образом связан с Россией, ее культурой, наукой и просвещением. Он необычайно любил книги и был истинным библиофилом. У него здесь было множество друзей, ко встрече с которыми он всегда стремился. Он был добрым и участливым человеком.

Акива Моисеевич Яглом умер 13 декабря 2007 года в Бостоне.

На эту смерть И. М. Гельфанд отозвался так: «Дорогие коллеги, А. Яглом был одним из самых талантливых математиков, с которыми я когда-либо встречался. Его смерть огромная потеря для всех нас.»

Наш семинар: математические сюжеты

Перечисление деревьев*

С. В. Дужин

— Счел ли ты деревья?
— Как счесть деревья? — смеясь, ска-
зал Степан Аркадьич, . . . — Сочесть
пески, лучи планет хотя и мог бы ум
высокий. . .

Л. Толстой. Анна Каренина

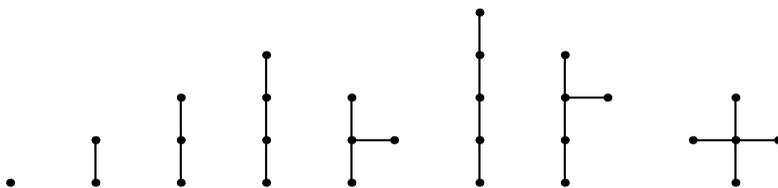
1. ФОРМУЛИРОВКА РЕЗУЛЬТАТОВ

Деревом называется связный граф, не имеющий циклов. На рисунке 1 изображены все деревья с числом вершин, не превосходящим 5. (Точный смысл этого утверждения заключается в том, что любое дерево, имеющее не более 5 вершин, *изоморфно* одному из деревьев, нарисованных на картинке, а никакие два из этих деревьев не изоморфны друг другу.)

Задача 1. Докажите, что связный граф является деревом тогда и только тогда, когда число его ребер на единицу меньше числа вершин.

Задача перечисления деревьев, т. е. нахождения формул для числа t_n различных деревьев с n вершинами — одна из основных, и притом самых красивых, задач перечислительной комбинаторики. Впервые эту задачу

*В тексте статьи наблюдается некоторый уклон в химию. Причина этого в том, что статья представляет собой обработку части курса лекций, прочитанных автором в Московском высшем химическом колледже весной 1993 года.

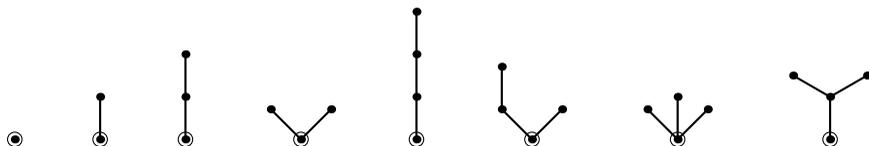
Рис. 1. Деревья с числом вершин ≤ 5

поставил знаменитый английский математик Артур Кэли (см. [1]) в связи с задачей определения числа изомеров предельных углеводородов C_nH_{2n+2} . Каждый такой изомер описывается способом соединения атомов углерода, т. е. деревом с n вершинами валентности, не превосходящей 4. Надо сказать, что А. Кэли, найдя изящное рекуррентное соотношение для числа всех деревьев, не нашел сколько-нибудь удовлетворительной формулы для числа предельных алканов — такая формула была впервые получена венгерским математиком Д. Пойа в работе [2].

Задача 2. Попробуйте вывести эту формулу, дочитав этот текст до конца и используя изложенные здесь методы.

Все известные науке способы перечисления деревьев основываются на предварительном перечислении так называемых *корневых* деревьев.

Корневым деревом называется дерево, в котором отмечена одна вершина, называемая корнем.

Рис. 2. Корневые деревья с числом вершин ≤ 4

Задача 3. Деревья и корневые деревья естественно возникают в различных, иногда весьма отдаленных друг от друга областях математики. Вот пример, недавно использованный Е. В. Бабаевым (МГУ) в его топологической теории структуры химических молекул. Проверьте, что различные, с точностью до гомеоморфизма, расположения n непересекающихся окружностей на сфере перечисляются деревьями с $n + 1$ вершиной, а различные расположения n непересекающихся окружностей на плоскости перечисляются корневыми деревьями с $n + 1$ вершиной. (Указание: области, на которые окружности делят поверхность, соответствуют вершинам дерева; при этом неограниченная часть плоскости отвечает корню.)

Корневые деревья считаются одинаковыми (изоморфными), если между ними существует изоморфизм, при котором корень переходит в корень. Сколько есть различных способов отметить корень в данном дереве? Столько, сколько у данного дерева неподобных (существенно различных) вершин, т. е. вершин, не переводимых друг в друга посредством автоморфизмов дерева как графа. Точное определение числа неподобных вершин — это число орбит в множестве вершин $V(G)$ данного дерева Γ при действии группы автоморфизмов $\text{Aut}(\Gamma)$.

Пусть t_n — число неизоморфных деревьев с n вершинами, а T_n — число неизоморфных корневых деревьев с n вершинами. Значения t_n и T_n для малых n приведены в нижеследующей таблице:

| | | | | | | | |
|-------|---|---|---|---|---|----|----|
| n | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| t_n | 1 | 1 | 1 | 2 | 3 | 6 | 11 |
| T_n | 1 | 1 | 2 | 4 | 9 | 20 | 48 |

Глядя на эту таблицу, трудно угадать какую-либо закономерность, управляющую поведением чисел t_n и T_n . Чтобы найти такую закономерность, оказывается чрезвычайно полезным изучать числа t_n и T_n не по отдельности, а объединенными в формальные степенные ряды («производящие функции»)

$$t(x) = \sum_{n=1}^{\infty} t_n x^n = x + x^2 + x^3 + 2x^4 + \dots$$

$$T(x) = \sum_{n=1}^{\infty} T_n x^n = x + x^2 + 2x^3 + 4x^4 + \dots$$

В терминах производящих функций рекуррентные соотношения между коэффициентами T_n и t_n допускают следующую компактную запись.

ТЕОРЕМА 1. $T(x) = x \exp \sum_{k=1}^{\infty} \frac{T(x^k)}{k}$.

ТЕОРЕМА 2. $t(x) = T(x) - \frac{1}{2}(T(x)^2 - T(x^2))$.

ЗАДАЧА 4. Считая известным лишь начальный отрезок разложения $T(x) = x + x^2 + 2x^3 + \dots$, найдите по теореме 1 значение T_4 , а затем по теореме 2 значения t_i для $i \leq 4$.

Для доказательства теоремы 1 мы воспользуемся теорией перечисления Пойа. Предварительно напомним ее основные положения.

2. ТЕОРИЯ ПЕРЕЧИСЛЕНИЯ ПОЙА

Теория перечисления Пойа имеет целью нахождение числа сложных комбинаторных конфигураций в условиях действия группы подстановок. Она развивается в следующих предпосылках.

Имеется некоторое конечное множество M , элементы которого называются «позициями». На множестве позиций задано действие конечной группы G .

Позиции можно заполнять «фигурами», т. е. элементами некоторого, возможно бесконечного, множества Φ . Каждой фигуре из множества Φ приписан некоторый «вес», являющийся неотрицательным целым числом, и для каждого $n \geq 0$ известно число F_n фигур веса n . Производящая функция $F(x) = \sum_{n=0}^{\infty} F_n x^n$ называется «ряд, перечисляющий фигуры по их весам».

В некоторых ситуациях вместо позиций удобнее говорить об «объектах», а вместо фигур — о свойствах этих объектов.

Конфигурацией называется расстановка фигур по позициям, т. е. отображение $f: M \rightarrow \Phi$. *Вес* конфигурации — это сумма весов всех расставленных фигур:

$$w(f) = \sum_{\mu \in M} w(f(\mu)),$$

где через w обозначена функция веса.

Действие группы G на множестве M естественным образом порождает ее действие на множестве конфигураций (фигуры, расставленные по позициям, переставляются вместе с позициями). Конфигурации, эквивалентные относительно действия группы G , имеют равные веса. Пусть K_n — число конфигураций веса n , различных с точки зрения действия группы G , т. е. число G -орбит в множестве конфигураций, имеющих вес n .

Теория перечисления Пойа объясняет, как найти числа K_n , зная числа F_n .

Оказывается, что эту связь удобнее всего сформулировать в виде соотношения между производящими функциями $F(x)$ и $K(x)$, используя специальный многочлен Z_G от нескольких переменных, который определяется группой G и ее действием на множестве M и называется *цикловой индекс* группы G .

По определению,

$$Z_G(y_1, y_2, \dots, y_m) = \frac{1}{|G|} \sum_{g \in G} y_1^{b_1(g)} y_2^{b_2(g)} \dots y_m^{b_m(g)},$$

где $b_i(g)$ — число циклов длины i , входящих в разложение подстановки множества M , которое отвечает элементу группы g . (Таким образом,

каждый моном $y_1^{b_1(g)} y_2^{b_2(g)} \dots y_m^{b_m(g)}$ войдет в сумму с коэффициентом, равным числу элементов группы G , действие которых на множестве M имеет одно и то же разложение на циклы.) Число переменных, от которых зависит многочлен Z_G , определяется наибольшей длиной цикла среди встречающихся при рассматриваемом действии группы; во всяком случае, оно не превосходит числа элементов множества M .

Ну вот, мы дали все определения, необходимые для того, чтобы выписать, наконец, основную формулу теории перечисления Пойа. После таких титанических усилий формула выглядит очень коротко и просто (трудно в ученье — легко в бою, говорил Суворов).

ТЕОРЕМА 3 (ФОРМУЛА ПЕРЕЧИСЛЕНИЯ ПОЙА).

$$K(x) = Z_G(F(x), F(x^2), \dots, F(x^m)).$$

Или словами: перечисляющий ряд для конфигураций получается при подстановке перечисляющего ряда для фигур в цикловой индекс группы.

Обратите внимание на способ подстановки функции $F(x)$ в многочлен Z_G : каждая переменная y_k заменяется на выражение $F(x^k)$ (не путать с $F(x)^k$!).

Стандартным примером конфигурации является ожерелье из n бусинок двух цветов, скажем белых и красных, рассматриваемое с точностью до самосовмещений в пространстве. В этом случае множество фигур состоит из двух элементов (красная и белая бусинка), которым можно приписать веса 0 и 1 соответственно. Многочлен, перечисляющий фигуры, имеет вид $1 + x$. Множество позиций представляет собой набор вершин правильного n -угольника, на котором действует группа всех его движений D_n .

ЗАДАЧА 5. Чтобы набить руку, напишите многочлен, перечисляющий двуцветные ожерелья из 4 и 5 бусинок. Ответ проверьте при помощи здравого смысла.

Другой, особенно важный для химиков пример возникает в следующей ситуации. Множество позиций есть некоторое множество точек в пространстве, образующее пространственную форму молекулы (например, вершины некоторого многогранника M). G — группа вращений этого многогранника. Фигуры — это атомы или группы атомов, которые имеют одинаковую валентность и могут располагаться в вершинах многогранника M . В этом случае конфигурации — это изомеры замещения данного состава.

Единственная трудность, которая возникает в этой химической ситуации, заключается в том, что для полного перечисления молекул по количеству входящих в них атомов разного вида необходимо, вообще

говоря, вводить векторные веса и производящие функции многих переменных. Например, если изучаются молекулы, состоящие из атомов трех типов, то перечисляющий многочлен для фигур будет $x + y + z$, а коэффициент при мономе $x^p y^q z^r$ в перечисляющем ряде для конфигураций есть число конфигураций, состоящих из p атомов первого типа, q атомов второго типа и r атомов третьего типа.

Задача 6. Напишите многочлен, который перечисляет изомеры, имеющие форму октаэдра и состоящие из шести четырехвалентных атомов типа A , B и C .

3. ДОКАЗАТЕЛЬСТВА

Для доказательства теоремы 1 заметим, что при отбрасывании корня корневое дерево с $n+1$ вершиной распадается на несколько корневых деревьев с суммарным числом вершин n . Эти части однозначно, с точностью до перестановки, определены данным деревом. Обратно, из нескольких корневых деревьев всегда можно составить новое большое корневое дерево. При этом дерево с 1 вершиной получается, если составить вместе 0 деревьев.

Постараемся переформулировать это простое наблюдение как некоторое свойство производящей функции $T(x)$, используя теорию перечисления Пойа.

В качестве множества фигур у нас будет выступать множество всех корневых деревьев. Весом дерева мы будем считать число вершин в нем. Тогда перечисляющий ряд для фигур есть в точности производящая функция для числа корневых деревьев $T(x)$.

Рассмотрим составление нового корневого дерева со степенью корня r как образование конфигурации из r фигур. Множество позиций есть множество ребер, выходящих из корня большого дерева. Это множество состоит из r элементов, и на нем действует полная группа подстановок S_r . Вес дерева, составленного из компонент, рассматриваемого как конфигурация, есть по определению сумма весов составляющих его фигур, т. е. на 1 меньше числа вершин в нем. Таким образом, перечисляющий ряд для конфигураций по весам есть $\sum_{n=0}^{\infty} T_{n+1}^{(r)} x^n$, где $T_{n+1}^{(r)}$ есть число корневых деревьев с данной степенью корня r . По формуле Пойа

$$\sum_{n=0}^{\infty} T_{n+1}^{(r)} x^n = \frac{1}{r!} Z_{S_r}(T(x), T(x^2), \dots).$$

Чтобы получить соотношение для числа всех корневых деревьев, надо просуммировать полученное равенство по всем r от 0 до бесконечности. (Значению 0 отвечает, как мы уже говорили, дерево с 1 вершиной; при этом

группа S_0 есть единичная группа, действующая на пустом множестве, а ее цикловой индекс есть константа 1 — в отличие от группы S_1 , которая тоже единичная, но действует на одноэлементном множестве и имеет цикловой индекс, равный y_1 .)

Суммирование дает:

$$\sum_{n=0}^{\infty} T_{n+1}x^n = \sum_{r=0}^{\infty} \frac{1}{r!} Z_{S_r}(T(x), T(x^2), \dots).$$

Для суммы цикловых индексов всех симметрических групп существует формула, которая доказывается сравнением коэффициентов при одинаковых мономах в левой и правой части равенства.

ЗАДАЧА 7. Докажите формулу

$$\sum_{r=0}^{\infty} \frac{1}{r!} Z_{S_r}(y_1, y_2, \dots) = \exp \sum_{k=1}^{\infty} \frac{y_k}{k}.$$

Теорема 1 непосредственно вытекает из утверждения задачи 7 и предыдущего соотношения.

СЛЕДСТВИЕ 1. *Имеет место следующая рекуррентная формула для числа корневых деревьев:*

$$T_n = \frac{1}{n-1} \sum_{m=1}^n \left(\sum_{p|m} p T_p \right) T_{n-m}.$$

(*Внутренняя сумма распространяется на все делители p числа m .*)

ДОКАЗАТЕЛЬСТВО СЛЕДСТВИЯ. Ряд $T(x)$ можно продифференцировать почленно:

$$T'(x) = \sum_{n=1}^{\infty} n T_n x^{n-1} = \sum_{n=0}^{\infty} (n+1) T_{n+1} x^n$$

Теперь возьмем производную от обеих частей уже доказанного равенства

$$T(x) = x \exp \sum_{k=1}^{\infty} \frac{T(x^k)}{k},$$

заменяя там, где надо, выражение $\exp \sum_{k=1}^{\infty} \frac{T(x^k)}{k}$ на $T(x)/x$. Получим:

$$xT'(x) - T(x) = T(x) \sum_{k=1}^{\infty} x^k T'(x^k).$$

Подставив сюда найденное выше выражение для T' , находим:

$$\sum_{n=1}^{\infty} (n-1)T_n x^n = \sum_{q=1}^{\infty} T_q x^q \cdot \sum_{k=1}^{\infty} x^k \left(\sum_{p=1}^{\infty} pT_p x^{(p-1)k} \right).$$

Меня здесь порядок суммирования, можно переписать это соотношение как

$$\sum_{n=1}^{\infty} (n-1)T_n x^n = \sum_{k,p,q} pT_p T_q x^{q+kp} = \sum_{n=1}^{\infty} \sum_{q+kp=n} pT_p T_q x^n.$$

(Последний знак суммы означает, для данного n , суммирование по всем тройкам целых чисел k, p, q , удовлетворяющим соотношению $q + kp = n$.) Наконец, приравняем коэффициенты при x^n в левой и правой части последнего равенства:

$$(n-1)T_n = \sum_{q+kp=n} pT_p T_q = \sum_{m=1}^n \left(\sum_{p|m} pT_p \right) T_{n-m},$$

где новый индекс суммирования m соответствует старому kp . Следствие доказано.

ЗАДАЧА 8. Запрограммируйте полученную формулу на компьютере и найдите числа T_n для $n \leq 15$.

ЗАДАЧА 9. Попробуйте найти прямое комбинаторное доказательство этой формулы, т. е. смысл разбиения числа $(n-1)T_n$ на слагаемые, указанные в правой части формулы.

ЗАДАЧА 10. При помощи тождественных преобразований со степенными рядами покажите, что теорема 1 эквивалентна следующей формуле А. Кэли:

$$T(x) = x \prod_{n=1}^{\infty} (1 - x^n)^{-T_n}.$$

Перейдем к доказательству теоремы 2, которая устанавливает связь между числом деревьев и корневым деревьям. Доказательство, которое будет дано, использует понятие *симметричного ребра* графа и понятие *реберно-корневого дерева*, и мы вначале их объясним.

Ребро e некоторого графа Γ называется симметричным, если существует автоморфизм графа, меняющий местами концевые вершины e .

ЗАДАЧА 11. Докажите, что дерево не может иметь более одного симметричного ребра.

Таким образом, все деревья делятся на два типа: имеющие одно симметричное ребро и не имеющие ни одного симметричного ребра. (Укажите примеры тех и других).

Оказывается, такое разделение играет важную роль в подсчете числа существенно различных (неподобных) вершин и ребер дерева. (В п. 1 мы говорили, что связь между числом деревьев и корневым деревьям осуществляется путем подсчета числа неподобных вершин.)

А именно, имеет место следующая лемма.

ЛЕММА (ТЕОРЕМА О ХАРАКТЕРИСТИКЕ НЕПОДОБИЯ ДЛЯ ДЕРЕВЬЕВ). Пусть p — число неподобных вершин, а q — число неподобных ребер некоторого дерева. Эти числа связаны между собой так:

$p = q$, если дерево обладает симметричным ребром,

$p = q + 1$, если дерево не обладает симметричным ребром.

ДОКАЗАТЕЛЬСТВО. По формуле Бернсайда для числа орбит при действии группы автоморфизмов графа $A = \text{Aut}(\Gamma)$ на множестве вершин:

$$p = \frac{1}{|A|} \sum_{\alpha \in A} v(\alpha),$$

где $v(\alpha)$ — число вершин, неподвижных под действием автоморфизма α .

Аналогично, для действия A на множестве ребер:

$$q = \frac{1}{|A|} \sum_{\alpha \in A} e(\alpha),$$

где $e(\alpha)$ — число ребер, неподвижных под действием α .

Утверждение леммы вытекает из следующих наблюдений.

(i) Если дерево не обладает симметричным ребром, то ребро может остаться на месте под действием автоморфизма, только если оба его конца остаются на месте. Следовательно, число ребер, которые сдвигаются, равно числу вершин, которые сдвигаются. А поскольку общее число вершин на 1 больше, мы получаем $v(\alpha) = e(\alpha) + 1$ для любого α .

(ii) Если дерево имеет симметричное ребро, то группа автоморфизмов распадается на две равные части: автоморфизмы, сохраняющие оба конца симметричного ребра, и автоморфизмы, переставляющие эти концы. Для автоморфизмов первого типа будет $v(\alpha) = e(\alpha) + 1$, а для автоморфизмов второго типа, наоборот, $v(\alpha) = e(\alpha) - 1$ (на самом деле, как нетрудно проверить, в этом случае $v(\alpha) = 0$, $e(\alpha) = 1$). Следовательно, суммы в обеих формулах Бернсайда совпадут.

Лемма доказана.

УПРАЖНЕНИЕ. Проверьте утверждение леммы для деревьев, изображенных на рисунке 1.

Чтобы вывести теорему 2 из доказанной леммы, перепишем ее утверждение в виде тождества

$$1 = p - (q - s),$$

где, как и выше, p и q обозначают, соответственно, число неподобных вершин и ребер некоторого дерева, а s есть число симметричных ребер в этом дереве.

Теперь просуммируем обе части этого тождества по всем деревьям с данным числом вершин n . Что мы при этом получим? В левой части равенства получится, очевидно, просто число всех деревьев с n вершинами t_n . Первое слагаемое правой части даст в точности число всех корневых деревьев T_n .

А каков гносеологический смысл суммы чисел $q - s$, т. е. чисел *несимметричных* ребер, по всем деревьям с данным числом вершин? Чтобы его установить, нам как раз и потребуется заявленное раньше понятие реберно-корневого дерева. По аналогии с обычными корневыми (или вершинно-корневыми) деревьями, *реберно-корневое* дерево — это дерево, в котором отмечено одно ребро, называемое, естественно, корневым ребром. (Проверьте для разминки, что число реберно-корневых деревьев с 4 вершинами равно 3, что коренным образом отличается от числа вершинно-корневых деревьев с 4 вершинами.)

Теперь мы готовы к тому, чтобы объяснить смысл суммы $\sum(q - s)$, которая нас так заинтриговала. Это число L_n реберно-корневых деревьев с n вершинами, у которых запрещается брать в качестве корня симметричное ребро. Давайте их перечислим. Для этого подумаем: к чему приводит удаление корневого ребра? Правильно, к распадению дерева на две (ровно на две!) части с таким же общим числом вершин. Эти части, как нетрудно понять, естественным образом снабжены структурой корневого (именно вершинно-корневого!) дерева. Если при этом не трогать симметричных ребер (не брать их в качестве корней — согласно уговору, который дороже денег), то мы получим такое выражение числа L_n через числа T_k :

$$L_n = \sum_{\substack{k+l=n \\ k < l}} T_k T_l,$$

(суммирование только по парам неравных чисел!). Тот же факт можно выразить на языке производящих функций, для чего достаточно рассмотреть произведение ряда $T(x)$ сам на себя в количестве (только!) двух экземпляров. Немного поразмыслив, вы поймете, что формула

$$L(x) = \frac{1}{2}(T(x)^2 - T(x^2))$$

как раз и выражает необходимое соотношение (вычитание $T(x^2)$ — это запрет на одинаковые индексы k и l , т. е. запрет на симметричные корни; двойка в знаменателе — дань тому факту, что перестановка частей при составлении реберно-корневого дерева не меняет результат этого действия).

ЗАДАЧА 12. Используя доказанную теорему и результат задачи 8, найдите значения t_n для $n \leq 15$.

СПИСОК ЛИТЕРАТУРЫ

- [1] A. Cayley. *Mathematical Papers*. Cambridge, 1891–1897: v.3, 242–246 (On the theory of the analytical forms called trees), v.9, 202–204 (On the math. theory of isomers), v.11, 365–367 (On the analytical forms called trees), v.13, 26–28 (A theorem on trees).
- [2] G. Pólya. *Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen* // Acta Math. B. 68, 1937. S. 145–254.
- [3] Ф. Харари, Э. Палмер. Перечисление графов. М.: Мир, 1977.
- [4] В. В. Белов, Е. М. Воробьев, В. Е. Шаталов. Теория графов. М., Высшая школа, 1976.

Случайные блуждания и электрические цепи

М. Скопенков*

В. Смыкалов

А. Устинов*

1. ОСНОВНЫЕ ПОНЯТИЯ

В данной статье мы докажем следующую знаменитую теорему.

ТЕОРЕМА ПОЙА. (А) *Если человек случайным образом перемещается по 2-мерной решетке, то он вернется в начальную точку с вероятностью 1.*

(В) *Если же он перемещается по 3-мерной решетке, то вероятность его возврата в начальную точку строго меньше 1.*

Предлагаемый подход к доказательству основан на физической интерпретации, использующей электрические цепи. Наше изложение следует книге [7], с небольшими упрощениями. Для понимания статьи специальных знаний не требуется, все необходимые определения будут даны.

1.1. ВЕРОЯТНОСТНЫЕ ОПРЕДЕЛЕНИЯ

Для начала введем некоторые обозначения и заодно дадим определения необходимых понятий теории вероятности.

Предположим, что у некоторого эксперимента имеется n равновероятных исходов, и событие X происходит ровно в m из них. Тогда вероятностью события X называется число $P_1(X) := m/n$.

Например, вероятность выпадения орла при бросании монеты — $1/2$; вероятность выпадения 6 очков на кубике — $1/6$.

Теперь предположим, что событие X зависит от последовательности нескольких независимых таких экспериментов. Последовательность из T экспериментов имеет n^T возможных исходов. Предположим, что событие X происходит ровно при m_T исходов из них. Тогда вероятностью события X называется число $P_T(X) := m_T/n^T$.

Например, есть ровно 4 возможных исхода при бросании монеты 2 раза:

1-й бросок

| |
|------|
| орел |
|------|

| |
|------|
| орел |
|------|

| |
|-------|
| решка |
|-------|

| |
|-------|
| решка |
|-------|

2-й бросок

| |
|------|
| орел |
| орел |

| |
|-------|
| решка |
| орел |

| |
|-------|
| решка |
| орел |

| |
|-------|
| решка |
| решка |

*Частично поддержаны фондом «Династия».

Пусть событие X состоит в появлении решки хотя бы один раз. Событие X происходит в 3 случаях из 4 возможных. Поэтому вероятность события X есть $P_2(X) = 3/4$.

Вероятность получения более 10 очков при бросании двух кубиков — $1/12$, так как это событие происходит в ровно 3 случаях ($5 + 6$, $6 + 5$ или $6 + 6$) из 36 возможных.

Наконец, пусть событие X зависит от бесконечной последовательности таких экспериментов. Мы будем называть число $P(X)$ *вероятностью* события X , если вероятности $P_T(X)$ стремятся к числу $P(X)$ при стремлении T к бесконечности¹⁾.

Например, вероятность выпадения решки хотя бы один раз в бесконечной серии бросков составляет $P(X) = 1$, так как $P_T(X) = 1 - 1/2^T$ стремится к 1 при стремлении T к бесконечности.

Мы готовы объяснить формулировку теоремы Пойа. Двумерная решетка — это бесконечная клетчатая плоскость, причем человек движется по сторонам клеток. Каждый раз, оказываясь на «перекрестке», он выбирает одно из четырех направлений дальнейшего движения с равной вероятностью, независимо от своих предыдущих выборов. Теорема Пойа утверждает, что вероятность когда-нибудь вернуться в начальную точку равна $P(X) = 1$.

Рассмотрим «игрушечный» пример, на котором мы увидим многие важные идеи доказательства теоремы Пойа.

ПРИМЕР 1. Пьяница ходит по отрезку улицы, состоящему из 5 кварталов. Начав свой путь на границе кварталов в точке x , он с вероятностью $1/2$ перемещается на один квартал влево и с вероятностью $1/2$ — на один квартал вправо. Подойдя к границе кварталов, он опять выбирает направление движения случайным образом. Если он оказывается в точке 5 (его дом) или в точке 0 (бар), то он прекращает движение: см. рисунок 1.

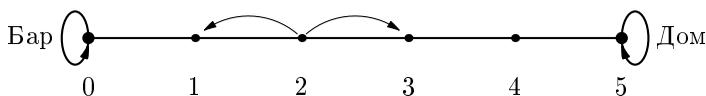


Рис. 1. Случайное движение по улице; см. пример 1

ЗАДАЧА 1. Напишите компьютерную программу, моделирующую движение этого пьяницы. Запустите ее много раз и определите процент числа случаев, в которых он приходит домой. Вы можете использовать этот способ для угадывания ответов в последующих задачах.

¹⁾Формально это означает, что для каждого $\varepsilon > 0$ существует число T_0 такое, что для каждого $T > T_0$ выполнено $|P(X) - P_T(X)| < \varepsilon$.

Задача 2. Пусть $P_T(x)$ — вероятность того, что пьяница, начавший свое движение в точке x и сделавший не более T ходов, оказался дома. Заполните таблицу 1 десятичными дробями с точностью до сотых.

Табл. 1. Вероятности $P_T(x)$ для малых T

| T | x | 0 | 1 | 2 | 3 | 4 | 5 |
|-----|-----|------|------|------|------|------|------|
| 1 | | 0.00 | 0.00 | 0.00 | 0.00 | 0.50 | 1.00 |
| 2 | | | | | | | |
| 3 | | | | | | | |
| 4 | | | | | | | |

Найдем вероятность $P(x)$ того, что пьяница когда-нибудь дойдет до дома.

Прежде всего отметим, что для каждого x указанная вероятность $P(x)$ существует, поскольку последовательность $P_T(x)$ из задачи 2 возрастает и ограничена сверху числом 1.

Заметим, что из точки $x \neq 0, 5$ первым ходом пьяница попадет в одну из точек $x - 1$ или $x + 1$ с равной вероятностью. Поэтому

$$P_T(x) = \frac{1}{2}P_{T-1}(x-1) + \frac{1}{2}P_{T-1}(x+1).$$

Переходя к пределу при T , стремящемся к бесконечности, получим при каждом $x \neq 0, 5$ равенство

$$P(x) = \frac{1}{2}P(x-1) + \frac{1}{2}P(x+1). \quad (1)$$

Поскольку при достижении точек 0 или 5 перемещения заканчиваются, получаем равенство

$$P(0) = 0 \quad P(5) = 1. \quad (2)$$

Из двух установленных свойств (1) и (2) вытекает, что $P(x)$ представляет собой арифметическую прогрессию: $P(x) = x/5$.

Задача 3. Петя и Паша играют на монетки. Всего у них есть 5 монеток. В каждом раунде Петя выигрывает у Паши одну монетку с вероятностью $1/2$ и проигрывает с вероятностью $1/2$. Они играют до тех пор, пока у Пети не станет 0 монеток (он проиграл) или 5 (он выиграл все монеты Паши). Найдите вероятность $P(x)$ того, что Петя выиграет, начав игру с x монетками.

Задача 4. Предположим, нашего «путешественника» сносит в одну сторону; точнее, пусть он каждый раз перемещается вправо с вероятностью

p и влево с вероятностью $q = 1 - p$. Найдите вероятности $P(x)$ попадания домой в этом случае.

ЗАДАЧА 5. Предположим, что вы играете на деньги. Сначала у вас 20 монет, а у вашего соперника — 50 монет. В каждой игре вы выигрываете одну монету с вероятностью 0.45 и проигрываете с вероятностью 0.55. Игра продолжается до тех пор, пока у кого-либо не закончатся деньги. Найдите вероятность своего разорения с точностью до первой цифры после запятой, отличной от 9.

1.2. ФИЗИЧЕСКИЕ ОПРЕДЕЛЕНИЯ

Для исследования случайного блуждания оказывается полезной физическая интерпретация, использующая электрические цепи. Поскольку мы собираемся применять электрические цепи для доказательства математического результата, то нам понадобится их формальное аксиоматическое определение²⁾.

ОПРЕДЕЛЕНИЕ. *Электрическая цепь* — это связный конечный граф, у которого каждому ребру xy приписано положительное вещественное число, называемое его *проводимостью*³⁾ $C(xy)$, и задано два непересекающихся выделенных множества вершин (P и N). Считается, что вершины из множества N соединены с отрицательным полюсом батарейки и землей, а вершины из множества P — с положительным; см. рисунок 2.

Потенциалы вершин $v(x)$ определяются следующими аксиомами:

1. *Граничное условие.* Если $x \in N$, то $v(x) = 0$. Если $x \in P$, то $v(x) = 1$.
2. *Правило Кирхгофа.* Если $x \notin P \cup N$, то $\sum_{xy} C(xy) (v(x) - v(y)) = 0$, где суммирование ведется по всем ребрам xy , содержащим вершину x .

ЗАМЕЧАНИЕ. Мы допускаем графы с кратными ребрами. Если граф имеет несколько ребер между вершинами x и y , то xy будет обозначать любое из них (путаницы из-за этого не возникнет).

ПРИМЕР 2. Пять одинаковых резисторов соединены последовательно и подключены к батарейке в 1 вольт как показано на рисунке 2.

Найдем потенциалы $v(x)$ в точках $x = 0, 1, 2, 3, 4, 5$. То, что резисторы одинаковы, означает, что все рёбра имеют равные проводимости. Тогда из аксиомы 2 получаем, что $v(x)$ — арифметическая прогрессия. Аксиома 1

²⁾ Есть и другие подходы к аксиоматическому построению теории электрических цепей; см., например, [3].

³⁾ Величина, обратная проводимости, называется *сопротивлением*.

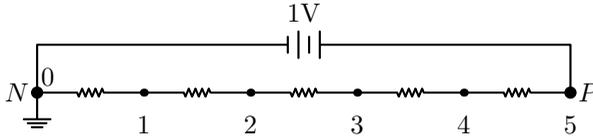


Рис. 2. Электрическая цепь; см. пример 2.

определяет начальный и конечный член этой прогрессии, поэтому $v(x) = x/5$.

Мы видим, что найденное значение совпадает с полученным раньше выражением для вероятности попадания домой, $v(x) = P(x)$. Это проявление общей закономерности, которую мы проиллюстрируем на более сложном примере.

ПРИМЕР 3. Рассмотрим город, схема которого приведена на рисунке 3 слева. Отрезки обозначают улицы. Пути отхода помечены буквой E , а буквой P помечены точки, занятые полицией. Из точки $x = (a, b)$ пьяница перемещается в каждую из точек $(a + 1, b)$, $(a - 1, b)$, $(a, b + 1)$, $(a, b - 1)$ с вероятностью $1/4$. Если он достигает одной из точек E или P , то его передвижения заканчиваются.

Найдем вероятность $P(x)$ того, что начав свой путь в точке x , пьяница не попадет в руки полиции.

Рассмотрим электрическую цепь на рисунке 3 справа, состоящую из единичных резисторов. Так же, как и в примере 1, мы видим, что функция $P(x)$ удовлетворяет аксиомам 1–2 из определения электрической цепи.

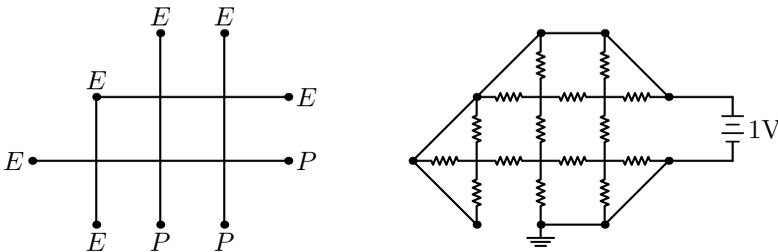


Рис. 3. Случайное движение по городу и электрическая цепь; см. пример 3

Обозначим вероятности $P(x)$ через a , b , c , d , и e ; см. рисунок 4 слева. Тогда аксиомы 1–2 примут вид:

$$\begin{aligned} a &= (b + d + 2)/4; \\ b &= (a + c + 2)/4; \\ c &= (d + 3)/4; \end{aligned}$$

$$d = (a + c + e)/4;$$

$$e = (b + d)/4.$$

Решая эту систему, находим искомые вероятности $P(x)$. На рисунке 4 справа значения вероятностей приведены с точностью до тысячных.

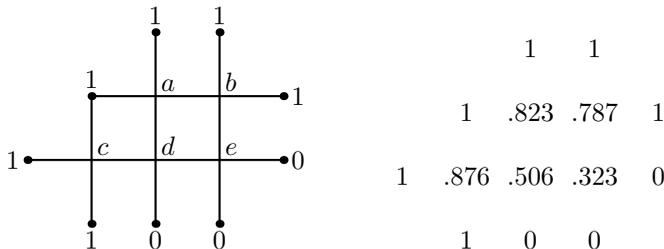


Рис. 4. Вероятности $P(x)$ для примера 3

Итак, для этого примера найденные вероятности опять совпадают с потенциалами в соответствующей электрической цепи. Наша ближайшая цель — доказать, что так будет всегда.

2. ОСНОВНЫЕ ТЕОРЕМЫ ДЛЯ ЭЛЕКТРИЧЕСКИХ ЦЕПЕЙ

2.1. ТЕОРЕМА ЕДИНСТВЕННОСТИ

ОПРЕДЕЛЕНИЕ. Функция $v(x)$ на вершинах электрической цепи называется *гармонической*, если она удовлетворяет аксиоме 2, но не обязательно аксиоме 1. Вершины, принадлежащие одному из множеств N и P называются *граничными*, а остальные — *внутренними*.

Установим несколько важных свойств гармонических функций.

ПРИНЦИП СУПЕРПОЗИЦИИ. Если функции $u(x)$ и $v(x)$ — гармонические, то при любых $a, b \in \mathbb{R}$ функция $au(x) + bv(x)$ — гармоническая.

ДОКАЗАТЕЛЬСТВО. Для любой внутренней вершины x

$$\begin{aligned} \sum_{xy} c(xy) (au(x) + bv(x) - au(y) - bv(y)) &= \\ &= a \sum_{xy} c(xy) (u(x) - u(y)) + b \sum_{xy} c(xy) (v(x) - v(y)) = 0, \end{aligned}$$

где суммирование ведется по всем ребрам xy , выходящим из x . Значит, $au(x) + bv(x)$ — гармоническая функция.

ПРИНЦИП МАКСИМУМА. Гармоническая функция на конечной электрической цепи принимает свое наибольшее и наименьшее значение на граничных вершинах.

ДОКАЗАТЕЛЬСТВО. Пусть $v(x)$ — гармоническая функция, которая принимает наибольшее значение в некоторой вершине x . Докажем, что если x — внутренняя вершина, то в ее соседях наша функция принимает такие же значения. Так как $v(x)$ — наибольшее значение, то для каждой соседней вершины y выполнено неравенство $v(x) - v(y) \geq 0$. Следовательно, $\sum_{xy} c(xy)(v(x) - v(y)) \geq 0$. По аксиоме 2 последнее неравенство обращается в равенство. Значит, $v(y) = v(x)$ для всех y .

Так как электрическая цепь — связный граф, то существует путь, соединяющий вершину x с одной из граничных вершин. По доказанному значения нашей функции во всех вершинах пути одинаковы. Значит, в одной из граничных вершин также принимается наибольшее значение функции $v(x)$, что и требовалось. Доказательство для наименьшего значения аналогично.

ТЕОРЕМА ЕДИНСТВЕННОСТИ. *В конечной электрической цепи не может быть двух различных расстановок потенциалов, удовлетворяющих обоим аксиомам 1–2.*

ДОКАЗАТЕЛЬСТВО. Пусть $u(x)$ и $v(x)$ — две расстановки потенциалов. Рассмотрим гармоническую функцию $u(x) - v(x)$. Она принимает значение 0 на всех граничных вершинах. По принципу максимума она равна 0 и во всех внутренних вершинах. Следовательно, $u(x)$ и $v(x)$ совпадают.

Теперь мы можем доказать закономерность, замеченную в примерах 1 и 3:

ФИЗИЧЕСКАЯ ИНТЕРПРЕТАЦИЯ ВЕРОЯТНОСТИ ДОСТИЖЕНИЯ. *Для любой конечной электрической цепи потенциал $v(x)$ вершины x равен вероятности $P(x)$ того, что случайное блуждание, начавшееся из вершины x , достигнет множества P раньше, чем множества N .*

ДОКАЗАТЕЛЬСТВО. Действительно, вероятность $P(x)$ удовлетворяет обоим аксиомам 1–2. Потенциал $v(x)$ также удовлетворяет этим аксиомам. По теореме единственности $v(x) = P(x)$ при всех x .

2.2. ТЕОРЕМА СУЩЕСТВОВАНИЯ

Естественный вопрос: а как *найти* потенциал $v(x)$ в произвольной электрической цепи? Да и в любой ли электрической цепи потенциал $v(x)$, удовлетворяющий нашим аксиомам, вообще существует?

Ответ на эти вопросы оказывается на удивление трудным. Конечно, потенциалы в вершинах можно найти, решая систему линейных уравнений, как мы делали в примере 3. Но на практике это оказывается слишком трудоемко. Поэтому мы приведем два способа нахождения *приближенного* значения потенциалов с любой точностью. Для каждого способа мы

«заодно» получим доказательство существования потенциала, удовлетворяющего нашим аксиомам.

Возможно, читатель спросит: а зачем вообще доказывать существование потенциала? Соберем настоящую электрическую цепь, какие-то потенциалы у ее вершин ведь *должны быть!* А из физики известно, что они удовлетворяют нашим аксиомам — вот и получается существование потенциала.

Однако это обоснование не выдерживает критики даже с точки зрения физики. Пусть мы собрали электрическую цепь. В первый момент, когда мы только ее замкнули, потенциалы еще не удовлетворяют нашим аксиомам. Эти аксиомы описывают *установившееся* потенциалы, которые появляются в цепи через большой отрезок времени. Но где гарантия, что с течением времени потенциалы будут стремиться к каким-то конечным значениям? Эта проблема возникает на практике: если цепь состоит из сверхпроводников (то есть ребер с нулевым сопротивлением), то никакого установившегося состояния нет: ток в цепи будет расти, пока проводник не выйдет из сверхпроводящего состояния. Для существования потенциала принципиально важна положительность сопротивлений.

Перейдем к обещанным способам нахождения потенциала.

Первый способ использует случайные блуждания. Он называется *методом Монте-Карло*, так как случайные блуждания связаны с вероятностями, а в Монте-Карло находятся известные игорные дома, азартные игры в которых тоже связаны с вероятностями. Мы моделируем много случайных блужданий из точки x и находим долю путей, закончившихся в точках множества P . Полученная оценка будет приближением для «настоящей» вероятности $P(x)$. Этот яркий и простой метод позволяет найти потенциал $v(x) = P(x)$, хотя он и не очень эффективен. Эта идея также позволяет доказать существование потенциала:

ТЕОРЕМА СУЩЕСТВОВАНИЯ. *В любой конечной электрической цепи существует расстановка потенциалов, удовлетворяющая аксиомам 1–2.*

ПЕРВОЕ ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ СУЩЕСТВОВАНИЯ. Рассмотрим случайное блуждание по электрической цепи. Пусть $P_T(x)$ — вероятность того, что, стартуя из вершины x и делая T шагов, мы достигнем положительного полюса батарейки раньше, чем отрицательного. Ясно, что при фиксированном x последовательность $P_T(x)$ возрастает и ограничена, значит, имеет предел $P(x)$. Функция $P(x)$ удовлетворяет аксиомам 1–2.

Теперь сделаем некоторое отступление: опишем более эффективный на практике *метод релаксаций* (для доказательства теоремы Пойа эти результаты не понадобятся). Напомним, что мы ищем функцию с заданными значениями на границе, у которой значение в любой внутренней вершине

равно взвешенному среднему арифметическому значений в соседних вершинах. Начнем с функции, которая равна 1 в вершинах множества P , и 0 — во всех остальных вершинах. Она имеет нужные нам граничные значения. Возьмем какую-нибудь внутреннюю точку. Значение функции в ней не будет, вообще говоря, равно среднему арифметическому значений в соседних точках. Тогда попробуем «подогнать»: положим новое значение функции в этой точке равным среднему арифметическому значений в соседних точках. Теперь будем по очереди брать остальные внутренние точки и делать с ними ту же операцию. Когда мы пройдем по всем внутренним точкам, функция не будет удовлетворять аксиоме 2, так как после изменения значения функции в одной точке мы могли изменить значения в соседних с ней точках, нарушив равенство. Тем не менее, полученная функция будет «лучше» удовлетворять аксиоме 2, чем та функция, с которой мы начали. Повторяя этот процесс (проходя каждый раз по всем внутренним точкам) мы будем получать приближения к решению лучше и лучше.

СХОДИМОСТЬ МЕТОДА РЕЛАКСАЦИИ. В каком бы порядке мы не проходили по внутренним вершинам (так, чтобы в каждой из них оказаться сколь угодно много раз), получаемые нами функции стремятся к функции, удовлетворяющей аксиомам 1–2. В частности, функция, удовлетворяющая аксиомам 1–2, существует.

ДОКАЗАТЕЛЬСТВО (И ЗАОДНО ВТОРОЕ ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ СУЩЕСТВОВАНИЯ). Разобьем доказательство на несколько шагов.

ЛЕММА 1. Значение функции в каждой вершине (за исключением вершин множества P) на каждом шаге процесса не превосходит взвешенного среднего арифметического соседей.

ДОКАЗАТЕЛЬСТВО. Индукция по номеру шага. Изначально это условие выполняется. В тот момент, когда мы делаем очередной шаг, значение в соответствующей вершине не уменьшается (по предположению индукции). Значит, взвешенное среднее у соседей этой вершины тоже не уменьшается. Поскольку ни на какие другие вершины это не влияет, индукционный переход доказан. Заодно мы доказали, что последовательность значений в каждой вершине не убывает. \square

ЛЕММА 2. Значения функции неотрицательны и не превосходят 1.

ДОКАЗАТЕЛЬСТВО. Пусть это не так. Рассмотрим первый шаг, когда появилось значение, большее единицы. Получим, что число, большее 1, равняется взвешенному среднему чисел, не больших 1, — противоречие. Аналогично получаем, что все значения неотрицательны. \square

ЛЕММА 3. В каждой вершине x последовательность получаемых значений функции имеет некоторый предел $u(x)$.

ДОКАЗАТЕЛЬСТВО. Действительно, по леммам 1 и 2, эта последовательность не убывает и ограничена сверху числом 1. \square

ЛЕММА 4. Полученная в пределе функция $u(x)$ удовлетворяет аксиомам 1–2.

ДОКАЗАТЕЛЬСТВО. Функция $u(x)$, полученная в пределе, удовлетворяет аксиоме 1, потому что функции на каждом шаге удовлетворяют этой аксиоме. Проверим аксиому 2. Возьмем произвольное $\varepsilon > 0$. По лемме 3, начиная с некоторого шага n нашего процесса, значение очередной функции в каждой вершине x будет отличаться от $u(x)$ не более, чем на ε . Возьмем произвольную внутреннюю вершину x . Рассмотрим первый момент после n -го шага, когда обновляется значение функции в вершине x .

Пусть значения функции сразу после обновления равны $u(x) - \varepsilon(x)$, где $0 \leq \varepsilon(x) \leq \varepsilon$. Поскольку после обновления значение в вершине x равно взвешенному среднему значений в соседних вершинах, то

$$\sum_{xy} c(xy)(u(x) - \varepsilon(x) - u(y) + \varepsilon(y)) = 0.$$

Переносим слагаемые, содержащие функцию $\varepsilon(x)$, в правую часть, получаем

$$\sum_{xy} c(xy)(u(x) - u(y)) = \sum_{xy} c(xy)(\varepsilon(y) - \varepsilon(x)).$$

Поскольку $0 \leq \varepsilon(x) \leq \varepsilon$, то

$$\left| \sum_{xy} c(xy)(u(x) - u(y)) \right| \leq \varepsilon \sum_{xy} c(xy).$$

Но число ε можно выбрать сколь угодно малым, значит

$$\sum_{xy} c(xy)(u(x) - u(y)) = 0.$$

Аксиома 2 выполнена. \square

Итак, мы показали, что получаемые нами функции стремятся к функции, удовлетворяющей аксиомам 1–2. Сходимость метода релаксации доказана.

ЗАДАЧА 6* (АЛЬТЕРНАТИВА ФРЕДГОЛЬМА). Пусть имеется система линейных уравнений

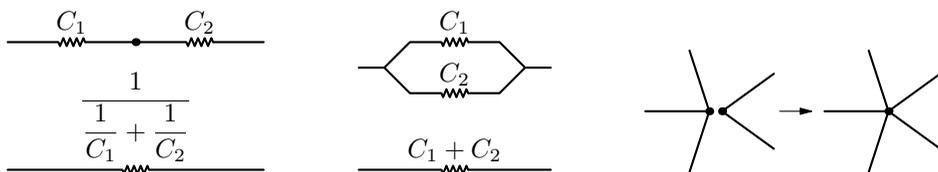


Рис. 5. Последовательное, параллельное соединение и объединение вершин цепи; см. теорему об электрических преобразованиях

ДОКАЗАТЕЛЬСТВО. (А) Докажем, что при нашем преобразовании потенциалы вершин не меняются (за исключением общей вершины для двух рассматриваемых резисторов, которая исчезает). Действительно, пусть вершины 1, 2, 3 с потенциалами v_1, v_2, v_3 соединены двумя последовательными резисторами проводимости C_1 и C_2 . Заменим C_1 и C_2 на один резистор проводимости $\frac{C_1 C_2}{C_1 + C_2}$ между 1 и 3. Умышленно оставим в каждой вершине прежнее значение потенциала.

Проверим аксиомы 1–2 для выбранных нами значений. Ясно, что аксиома 1 по-прежнему выполнена. Также ясно, что аксиома 2 для каждой из вершин, кроме 1 и 3, тоже выполнена, поскольку наше преобразование их не затрагивает. Найдем токи, втекающие в вершину 3. В исходной цепи ток из 2 в 3 равен $C_2(v_2 - v_3)$. В новой цепи ток из 1 в 3 равен $\frac{C_1 C_2}{C_1 + C_2}(v_1 - v_3)$. Но по аксиоме 2 для вершины 2 исходной цепи получаем $C_1(v_1 - v_2) = C_2(v_2 - v_3)$, откуда $C_1(v_1 - v_3) = (C_1 + C_2)(v_2 - v_3)$, значит, $\frac{C_1 C_2}{C_1 + C_2}(v_1 - v_3) = C_2(v_2 - v_3)$. Мы видим, что токи, втекающие в вершину 3, не изменились. Значит, аксиома 2 для вершины 3 по-прежнему выполнена. Аналогично для вершины 1.

Итак, выбранные нами умышленно значения потенциала удовлетворяют аксиомам 1–2 после преобразования. По теореме единственности это и есть потенциал в новой цепи. Раз потенциалы вершин не изменились, то не изменились ни токи через ребра, ни проводимость цепи.

(В) Аналогично предыдущему пункту, докажем, что если в вершинах новой электрической цепи сохранить старые значения потенциала, то аксиомы 1–2 останутся выполнены. Пусть вершины 1, 2 с потенциалами v_1, v_2 соединены параллельными резисторами проводимости C_1 и C_2 . До преобразования ток из вершины 1 в вершину 2 равен $C_1(v_2 - v_1) + C_2(v_2 - v_1)$. Это равняется $(C_1 + C_2)(v_2 - v_1)$, току между вершинами 1 и 2 в после преобразования, при сохранении прежних значений потенциалов. Значит, аксиомы 1–2 останутся выполнены, и проводимость цепи не изменится.

(С) Пусть потенциалы вершин 1 и 2 равны. Объединим эти две вершины, не меняя потенциала.

Очевидно, аксиома 1 по-прежнему выполняется. Для новой вершины, полученной объединением вершин 1 и 2, аксиома 2 выполняется, так как получается сложением аксиом 2 для вершин 1 и 2 исходной цепи. Остальные вершины наше преобразование не затрагивает, поэтому для них аксиома 2 также остается справедливой. Поскольку потенциалы вершин не изменились, то не изменились ни токи через рёбра, ни проводимость цепи.

Выясним теперь вероятностный смысл проводимости:

ФИЗИЧЕСКАЯ ИНТЕРПРЕТАЦИЯ ВЕРОЯТНОСТИ ВОЗВРАТА. Пусть в электрической цепи множество N состоит из одной вершины (которую мы также обозначим через N), а проводимости всех ребер равны 1. Тогда вероятность того, что случайное блуждание по этой цепи, стартующее из вершины N , достигнет множества P раньше первого возврата в вершину N , равна

$$C / \deg N,$$

где C — проводимость цепи между N и P , а $\deg N$ — число ребер, выходящих из вершины N .

ДОКАЗАТЕЛЬСТВО. Пусть рёбра из вершины N ведут в вершины с номерами $1, 2, \dots, k = \deg N$. Обозначим через v_1, v_2, \dots, v_k их потенциалы. Согласно физической интерпретации вероятности достижения, потенциал v_i равен вероятности достижения множества P из вершины i раньше первого возврата в N .

Вероятности сделать первый шаг в любую из вершин $1, 2, \dots, k$ одинаковы и равны $\frac{1}{k}$. Значит, вероятность достижения множества P , стартуя из N , до первого возврата в N равна

$$\frac{1}{k}v_1 + \frac{1}{k}v_2 + \dots + \frac{1}{k}v_k = \frac{-i(N)}{k} = \frac{C}{k} = \frac{C}{\deg N}.$$

ЗАДАЧА 7. Паук перемещается случайным образом по ребрам

(А) куба; (В) октаэдра; (С) додекаэдра; (D) икосаэдра.

Если он начинает движение в точке a , то какова вероятность того, что он достигнет противоположной вершины b быстрее, чем вернется в начальную вершину a ; см. рисунок 6 слева?

ЗАДАЧА 8. Найдите эффективную проводимость между противоположными вершинами

(А) куба; (В) октаэдра; (С) додекаэдра; (D) икосаэдра

с ребрами единичной проводимости; см. рисунок 6 справа.

ЗАДАЧА 9. Пьяный турист выходит из отеля H и перемещается случайным образом по улицам Парижа, схема центра которого приведена на

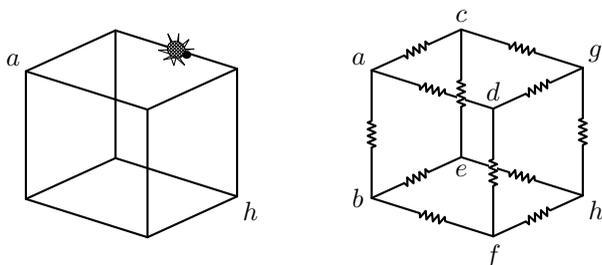


Рис. 6. Случайное блуждание по кубу и электрическая цепь; см. задачи 7(A) и 8(A)

рисунке 7. Найдите вероятность того, что он дойдет до Триумфальной арки T до того, как доберется до окраины города.

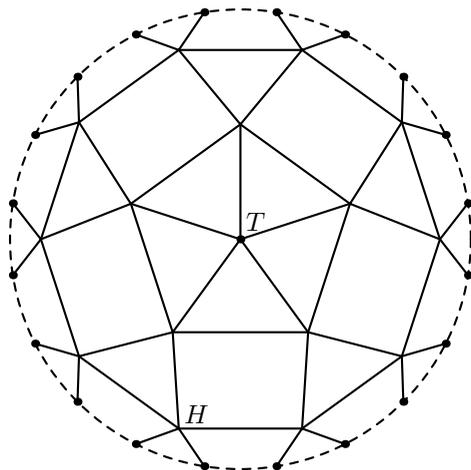


Рис. 7. Туристическая карта Парижа; см. задачу 9

2.4. Принцип монотонности и тепловая мощность

Видно, что понятие проводимости цепи очень близко к вероятности возврата, о которой идет речь в теореме Пойа. Нам потребуется следующее свойство проводимости, которое кажется вполне естественным, но которое при этом довольно трудно доказать.

ПРИНЦИП МОНОТОННОСТИ. Если в цепи проводимость одного из ребер увеличить, то ее эффективная проводимость не уменьшится.

Доказательство использует понятие тепловой мощности (см. также [2]). *Тепловой мощностью* цепи называется величина

$$Q := \sum_{xy} C(xy) (v(x) - v(y))^2,$$

где суммирование ведется по всем ребрам цепи.

Пусть внутренние вершины имеют номера $1, \dots, k$, а граничные — $k + 1, \dots, n$. Пусть $v(x)$ — произвольная функция на вершинах конечной электрической цепи, удовлетворяющая аксиоме 1. Обозначим $v_1 = v(1), \dots, v_k = v(k)$. Рассмотрим тепловую мощность $Q(v_1, \dots, v_k)$ как функцию от переменных v_1, \dots, v_k .

ПРИНЦИП ДОСТИЖЕНИЯ НАИМЕНЬШЕГО ЗНАЧЕНИЯ. *Функция*

$$Q(v_1, \dots, v_k)$$

достигает своего наименьшего значения.

ДОКАЗАТЕЛЬСТВО. Обозначим $Y := Q(0, \dots, 0)$. Докажем, что если хотя бы одно из чисел v_1, \dots, v_k превышает по модулю число $X := n\sqrt{Y/\min c(xy)}$, то $|Q(v_1, \dots, v_k)| > Y$. Пусть, скажем, $|v_1| > X$. Возьмем кратчайший путь, соединяющий вершину 1 с одной из вершин множества N . В этом пути не более n ребер, поэтому найдется ребро xy , на котором $|v(x) - v(y)| > \sqrt{Y/\min c(xy)}$. На этом ребре выражение $c(xy)(v(x) - v(y))^2$ уже превышает Y . Поскольку все слагаемые в сумме $\sum_{xy} c_{xy}(v(x) - v(y))^2$ неотрицательны, получаем требуемое неравенство.

Ограничим область определения функции $Q(v_1, \dots, v_k)$ на множестве $[-X; X]^k$. Так как рассматриваемое множество компактно, а функция $Q(v_1, \dots, v_k)$ непрерывна, то она принимает на нем наименьшее значение. Это наименьшее значение заведомо не больше $Y = Q(0, \dots, 0)$, поэтому оно не больше значений функции $Q(v_1, \dots, v_k)$ вне множества $[-X; X]^k$. Значит, найденное значение — наименьшее на *всем* пространстве \mathbb{R}^k .

ВАРИАЦИОННЫЙ ПРИНЦИП. *Функция $Q(v_1, \dots, v_k)$ принимает наименьшее значение тогда и только тогда, когда функция $v(x)$ — гармоническая.*

ДОКАЗАТЕЛЬСТВО. Рассмотрим произвольную внутреннюю вершину x . Пусть, без ограничения общности, она имеет номер 1. Рассмотрим $Q(v_1, \dots, v_k)$ как квадратный трехчлен относительно v_1 . Старший коэффициент положителен, а значит наименьшее значение принимается при $v_1 = \sum_{xy} c(xy)v(y)/\sum_{xy} c(xy)$, где суммирование производится по всем ребрам xy , выходящим из x . Значит, наименьшее значение принимается в точности, когда выполняется аксиома 2 для вершины x .

ЗАКОН СОХРАНЕНИЯ ЭНЕРГИИ. *Минимальное значение тепловой мощности $Q(v_1, \dots, v_k)$ численно равно эффективной проводимости цепи.*

ДОКАЗАТЕЛЬСТВО. Имеем

$$\begin{aligned} \sum_{xy} c(xy)(v(x) - v(y))^2 &= \\ &= \sum_{xy} (v(x)c(xy)(v(x) - v(y)) + v(y)c(xy)(v(y) - v(x))) = \\ &= \sum_{x=1}^n \left(v(x) \sum_{xy} c(xy)(v(x) - v(y)) \right). \end{aligned}$$

Значение $v(x) \sum_{xy} c_{xy}(v(x) - v(y))$ равно нулю для всех внутренних вершин по аксиоме 2 и для всех вершин множества N . Следовательно:

$$Q(v_1, \dots, v_k) = \sum_{x \in P} \sum_{xy} c_{xy}(1 - v(y)) = C.$$

ДОКАЗАТЕЛЬСТВО ПРИНЦИПА МОНОТОННОСТИ. Пусть C — проводимость исходной цепи, а C' — проводимость цепи после увеличения проводимости одного из ребер. Обозначим через v_1, \dots, v_k потенциалы вершин в исходной цепи, а через v'_1, \dots, v'_k — в новой. Обозначим через $Q(v_1, \dots, v_k)$ тепловую мощность исходной цепи, а $Q'(v_1, \dots, v_k)$ — новой. Будем рассматривать их как функции от переменных v_1, \dots, v_k . Тогда, согласно закону сохранения энергии и вариационному принципу, получаем:

$$C = Q(v_1, \dots, v_k) \leq Q(v'_1, \dots, v'_k) \leq Q'(v'_1, \dots, v'_k) = C'.$$

Аналогично доказывается, что если в цепи одну проводимость уменьшить, то эффективная проводимость не увеличится.

В качестве следствия принципа монотонности получаем:

ПРИНЦИП РАЗРЕЗАНИЯ И СКЛЕЙКИ. *Разрезание каких-либо ребер цепи может только уменьшить эффективную проводимость между данными*

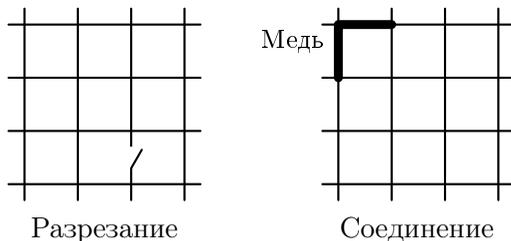


Рис. 8. Разрезание ребер и соединение вершин цепи; см. принцип разрезания и склейки

вершинами; см. рисунок 8 слева. Объединение каких-либо вершин в одну вершину может только увеличить эффективную проводимость между данными вершинами; см. рисунок 8 справа.

3. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ ПОЙА

3.1. ОДНОМЕРНОЕ БЛУЖДЕНИЕ

Чтобы пояснить нашу основную идею, докажем сначала одномерный аналог теоремы Пойа.

ТЕОРЕМА ПОЙА. (С) При случайном блуждании по 1-мерной решетке вероятность когда-нибудь вернуться в начальную точку равна 1; см. рисунок 9.

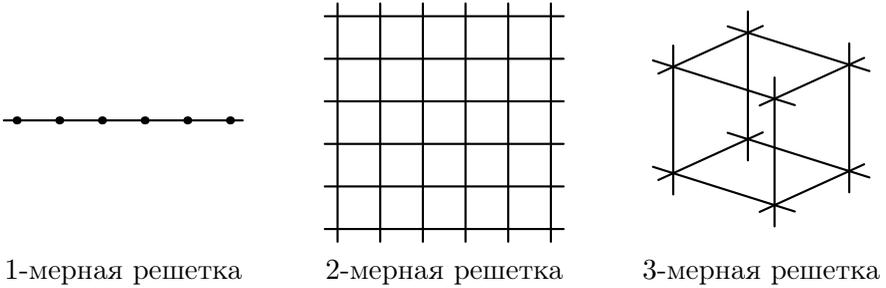


Рис. 9. Одномерная, двумерная и трехмерная решетки

ДОКАЗАТЕЛЬСТВО. Пусть P — вероятность когда-нибудь вернуться в начальную точку. Обозначим P_n вероятность вернуться в начальную точку до попадания в n или $-n$. Предположим, что все эти вероятности существуют. Тогда $P_n \leq P \leq 1$ для любого n .

Сейчас мы докажем, что $P_n = 1 - 1/n$. После первого «хода» человек попадает в одну из точек 1 и -1 с вероятностью $1/2$. Если он оказался в точке 1, то из примера 1 получаем, что вероятность вернуться в начало до попадания в точку n равна $1 - 1/n$. Если он оказался в точке -1 , рассуждаем аналогично. Значит, $P_n = \frac{1}{2} \left(1 - \frac{1}{n}\right) + \frac{1}{2} \left(1 - \frac{1}{n}\right) = 1 - \frac{1}{n}$. (Еще можно было заметить, что $P_n = 1 - C_n$, где $C_n = 1/n$ — проводимость цепи из n последовательно соединенных ребер единичной проводимости.)

Так как $1 - 1/n \leq P \leq 1$ для каждого n , то P равно 1.

3.2. ДВУМЕРНОЕ БЛУЖДЕНИЕ

ЛЕММА О ПРОВОДИМОСТИ КВАДРАТА. Проводимость C_n между центром и границей квадратной решетки размером $2n \times 2n$ с единичными

проводимостями ребер (см. рисунок 10) удовлетворяет неравенству

$$C_n \leq \frac{4}{\ln n} \quad (n \geq 2). \quad (3)$$

В частности, C_n стремится к нулю при неограниченном возрастании n .

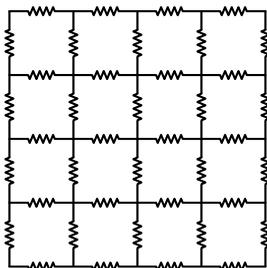


Рис. 10. Квадратная решетка 4×4

ДОКАЗАТЕЛЬСТВО. Применим принцип разрезания и склейки: объединим вместе точки, расположенные на квадратах, как показано на рисунке 11 сверху. Полученная цепь эквивалентна цепи на рисунке 11 в центре. Применим теорему об электрических преобразованиях. Так как можно заменить n параллельных резисторов проводимости 1 на один резистор проводимости n , то цепь эквивалентна цепи на рисунке 11 снизу. Проводимость этой цепи равна

$$\left(\sum_{k=1}^n \frac{1}{8k-4} \right)^{-1} \leq \left(\sum_{k=1}^n \frac{1}{4k} \right)^{-1} \leq \frac{4}{\ln n}.$$

Это число стремится к нулю при стремлении n к бесконечности. Так как проводимость C_n старой цепи не больше, то C_n тоже стремится к нулю.

ЗАДАЧА 10*. Докажите, что оценка, полученная в лемме о проводимости квадрата, является правильной по порядку. Проверьте, что при $n \geq 2$ проводимость квадрата $2n \times 2n$ удовлетворяет неравенству $C_n \geq \frac{1}{2 \ln n}$.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ ПОЙА (А). Пусть P — вероятность того, что при случайном блуждании по 2-мерной решетке мы когда-нибудь вернемся в начальную точку. Обозначим за P_n вероятность того, что случайное блуждание вернется в начальную точку до достижения граничных точек квадрата $2n \times 2n$ с центром в начальной точке. Если вероятность P существует, то $P_n \leq P \leq 1$ для каждого n . Из физической интерпретации вероятности возврата получаем, что $P_n = 1 - C_n/4$, где C_n — эффективная проводимость между центром и границей квадрата $2n \times 2n$. По доказанной

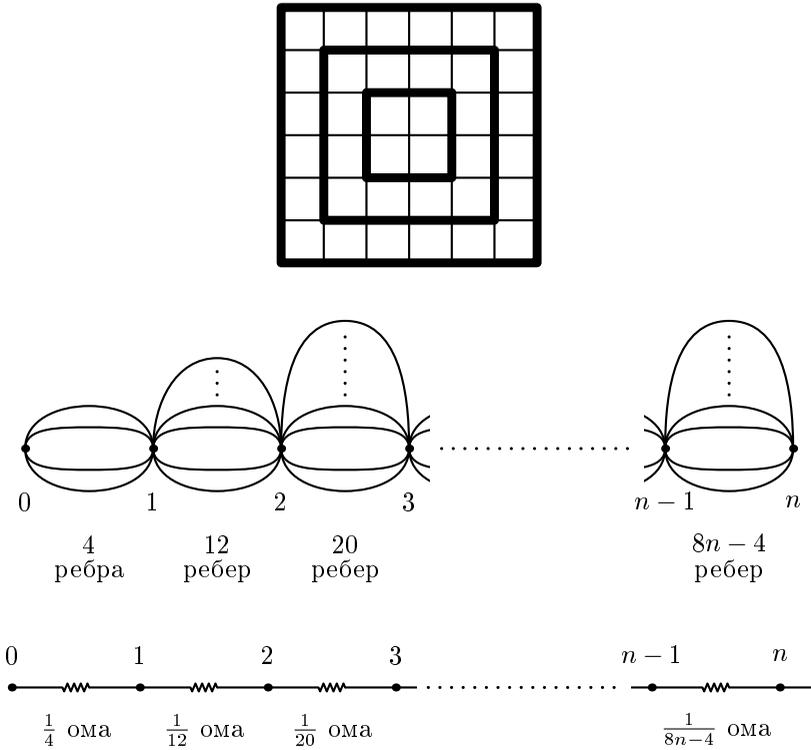


Рис. 11. Объединение в квадратной цепи и эквивалентная цепь

лемме проводимость C_n стремится к нулю при стремлении n к бесконечности. Поэтому $P_n \rightarrow 1$ при $n \rightarrow \infty$, значит, вероятность P существует и равна 1.

Наш метод позволяет установить и более тонкие результаты:

ТЕОРЕМА ПОЙА для «ДЫРЯВОЙ РЕШЕТКИ». Пусть из 2-мерной решетки выбросили произвольное множество ребер. Тогда по-прежнему с вероятностью 1 случайное блуждание возвращается в начальную точку (это утверждение задачи 12 из 14-го выпуска «Математического Просвещения», с. 274).

ДОКАЗАТЕЛЬСТВО. Действительно, рассмотрим часть полученной «дырявой решетки», лежащую в квадрате $2n \times 2n$. По принципу разрезания и склейки при выбрасывании ребер проводимость может только уменьшиться. Значит, проводимость C'_n нашей части квадрата не превосходит проводимости C_n всего квадрата. По лемме о проводимости квадрата $C_n \rightarrow 0$ при $n \rightarrow \infty$, значит, и $C'_n \rightarrow 0$ (в частности, мы не исключаем

случай $C'_n = 0$). Для доказательства нашего утверждения остается повторить рассуждение из доказательства теоремы Пойа (а).

3.3. ТРЕХМЕРНОЕ БЛУЖДЕНИЕ

При доказательстве теоремы Пойа в двух измерениях мы склеивали вершины электрической цепи, чтобы оценить вероятность возврата снизу. В трехмерном случае нам нужно оценить вероятность возврата сверху, поэтому мы, наоборот, будем выбрасывать некоторые рёбра из нашей цепи. При этом будем стремиться получить такую цепь, для которой проводимость легко посчитать. Для этого идеально подходят деревья.

Прежде чем привести доказательство, предоставим читателю возможность придумать его самому, решив следующую серию задач.

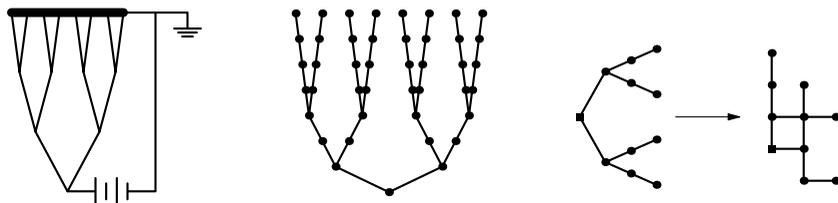


Рис. 12. (Слева) бинарное дерево глубины 3; (в центре) модифицированное бинарное дерево глубины 3; (справа) разрешенные пересечения ребер в этом дереве; см. задачи 11, 12 и 14

ЗАДАЧА 11. Найдите сопротивление бинарного дерева глубины (А) 3; (В) 2010, составленного из единичных резисторов (см. рис. 12 слева).

ЗАДАЧА 12. Найдите сопротивление *модифицированного* бинарного и троичного деревьев глубины 2010, в которых каждый резистор на k -м уровне заменяется на 2^k последовательно соединенных единичных резисторов (см. рис. 12 в центре).

ЗАДАЧА 13. Какие из деревьев, упомянутых (А) в задаче 11; (В) в задаче 12 можно вырезать из трехмерной решетки?

ЗАДАЧА 14. А если разрешаются пересечения (см. рис. 12 справа) ребер на равном расстоянии от корня?

ЛЕММА О ПРОВОДИМОСТИ ДЕРЕВА. *Проводимость модифицированного троичного дерева любой глубины больше 1.*

ДОКАЗАТЕЛЬСТВО. Потенциалы в точках, расположенных на одинаковом расстоянии от корня дерева, равны из симметрии. Объединим такие

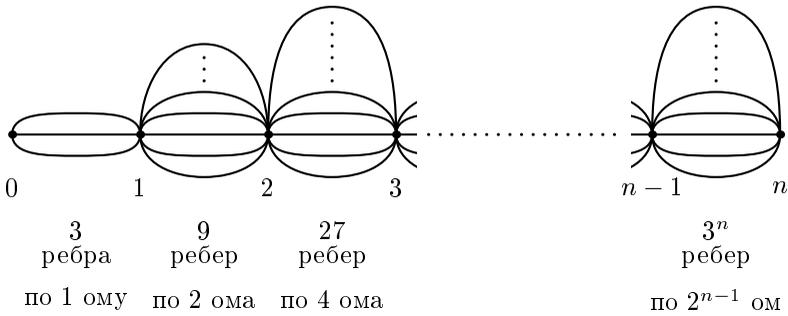


Рис. 13. Подсчет проводимости дерева; см. доказательство леммы о проводимости дерева

точки. Получим цепь, изображенную на рисунке 13. Проводимость цепи не изменилась, и она равна

$$\frac{1}{\frac{1}{3} + \frac{2}{9} + \dots + \frac{2^{n-1}}{3^n}} = \frac{1}{1 - \frac{2^n}{3^n}} > 1.$$

ЛЕММА О ВЫРЕЗАНИИ ДЕРЕВА. Из трехмерной решетке можно вырезать модифицированное троичное дерево любой глубины, в котором некоторые вершины, расположенные на одинаковом расстоянии от корня, склеены.

Доказательство проводится индукцией по глубине дерева, см. рисунок 14.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ ПОЙА (В). Докажем, что вероятность возврата в начальную точку не превосходит $5/6$. Для любого $n = 2^i - 1$ рассмотрим множество вершин (x, y, z) , где $|x| + |y| + |z| \leq n$. Пусть C_i — проводимость между началом координат и границей такой фигуры. По лемме о вырезании дерева из такой части решетки можно вырезать модифицированное троичное дерево глубины i с пересечениями ребер на равном расстоянии от корня. Легко заметить, что проводимость дерева с такими пересечениями равно проводимости такого же дерева без пересечений. По лемме о проводимости дерева проводимости модифицированных троичных деревьев больше 1. Поэтому и проводимости вырезаемых деревьев с пересечениями больше 1. По принципу монотонности получаем $C_i > 1$. Значит, ток, втекающий в цепь, не меньше 1. Следовательно, потенциалы в вершинах, соседних с началом координат, не больше $1 - \frac{1}{6} = \frac{5}{6}$. Они равны вероятности возврата в начало координат раньше попадания на границу рассматриваемого множества. Переходя к пределу при $i \rightarrow \infty$, получаем требуемое.

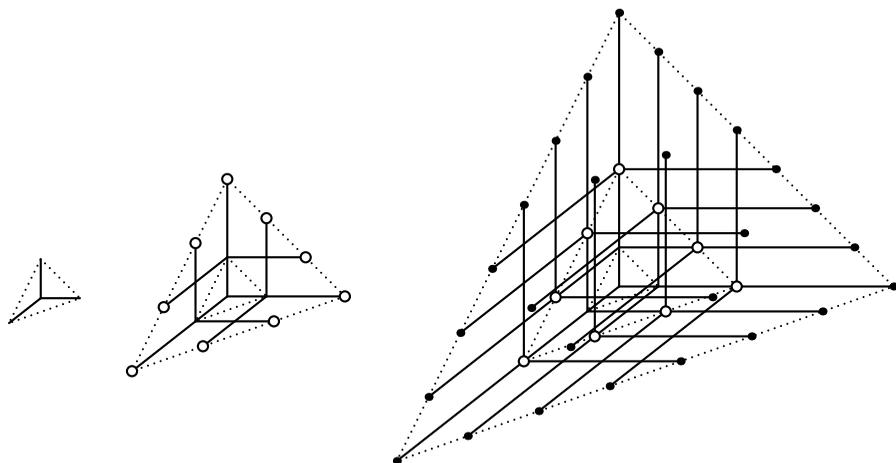


Рис. 14. Вырезание модифицированного трюичного дерева со склеенными вершинами из трехмерной решетки

БЛАГОДАРНОСТИ

Авторы благодарны Д. В. Баранову, И. В. Богданову, А. Я. Канелю, М. В. Прасолову, Д. С. Челкаку и Г. Р. Челнокову за полезные обсуждения.

СПИСОК ЛИТЕРАТУРЫ

- [1] Д. Баранов, М. Скопенков, А. Устинов. *Сопротивление между узлами решетки* // Математическое Просвещение. Сер. 3, вып. 15. 2011. С. 198–199.
- [2] О. Ляшко. *Почему не уменьшится сопротивление* // Квант, №1. 1985. С. 10–15.
- [3] М. Скопенков, М. Прасолов, С. Дориченко. *Разрезания металлического прямоугольника* // Квант, №3. 2011. С. 10–16. Доступно также: <http://arxiv.org/abs/1011.3180>
- [4] Е. Соколов. *И снова задачи на сопротивление* // Квант, №3. 2011. С. 43–46.
- [5] D. Chelkak, S. Smirnov. *Discrete complex analysis on isoradial graphs* // Adv. Math. Vol. 228. 2011. P. 1590–1630. Доступно также: <http://arxiv.org/abs/0810.2188v2>.
- [6] R. Courant, K. Friedrichs, H. Lewy. *Über die partiellen Differenzgleichungen der mathematischen Physik* // Math. Ann., Bd. 100. 1928, S. 32–74. Рус. пер.: УМН. Вып 8. 1941, С. 125–160. Доступно также:

<http://www.stanford.edu/class/cme324/classics/courant-friedrichs-lewy.pdf>

- [7] P.G. Doyle, J.L. Snell. *Random walks and electrical networks*. Mathematical Association of America, 1984. Доступно также: <http://arxiv.org/abs/math.PR/0001057>
- [8] F. Spitzer *Principles of Random Walks*. New York: Van Nostrand, 1964. Рус. пер.: Спицер Ф. *Принципы случайного блуждания*. М.: Мир, 1969.

М. Скопенков, ИППИ РАН, KAUST

Email: skopenkov@rambler.ru

В. Смыкалов, мат.-мех. ф-т СПбГУ

Email: vladimir.smykalov@gmail.com

А. Устинов, ХО ИПМ ДВО РАН

Email: ustinov.alexey@gmail.com

Еще одно доказательство «из Книги»: теорема Менгера

А. Б. Скопенков*

«Теорема Менгера является одним из краеугольных камней теории графов.» [2] Она изучается в большинстве кружков и летних школ. Предлагаемые доказательства, как правило, основаны на простой идее, но содержат много технических деталей, ср. [1, 3, 4]. Здесь приводится простое доказательство, полученное незначительным упрощением из [2]. (Это доказательство близко к приведенным в [1, 3, 4] и, возможно, к другим; однако, трюк со стягиванием ребра позволяет избежать технических трудностей.)

В этой заметке графы могут иметь петли и кратные ребра.

ТЕОРЕМА МЕНГЕРА. *Если вершины a и b графа G , не соединенные ребром, остаются в одной компоненте связности после удаления любых $k-1$ других вершин, то a и b можно соединить k путями, любые два из которых пересекаются только в концах.*

ДОКАЗАТЕЛЬСТВО. Докажем теорему для $k = 3$; для произвольного k доказательство аналогично. Назовем *тройкой $a - b$ путей* тройку путей из a в b , любые два из которых пересекаются только в концах.

Пусть G — минимальный по числу ребер контрпример к теореме Менгера (для $k = 3$). Тогда вершины a и b оказываются в разных компонентах после удаления некоторых трех вершин x, y, z , две из которых соединены ребром.

(Действительно, если любое ребро графа G содержит a или b , то это утверждение очевидно. Иначе обозначим через e ребро графа G , не содержащее ни a , ни b . Обозначим через G/e граф, полученный из G стягиванием ребра e . Так как в G нет тройки $a - b$ путей, то в G/e нет тройки $(a/e) - (b/e)$ путей. Ввиду минимальности графа G граф G/e содержит две вершины, разделяющие a/e и b/e . Среди них есть вершина e/e , ибо в G нет двух вершин, разделяющих a и b . Значит, прообразы в G этих двух вершин являются искомыми тремя вершинами.)

*Поддержан грантом фонда Саймонса.

Обозначим через G_a граф, состоящий из

- ▷ компоненты A связности графа $G - \{x, y, z\}$, содержащей вершину a ,
- ▷ вершин x, y, z и ребер, соединяющих их с вершинами из A ,
- ▷ новой вершины b' и ребер $b'x, b'y$ и $b'z$.

Вершины a и b' графа G_a остаются в одной компоненте связности после удаления любых двух вершин графа G_a . Так как степень вершины b в графе G не менее 3, то в графе G_a меньше ребер, чем в графе G . Значит, в G_a есть тройка $a - b'$ путей.

Аналогично определяем граф G_b и находим в нем тройку $a' - b$ путей. Построенные шесть путей дают тройку $a - b$ путей в G . \square

СПИСОК ЛИТЕРАТУРЫ

- [1] А. Я. Белов. *Метод минимального контрпримера и спуск в графах* // Математика в задачах. Под ред. А. Заславского, Д. Пермякова, А. Скопенкова, М. Скопенкова и А. Шаповалова. М.: МЦНМО, 2009.
- [2] R. Diestel. *Graph Theory*. Electronic Edition. New York: Springer Verlag. 2000.
- [3] Д. В. Карпов. *Теория графов*.
http://logic.pdmi.ras.ru/dvk/211/graphs_dk.pdf
- [4] А.Ю. Эвнин. *Вокруг теоремы Холла: учебное пособие* // Мат. Образование, №3, 2005. С. 2–23.

А. Б. Скопенков, механико-математический факультет Московского государственного университета, Независимый московский университет и Московский институт открытого образования

Email: skopenko@mccme.ru

Инфо: <http://dfgm.math.msu.su/people/skopenkov/papersc.ps>

Биективное доказательство дискретного закона арксинуса

Э. Э. Лернер, Э. Ю. Лернер

Найдено геометрическое преобразование, устанавливающее явное взаимно однозначное соответствие между траекториями одномерного случайного блуждания длины $2n$: а) начинающимися и заканчивающимися в нуле и проходящими через него в момент времени $2i$; б) начинающимися в нуле и пребывающими $2i$ единиц времени на положительной полуоси. Равномощность множеств этих траекторий хорошо известна. Преобразование, излагаемое в статье, является обобщением конструкции Э. Нелсона, рассмотревшего случай $i = n$.

1. Увидев картинку с колоколообразной кривой, типичный математик узнает в рисунке не шляпу и не змею, проглотившую слона, а плотность нормального (гауссовского) распределения. К сожалению, менее идентифицируема сообществом плотность распределения, изображаемая кривой с «пузом вниз». Лишь искушённый человек узнает в таком рисунке функцию

$$f(x) = \frac{1}{\pi\sqrt{x(1-x)}}, \quad 0 < x < 1, \quad (1)$$

— плотность знаменитого закона арксинуса, служащего философским оправданием продолжительности «светлых» (а также и «тёмных») полос жизни. В этой заметке будет представлено геометрическое доказательство комбинаторной основы этого закона (в дальнейшем изложении отсутствуют какие-либо формулы, за исключением формулы (2)).

Симметричное одномерное случайное блуждание — это белая мышь теории вероятностей. Медики и биологи проводили много экспериментов на белых мышах, вероятностники же изучение сложных законов начинали с анализа следующей модели. В игровом её варианте (см. [3]) рассматривается пьяница, идущий по дороге и делающий каждый раз шаг вперёд или назад с равными вероятностями. Ответ на вопрос о том, далеко ли он уйдёт от дома, двигаясь таким образом, хорошо известен (см., например, [2]).

Более интригующий вопрос — свалится ли пьяница с обрыва, если таковым заканчивается дорога с одной из сторон, — также очень популярен и ему посвящено много литературы (см. [2, 3]).

В этой заметке рассмотрена другая задача — какова доля времени, которое пьяница будет проводить слева или справа от дома (начала координат), двигаясь по бесконечной в обе стороны дороге (целочисленной прямой, на которой он и передвигается). Естественно, ответы на все эти вопросы есть в учебниках по теории вероятностей (см. [2, 6]), в них, в частности, есть описание результатов экспериментов, подтверждающих, что распределение доли времени, проведённым пьяницей слева (справа) от дома описывается функцией (1). Неожиданность такого распределения состоит в том, что согласно ему в большинстве экспериментов значение доли времени будет далеко от среднего, равного $1/2$, чаще оно будет близко либо к нулю, либо к единице. Мы будем рассматривать дискретный закон арксинуса, дающий распределение доли времени при фиксированном общем числе шагов, равном $2n$. Согласно этому закону (см. [2, 6]), справедлива следующая формула для вероятности того, что доля времени проведённого на положительной полуоси, не превышает x :

$$\sum_{i: i/n \leq x} \frac{\binom{2i}{i} \binom{2n-2i}{n-i}}{2^{2n}}. \quad (2)$$

При $n \rightarrow \infty$ сумма (2) стремится к функции распределения $2 \arcsin(\sqrt{x})/\pi$. Случайной величине с такой функцией распределения и соответствует плотность (1).

Заметим, что числитель каждого слагаемого в сумме (2) представляет собой количество траекторий длины $2n$, проходящих через начало координат в нулевой, $2i$ -й и $2n$ -й моменты времени. С другой стороны (как фактически утверждается в формуле (2)), то же выражение описывает количество траекторий длины $2n$, пребывающих на положительной полуоси $2i$ единиц времени. Цель заметки — описать геометрическое преобразование, устанавливающее взаимно однозначное соответствие между множествами этих траекторий. Задача поиска такого соответствия между элементами двух равномоощных множеств традиционна для перечислительной комбинаторики (см. [4, 5]).

Во всех окончательных результатах дальнейшего (несколько более формального) изложения мы будем рассматривать траектории одномерного случайного блуждания, начинающиеся в нуле. Если при этом траектория в нуле заканчивается, то будем называть её замкнутой. Траектория, проходящая лишь по положительной полуоси (включая ноль), называется неотрицательной. Как обычно в таких случаях, будем рассматривать геометрическое представление траекторий в виде ломаной в плоскости (t, x) ,

соединяющей точки с целочисленными координатами, указывающими положение x пьяницы после t шагов.

2. ПРЕОБРАЗОВАНИЕ НЕЛСОНА. Сначала напомним придуманное Э. Нелсоном взаимно однозначное соответствие между неотрицательными траекториями длины $2n$, начинающимися в нуле, и замкнутыми траекториями той же длины (это частный случай того биективного соответствия, которое мы хотим получить, для $i = n$).

Вот ([6, с. 115]) описание преобразования, переводящего замкнутую траекторию в неотрицательную: «Обозначим *самую левую* точку минимума заданного пути, ведущего из начала координат в точку $(2n, 0)$, через $M = (k, m)$. Отразим участок, ведущий из начала координат в точку M , относительно вертикальной прямой $t = k$ и передвинем отражённый участок так, чтобы его начальная точка совпала с точкой $(2n, 0)$. Если M принять за начало координат, то в новой системе координат новый путь ведёт из начала в точку $(2n, 2m)$ и все его вершины лежат выше оси или на ней.»

Обратное преобразование неотрицательной траектории, заканчивающейся в точке $(2n, 2m)$, в траекторию, заканчивающуюся в $(2n, 0)$, очевидно, происходит так: отсечём участок от *самого правого* пересечения траектории с горизонтальной прямой $x = m$, отразим его зеркально относительно соответствующей вертикальной прямой и приставим перед началом траектории, перенеся начало координат (см. рис. 1). Заметим, что при последнем преобразовании траектория перейдёт сама в себя, если $m = 0$.

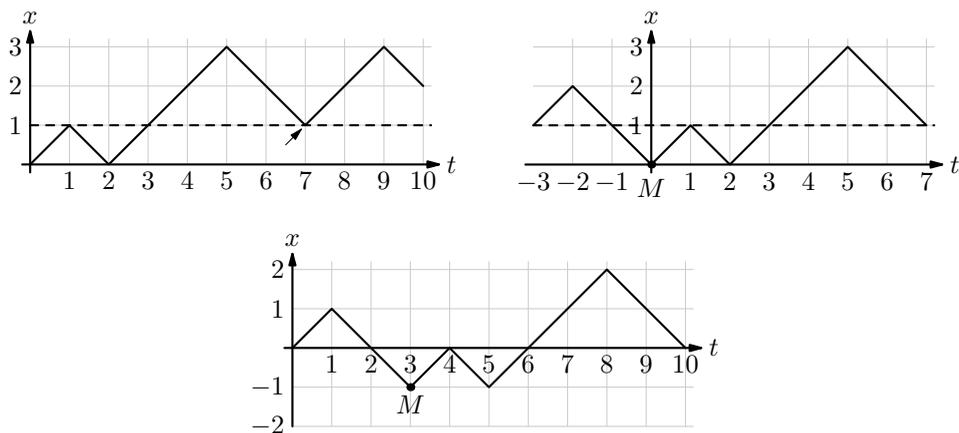


Рис. 1. Соответствие между неотрицательной траекторией (слева сверху) и замкнутой траекторией (нижний график)

Если же $t > 0$, то получится траектория, часть которой будет отрицательна (последнее означает, что имеется часть ломаной, расположенная ниже горизонтальной оси).

Все рассуждения выше после очевидных замен могут быть применены для установления биективного соответствия между неположительными траекториями длины $2n$ и замкнутыми траекториями той же длины (это другой частный случай общего результата для $i = 0$).

3. СООТВЕТСТВИЕ МЕЖДУ ЗАМКНУТЫМИ ТРАЕКТОРИЯМИ. Опишем теперь соответствие между траекториями, пребывающими $2i$ ($0 < i < n$) единиц времени на положительной полуоси, а $2n - 2i$ — на отрицательной полуоси, и траекториями, проходящими через ноль в моменты времени $2i$ и $2n$. Рассмотрим сначала частный случай, когда первый вид траектории также заканчивается в нуле. Соответствие в этом частном случае строится достаточно просто и естественно.

Назовём куском часть траектории, начинающуюся и заканчивающуюся в нуле и нигде больше в ноль не заходящую. Знаком куска назовём знак неконцевых его точек. Очевидно, что симметрия относительно горизонтальной оси координат устанавливает взаимно однозначное соответствие между положительными и отрицательными кусками. Знаковой последовательностью замкнутой траектории назовём последовательность знаков всех кусков этой траектории.

Преобразование, которое переводит замкнутую траекторию длины $2n$, являющуюся неотрицательной $2i$ шагов, в замкнутую траекторию, проходящую через ноль в момент $2i$ (не любую такую траекторию, точное описание образа дано ниже), устроено следующим образом. Пусть A_+ — совокупность всех положительных кусков исходной траектории, A_- — отрицательных кусков. Пусть S — знаковая последовательность исходной

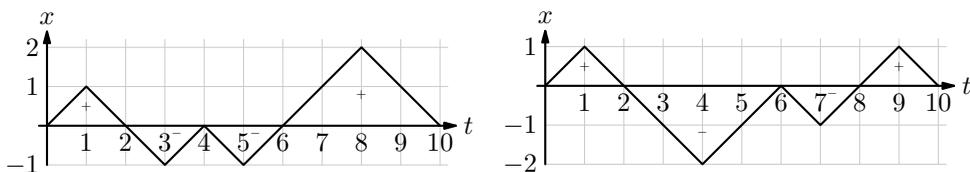


Рис. 2. Соответствие между замкнутой траекторией длины 10, неотрицательной в течении 6 шагов (слева) и замкнутой траекторией той же длины, проходящей через $(6, 0)$ (справа). Куски из множеств A_+ , A_- отмечены соответствующими знаками на левом графике. На правом графике эти куски расположены слева (справа) от точки $(6, 0)$. Знаковая последовательность $S = (+, -, -, +)$

траектории. Рассмотрим теперь замкнутую траекторию, у которой набор кусков совпадает с точностью до симметрии относительно горизонтальной оси с конкатенацией A_+ , A_- , а знаковая последовательность совпадает с S . Очевидно, что эта траектория проходит через ноль в момент времени $2i$. Это и будет результат преобразования (см. рис. 2).

Опишем обратное преобразование. Нам известно, что в момент времени $2i$ траектория проходит через ноль. Помещаем в A_+ все куски траектории, соответствующие моментам времени до $2i$ включительно, в A_- — оставшиеся. Затем с помощью симметрии относительно горизонтальной оси ориентируем все куски в A_+ так, чтобы они приобрели положительный знак, в A_- — отрицательный. Так как знаковые последовательности рассматриваемых траекторий совпадают, последовательность S известна. Берём по очереди куски либо из A_+ , либо из A_- в зависимости от очередного знака элемента S , и приставляем их друг к другу. Получаем замкнутую траекторию, которая $2i$ единиц времени положительна и $2n - 2i$ единиц времени отрицательна.

Очевидно, что обратное преобразование определено не в любом случае, а только если количество положительных знаков в S совпадает с мощностью A_+ , а отрицательных — с A_- . Это свойство и определяет совокупность рассмотренных траекторий, проходящих через ноль в момент времени $2i$. В общем случае мы нуждаемся в доопределении обратного преобразования. При этом результирующая траектория уже будет незамкнутой.

4. СООТВЕТСТВИЕ В ОБЩЕМ СЛУЧАЕ. Итак, пусть у нас имеется произвольная замкнутая траектория, проходящая через ноль в момент времени $2i$. Сформируем множества A_+ , A_- , S как описано выше. Будем строить траекторию, подсоединяя кусок к куску в соответствии с вышеописанным алгоритмом. Пусть при рассмотрении очередного знака S алгоритм не срабатывает — куски в соответствующем множестве A уже все изъяты (рассмотрены). Пусть, для определённости, очередной знак S отрицателен, а из множества A_- изъяты все куски. Тогда уберём из уже сформированной траектории все куски, взятые после последнего куска из A_- . Из этих кусков (они были взяты, очевидно, из множества A_+) и всех оставшихся неизъятыми кусков множества A_+ сформируем вспомогательную замкнутую траекторию, знаковая последовательность которой совпадает со взятыми в нужном количестве последними элементами из S (отрицательные куски этой вспомогательной траектории получаются из исходных с помощью симметрии относительно горизонтальной оси).

Далее преобразуем эту вспомогательную траекторию в неотрицательную траекторию той же длины алгоритмом Нелсона, описанным в начале этой работы. Заметим, что получившаяся неотрицательная траектория

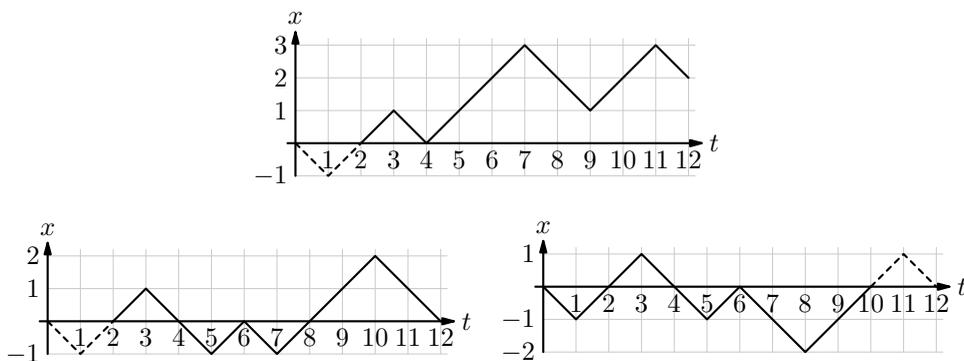


Рис. 3. Соответствие между траекторией длины 12, неотрицательной в течении 10 шагов (верхний график) и замкнутой траекторией той же длины, проходящей через $(10, 0)$ (нижний график справа). Снизу слева изображён результат первого этапа преобразования верхней траектории. Сплошной линией выделены части траекторий, соответствующие кускам из A_+ , штриховой линией — куску из A_- ; $|A_+| = 4$, $|A_-| = 1$. Финальная часть верхней траектории совпадает с траекторией на рис. 1 слева сверху. Знаковая последовательность устанавливается из результата первого этапа преобразования и совпадает со знаковой последовательностью последнего графика: $S = (-, +, -, -, +)$.

уже не будет заканчиваться в нуле. Приставив её к концу ранее сформированной траектории, получим график случайного блуждания, пребывающего $2i$ единиц времени на положительной и $2n - 2i$ единиц времени на отрицательной полуоси.

Нам осталось описать общее прямое преобразование траектории, пребывающей $2i$ единиц времени на положительной полуоси, в замкнутую траекторию, проходящую через ноль в момент времени $2i$. Первый этап этого преобразования состоит в изменении неположительного (или неотрицательного) конца исходной траектории (берётся максимально длинная финальная часть траектории, имеющая постоянный знак) в замкнутую траекторию той же длины по правилу Нелсона. Второй этап общего преобразования применяется к результату первого этапа и почти совпадает с частным случаем прямого преобразования для замкнутой траектории. Единственное отличие состоит в том, что набор кусков, представляющий собой преобразованный конец траектории, целиком помещается либо в A_+ , либо в A_- в зависимости от знака финальной части исходной траектории. При этом последовательность S считывается со всей результирующей траектории первого этапа и потому может быть совершенно произвольной

(с естественным ограничением $|S| = |A_+| + |A_-|$). В результате двух этапов мы получаем произвольную замкнутую траекторию, проходящую через ноль в момент времени $2i$ (см. рис. 3). Очевидно, что прямому преобразованию соответствует описанное ранее обратное.

5. Дискретный закон арксинуса заставляет задуматься об условиях, при которых индивидуальное поведение будет резко отличаться от типичного (ведь если много «экземпляров пьяниц» выйдут из дома, то в достаточно большой момент времени почти в точности половина из них будет находиться слева от начальной точки). Такие размышления привели к понятию эргодичности, яркое изложение соответствующих результатов для естественного обобщения случайных блужданий — марковской цепи — дано в книге [1] (см. также [6]). Случайное блуждание на бесконечной прямой оказывается неэргодичным, к тому же время возвращения в начало координат является бесконечным, в этом глубинная причина «экстремистского» поведения индивидуальных траекторий.

СПИСОК ЛИТЕРАТУРЫ

- [1] Кельберт М.Я., Сухов Ю.М. *Вероятность и статистика в примерах и задачах. Т. 2: Марковские цепи как отправная точка теории случайных процессов и их приложения.* М.: МЦНМО. 2009.
- [2] Колмогоров А.Н., Журбенко И.Г., Прохоров А.Б. *Введение в теорию вероятностей.* М.: Наука. 1982.
- [3] Мостеллер Ф. *Пятьдесят занимательных вероятностных задач с решениями.* М.: Наука. 1975.
- [4] Стенли Р. *Перечислительная комбинаторика.* Т. 1. М.: Мир. 1990.
- [5] Стенли Р. *Перечислительная комбинаторика.* Т. 2. М.: Мир. 2005.
- [6] Феллер В. *Введение в теорию вероятностей и её приложения.* Т. 1. М.: Мир. 1984.

Э. Э. Лернер, студент, Московский государственный университет
Email: neex.emil@gmail.com

Э. Ю. Лернер, доцент, Казанский (Приволжский) федеральный университет. 20008, Казань, Кремлёвская 18, К(П)ФУ, факультет ВМК
Email: eduard.lerner@gmail.com

Контактные числа, коды и сферические многочлены

А. В. Акопян*

Г. А. Кабатянский†

О. Р. Мусин‡

1. ВВЕДЕНИЕ

В этой статье мы расскажем об одной интересной геометрической задаче с более чем трехсотлетней историей, где первые результаты стали появляться сравнительно недавно. Зададимся следующим вопросом:

какое максимальное число шаров одинакового радиуса можно расположить в n -мерном пространстве так, чтобы все они касались («были в контакте») одного (центрального) шара такого же радиуса?

Соответствующее число шаров называется контактным числом $\tau(n)$ n -мерного евклидова пространства. Из рисунка 1 очевидно, что $\tau(2) = 6$.

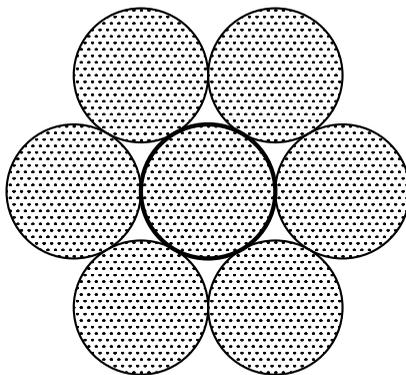


Рис. 1.

*Работа выполнена при частичной поддержке фонда «Династия», грантов РФФИ 10-01-00096 и 11-01-00735 и гранта Правительства РФ №11.G34.31.0053.

†Работа выполнена при частичной поддержке гранта 11-01-00735 и гранта Правительства РФ №11.G34.31.0073.

‡Работа выполнена при частичной поддержке гранта 11-01-00735 и гранта Правительства РФ №11.G34.31.0053.

Поместим для простоты центр центрального шара в точку 0. Обозначим A_1, \dots, A_L точки (векторы) касания шарами центрального шара. Тогда угол между любыми двумя векторами A_i и A_j не меньше $\pi/3$ и очевидно, что наша задача эквивалентна нахождению максимального числа точек на сфере в n -мерном пространстве с попарными углами не меньше 60° . Отметим, что такое множество точек называется *сферическим кодом* с угловым расстоянием 60° . Похожий объект под названием «двоичные коды с исправлением ошибок» также будет рассматриваться в нашей статье.

Чему равно $\tau(3)$: 12 или 13, было предметом спора в 1694 году между сэром Ньютоном и сэром Грегори (пример расположения 12 шаров привести несложно, в этом случае центры шаров можно поместить в вершины икосаэдра подходящего размера). Ньютон оказался прав, и $\tau(3) = 12$, но первое доказательство этого факта появилось лишь в середине XX века [19]. Отметим, что полное элементарное доказательство этого факта было найдено сравнительно недавно. Его можно найти в статье [7], опубликованной в предыдущем выпуске этого сборника.

Никаких других значений $\tau(n)$ не было известно до 1979 года, когда с помощью неожиданного для геометрии метода, придуманного незадолго до этого Ф. Дельсартом [3], удалось доказать, что $\tau(8) = 240$ и $\tau(24) = 196560$. Этот замечательный результат был получен В. И. Левенштейном [6] и независимо от него А. Одлыжко и Н. Слоэном [17]. На самом деле, уже было известно, что $\tau(8) \geq 240$ и $\tau(24) \geq 196560$ благодаря двум замечательным решеткам: E_8 и Λ_{24} , у которых число «соседей» равнялось в точности этим значениям. Трудность состояла в доказательстве, что большего числа шаров разместить нельзя.

Следующим, и на сегодня последним, известным значением $\tau(n)$, стало ожидаемое равенство $\tau(4) = 24$, которое удалось доказать одному из авторов этой статьи, см. [16]. Для доказательства этого результата понадобилось модифицировать метод Дельсарта.

Метод Дельсарта позволяет получать верхние оценки (оценки несуществования) для многих других дискретных задач. В частности, сам метод был придуман Дельсартом для получения верхних оценок на мощность кодов, исправляющих ошибки. Эти идеи также нашли применение в других задачах об оптимальных расположениях точек на сфере, в частности, в задаче о конфигурации электронов с минимальной энергией, см. [12] или более простое изложение в [1].

В этой статье мы расскажем об оптимальных расположениях точек на сфере, решетках в евклидовых пространствах и кодах с исправлением ошибок и о том, как эти задачи связаны между собой и как к ним применять метод Дельсарта.

2. КОДЫ И РЕШЕТКИ

Как мы уже упоминали выше, есть две замечательные решетки: E_8 в 8-мерном пространстве и A_{24} в 24-мерном пространстве, число касаний для которых равно 240 и 196560, соответственно. Наиболее простой путь описать эти решетки лежит, на наш взгляд, через *теорию кодирования*. Теория кодирования или теория кодов, исправляющих ошибки, ведет свой отсчет от опубликованной 60 лет назад работы Р. Хэмминга [13], в которой были построены коды, исправляющие одиночные ошибки. С математической точки зрения основная часть теории кодирования может рассматриваться как теория упаковок одного класса дискретных метрических пространств, называемых пространствами Хэмминга, которые мы сейчас и определим.

Зададим на множестве \mathcal{B}^n всех *двоичных* слов (векторов) длины n из алфавита $\{0, 1\}$ расстояние Хэмминга d_H как число позиций, в которых два слова различаются. Т.е. для двух произвольных двоичных слов $\mathbf{a} = (a_1, \dots, a_n)$ и $\mathbf{b} = (b_1, \dots, b_n)$ из \mathcal{B}^n расстояние Хэмминга между ними равно $d_H(\mathbf{a}, \mathbf{b}) = \sum_{i=1}^n |a_i - b_i|$. Расстояние от нулевого слова $\mathbf{0}$ до слова $\mathbf{a} = (a_1, \dots, a_n)$, равное числу единиц среди координат a_i , называется весом Хэмминга слова \mathbf{a} и обозначается $wt(\mathbf{a})$.

Почему $d_H(\mathbf{a}, \mathbf{b})$ это метрика, т.е. почему выполнена аксиома треугольника (две другие аксиомы очевидны)? Определим на \mathcal{B}^n структуру графа, связав вершины \mathbf{a} и \mathbf{b} ребром, если они различаются ровно в одной позиции, т.е. если $d_H(\mathbf{a}, \mathbf{b}) = 1$. Легко видеть, что $d_H(\mathbf{a}, \mathbf{b})$ — это длина кратчайшего пути в этом графе, а для длины кратчайшего пути в графе аксиома треугольника, очевидно, выполнена.

Обозначим через

$$\mathcal{S}(n, t)(\mathbf{a}) = \{\mathbf{x} \in \mathcal{B}^n : d_H(\mathbf{x}, \mathbf{a}) \leq t\}$$

шар радиуса t в пространстве Хэмминга \mathcal{B}^n с центром в точке (слове) \mathbf{a} .

Его мощность очевидно равна $S(n, t) = \sum_{i=0}^t \binom{n}{i}$.

Подмножество C пространства Хэмминга \mathcal{B}^n называется *упаковкой шарами радиуса t* , если шары радиуса t с центрами в точках C не пересекаются.

Если точки (слова) упаковки $C \subset \mathcal{B}^n$ использовать для передачи сообщений по каналу связи, в котором при передаче n символов происходит не более t ошибок, то на приемной стороне возможно однозначное восстановление (*декодирование*) переданного сообщения, так как шары радиуса t с центрами в разных кодовых словах не пересекаются. По этой причине упаковка шарами радиуса t также называется *двоичным кодом длины n , исправляющим t ошибок*. Расстояние $d(C)$ кода C определяется как

минимальное из попарных расстояний между его словами

$$d(C) = \min_{\mathbf{c} \neq \mathbf{c}' \in C} d(\mathbf{c}, \mathbf{c}'), \quad (1)$$

и код C является упаковкой шарами радиуса t , т. е. исправляет t ошибок, если и только если $d(C) \geq 2t + 1$.

Всюду ниже код — это синоним подмножества пространства Хэмминга. Для кода C с исправлением t ошибок, т. е. для упаковки шарами радиуса t , определим плотность упаковки $\mu(C, t)$ как долю всего пространства \mathcal{B}^n , покрываемую шарами с центрами в C , т. е.

$$\mu(C, t) = \frac{|C|S(n, t)}{2^n}.$$

Очевидно, что плотность упаковки (кода) не более 1, т. е. для мощности произвольного кода C с исправлением t ошибок справедливо ограничение

$$|C| \leq \frac{2^n}{S(n, t)},$$

называемое границей Хэмминга.

Коды, достигающие границу Хэмминга, называются *совершенными* — они плотно, «без дыр» заполняют все пространство Хэмминга. Р. Хэмминг построил совершенные коды, исправляющие одиночные ошибки — при длине $n = 2^r - 1$ они имеют мощность 2^{n-r} , где $r = 2, 3, \dots$. Тогда же, на заре теории кодирования (конец 1940-х), были построены два совершенных кода: двоичный код Голея длины 23, исправляющий три ошибки, и троичный (т. е. над алфавитом $\{-1, 0, 1\}$) код Голея длины 11, исправляющий две ошибки. Одним из самых замечательных результатов теории кодирования является доказанная в начале 70-х годов XX века гипотеза, что других совершенных кодов, исправляющих t ошибок, при $t > 1$ не существует, см. [8].

Неудивительно, что для построения оптимальных расположений точек на сфере нам понадобятся именно совершенные двоичные коды. Начнем с кодов Хэмминга. Код Хэмминга длины 7 (самый простой и самый известный из кодов) задается как множество решений системы линейных уравнений

$$\begin{aligned} x_1 \oplus x_3 \oplus x_5 \oplus x_7 &= 0, \\ x_2 \oplus x_3 \oplus x_6 \oplus x_7 &= 0, \\ x_4 \oplus x_5 \oplus x_6 \oplus x_7 &= 0, \end{aligned} \quad (2)$$

где $x_i \in \mathbb{Z}_2$ и \oplus означает сложение по модулю 2. Легко увидеть закон, по которому выбраны коэффициенты этой системы. А именно, коэффициент при x_j в i -м уравнении равен коэффициенту при 2^{i-1} в двоичном разложении числа j . Также легко видеть, что у этой системы есть 16 решений.

Действительно, перепишем систему в виде

$$x_1 = x_3 \oplus x_5 \oplus x_7,$$

$$x_2 = x_3 \oplus x_6 \oplus x_7,$$

$$x_4 = x_5 \oplus x_6 \oplus x_7.$$

Переменные x_3 , x_5 , x_6 и x_7 можно выбрать произвольно (так называемые информационные символы), и через них однозначно определяются остальные переменные x_1 , x_2 и x_4 (так называемые проверочные символы).

Итак, мы описали знаменитый $(7, 4)$ -код Хэмминга. Здесь 7 означает размерность пространства, называемую длиной кода, а 4 — число информационных символов. Проверим, что множество решений этой системы является кодом с расстоянием 3, т.е. упаковкой шарами радиуса 1 или, что тоже самое, кодом с исправлением одиночных ошибок. Заметим, что любое ненулевое решение системы должно иметь как минимум три единицы среди своих координат, потому что иначе найдется уравнение из (2), в котором присутствует только одна из этих единиц (столбцы коэффициентов при различных переменных различны и отличны от нулевого столбца). Пусть теперь $\mathbf{a} = (a_1, \dots, a_7)$ и $\mathbf{b} = (b_1, \dots, b_7)$ — два произвольных различных решения системы. Рассмотрим вектор $\mathbf{a} \oplus \mathbf{b} = (a_1 \oplus b_1, \dots, a_7 \oplus b_7)$. Число единиц в нем и есть расстояние Хэмминга между векторами \mathbf{a} и \mathbf{b} , а так как он также является решением системы, то в нем не менее трех единиц, что и требовалось доказать. Отметим, что код C со свойством, что вместе с двумя любыми векторами \mathbf{a} и \mathbf{b} из кода их сумма $\mathbf{a} \oplus \mathbf{b}$ также принадлежит коду, называется *групповым* (или *линейным*) кодом.

Сопоставим произвольному двоичному вектору $\mathbf{c} = (c_1, \dots, c_n)$ вектор $\hat{\mathbf{c}} = (c_1, \dots, c_{n+1})$, где $c_{n+1} = c_1 \oplus \dots \oplus c_n$. Такая операция называется 1-удлинением с помощью общей проверки на четность. Ясно, что применение этой операции к произвольному линейному коду с нечетным расстоянием $2t + 1$ приводит к линейному коду с той же мощностью, но на единицу большими расстоянием и длиной. И на самом деле нам будет нужен не сам $(7, 4)$ -код Хэмминга, а его 1-удлинение, т.е. $(8, 4)$ -код с расстоянием 4 (также называемый кодом Хэмминга). Кроме того, нам понадобится тот факт, что у нулевого вектора в $(8, 4)$ -коде имеется ровно 14 «соседей», т.е. в коде имеется 14 кодовых слов веса 4.

УПРАЖНЕНИЕ. Докажите это (подсказка — этот код групповой, и в нем есть вектор $\mathbf{1}$ из всех единиц).

Решеткой \mathbb{L} в n -мерном евклидовом пространстве \mathbb{R}^n называется дискретная подгруппа этого пространства, т.е. для любых двух векторов решетки их сумма и разность также являются векторами решетки. Простейшей решеткой является целочисленная решетка \mathbb{Z}^n , состоящая из всех точек с целочисленными координатами. Легко показать, что любая

решетка имеет базис (и не один), т. е. набор линейно независимых векторов $\mathbf{v}^{(1)}, \dots, \mathbf{v}^{(k)}$ таких, что любой вектор решетки \mathbf{v} представим в виде их целочисленной комбинации, т. е. $\mathbf{v} = a_1\mathbf{v}^{(1)} + \dots + a_k\mathbf{v}^{(k)}$, где a_1, \dots, a_k — целые числа, а число k называется рангом решетки. Определим для решетки \mathbb{L} ее минимальное расстояние $d(\mathbb{L})$ (аналогично тому, как это было сделано для кода, см. (1))

$$d(\mathbb{L}) = \min_{\mathbf{v} \neq \mathbf{v}' \in \mathbb{L}} d(\mathbf{v}, \mathbf{v}').$$

С каждой решеткой связано соответствующее число касаний. «Соседями» точки $\mathbf{v} \in \mathbb{L}$ называются точки решетки \mathbb{L} , которые находятся на расстоянии $d(\mathbb{L})$ от \mathbf{v} . Число соседей не зависит от выбора точки \mathbf{v} и обозначается $\tau(\mathbb{L})$, так как, поместив в точку \mathbf{v} и ее соседей шары радиуса $d(\mathbb{L})/2$, мы получим $\tau(\mathbb{L})$ шаров, касающихся центрального шара. Например, для решетки \mathbb{Z}^n ее расстояние равно 1, а число касаний $2n$, что меньше $\tau(n)$ для всех $n \geq 2$. Более того, известно, что $\tau(n)$ при больших n растет экспоненциально, а именно (см. [4])

$$(1.15470\dots)^{n(1+o(1))} \leq \tau(n) \leq (1.32042\dots)^{n(1+o(1))}$$

Сопоставим теперь двоичному линейному коду C длины n решетку \mathbb{L}_C в \mathbb{R}^n

$$\mathbb{L}_C = \{\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n : (x_1 \bmod 2, \dots, x_n \bmod 2) \in C\}.$$

Расстояние этой решетки равно $\min\{2, \sqrt{d}\}$, где $d = d_H(C)$ — это расстояние кода C . В случае $d = 4$ соседи нулевого вектора в этой решетке это векторы, у которых все координаты равны 0, кроме одной, равной ± 2 , и векторы, полученные из векторов кода C веса 4, в которых «двоичные» 1 заменены на ± 1 . Итого имеем $2n + 2^d A_d$ соседей, где A_d — это число слов минимального веса в коде C . Наконец, возьмем в качестве C описанный выше (8, 4) код Хэмминга с $d = 4$ и $A_d = 14$. Получаемая решетка известна как решетка E_8 и число соседей у нее равно $2 \times 8 + 2^4 \times 14 = 240$, что и хотелось получить!

Для построения решетки Лича нам понадобится 1-удлиненный код Голея (обозначается \mathbb{G}_{24}). Это двоичный линейный код длины 24 с расстоянием 8, состоящий из 2^{12} слов (среди них есть и вектор $\mathbf{1}$), из которых 759 слов веса 8. Эти слова веса 8 образуют замечательную комбинаторную конфигурацию, называемую системой Штейнера $S(5, 8, 24)$. А именно, для любых 5-и позиций из 24-х найдется и ровно одно кодовое слово веса 8, имеющее единицы на этих позициях (заметим, что слова минимального веса в (8, 4)-коде Хэмминга, образуют $S(3, 4, 8)$). Решетку $\mathbb{L}_{\mathbb{G}_{24}}$ в \mathbb{R}^{24} , построенную на коде \mathbb{G}_{24} , разобьем на две подрешетки $\mathbb{L}^0 = \{\mathbf{x} \in \mathbb{L}_{\mathbb{G}_{24}} : x_1 + \dots + x_n = 0 \bmod 4\}$ и $\mathbb{L}^1 = \{\mathbf{x} \in \mathbb{L}_{\mathbb{G}_{24}} : x_1 + \dots + x_n = 2 \bmod 4\}$. Тогда решетка Лича $\Lambda_{24} = 2\mathbb{L}^0 \cup \{\mathbf{1} + 2\mathbb{L}^1\}$.

К сожалению, ни одно из многочисленных описаний кода Голея и решетки Лича не позволяет просто, т. е. в рамках данной статьи, получить их основные свойства, в том числе, подсчитать соответствующее контактное число, равное 196560. Поэтому мы отсылаем заинтересовавшегося читателя к книге [5].

3. РЕЦЕПТ

В этой части, мы покажем как работает метод Дельсарта в наиболее общем случае.

Нам понадобятся *положительно определенные функции*.

ОПРЕДЕЛЕНИЕ. Пусть \mathcal{M} — метрическое пространство с функцией расстояния $\tau(x, y)$. Функция $g(\tau)$ (определенная на множестве всех расстояний \mathcal{M}), называется *положительно определенной* на \mathcal{M} , если для любого набора точек x_1, x_2, \dots, x_N и любых чисел u_1, u_2, \dots, u_N выполнено:

$$\sum_{i,j=1}^N g(\tau(x_i, x_j))u_i u_j \geq 0. \quad (3)$$

Иногда удобно рассматривать «непрерывный» вариант этого определения. То есть, потребовать, чтобы для любой непрерывной функции $u(x)$ и меры μ на \mathcal{M}

$$\iint g(\tau(x, y))u(x)u(y) d\mu_x d\mu_y \geq 0.$$

Легко видеть, что если $g_1(t)$ и $g_2(t)$ — положительно определенные функции, то $c_1 g_1(t) + c_2 g_2(t)$ — положительно определенная функция для любых $c_1, c_2 \geq 0$. Из леммы Шура ([9, задача 7.35]) следует, что и произведение двух положительно определенных функций также положительно определенная функция. Но нам это не понадобится в дальнейшем.

ПРИМЕР 1. Если в качестве метрического пространства взять единичную окружность \mathcal{S}^1 с угловым расстоянием, то примерами положительно определенной функции могут служить функции $\cos kt$, где $k \in \mathbb{N}$. В разделе 5 мы дадим ясное объяснение этому факту. Оказывается, что любая положительно определенная функция на окружности является линейной комбинацией с неотрицательными коэффициентами этих функций, а также функции, тождественно равной единице на всей окружности.

Теперь перейдем к самому трюку. Пусть нам удалось найти такие положительно определенную функцию $g(t)$ на пространстве \mathcal{M} и число $c > 0$, что для функции $f(t) = g(t) + c$, выполнено следующее

$$\begin{aligned} f(0) &= 1, \\ f(t) &\leq 0, \text{ при всех } t \geq d. \end{aligned}$$

Рассмотрим набор точек x_i , $i = 1, \dots, N$ в \mathcal{M} таких, что расстояния между любыми двумя точками не меньше d . Давайте оценим сверху максимально возможное количество точек N . Для этого оценим сумму $\sum_{i,j=1}^N f(\tau(x_i, x_j))$ двумя способами.

С одной стороны

$$\sum_{i,j=1}^N f(\tau(x_i, x_j)) = \sum_{i,j=1}^N g(\tau(x_i, x_j)) + cN^2 \geq cN^2, \quad (4)$$

поскольку функция $g(t)$ положительно определена.

С другой стороны

$$\sum_{i,j=1}^N f(\tau(x_i, x_j)) = \sum_{\substack{i,j=1 \\ i \neq j}}^N f(\tau(x_i, x_j)) + \sum_{i=1}^N f(0) \leq N, \quad (5)$$

поскольку расстояние между любыми двумя точками x_i и x_j больше d , а значит $f(\tau(x_i, x_j)) \leq 0$.

Объединяя эти два неравенства, мы получаем, что $N \leq c^{-1}$. Таким образом, нам удалось оценить возможное количество точек в \mathcal{M} на расстоянии d друг от друга. Несмотря на то, что данный план выглядит чересчур абстрактным, он действительно работает, что мы и продемонстрируем в последующих разделах.

4. МНОГОЧЛЕНЫ ГЕГЕНБАУЭРА

И. Шонберг в [18] нашел все положительно определенные функции на сфере. Оказывается, что любая п. о. ф. является линейной комбинацией с неотрицательными коэффициентами многочленов Гегенбауэра (от косинусов углов между точками). Многочлены Гегенбауэра можно определить разными способами. Например, рекуррентно

$$\begin{aligned} G_0^{(n)}(x) &= 1, & G_1^{(n)}(x) &= x, & G_2^{(n)}(x) &= \frac{nx^2 - 1}{n-1}, & \dots, \\ G_k^{(n)}(x) &= \frac{(2k+n-4)xG_{k-1}^{(n)}(x) - (k-1)G_{k-2}^{(n)}(x)}{k+n-3}. \end{aligned} \quad (6)$$

Данные формулы выглядят достаточно непонятными. Геометрический смысл многочленов Гегенбауэра мы объясним в разделе 5. Отметим лишь, что верхний индекс обозначает размерность, которой соответствует данный многочлен. В частности, $G_k^{(2)}(\cos t) = \cos kt$. Так, утверждение из примера 1 обобщается следующим образом.

ТЕОРЕМА 1 (ШОНБЕРГ И. Я. [18]). *Функции имеющие вид*

$$g(t) = \sum_{i=0}^{\infty} a_i G_i^{(n)}(\cos t), \quad a_i \geq 0,$$

являются положительно определенными функциями на сфере.

Обратное тоже верно, любая положительно определенная функция на сфере представляется в таком виде.

К сожалению, все доказательства данной теоремы либо слишком длинны, для того чтобы приводить их здесь полностью, либо используют дополнительные идеи и понятия, которые тоже выходят за пределы освещаемой в статье темы. Хотя в следующем разделе мы попытаемся несколько осветить происходящее с точки зрения гармонического анализа.

Сейчас же приведем здесь доказательство первой (нужной нам) части теоремы 1, использующее так называемую *теорему о сложении*. Доказательство этой теоремы достаточно длинно, но поскольку в дальнейшем нам понадобится положительная определенность не всех многочленов Гегенбауэра, а только некоторых из них, то корректность соответствующих формул можно (теоретически) проверить вручную или на компьютере (практически). Почти все современные математические пакеты, предоставляющие возможность работать с символьными выражениями (MATLAB, Mathematica, Maxima), имеют встроенные библиотеки позволяющие манипулировать стандартными многочленами, в частности с многочленами Гегенбауэра. Итак, сформулируем теорему о сложении.

ТЕОРЕМА 2 (ТЕОРЕМА О СЛОЖЕНИИ).

$$\begin{aligned} G_k^{(n)}(\cos \theta_1 \cos \theta_2 + \sin \theta_1 \sin \theta_2 \cos \varphi) &= \\ = \sum_{s=0}^k m_{n,k,s} G_{k-s}^{(n+2s)}(\cos \theta_1) G_{k-s}^{(n+2s)}(\cos \theta_2) (\sin \theta_1)^s (\sin \theta_2)^s G_s^{(n-1)}(\cos \varphi), \end{aligned} \tag{7}$$

где $m_{n,k,s}$ — некоторые положительные коэффициенты.

ДОКАЗАТЕЛЬСТВО ПЕРВОЙ ЧАСТИ ТЕОРЕМЫ 1. Доказательство будем проводить индукцией по размерности многочленов Гегенбауэра. Как мы уже упоминали в начале этого раздела, $G_k^{(2)}(\cos t) = \cos kt$, что есть положительно определенная функция. Поэтому базу индукции можно считать доказанной.

Пусть точки x_i , $i = 1, \dots, N$, располагаются на сфере \mathcal{S}^n , а z — это отмеченная точка на этой сфере, которую мы будем называть *северным полюсом*. Обозначим через θ_i величину большой дуги, соединяющей x_i и z (то есть расстояние между этими двумя точками). Если φ_{ij} — угол при вершине z в сферическом треугольнике $zx_i x_j$, а x_{ij} — величина дуги $x_i x_j$,

то сферическая теорема косинусов говорит нам следующее:

$$\cos x_{ij} = \cos \theta_i \cos \theta_j + \sin \theta_i \sin \theta_j \cos \varphi_{ij}. \quad (8)$$

Объединим выражения (7) и (8) и получим:

$$\begin{aligned} G_k^{(n)}(\cos x_{ij})u_i u_j &= G_k^{(n)}(\cos \theta_i \cos \theta_j + \sin \theta_i \sin \theta_j \cos \varphi_{ij})u_i u_j = \\ &= \sum_{s=0}^k m_{n,k,s} G_{k-s}^{(n+2s)}(\cos \theta_i) G_{k-s}^{(n+2s)}(\cos \theta_j) (\sin \theta_i)^s (\sin \theta_j)^s u_i u_j \cdot \\ &\quad \cdot G_s^{(n-1)}(\cos \varphi_{ij}) = \\ &= \sum_{s=0}^k m_{n,k,s} w_i^{(s)} w_j^{(s)} G_s^{(n-1)}(\cos \varphi_{ij}), \end{aligned}$$

где $w_i^{(s)} = u_i G_{k-s}^{(n+2s)}(\cos \theta_i) (\sin \theta_i)^s$. Теперь просуммируем данное выражение по всем парам точек

$$\sum_{i,j=0}^N G_k^{(n)}(\cos x_{ij})u_i u_j = \sum_{s=0}^k m_{n,k,s} \sum_{i,j=0}^N w_i^{(s)} w_j^{(s)} G_s^{(n-1)}(\cos \varphi_{ij}). \quad (9)$$

Отметим, что φ_{ij} можно интерпретировать как расстояние между проекциями точек x_i и x_j на экватор, соответствующий точке z . Поэтому, в силу положительной определенности многочленов Гегенбауэра размерности $n-1$,

$$\sum_{i,j=0}^N w_i^{(s)} w_j^{(s)} G_s^{(n-1)}(\cos \varphi_{ij}) \geq 0.$$

Пользуясь этим и тем, что коэффициенты $m_{m,k,s} > 0$, получаем из (9)

$$\sum_{i,j=0}^N G_k^{(n)}(\cos x_{ij})u_i u_j = \sum_{s=0}^k m_{n,k,s} \sum_{i,j=0}^N w_i^{(s)} w_j^{(s)} G_s^{(n-1)}(\cos \varphi_{ij}) \geq 0.$$

5. СФЕРИЧЕСКИЕ ФУНКЦИИ

В этой части мы попытаемся коротко объяснить «природу» многочленов Гегенбауэра. Все утверждения этого раздела мы оставим без доказательств. Заинтересовавшийся читатель, не знакомый с этой областью, может обратиться к [2, 10] или другим книгам за более подробными объяснениями.

Физикам хорошо известны *гармонические функции*, то есть функции, оператор Лапласа от которых тождественно равен нулю. Нас будут интересовать однородные гармонические многочлены $S(x_1, x_2, \dots, x_n)$.

Размерность пространства однородных гармонических многочленов степени k от n переменных равна $c_{k,n} = \binom{n+k-2}{k} + \binom{n+k-3}{k-1}$.

Рассмотрим гильбертово пространство измеримых функций $L^2(\mathcal{S}^{n-1})$ со стандартным скалярным произведением:

$$\langle f, g \rangle = \int f(x)g(x) d\omega_x.$$

Оказывается, любые два однородных гармонических многочлена разной степени ортогональны. Однородные многочлены одинаковой степени, конечно, ортогональными быть не обязаны.

Выберем ортонормированный базис $S_{k,l}$, $l = 1, \dots, c_{k,n}$, в пространстве гармонических многочленов степени k . Можно показать, что объединение этих базисов по всем k будет полным базисом в $L^2(\mathcal{S}^{n-1})$. Именно на этом основано доказательство второй части теоремы 1.

Рассмотрим отображение $\varphi: \mathbb{R}^n \rightarrow \mathbb{R}^{c_{k,n}}$, определенное следующим образом:

$$\varphi_k^{(n)}(x) = (S_{k,1}(x), S_{k,2}(x), \dots, S_{k,c_{k,n}}(x)).$$

Отображение φ переводит единичную сферу в \mathcal{S}^{n-1} в некоторое множество, лежащее на сфере (не единичной) в пространстве $\mathbb{R}^{c_{k,n}}$.

Ключевым свойством данного отображения является то, что расстояние между образами любых двух точек $x, y \in \mathcal{S}^{n-1}$ зависит только от самого расстояния между ними. Таким образом, мы можем выразить скалярное произведение от векторов из образа $\varphi_k^{(n)}(x)(\mathcal{S}^{n-1})$ через скалярное произведение в самом пространстве \mathbb{R}^n .

Многочлены Гегенбауэра — это и есть (нормированное) скалярное произведение в пространстве $\mathbb{R}^{c_{k,n}}$:

$$G_k^n(\langle x, y \rangle) = \frac{\text{area}(\mathcal{S}^{n-1})}{c_{k,n}} \sum_{l=1}^{c_{k,n}} S_{k,l}(x)S_{k,l}(y).$$

Из последней формулы положительная определенность функций $G_k^n(\cos t)$ следует автоматически. Действительно, значение суммы из левой части неравенства (3) будет равно квадрату длины вектора $\sum x_i \varphi(x_i)$, умноженной на соответствующий нормирующий коэффициент.

ПРИМЕР 2 (ПРОДОЛЖЕНИЕ ПРИМЕРА 1). Однородные гармонические многочлены от двух переменных степени k являются линейной комбинацией двух следующих многочленов

$$\begin{aligned} S_{k,1}(x, y) &= \text{Re}(x + iy)^k, \\ S_{k,2}(x, y) &= \text{Im}(x + iy)^k. \end{aligned}$$

Таким образом, отображение $\varphi_k^{(2)}(x)$ переводит точку из \mathcal{S}^1 с координатами $(\cos \alpha, \sin \alpha)$ в точку с координатами $(\cos k\alpha, \sin k\alpha)$. Поэтому, для любых двух точек $x, y \in \mathcal{S}^1$, величина дуги между которыми равна γ , мы получаем

$$\langle \varphi_k^{(2)}(x), \varphi_k^{(2)}(y) \rangle = \cos k\gamma.$$

Получаем ровно то, что и обещали, $G_k^{(2)}(\cos x) = \cos kx$.

6. ОТ ТЕОРИИ К ПРАКТИКЕ

В этом разделе мы покажем как работает метод Дельсарта на конкретных примерах. Мы докажем, что $\tau(8) = 240$ и $\tau(24) = 196560$. Кроме того, покажем, что среди $2n + 1$ векторов в \mathbb{R}^n найдутся два, угол между которыми острый.

Для начала сформулируем результат раздела 3 (соотношения (4) и (5)) в виде следующей леммы (где $x = \cos t$).

ЛЕММА 3 (КЛЮЧЕВАЯ ЛЕММА). *Пусть,*

$$f(x) = c_0 + c_1 G_1^n(x) + \dots + c_k G_k^n(x),$$

где $c_0 > 0$ и $c_i \geq 0$, при $i \geq 1$. Если $f(1) = 1$ и $f(x) \leq 0$ при $x < \cos \varphi$, то на единичной сфере \mathcal{S}^{n-1} нельзя расположить более чем c_0^{-1} точек, расстояния между которыми не меньше φ .

Начнем с последней задачи, обозначенной в начале этого раздела. Сопоставим каждому вектору точку на единичной сфере, соответствующую направлению этого вектора. Рассмотрим многочлен $P(x) = \frac{1}{2}(x^2 + x)$. Данный многочлен неположительный на отрезке $[-1, 0]$ и обнуляется только в точках $x = 0$ и $x = -1$. Если его представить как сумму многочленов Гегенбауэра $G_k^{(n)}(x)$ (см. формулы (6)), получим:

$$P(x) = \frac{1}{2}(x^2 + x) = \frac{1}{2n} + \frac{1}{2}G_1^{(1)}(x) + \frac{n-1}{2n}G_2^{(n)}(x),$$

$c_0 = \frac{1}{2n}$. Таким образом, на единичной сфере в \mathbb{R}^n нельзя расположить более $2n$ точек с попарными расстояниями не меньшими чем 90° . Кроме того, если посмотреть внимательнее на рассуждения в разделе 3, то можно заключить, что $2n$ точек могут располагаться на сфере тогда и только тогда, когда косинус расстояния между ними равен либо 0, либо -1 . Поэтому эти точки суть вершины правильного октаэдра¹⁾.

На самом деле, данная задача несложно решается и обычными геометрическими соображениями. Более того, если в пространстве \mathbb{R}^n выбрано

¹⁾В больших размерностях это тело называют кроссполитопом.

k векторов, где $n + 2 \leq k \leq 2n$, то угол между какими-то двумя всегда будет не больше чем 90° . Причем конфигурации, когда между ними нет острых углов, несложно классифицировать, см. [14]. (Подумайте над тем, как расположить пять точек на двумерной сфере «оптимальным» образом).

Для других же двух задач геометрическое доказательство неизвестно, но они запросто решаются с помощью леммы 3.

Итак, если рассмотреть (предположительное) оптимальное расположение точек на семимерной сфере, то можно заметить, что расстояния между ними принимают следующие значения $\{60^\circ, 90^\circ, 120^\circ, 180^\circ\}$. Косинусы соответствующих углов равны $1/2, 0, -1/2, -1$. Поэтому многочлен для леммы 3 разумно выбрать таким, чтобы он обнулялся в этих значениях и только в них:

$$f(x) = \frac{4}{9}\left(x - \frac{1}{2}\right)x^2\left(x + \frac{1}{2}\right)^2(x + 1).$$

Если разложить данный многочлен по многочленам Гегенбауэра, мы получим:

$$f(x) = \frac{1}{240} + \frac{1}{30}G_1^8(x) + \frac{5}{48}G_2^8(x) + \frac{13}{60}G_3^8(x) + \frac{133}{480}G_4^8(x) + \frac{1}{4}G_5^8(x) + \frac{11}{96}G_6^8(x).$$

Таким образом, $f(x)$ удовлетворяет всем требованиям леммы 3: коэффициенты при разложении многочлена по многочленам Гегенбауэра положительные, а $f(1) = 1$. Получаем, что количество точек на сфере с попарными расстояниями не меньшими чем 60° , не превосходит $c_0^{-1} = 240$. Более того, если уж 240 точек как-то расположились, то набор расстояний между ними обязан принимать одно из следующих значений $\{60^\circ, 90^\circ, 120^\circ, 180^\circ\}$. Благодаря этому можно показать, что такое расположение 240 точек единственно с точностью до вращения.

Для $\tau(24)$ аналогичный многочлен будет следующим

$$f(x) = \frac{128}{405}\left(x - \frac{1}{2}\right)\left(x - \frac{1}{4}\right)^2x^2\left(x + \frac{1}{4}\right)^2\left(x + \frac{1}{2}\right)^2(x + 1).$$

Вот его разложение по многочленам Гегенбауэра:

$$\begin{aligned} f(x) = & \frac{1}{196560} + \frac{1}{8190}G_1^{24}(x) + \frac{1219}{1028160}G_2^{24}(x) + \\ & + \frac{11569}{1909440}G_3^{24}(x) + \frac{249205}{10692864}G_4^{24}(x) + \frac{3289}{51408}G_5^{24}(x) + \\ & + \frac{376487}{2757888}G_6^{24}(x) + \frac{4439}{20672}G_7^{24}(x) + \frac{23345}{88128}G_8^{24}(x) + \\ & + \frac{3335}{15504}G_9^{24}(x) + \frac{20677}{279072}G_{10}^{24}(x). \end{aligned}$$

Как видим, все коэффициенты положительны, $f(1) = 1$, а $c_0^{-1} = 196560$.

7. ПРОБЛЕМА 13 ШАРОВ

По всей видимости, с помощью метода Дельсарта можно решить проблему контактных чисел только в размерностях $n = 2, 8, 24$. Используя компьютер, Д. Штрот [11] проверил этот метод для $\tau(n)$ аж до размерности 161, и нигде не обнаружил таких замечательных равенств, как при $n = 2, 8, 24$.

В этом параграфе мы вкратце остановимся на геометрическом обобщении метода Дельсарта, которое позволяет решить проблемы 13 и 25 шаров, т. е. доказать, что $\tau(3) = 12$ и $\tau(4) = 24$. Доказательства обоих равенств очень похожи, однако технически случай $n = 4$ намного сложнее случая $n = 3$. Поэтому здесь мы разберем только план доказательства случая $n = 3$, опуская технические детали. Подробные доказательства для $n = 3$ и $n = 4$ можно найти в работах [15] и [16] соответственно.

При $n = 3$ многочлены Гегенбауэра $G_k^{(3)}$ являются *многочленами Лежандра* P_k , т. е. $P_k = G_k^{(3)}$. Эти многочлены можно определить как рекуррентно (см. (6)), так и по формуле Родригеса:

$$P_k(t) = \frac{1}{2^k k!} \frac{d^k}{dt^k} (t^2 - 1)^k.$$

Рассмотрим следующий многочлен:

$$f(t) = \frac{2431}{80}t^9 - \frac{1287}{20}t^7 + \frac{18333}{400}t^5 + \frac{343}{40}t^4 - \frac{83}{10}t^3 - \frac{213}{100}t^2 + \frac{t}{10} - \frac{1}{200}.$$

ЛЕММА 4. Пусть $X = \{x_1, x_2, \dots, x_N\} \subset \mathcal{S}^2$. Тогда

$$S(X) := \sum_{i=1}^N \sum_{j=1}^N f(\cos(\varphi_{i,j})) \geq N^2.$$

Здесь $\varphi_{i,j} = \text{dist}(x_i, x_j)$ обозначает сферическое (угловое) расстояние между x_i и x_j .

ДОКАЗАТЕЛЬСТВО. Разложим f по P_k :

$$f = \sum_{k=0}^9 c_k P_k = P_0 + \frac{8}{5}P_1 + \frac{87}{25}P_2 + \frac{33}{20}P_3 + \frac{49}{25}P_4 + \frac{1}{10}P_5 + \frac{8}{25}P_9.$$

Здесь $c_0 = 1$, $c_k \geq 0$, $k = 1, 2, \dots, 9$. По соотношению (4) получаем

$$S(X) = \sum_{k=0}^9 c_k \sum_{i=1}^N \sum_{j=1}^N P_k(\cos(\varphi_{i,j})) \geq \sum_{i=1}^N \sum_{j=1}^N c_0 P_0 = N^2.$$

ЛЕММА 5. Пусть $X = \{x_1, x_2, \dots, x_N\}$ — точки на \mathcal{S}^2 , угловое расстояние $\varphi_{i,j}$ между различными x_i, x_j не меньше 60° . Тогда

$$S(X) = \sum_{i=1}^N \sum_{j=1}^N f(\cos(\varphi_{i,j})) < 13N.$$

Сначала покажем как доказывать главную теорему.

ТЕОРЕМА 6. $\tau(3) = 12$.

ДОКАЗАТЕЛЬСТВО. Предположим, что $X = \{x_1, x_2, \dots, x_N\}$ — такое расположение точек на \mathcal{S}^2 , при котором $N = \tau(3)$. Тогда X удовлетворяет предположениям в леммах. Стало быть, $N^2 \leq S(X) < 13N$. Отсюда $N < 13$, т.е. $N \leq 12$. С другой стороны, мы знаем, что $\tau(3) \geq 12$, т.е. $N = \tau(3) = 12$.

План ДОКАЗАТЕЛЬСТВА ЛЕММЫ 5. 1. Многочлен $f(t)$ для $t_0 \approx 0.5907$ удовлетворяет следующим свойствам (см. рис. 2):

- (i) $f(t)$ — монотонно убывающая функция на отрезке $[-1, -t_0]$.
- (ii) $f(t) < 0$ при $t \in (-t_0, 1/2]$ и $f(-t_0) = 0$.

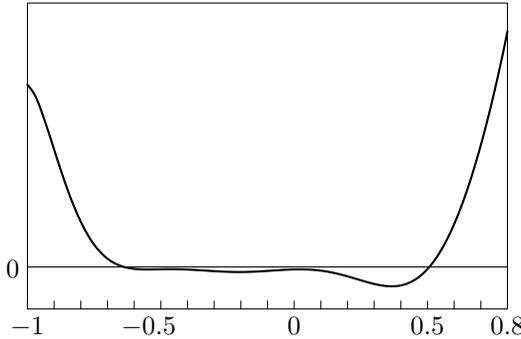


Рис. 2. График функции $f(t)$

Пусть $S_i(X) := \sum_{j=1}^N f(\cos(\varphi_{i,j}))$, тогда $S(X) = \sum_{i=1}^N S_i(X)$. Покажем, что $S_i(X) < 13$ при $i = 1, 2, \dots, N$, отсюда будет следовать, что $S(X) < 13N$.

Поскольку $\varphi_{i,i} = 0$, то $f(\cos \varphi_{i,i}) = f(1)$. По условию $\varphi_{i,j} \geq 60^\circ$, $i \neq j$, и получаем, что $\cos \varphi_{i,j} \leq 1/2$ и $\cos \varphi_{i,j}$ лежит на отрезке $[-1, 1/2]$. Из (ii) следует, что $f(\cos \varphi_{i,j}) \leq 0$ при $\cos \varphi_{i,j} \in [-t_0, 1/2]$. Обозначим $J(i) := \{j : \cos \varphi_{i,j} \in [-1, -t_0]\}$. Мы получили неравенство

$$S_i(X) \leq T_i(X) := f(1) + \sum_{j \in J(i)} f(\cos \varphi_{i,j}).$$

Пусть $\theta_0 = \arccos t_0 \approx 53.794^\circ$. Тогда $j \in J(i)$, если и только если $\varphi_{i,j} > 180^\circ - \theta_0$, т. е. $\theta_j < \theta_0$, где $\theta_j = 180^\circ - \varphi_{i,j}$. Другими словами, все $x_{i,j}$, $j \in J(i)$, лежат внутри сферической шапочки с центром e_0 радиуса θ_0 , где $e_0 = -x_i$ является антиподом точки x_i .

2. Рассмотрим теперь на \mathcal{S}^2 такие точки e_0, y_1, \dots, y_m , что

$$\varphi_{i,j} := \text{dist}(y_i, y_j) \geq 60^\circ, \quad \forall i \neq j, \quad \theta_i := \text{dist}(e_0, y_i) < \theta_0. \quad (10)$$

Обозначим через μ наибольшую величину m такую, что неравенства в (10) определяют непустое множество точек y_1, \dots, y_m .

Предположим, что $0 \leq m \leq \mu$ и $Y = \{y_1, \dots, y_m\}$ удовлетворяют (10). Введем обозначения:

$$H(Y) = H(y_1, \dots, y_m) := f(1) + f(-\cos \theta_1) + \dots + f(-\cos \theta_m),$$

$$h_m := \sup_{Y:|Y|=m} \{H(Y)\}, \quad h_{max} := \max \{h_0, h_1, \dots, h_\mu\}.$$

По определению, $T_i(X) \leq h_m$, где $m = |J(i)|$, и, следовательно, $S_i(X) \leq h_m$. Таким образом, если мы докажем неравенство $h_{max} < 13$, то мы докажем и лемму.

3. Теперь покажем, что $\mu \leq 4$.

Предположим, что $Y = \{y_1, \dots, y_m\} \subset \mathcal{S}^2$ удовлетворяет (10). Можно считать, что e_0 — северный полюс на сфере и у y_j сферические координаты (θ_j, φ_j) . Заметим, что $\theta_i > 0$ при $m \geq 2$. В противном случае расстояние от y_j до всех точек шапочки будет меньше 60° , а значит в ней не могут находиться точки из $J(j)$. Тогда, используя методы элементарной сферической геометрии (сферическую теорему косинусов или неравенство «напротив большего угла лежит большая сторона треугольника»), можно показать, что расстояние между точками с координатами (θ_j, φ_j) и (θ_k, φ_k) будет не больше расстояния между точками (θ_0, φ_j) и (θ_0, φ_k) . Поэтому без ограничения общности можно считать, что все точки y_j лежат на «краю шапочки», то есть окружности с центром e_0 и радиусом θ_0 .

Но на такой окружности можно расположить не более четырех точек с попарным расстоянием не меньшим 60° . Мы пропустим требуемые в этом месте вычисления, впрочем, любой может провести их самостоятельно.

4. Итак, мы должны доказать неравенство

$$h_{max} = \max \{h_0, h_1, h_2, h_3, h_4\} < 13.$$

Несложно видеть, что

$$h_0 = f(1) = 10.11 < 13.$$

Из (i) вытекает что $f(-\cos \theta)$ является монотонно убывающей функцией от $\theta \in [0, \theta_0]$. Тогда при $m = 1$ функция $H(\theta_1) = f(1) + f(-\cos \theta_1)$ достигает максимума при $\theta_1 = 0$. Отсюда

$$h_1 = f(1) + f(-1) = 12.88 < 13.$$

5. Пусть $m = 2, 3, 4$. Рассмотрим оптимальные расположения точек $\{e_0, y_1, \dots, y_m\}$ на \mathcal{S}^2 , которые задают равенства $H(Y) = h_m$.

Заметим, что y_k не могут быть сдвинуты по направлению к e_0 , так как иначе $H(Y)$ увеличится. Используя это наблюдение и еще некоторые несложные геометрические рассуждения, можно показать, что:

при $m = 2$, $e_0 \in y_1 y_2$ и $\text{dist}(y_1, y_2) = 60^\circ$,

при $m = 3$, треугольник $\Delta_3 := y_1 y_2 y_3$ — равносторонний с длиной стороны 60° (как и выше, $e_0 \in \Delta_3$),

при $m = 4$, $\Delta_4 := y_1 y_2 y_3 y_4$ — ромб со стороной 60° и $e_0 \in \Delta_4$.

6. Пункт **5** показывает, что для нахождения h_m , $m = 2, 3, 4$, мы должны найти максимум функции $H(Y)$ на отрезке $[0, 60^\circ]$ ($m = 2$), равностороннем треугольнике Δ_3 ($m = 3$) и ромбе Δ_4 ($m = 4$). Для этого можно использовать стандартные численные методы. Вычисления показывают, что $h_2 \approx 12.8749$, $h_3 \approx 12.8721$, $h_4 \approx 12.4849$, т.е. во всех трех случаях $h_m < h_1 = 12.88 < 13$. В статье [15] эти вычисления были упрощены и, в худшем случае, сводятся к вычислению максимумов функций от одной переменной. Итак, $h_m < 13$ для всех m , как и требовалось.

СПИСОК ЛИТЕРАТУРЫ

- [1] Н. Н. Андреев, В. А. Юдин. *Экстремальные расположения точек на сфере* // Математическое просвещение. Сер. 3, вып. 1. 1997. С. 115–125.
- [2] Н. Я. Виленкин. *Специальные функции и теория представлений групп*. М.: Наука, 1965.
- [3] Ф. Дельсарт. *Алгебраический подход к схемам отношений теории кодирования*. М.: Мир, 1976.
- [4] Г. А. Кабатянский, В. И. Левенштейн. *О границах для упаковок на сфере и в пространстве* // Проблемы передачи информации. Т. 14, вып. 1. 1978. С. 3–25.
- [5] Д. Конвей, Н. Д. А. Слоэн. *Упаковки шаров, решетки и группы*. М.: Мир, 1990.
- [6] В. И. Левенштейн. *О границах для упаковок в n -мерном евклидовом пространстве* // Докл. АН СССР. Т. 245. 1979. С. 1299–1303.

- [7] Х. Маехара. *Проблема тринадцати шаров (элементарный подход)* // Математическое просвещение. Сер. 3, вып. 15. 2011. С. 76–88.
- [8] Ф. Д. Мак-Вильямс, Н. Д. А. Слоэн. *Теория кодов, исправляющих ошибки*. М.: Связь, 1979.
- [9] Г. Поляа, Г. Сеге. *Задачи и теоремы из анализа*. Часть II. М.: Наука, 1978.
- [10] Г. Сеге. *Ортогональные многочлены*. М.: ГИФМЛ, 1962.
- [11] Д. В. Штром. *Метод Дельсарта в задаче об антиподальных контактных числах в евклидовых пространствах больших размерностей* // Известия Уральского государственного университета. Т. 30, вып. 6. 2004. С. 154–182.
- [12] В. А. Юдин. *Минимум потенциальной энергии точечной системы зарядов* // Дискретная математика. Т. 4, вып. 2. 1992. С. 115–121.
- [13] R. W. Hamming. *Error detecting and error correcting codes* // Bell System Technical Journal. Vol. 29, no 2. 1950. P. 147–160.
- [14] W. Kuperberg. *Optimal arrangements in packing congruent balls in a spherical container* // Discrete & Computational Geometry. Vol. 37, no 2. 2007. P. 205–212.
- [15] O. R. Musin. *The kissing problem in three dimensions* // Discrete & Computational Geometry. Vol. 35, no 3. 2006. P. 375–384.
- [16] O. R. Musin. *The kissing number in four dimensions* // Annals of Mathematics. Vol. 168, no 1. 2008. P. 1–32.
- [17] A. M. Odlyzko, N. J. A. Sloane. *New bounds on the number of unit spheres that can touch a unit sphere in n dimensions* // Journal of Combinatorial Theory. Ser. A. Vol. 26, no 2. 1979. P. 210–214.
- [18] I. J. Schoenberg. *Positive definite functions on spheres* // Duke Mathematical Journal. Vol. 9, no 1. 1942. P. 96–108.
- [19] K. Schütte, B. L. Van der Waerden. *Das problem der dreizehn kugeln* // Mathematische Annalen. Bd. 125, Nu 1. 1952. S. 325–334.

А. В. Акопян, Институт проблем передачи информации им. А. А. Харкевича РАН и Ярославский государственный университет им. П. Г. Демидова
Г. А. Кабатянский, Институт проблем передачи информации им. А. А. Харкевича РАН и Московский физико-технический институт (государственный университет)

О. Р. Мусин, Институт проблем передачи информации им. А. А. Харкевича РАН и Ярославский государственный университет им. П. Г. Демидова

Ультраметрики, деревья, потоки и узкие места

М. Н. Вялый

В. А. Гурвич

Между конечными ультраметрическими пространствами, остовами минимального веса на графах, а также потоками и узкими местами в сетях имеются интересные связи, на которых мы и сосредоточимся в этой статье.

Мы начнем с канонического комбинаторного представления конечной ультраметрики (УМ). Вопрос о таком представлении задавал в 90е годы прошлого столетия И. М. Гельфанд. Один из возможных ответов на этот вопрос дается в работах А. Ю. Лемина (см., например, [14]). Мы приводим удобную форму представления УМ монотонными корневыми деревьями. Из этого представления мгновенно следует, например, что УМ на n точках принимает не более $n - 1$ различных значений.

Еще раньше конечные УМ возникли при анализе узких мест (bottle-necks) и потоков в сетях. В знаменитой статье Р. Гомори и Т. Ху [9] доказано, что любая конечная УМ может быть реализована решением потоковой задачи, а Б. Леклерк [13] доказал аналогичное утверждение для задач на узкие места (точные определения см. в разделе 2). Мы опишем эти представления и укажем связь теорем Гомори – Ху и Леклерка с ультраметрическими пространствами сопротивлений (раздел 3).

И задачи на узкие места, и потоковые задачи естественно формулируются для ориентированных графов (когда пропускные способности не симметричны). Вообще, отказ от симметрии — естественное обобщение понятия метрики. Вспомните об одностороннем движении или о том, что объекты могут располагаться на разной высоте. В несимметричном случае возникают *квазиультраметрики* (КУМ). На них мы кратко остановимся в разделе 4, оставляя доказательства читателю в качестве упражнений (иногда непростых).

Объединяет указанные выше две группы задач то, что они совпадают при ограничении на остовные деревья. Поэтому в последнем разделе мы коснемся жадных алгоритмов построения остовных деревьев и приведем общее описание стратегий в таких алгоритмах.

Собственно алгоритмические вопросы не затрагиваются в этой заметке. Читатель может обратиться к имеющимся учебникам, например, [6].

Мы также пропускаем утомительное введение основных понятий теории графов в надежде, что они знакомы читателю. В качестве хорошего учебника по теории графов укажем [5].

1. КАНОНИЧЕСКОЕ ПРЕДСТАВЛЕНИЕ УМ НА КОНЕЧНОМ МНОЖЕСТВЕ

Напомним определения метрики и ультраметрики.

Метрикой на множестве V называется функция $d: V \times V \rightarrow \mathbb{R}_+$, удовлетворяющая следующим свойствам:

- (i) $d(u, w) = 0$ тогда и только тогда, когда $u = w$;
- (ii) $d(u, w) = d(w, u)$ для всех $u, w \in V$;
- (iii) $d(u, w) \leq d(u, v) + d(v, w)$ для всех $u, v, w \in V$.

Ультраметрика (УМ) удовлетворяет свойствам (i), (ii), а свойство (iii) (неравенство треугольника) заменяется на более сильное

- (iii') $d(u, w) \leq \max(d(u, v), d(v, w))$ для всех $u, v, w \in V$.

Нетрудно проверить, что если неравенство в (iii') строгое, то $d(u, v) = d(v, w)$; иначе говоря, в любом треугольнике две самые длинные стороны имеют одинаковую длину. По этой причине УМ иногда называют равнобедренными метриками.

Нас будет интересовать случай УМ на конечном множестве. Оказывается, что все такие УМ описываются следующей конструкцией.

Рассмотрим корневое дерево с множеством вершин T , множеством листьев $V \subseteq T$ и корнем $v_0 \in N = T \setminus V$. Вершины из множества N (т. е. не листья), будем называть *внутренними*. Для каждой вершины $v \in T$ однозначно определен путь $p(v)$ из корня v_0 в вершину v . Вершина u называется потомком вершины v , если $p(v)$ является частью $p(u)$ (а вершина v называется предком u). Для пары вершин u, v определим $a(u, v)$ как самого младшего общего предка u и v . Другими словами, $a(u, v)$ — последняя общая вершина путей $p(u), p(v)$.

Каждой внутренней вершине $v \in N = T \setminus V$ поставим в соответствие положительное действительное число и потребуем, чтобы полученная функция $d: N \rightarrow \mathbb{R}_+$ строго убывала на любом пути из корня. Тогда функция

$$d(u, v) = \begin{cases} d(a(u, v)), & \text{если } u \neq v; \\ 0, & \text{если } u = v. \end{cases} \quad (1)$$

задает УМ на множестве листьев V (см. пример на рис. 1).

Свойства (i) и (ii) выполняются по очевидным причинам. Далее, для любых трех листьев $u, v, w \in V$ хотя бы два из трех самых младших общих предков $u' = a(v, w)$, $v' = a(u, w)$, $w' = a(u, v)$ совпадают (см. рис. 1).

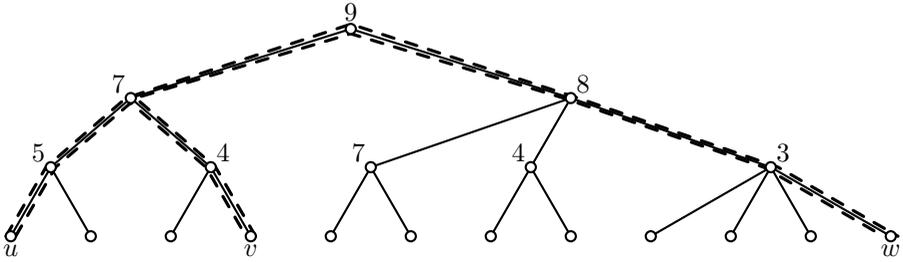


Рис. 1. $d(u, v) = 7, d(v, w) = 9, d(u, w) = 9$

Пусть это будут u' и v' . Тогда w' является потомком $u' = v'$ и поэтому $d(w') \leq d(u')$, откуда следует выполнение ультраметрического неравенства (iii').

Заметим, что число $d(v)$ не играет никакой роли, если внутренняя вершина v имеет всего одного непосредственного потомка. Поэтому потребуем, чтобы их было не менее двух. Тогда представление (1) становится взаимно однозначным соответствием.

ТЕОРЕМА 1. *Любая УМ определяется формулой (1). Входящие в эту формулу дерево и функция на вершинах дерева единственны, с точностью до изоморфизма, если потребовать, чтобы у каждой внутренней вершины дерева было не менее двух непосредственных потомков.*

Будем называть такое представление *каноническим деревом УМ*.

ДОКАЗАТЕЛЬСТВО. Пусть $0 < d_1 < d_2 < \dots < d_k$ — множество всех расстояний УМ (V, d) , упорядоченное по возрастанию.

Для $i \in [k] = \{1, \dots, k\}$ обозначим

$$D_i = \{d_1, \dots, d_i\}, \quad E_i = \{(x, y) \mid d(x, y) \in D_i\}, \quad G_i = (V, E_i).$$

Другими словами, G_i — это граф на множестве точек V , ребра которого отвечают парам точек, которые находятся на расстоянии не больше d_i .

Из ультраметрического неравенства следует, что граф G_i — *транзитивный*, т. е. из $(x, y) \in E_i, (y, z) \in E_i$ следует $(x, z) \in E_i$.

Легко понять, как устроены транзитивные графы. Нетрудно видеть, что любой связный транзитивный граф — это *клика*, т. е. каждые две его вершины соединены ребром. В общем случае транзитивный граф является объединением непересекающихся клик.

Проведем индукцию по числу k различных расстояний. Граф G_k является, очевидно, кликой на V . Таким образом, при $k = 1$ УМ представляется деревом глубины 1, корень которого отвечает G_k , а листья — точкам из V . Легко видеть, что такое представление единственно, так как любое дерево глубины > 1 порождает метрику с $k > 1$.

Предполагая утверждение доказанным для УМ с $k' < k$ различными расстояниями, докажем его для УМ с k различными расстояниями. При $k > 1$ граф G_{k-1} непуст и является объединением $m \geq 2$ непересекающихся клик C_1, \dots, C_m . Иными словами, рёбра длины d_k образуют полный m -дольный граф с долями C_1, \dots, C_m и более нигде не встречаются. Ограничение УМ $d(\cdot, \cdot)$ на клику C_j порождает УМ с меньшим набором значений расстояний.

По предположению индукции для всех таких метрик (C_j, d_j) существует однозначное представление каноническим деревом. Тогда для метрики (V, d) каноническое дерево получается добавлением нового корня (отвечающего клике G_k), к которому присоединены деревья, отвечающие метрикам (C_j, d_j) , $|C_j| \geq 2$, и листья, отвечающие одноточечным кликам C_j . \square

СЛЕДСТВИЕ 1. Пусть (V, d) — УМ на множестве из n точек, принимающая k различных значений. Обозначим через N_d количество внутренних вершин канонического дерева (нелистьев). Тогда

$$k \leq N_d \leq n - 1. \quad (2)$$

Первое неравенство обращается в равенство, если числа, присвоенные всем внутренним вершинам канонического дерева, различны.

Второе неравенство обращается в равенство для бинарного дерева, в котором каждая внутренняя вершина имеет ровно двух потомков.

В частности, из неравенств (2) следует, что УМ принимает не слишком много значений, а именно, не более $n - 1$. В случае метрики общего вида это не так: все попарные расстояния могут быть различными.

2. ДРУГИЕ ПРЕДСТАВЛЕНИЯ УМ

2.1. Остовное дерево и УМ узких мест

Рассмотрим дерево T с множеством вершин V . Ребрам дерева припишем положительные веса, т.е. зададим функцию $d: E \rightarrow \mathbb{R}_+$. Заметим, что любые две вершины u, w дерева соединены в нем единственным путем $p(u, w)$. Определим функцию на парах вершин

$$d_T(u, v) = \begin{cases} \max(d(e) \mid e \in p(u, w)), & \text{если } u \neq v; \\ 0, & \text{если } u = v. \end{cases} \quad (3)$$

УТВЕРЖДЕНИЕ 1. Функция (3) задает УМ.

ДОКАЗАТЕЛЬСТВО. Для любых трех вершин u, v, w дерева найдется единственная вершина o , которая лежит на всех трех путях $p(u, v)$, $p(v, w)$, $p(w, u)$. Эти пути и пути $p(o, u)$, $p(o, v)$, $p(o, w)$ состоят из одних и тех же ребер, причем каждое ребро встречается дважды в первой тройке путей и

один раз — во второй. Без ограничения общности считаем, что среди них ребро самого большого веса лежит на пути $p(o, v)$. Тогда из (3) получаем

$$d(u, v) = d(v, w) \geq d(u, w),$$

откуда следует ультраметрическое неравенство.

Остальные свойства метрики выполняются по очевидным причинам. \square

Метрику вида (3) мы назовем УМ узких мест. Название нуждается в пояснении. Представим, что дерево задает систему коридоров, а веса ребер равны обратным ширинам. Тогда максимальная ширина предмета, который можно протащить из вершины u в вершину v , определяется самым узким коридором на пути $p(u, v)$ и потому равна $d(u, v)^{-1}$.

Верно и обратное: любая УМ может быть представлена как УМ узких мест. Этот факт (как и аналогичное утверждение из следующего подраздела) впервые появился в работе Гомори и Ху [9].

Рассмотрим УМ (V, d) и соответствующий ей полный взвешенный граф $G = (V, E)$, $d: E \rightarrow \mathbb{R}_+$, в котором вес ребра равен расстоянию между концами ребра.

Возьмем любое кратчайшее остовное дерево, т. е. дерево с множеством вершин V («остовное дерево»), вес которого не превосходит веса любого другого остовного дерева. Весом дерева считаем сумму весов его ребер.

ТЕОРЕМА 2. *Метрика d совпадает с метрикой узких мест d_T , порожденной кратчайшим остовным деревом T .*

ДОКАЗАТЕЛЬСТВО. Неравенство $d(u, v) \leq d_T(u, v)$ легко получается по индукции применением ультраметрического неравенства.

Неравенство $d(u, v) \geq d_T(u, v)$ сразу следует из того, что T имеет наименьший возможный вес среди остовных деревьев. \square

Задачу на узкие места можно сформулировать не только для дерева, но и для произвольного графа. Мы приведем формулировку для случая полного графа.

Рассмотрим полный взвешенный граф $G = (V, E)$, $c: E \rightarrow \mathbb{R}_+$. Веса ребер указывают на «ширину» ребра. Шириной пути $p(u, v)$ между двумя вершинами назовем

$$c(p(u, v)) = \min\{c(e) \mid e \in p(u, v)\}$$

ширину самого узкого ребра вдоль пути. Эта величина определяет максимальную ширину «объекта», который можно протащить вдоль пути. Поскольку путей между двумя вершинами много, то максимальная ширина объекта, который можно протащить из u в v равна максимуму ширины по путям из u в v :

$$C(u, v) = \max_{p(u, v)} c(p(u, v)). \quad (3')$$

УТВЕРЖДЕНИЕ 2. Функция $d_b(u, v) = C(u, v)^{-1}$ при $u \neq v$, $d_b(u, u) = 0$, является УМ.

ДОКАЗАТЕЛЬСТВО. Если объект можно протащить из u в v и из v в w , то его, конечно же, можно протащить из u в w . Значит, для ширины между двумя вершинами выполняется неравенство

$$C(u, w) \geq \min(C(u, v), C(v, w))$$

для всех $u, v, w \in V$.

Переходя к обратным величинам, получаем ультраметрическое неравенство для функции d_b . Остальные свойства метрики очевидны. \square

УМ, заданную в утверждении 2, также будем называть УМ узких мест.

УТВЕРЖДЕНИЕ 3 ([13]). Любая УМ может быть реализована как УМ узких мест на полном взвешенном графе.

ДОКАЗАТЕЛЬСТВО. В силу теоремы 2 достаточно проверить, что УМ узких мест на остовном дереве реализуется. Для этого достаточно приписать ребрам дерева ширины, равные $d(e)^{-1}$, а ширины ребер, не входящих в дерево, положить равными достаточно малому числу (меньшему, минимальной ширины ребер дерева). \square

ЗАМЕЧАНИЕ. Аналогично можно определить УМ узких мест на любом взвешенном графе $G = (V, E)$, $c: E \rightarrow \mathbb{R}_+$. Для перехода к случаю полного взвешенного графа нужно положить ширину ребер полного графа, не входящих в E , равной достаточно малому числу.

2.2. ПОТОКИ НА ГРАФАХ

Опять рассмотрим взвешенный граф (V, E) , $c: E \rightarrow \mathbb{R}_+$, но теперь вес ребра $c(u, w)$ будем называть *пропускной способностью* и считать, что он указывает наибольшее количество *материала*, которое можно пересылать по ребру в единицу времени в одном направлении. Под «материалом», в отличие от «объекта» из предыдущего раздела, мы понимаем сколь угодно делимую субстанцию: вода, нефть или газ дают примеры «материалов» из реальной жизни. Для пары вершин u, w , не связанных ребром в графе, полагаем $c(u, w) = 0$.

При такой интерпретации *пропускной способностью* пути $p(u, w)$ из вершины u в вершину w естественно опять считать минимум пропускных способностей ребер вдоль пути $c(p(u, w)) = \min\{c(e) \mid e \in p(u, w)\}$.

Определение пропускной способности между вершинами теперь будет другим. Если «объекты» из предыдущего раздела были неделимы, так что перетаскивать их можно было по какому-то определенному пути, то «материал» можно дробить и посылать разными маршрутами.

Поэтому введем понятие *потока* из u в w , т. е. функции $f: V \times V \rightarrow \mathbb{R}_+$ которая удовлетворяет следующим условиям

- (i) $f(x, y) \leq c(x, y)$;
- (ii) $\sum_x f(x, v) = \sum_y f(v, y)$, для всех $v \notin \{u, w\}$.

Первое условие означает, что по ребру течет не больше возможного. Второе условие выражает закон сохранения транспортируемого материала. В случае электрических сетей это заряд. Тогда говорят о первом законе Кирхгофа. Оно означает, что во внутренних вершинах выполняется закон сохранения: сколько материала поступает в вершину, столько же его и отправляется дальше.

Величиной потока называется разность

$$C_f(u, w) = \sum_y f(u, y) - \sum_x f(x, u),$$

которая определяет, сколько материала отправляется из u .

УПРАЖНЕНИЕ 1. *Докажите, что такое же количество материала поступает в w , т. е.*

$$C_f(u, w) = \sum_y f(y, w) - \sum_x f(w, x).$$

Теперь можно определить пропускную способность $C(u, w)$ между вершинами u и w как максимальную величину потока $C_f(u, w)$ из u в w . Следующий факт был замечен в работе Гомори и Ху [9].

УТВЕРЖДЕНИЕ 4. *Для любых u, v, w выполняется неравенство*

$$C(u, w) \geq \min(C(u, v), C(v, w)).$$

СЛЕДСТВИЕ 2. *Функция $d_f(u, w) = C(u, w)^{-1}$ при $u \neq w$, $d_f(u, u) = 0$ является УМ. (Будем называть такую УМ *потокковой*.)*

Эти утверждения аналогичны утверждениям из предыдущего раздела об УМ узких мест. Но теперь простое рассуждение «если объект можно протащить из u в v и из v в w , то его можно протащить из u в w » не проходит, поскольку в результате сложения потоков из u в v и из v в w пропускная способность какого-нибудь ребра может оказаться превышенной. На помощь приходит знаменитая теорема Форда – Фалкерсона о максимальном потоке и минимальном разрезе.

Разрезом, разделяющим вершины u и w , назовем такое разбиение множества вершин V на два множества U, W , что $u \in U, w \in W$. *Весом разреза* назовем сумму весов ребер между U и W (т. е. таких ребер, что один конец ребра принадлежит множеству U , а другой — множеству W).

ТЕОРЕМА ФОРДА – ФАЛКЕРСОНА. *Наибольший поток между u и w равен наименьшему весу разреза, разделяющего u и w .*

Мы не приводим доказательства этой теоремы. Они имеются во многих книгах. Укажем на [6], где доказательство вытекает из анализа алгоритма построения максимального потока, и на короткую брошюру одного из авторов [1], в которой теорема Форда – Фалкерсона возникает как частный случай теоремы двойственности в линейном программировании.

ДОКАЗАТЕЛЬСТВО УТВЕРЖДЕНИЯ 4. Рассмотрим любой разрез (U, W) минимального веса, разделяющий u и w . Ясно, что та же пара множеств U и W разделяет v и w (соответственно, u и v), если $v \in U$ (соответственно, $v \in W$). В обоих случаях выполняется неравенство $C(u, w) \geq \geq \min(C(u, v), C(v, w))$. \square

Из утверждения 4 и следствия 1 получаем такое наблюдение.

СЛЕДСТВИЕ 3. *Максимальные потоки на графе с n вершинами принимают не более $n - 1$ различного значения.*

ЗАМЕЧАНИЕ. Это наблюдение оказывается полезным, когда надо найти максимальные потоки сразу между всеми парами вершин.

УТВЕРЖДЕНИЕ 5. *Любая УМ может быть реализована как метрика обратных пропускных способностей.*

ДОКАЗАТЕЛЬСТВО. Достаточно заметить, что для дерева узкие места и потоки совпадают. Поэтому, реализовав УМ как УМ узких мест на дереве (теорема 2), получаем также и ее представление в виде потоковой УМ. (Ребрам, не входящим в дерево, нужно приписать нулевые пропускные способности.)

3. ЕЩЕ РАЗ О МЕТРИКАХ СОПРОТИВЛЕНИЙ

И УМ узких мест, и потоковая УМ являются частным случаем метрик сопротивлений (см. [2, 4]).

Напомним, как строятся метрики сопротивлений. Пусть каждое ребро $e \in E$ связного графа (сети) $G = (V, E)$ представляет собой проводник со степенным законом проводимости

$$y_e^* = y_e^r / \mu_e^s.$$

Здесь y_e — напряжение, y_e^* — ток, а μ_e — сопротивление ребра e . Положительные действительные параметры r и s одинаковы для всех ребер сети. Первый параметр определяется физикой сети. Например, $r = 1$ отвечает закону Ома, а $r = 0.5$ — типичный для гидро- или газовой динамики

квадратичный закон сопротивления. Хотя от параметра s (в отличие от r) можно было бы легко избавиться, но он тоже будет играть важную роль.

Нетрудно видеть, что для любых двух вершин $u, w \in V$ двухполосная схема (G, u, w) удовлетворяет тому же закону проводимости $y_{u,w}^* = y_{u,w}^r / \mu_{u,w}^s$, где $y_{u,w}^*$ — полный ток, а $y_{u,w}$ напряжение между u и w . Здесь $\mu_{u,v}$ — *эффективное сопротивление* схемы (G, u, w) . Другими словами, (G, u, w) можно заменить на одно ребро $e = (u, w)$ с сопротивлением $\mu_{u,w}$ для тех же самых значений параметров r и s . В силу изотропности законы проводимости симметричны и $\mu_{u,w} = \mu_{w,u}$, ясно также, что $\mu_{u,w} > 0$ при $u \neq w$. Для удобства полагаем по определению $\mu_{u,u} = 0$.

В [2] доказано неравенство

$$\mu_{u,w}^{s/r} \leq \mu_{u,v}^{s/r} + \mu_{v,w}^{s/r}. \quad (4)$$

для произвольных трех вершин u, v, w .

В [3] было также показано, что равенство в (4) достигается тогда и только тогда, когда v лежит на любом пути из u в w . Более подробно эти результаты обсуждаются в [4, 10].

Легко видеть, что при $s \geq r$ (4) дает обычное неравенство треугольника $\mu_{u,w} \leq \mu_{u,v} + \mu_{v,w}$, а при $s/r \rightarrow \infty$ получается ультраметрическое неравенство $\mu_{u,w} \leq \max(\mu_{u,v}, \mu_{v,w})$.

УМ узких мест и потоковая УМ получаются как предельные случаи. Пусть $r = r(t)$ и $s = s(t)$ зависят от действительного параметра t , $t \rightarrow \infty$. Тогда метрика узких мест отвечает предельному случаю $s(t) \rightarrow \infty$ и $r(t) \equiv 1$, а метрика обратных пропускных способностей — случаю $s(t) \equiv 1$ и $r(t) \rightarrow 0$.

В [4] для метрики электрических сопротивлений ($r = 1, s = 1$) было показано, что для каждой k -полосной схемы с n вершинами существует эквивалентная ей k -полосная схема с k вершинами.

Приведенные выше реализации любой УМ как УМ узких мест или потоковой УМ (утверждения 3 и 5) показывают, что аналогичный результат справедлив для предельных случаев $s(t) \rightarrow \infty, r(t) \equiv 1$ и $s(t) \equiv 1, r(t) \rightarrow 0$.

В общем случае это утверждение не имеет места.

ЗАДАЧА 1. *Докажите, что для некоторых r, s существует 3-полосная схема с 4 вершинами, которая не эквивалентна никакой 3-полосной схеме с 3 вершинами.*

4. НЕСИММЕТРИЧНЫЙ СЛУЧАЙ: КВАЗИУЛЬТРАМЕТРИКИ

Квазиультраметрика (КУМ) удовлетворяет свойствам (i) и (iii'), т. е. в этом случае функция $d(x, y)$ не обязательно симметрическая.

Для КУМ справедливы аналоги основных утверждений, которые приводились выше в симметрическом случае.

Вместо обычных графов, ребра которых не имеют направления, теперь нужно рассматривать ориентированные графы (орграфы). Дуга (ребро) в орграфе (u, v) имеет начало u и конец v . В полном ориентированном графе дугами являются все упорядоченные пары вершин.

Рассмотрим каноническое представление КУМ. По-прежнему справедливо утверждение о транзитивности графа, дуги которого отвечают парам точек на расстоянии не больше d_i . Орграф называется транзитивным, если (u, w) — дуга всякий раз, когда найдется такая вершина v , что (u, v) и (v, w) — дуги.

Транзитивные орграфы задают отношения частичного порядка, точнее говоря предпорядка. Имеется несколько классов эквивалентных вершин (любая пара которых соединена дугой), а между классами — частичный порядок (т. е. дуга идет из u в w всякий раз, когда $u \in U, w \in W$ и $U < W$).

ЗАДАЧА 2. Взвешенный орграф задает КУМ тогда и только тогда, когда для любого t транзитивен орграф, образованный всеми дугами, веса которых не превосходят t .

Разумеется, можно ограничиться порогами, соответствующими попарным расстояниям. Вспомним, что расстояния в n -элементной УМ принимают $k \leq n - 1$ различных значений и эта оценка точна. Для КУМ также имеется аналогичная точная оценка, но она гораздо слабее.

ЗАДАЧА 3. Докажите, что расстояния в n -элементной КУМ принимают $k \leq (1/2)(n - 1)(n + 2)$ различных значений и эта оценка точна.

ЗАМЕЧАНИЕ. В [8] показано, что равенство может достигаться даже на потоковых КУМ.

Задача на узкие места и задача о максимальном потоке формулируются для несимметрического случая совершенно так же и, более того, несимметричные формулировки более естественны (вспомним об улицах с односторонним движением). В этом случае вместо УМ получаются КУМ.

На КУМ узких мест обобщается утверждение 3.

ЗАДАЧА 4. Докажите, что любая КУМ реализуется как КУМ узких мест.

А вот на потоковые КУМ утверждение 5 не распространяется. На рис. 2 приведен простой пример (веса не указанных на рисунке дуг равны достаточно большому числу, для определенности 10).

УПРАЖНЕНИЕ 2. Проверьте, что граф на рис. 2 задает КУМ. Докажите, что она не реализуется как потоковая КУМ.

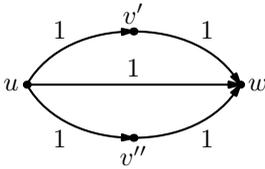


Рис. 2.

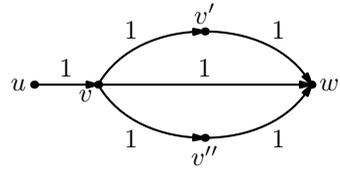


Рис. 3.

Заметим, что потоковая КУМ получится, если заменить $d(u, w) = 1$ на любое $d(u, w) \in [0, 1/2]$. Если же заменить на $d(u, w) > 1/2$, то получится не потоковая КУМ.

Однако любая КУМ является подпространством некоторой потоковой КУМ, т. е. может быть реализована многополусной потоковой сетью, в которой полюсы — элементы КУМ, а все остальные вершины — транзитные, в них выполняется закон сохранения материала.

УПРАЖНЕНИЕ 3. Проверьте, что потоковая КУМ, определенная графом на рис. 3, при ограничении на множество $\{u, v', v'', w\}$ дает КУМ на рис. 2.

Вообще, КУМ на рис. 2 играет особую роль.

ЗАДАЧА 5. Если расстояния в КУМ принимают всего два значения 1 и ∞ , то эта КУМ потоковая тогда и только тогда, когда она не содержит индуцированной подсети, изоморфной сети на рис. 2.

ЗАДАЧА 6. Опираясь на результат задачи 5, постройте алгоритм, который проверяет, является ли данная КУМ потоковой, и предъявляет соответствующую потоковую сеть в случае положительного ответа.

ЗАДАЧА 7. Докажите, что любая КУМ реализуется как ограничение потоковой КУМ на часть вершин.

Указание: используйте критерий задачи 2.

5. О ЖАДНЫХ АЛГОРИТМАХ ПОСТРОЕНИЯ ОСТОВА НАИМЕНЬШЕГО ВЕСА

Теорема 2 обобщается на УМ узких мест на любом (связном) взвешенном графе.

УТВЕРЖДЕНИЕ 6. УМ d_b узких мест, заданная связным взвешенным графом $G = (V, E)$, совпадает с УМ d_T остовного дерева T наименьшего веса в графе G .

ДОКАЗАТЕЛЬСТВО. Если в графе G нет циклов, то это дерево и утверждение выполняется тривиальным образом.

В противном случае выберем некоторый цикл C в графе G и ребро e максимального веса в графе G . Обозначим через G' граф, который получается из G выбрасыванием ребра e . Докажем, что УМ узких мест для графов G и G' совпадают. Тогда утверждение будет следовать по индукции.

С одной стороны $d_{b,G'}(u, v) \geq d_{b,G}(u, v)$: минимум берется по меньшему множеству путей. С другой стороны, $d_{b,G'}(u, v) \leq d_{b,G}(u, v)$: на любом пути замена ребра e на $C \setminus \{e\}$ не увеличивает веса пути. \square

В доказательстве утверждения 6 фактически описана стратегия построения остовного дерева наименьшего веса: на каждом шаге удаляем из графа ребро, которое имеет максимальный вес на некотором цикле. Алгоритмы подобного типа называются «жадными». В большинстве случаев жадные алгоритмы не дают оптимального решения. Однако есть несколько важных исключений и построение остовного дерева наименьшего веса — одно из них.

Поскольку количество ребер в дереве намного меньше общего количества ребер в полном графе ($n - 1$ и $n(n - 1)/2$ соответственно), остовное дерево обычно строят добавлением ребер, а не удалением. В этом случае также применимы жадные стратегии. Есть несколько алгоритмов, основанных на таких стратегиях, например, алгоритмы Борувки [7], Краскала [12], Прима [15].

Опишем общую схему таких алгоритмов. Перед началом каждого шага имеется граф без циклов (лес) F , который является частью некоторого остовного дерева наименьшего веса. Шаг состоит в добавлении к этому графу нового ребра так, чтобы расширенный граф F' удовлетворял тем же самым условиям. Оказывается, верно следующее общее утверждение.

УТВЕРЖДЕНИЕ 7. Пусть лес F состоит из деревьев F_1, \dots, F_m и является частью остовного дерева наименьшего веса. Тогда для любой i выполняется следующее: если добавить к F ребро наименьшего веса, соединяющее вершину из F_i и вершину не из F_i , то полученный лес F' также является частью некоторого остовного дерева минимального веса.

ДОКАЗАТЕЛЬСТВО. В любом остовном дереве есть рёбра, соединяющие вершины из F_i с вершинами не из F_i . Если веса всех этих ребер больше минимального веса ребра в разрезе (F_i, \bar{F}_i) , то добавление ребра минимального веса в этом разрезе и удаление одного из имеющихся ребер остовного дерева дают уменьшение веса.

СПИСОК ЛИТЕРАТУРЫ

- [1] Вялый М. Н. *Линейные неравенства и комбинаторика*. М.: МЦНМО. 2003.
- [2] Гвишиани А. Д., Гурвич В. А. *Метрические и ультраметрические пространства сопротивлений* // УМН, 1987. Т. 42, вып. 6. С. 187–188.
- [3] Гвишиани А. Д., Гурвич В. А. *Динамические задачи классификации и выпуклое программирование в приложениях*. М.: Наука. 1992.
- [4] Гурвич В. А. *Метрические и ультраметрические пространства сопротивлений* // Математическое просвещение. Сер. 3, вып. 13. 2009. С. 134–141.
- [5] Емеличев В. А., Мельников О. И., Сарванов В. И., Тышкевич Р. И. *Лекции по теории графов*. М.: Наука. 1990.
- [6] Кормен Т., Лейзерсон Ч., Ривест Р. *Алгоритмы: построение и анализ*. М.: МЦНМО. 2000.
- [7] Borůvka, O. *O jistém problému minimálním* (Об одной задаче минимизации, на чешском с немецкой аннотацией) // Práce mor. přírodověd. spol. v Brně III, 3. 1926. S. 37–58.
- [8] Frank H., Frisch I. T. *Communication, Transmission, and Transportation Networks*. Reading, MA: Addison-Wesley. 1971.
- [9] Gomory R. E., Hu T. C. *Multi-terminal network flows* // J. SIAM, vol. 9, no 4. 1961. P. 551–570.
- [10] V. Gurvich. *Metric and ultrametric spaces of resistances* // Discrete Appl. Math., vol. 158, 2010. P. 1496–1505.
- [11] Gurvich V., Vyalyi M. *Characterization of (quasi-)ultrametric finite spaces in terms of (directed) graphs*. RUTCOR research report. RRR-7-2011, 2011.
- [12] Kruskal J. B. *On the Shortest Spanning Subtree of a Graph and the Traveling Salesman Problem* // Proceedings of the American Math. Soc. Vol. 7, no 1. 1956. P. 48–50.
- [13] Leclerc B. *Description combinatoire des ultrametriques* // Centre de Mathematique Sociale, Ecole Pratique des Hautes Etudes Mathematiques et Sciences Humaines. Vol. 73. 1981. P. 5–37.

- [14] Lemin A. J. *The category of ultrametric spaces is isomorphic to the category of complete, atomic, tree-like, and real graduated lattices LAT** // Algebra Universalis, vol. 50, no 1. 2003. P. 35-49.
- [15] Prim R. C. *Shortest connection networks and some generalizations* // Bell System Technical Journal, vol. 36. 1957. P. 1389–1401.

Об асимптотике эргодических перестановок Арнольда

Д. А. Байгушев

В данной заметке исследуется специальный класс перестановок, введенный В. И. Арнольдом в 1958 г. для упрощения задачи о перекладывании отрезков.

В 1958 г. на своем семинаре В. И. Арнольд поставил следующую задачу (так называемую *задачу о перекладывании отрезков*; см. [1]). Разобьем отрезок $[0, 1]$ на три непустые части $\{A, B, C\}$ и переложим их в порядке $\{C, B, A\}$. *Исследовать получившуюся динамическую систему на отрезке $[0, 1]$.*

Эта задача активно изучалась, в результате чего были обнаружены связи этой задачи с самыми разными разделами математики (см., например, [4]).

Но в то же время осталась без внимания другая задача Арнольда, поставленная на том же семинаре (см. [3]): *исследовать дискретный аналог задачи о перекладывании отрезков*; в частности, *исследовать дискретные аналоги динамических систем со всюду плотными траекториями.*

Естественно считать, что дискретным аналогом перекладывания отрезков является перекладывание конечного множества точек, т. е. *перестановка*. Более точно, рассмотрим множество $\{1, 2, \dots, n\}$. Разобьем его на три непустых блока $\{A, B, C\}$ размеров a , b и c соответственно и переставим их в порядке $\{C, B, A\}$. Получившуюся перестановку мы будем называть (C, B, A) -*перестановкой* (или *перестановкой Арнольда*) и будем обозначать ее через $\sigma(a, b, c)$.

Перестановки можно рассматривать как динамические системы на конечном пространстве. Одним из важных свойств динамической системы является плотность ее траекторий. В случае перестановок это условие означает, что перестановка состоит из одного цикла. Такие перестановки мы будем называть *эргодическими*.

Основной целью данной заметки является исследование эргодических перестановок Арнольда. А именно, мы докажем критерий, позволяющий определить эргодичность перестановки Арнольда, зная размеры блоков A ,

B и C , а также вычислим асимптотику доли эргодических перестановок Арнольда (задача 8 из [3]).

ЗАМЕЧАНИЕ 1. Отметим, что доля эргодических перестановок среди всех перестановок длины n равна $1/n$ и стремится к 0 при $n \rightarrow \infty$.

Для изучения эргодических перестановок Арнольда нам понадобится следующее определение.

ОПРЕДЕЛЕНИЕ. Назовем шагами перестановки σ величины $\sigma(i) - i$, где $i = 1, \dots, n$.

Отметим, что в (C, B, A) -перестановках возможны всего три шага, которые мы обозначим через S_C , S_B и S_A соответственно. А именно, S_C — шаг, на который увеличивается число, переходящее в число из блока C , S_B — из блока B и S_A — из блока A .

Легко видеть, что

$$S_C = a + b, \quad S_B = a - c, \quad S_A = -b - c.$$

Кроме того, $S_B = S_A + S_C$.

ТЕОРЕМА 1 (КРИТЕРИЙ ЭРГОДИЧНОСТИ). *Перестановка Арнольда $\sigma(a, b, c)$ эргодична тогда и только тогда, когда $\text{НОД}(S_A, S_C) = 1$.*

ДОКАЗАТЕЛЬСТВО. « \Rightarrow » Если $\text{НОД}(S_A, S_C) = d \neq 1$, то, передвигаясь по циклу перестановки $\sigma(a, b, c)$ с шагами S_A , S_B и S_C , мы не сможем попасть из 1 в 2, так как мы будем попадать только в числа, сравнимые с 1 по модулю d .

« \Leftarrow » Рассмотрим какой-либо цикл перестановки $\sigma(a, b, c)$. Пройдя по нему один раз, мы получим: $xS_A + yS_B + zS_C = 0$ (здесь x — количество шагов S_A в цикле, y — количество шагов S_B и z — количество шагов S_C).

Подставив в это равенство значения шагов, получаем: $(x + y)(b + c) = (y + z)(a + b)$.

Так как $\text{НОД}(a + b, b + c) = 1$, то

$$\begin{cases} x + y \geq a + b, \\ y + z \geq b + c. \end{cases}$$

Сложим два получившихся неравенства: $x + 2y + z \geq a + 2b + c$.

Так как $y \leq b$, то $x + y + z \geq a + b + c = n$, т. е. длина цикла не меньше n . Но это означает, что она в точности равна n , и перестановка $\sigma(a, b, c)$ эргодична.

ТЕОРЕМА 2. *Доля эргодических перестановок Арнольда асимптотически равна $6/\pi^2 \approx 0,608$ (рис. 1).*

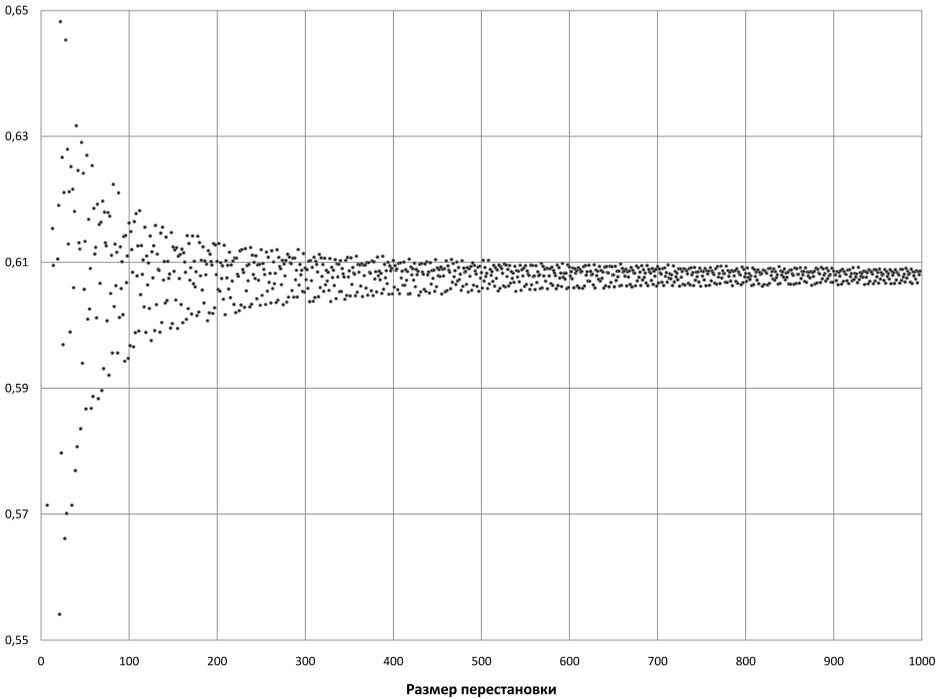


Рис. 1. Доли эргодических перестановок Арнольда

ДОКАЗАТЕЛЬСТВО. Рассмотрим перестановку Арнольда $\sigma(a, b, c)$. Положим $x := b + c = n - a$ и $y := a + b = n - c$. Тогда множество перестановок Арнольда соответствует множеству точек

$$\Delta_n = \{(x, y) \in \mathbb{Z}^2 : x < n, y < n, x + y > n\}.$$

В то же время согласно критерию эргодичности множество эргодических перестановок Арнольда соответствует множеству точек в Δ_n со взаимно простыми координатами.

Таким образом, нам необходимо вычислить долю точек в Δ_n со взаимно простыми координатами при $n \rightarrow \infty$. Для этого мы воспользуемся следующей теоремой.

ТЕОРЕМА 3 (Арнольда о равномерной распределенности [2]). *Множество целочисленных точек со взаимно простыми координатами равномерно распределено на плоскости (рис. 2), т. е. число точек этого множества в гомотетично растянутой в N раз области плоскости становится асимптотически пропорциональным произведению площади*

этой области на число N^2 при $N \rightarrow \infty$. Коэффициент этой пропорциональности (плотность) оказывается равным $1/\zeta(2) = 6/\pi^2$.

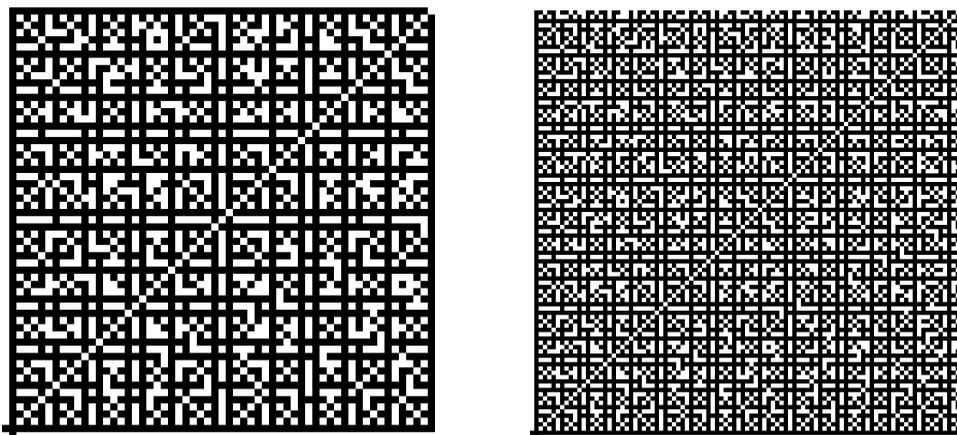


Рис. 2. Равномерное распределение: черным цветом показаны точки со взаимно простыми координатами, а белым — остальные

Применим теорему Арнольда о равномерной распределенности к выпуклым оболочкам множеств Δ_n . Их площади асимптотически равны $|\Delta_n|$, поэтому доля точек в Δ_n со взаимно простыми координатами асимптотически (при $n \rightarrow \infty$) равна $1/\zeta(2) = 6/\pi^2$, что и требовалось доказать.

В заключение отметим, что теорема 2 хорошо подтверждается численными экспериментами (см. таблицу).

| | | | | |
|---|-----------------|-----------------|-----------------|-----------------|
| размер перестановки | 10 | 10^2 | 10^3 | 10^4 |
| всего (C, B, A)-перестановок | 36 | 4851 | 498501 | 49985001 |
| эргодических (C, B, A)-перестановок | 24 | 2964 | 303392 | 30389486 |
| доля эргодических (C, B, A)-перестановок | 0,666667 | 0,611008 | 0,608609 | 0,607972 |
| константа $6/\pi^2$ | 0,607927 | 0,607927 | 0,607927 | 0,607927 |

Автор благодарит П. В. Бибикова за постановку задачи и внимание к работе.

СПИСОК ЛИТЕРАТУРЫ

- [1] Арнольд В.И. *Задачи Арнольда*. М.: ФАЗИС, 2000 г.
- [2] Арнольд В.И. *Равномерное распределение неделимых векторов в целочисленном пространстве* // Изв. РАН. Сер. матем. Т. 79, №1. 2009. С. 21–29.
- [3] Арнольд В.И. *Что такое математика?* М.: МЦНМО, 2008 г.
- [4] Каток А.Б., Синай Я.Г., Степин А.М. *Теория динамических систем и общих групп преобразований с инвариантной мерой* // Итоги науки и техн. Сер. Мат. анализ. Т. 13. ВИНТИ, М., 1975. С. 129–262.

Четырехвалентные графы с крестовой структурой. Вложения в двумерные поверхности

В. О. Мантуров

В предыдущей статье [7] было рассказано о критерии планарности четырехвалентных графов с крестовой структурой. В настоящей работе мы расскажем об обобщении этой задачи: приведем алгоритмы распознавания вложимости графов с крестовой структурой в сферу, проективную плоскость и бутылку Клейна, а также переформулируем задачу для произвольных поверхностей в терминах одной задачи о матрицах над полем из двух элементов.

Одним из важнейших классов графов является класс *крестовых графов*: таковыми мы будем называть четырехвалентные графы, у которых в каждой вершине указывается разбиение четырех полурёбер, инцидентных каждой вершине графа, на две пары «противоположных». Понятие противоположности будет важно при вложениях крестовых графов в поверхность: будем говорить, что вложение графа в двумерную поверхность *согласовано с крестовой структурой*, если полурёбра, противоположные в вершине, являются противоположными на поверхности. Любой четырехвалентный граф, вложенный в поверхность, естественным образом наследует из этой поверхности крестовую структуру. Будем называть не противоположные полурёбра, инцидентные одной вершине, *соседними*.

Отметим, что все используемые в настоящей работе понятия, могут быть определены как комбинаторно, так и топологически. Более того, все утверждения относительно оснащенных четырехвалентных графов можно переформулировать на языке хордовых диаграмм. Этот подход используется в работе Д. П. Ильютко в настоящем сборнике [3]. Дело в том, что результаты работы Д. П. Ильютко позволяют сделать утверждения о матрицах, которые не соответствуют никаким топологическим объектам. Хотя хордовые диаграммы соответствуют оснащённым четырехвалентным графам и кодируются матрицами пересечения, такое кодирование неоднозначно: одной матрице могут соответствовать разные хордовые диаграммы, более того, существуют матрицы, которым хордовые диаграммы не соответствуют. Это позволило Д. П. Ильютко доказать более общие результаты, напрямую не связанные с графами на плоскости и в двумерных поверхностях.

На протяжении всей статьи графы подразумеваются связными и конечными; петли и кратные ребра допускаются (иногда графы с петлями и кратными ребрами называют *мультиграфами*).

ЗАМЕЧАНИЕ. Для определения валентности графа в вершине удобно ввести понятие *полуребра*. Добавляя на каждом ребре графа по новой вершине, мы получим разбиение ребер на *полурёбра*. Полурёбра удобны для подсчета валентности вершин графа: если вершина исходного графа инцидентна некоторому ребру дважды, то это значит, что на преобразованном графе эта вершина инцидентна двум разным полуребрам.

В работе [4] (см. также [7]) была доказана следующая теорема (выдвинутая В. А. Васильевым в качестве гипотезы в [1]).

ТЕОРЕМА 1. *Граф не вложим в плоскость тогда и только тогда, когда у него имеются два цикла без общих ребер, обладающие единственной точкой перекрестья.*

Здесь *циклом* мы называем непрерывное отображение окружности в граф, взаимно однозначное вне прообразов вершин графов. Этим мы подчеркиваем, что в цикле каждое ребро встречается не более одного раза. Мы говорим, что два цикла без общих ребер имеют *перекрестье* в некоторой вершине v , если один из них содержит одну пару противоположных полуребер в этой вершине, а другой — вторую. При этом в формулировке теоремы не накладывается никаких ограничений на количество (нетрансверсальных) пересечений двух циклов. Далее мы будем называть *препятствием Васильева* два цикла без общих ребер, имеющие единственную точку перекрестья. Ясно, что на плоскости нельзя изобразить две несамопересекающиеся замкнутые кривые, которые бы имели перекрестье в одной точке. С другой стороны, если две кривые «касаются» в нескольких точках, то эти касания можно «развести» в точках нетрансверсального пересечения.

Таким образом, предполагая, что граф вложен в плоскость с сохранением крестовой структуры, мы можем «развести» два цикла во всех точках, где они пересекаются не трансверсально; если окажется, что при этом останется ровно одна точка перекрестья, то это будет противоречить планарности графа.

Настоящая статья будет посвящена вопросу: в какую поверхность можно вложить четырехвалентный граф с крестовой структурой? Для этого нам понадобится техника поворачивающих обходов и хордовых диаграмм.

1. ПОВОРАЧИВАЮЩИЕ ОБХОДЫ. ХОРДОВЫЕ ДИАГРАММЫ

Назовем *хордовой диаграммой* конечный трехвалентный граф, состоящий из цикла, проходящего через все вершины (*окружности хордовой диаграммы*) по одному разу и оставшихся ребер, которые мы будем называть *хордами* хордовой диаграммы. Такие хордовые диаграммы рассматриваются с точностью до эквивалентности — изоморфизма графов, переводящего окружность в окружность. Хордовую диаграмму будем называть *ориентированной*, если ориентирована ее окружность; для ориентированных хордовых диаграмм изоморфизм предполагает сохранение ориентации. Назовем *поворачивающим обходом* такой способ прохождения всех ребер графа с заходом в каждую вершину дважды, при котором в каждой вершине мы переходим с ребра на *не противоположное* ему (его же можно считать отображением f окружности S^1 в граф). Хордовая диаграмма $C(\Gamma)$, соответствующая поворачивающему обходу Γ , строится следующим образом. Окружностью хордовой диаграммы является отображаемая окружность S^1 , а хордами соединяются пары точек, имеющие один и тот же образ относительно отображения f .

УПРАЖНЕНИЕ 1. *Покажите, что у каждого связного крестового графа существует поворачивающий обход.*

При этом хорды хордовой диаграммы, соответствующей поворачивающему обходу, естественно делить на два типа. Хорды *первого типа* соответствуют перекресткам первого типа, которые выглядят следующим образом. В данном перекрестке по двум противоположным (полу)ребрам ориентация обхода направлена к вершине, а по двум другим противоположным (полу)ребрам она ориентирована во внешнюю сторону. В ином случае, если некоторое (полу)ребро ориентировано внутрь вершины, а противоположное ему (полу)ребро ориентировано из вершины, будем говорить, что хорда *имеет второй тип*.

На рис. 1 каждая вершина пронумерована два раза согласно двум моментам прохождения поворачивающего обхода через вершину (на этом примере все хорды имеют первый тип).

Как выглядят хордовые диаграммы, соответствующие четырехвалентным графам с крестовой структурой, вложимым в различные двумерные замкнутые поверхности? Мы ограничимся лишь *шахматными вложениями*. Назовем вложение оснащенного четырехвалентного графа в двумерную поверхность *шахматным*, если дополнение к образу этого графа состоит из двумерных клеток, причем клетки допускают раскраску в черный и белый цвета таким образом, что клетки, соседствующие по ребру, имеют разные цвета. Очевидно, что любое вложение графа в плоскость (в сферу)

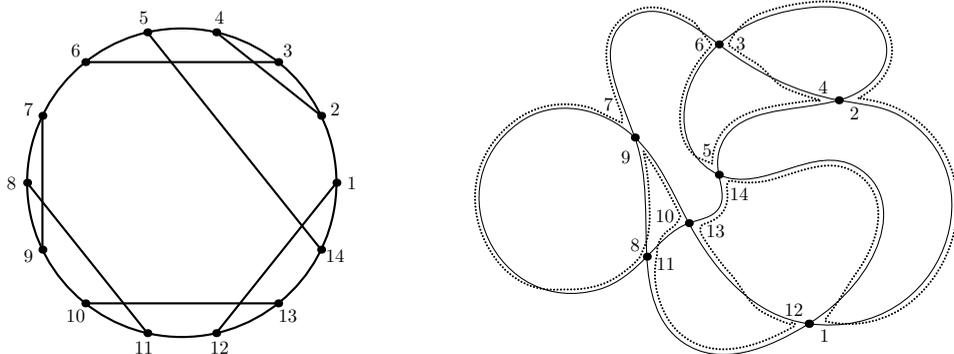


Рис. 1. Поворачивающий обход и поворачивающая хордовая диаграмма

является шахматным. В конце работы мы укажем, что означает условие шахматности для произвольной поверхности.

2. ОРИЕНТИРУЕМЫЙ И НЕОРИЕНТИРУЕМЫЙ СЛУЧАИ

Начнем с простого наблюдения.

Скажем, что крестовый граф обладает *седловой ориентацией*, если можно ориентировать его ребра таким образом, чтобы в каждой вершине V некоторые два противоположных ребра были направлены в сторону вершины V , а другие два — в сторону от вершины V . На рисунке 2 слева изображен планарный крестовый граф и его седловая ориентация, а на рисунке справа — крестовый граф (с двумя вершинами), седловой ориентацией не обладающий.

ТЕОРЕМА 2. Пусть оснащеному четырехвалентному графу Γ с крестовой структурой при некотором его поворачивающем обходе с соответствует хордовая диаграмма $D_{\Gamma,c}$. Тогда у хордовой диаграммы $D_{\Gamma,c}$ найдется хотя одна хорда второго типа, то все поверхности, в которые

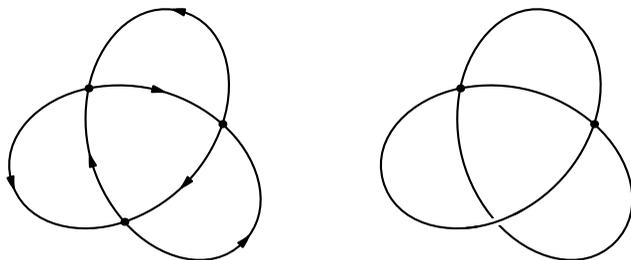


Рис. 2. Граф с седловой ориентацией и граф без седловой ориентации

граф Γ вложим шахматным образом, являются неориентируемыми, а если все хорды хордовой диаграммы имеют первый тип, то все поверхности, в которые граф вложим шахматным образом, являются неориентируемыми.

ЗАМЕЧАНИЕ. Как видно из формулировки настоящей теоремы, определить то, в какие поверхности — ориентируемые или неориентируемые — настоящий граф можно вложить шахматным образом, можно исходя из *любого* поворачивающего обхода. Это значит, что если для какого-нибудь поворачивающего обхода найдется хорда второго типа, то хорда второго типа найдется и для любого другого поворачивающего обхода.

УПРАЖНЕНИЕ 2. *Докажите это утверждение.*

Указание: показать, что наличие у четырехвалентного графа структуры седловой ориентации равносильно отсутствию у соответствующей хордовой диаграммы (при любом обходе) хорд второго типа.

Как понять, что два поворачивающих обхода задают один и тот же четырехвалентный граф с крестовой структурой? Естественно, эта задача решается явным построением. Оказывается, что есть замечательная формула на языке матриц над полем из двух элементов, связывающая разные поворачивающие обходы одного и того же графа. Эта формула принадлежит Д. П. Ильютко, и ей посвящена следующая статья [3] в настоящем номере.

3. ШАХМАТНЫЕ ВЛОЖЕНИЯ ГРАФА С КРЕСТОВОЙ СТРУКТУРОЙ В ДВУМЕРНЫЕ ПОВЕРХНОСТИ

Скажем, что две хорды p, q хордовой диаграммы D *зацеплены*, если их концы расположены на окружности в чередующемся порядке.

Таким образом, при изображении хордовой диаграммы на плоскости посредством евклидовой окружности и прямолинейных хорд, зацепленные хорды изображаются пересекающимися, как это изображено на рис. 1.

Пусть граф Γ с крестовой структурой вложен в замкнутую двумерную поверхность S шахматным образом.

Рассмотрим произвольный обход графа Γ . Построим вложение соответствующей этому обходу хордовой диаграммы в поверхность S следующим образом. Образ окружности хордовой диаграммы будет совпадать с ребрами графа Γ везде, за исключением окрестностей образов вершин. В окрестностях образов вершин окружность хордовой диаграммы будет локально выглядеть так, как показано на рисунке 3. Две части окружности будут соединены хордой, отвечающей данной вершине.

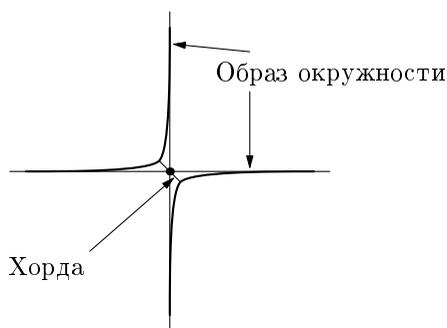


Рис. 3. Локальное построение хордовой диаграммы в окрестности вершины

Обозначим через γ простую замкнутую кривую — образ окружности. Нетрудно заметить, что кривая γ является *разделяющей*: ее дополнение состоит из двух компонент связности.

Действительно, эти компоненты связности почти полностью (за исключением малых фрагментов вершин) совпадают с объединением черных клеток и объединением белых клеток, соответственно.

Таким образом, мы имеем две поверхности с краем: S_B и S_W , склейка которых по их общему краю — окружности — дает исходную поверхность S .

Будем далее использовать следующее определение рода для двумерной замкнутой поверхности: $g(M) = 1 - \frac{\chi(M)}{2}$, где χ — эйлерова характеристика; для компактной поверхности с краем род определяется как род поверхности, получающейся из исходной заклеивкой компонент края дисками.

Так, для листа Мёбиуса и для проективной плоскости род равен $\frac{1}{2}$, а для бутылки Клейна он равен 1. Замкнутая двумерная поверхность определяется своим родом и ориентируемостью/неориентируемостью.

Очевидно, что род поверхности S равен сумме родов поверхностей S_B и S_W .

Наша дальнейшая задача будет состоять в оценке суммы $g(S_B) + g(S_W)$.

Как оказывается, эту оценку можно переформулировать на языке матриц.

Если задано шахматное вложение четырехвалентного графа с крестовой структурой в некоторую двумерную поверхность и задан поворачивающий обход на этом графе, то все хорды соответствующей хордовой диаграммы естественным образом делятся на «черные» и «белые», а именно, черными хордами мы называем те хорды, которые отвечают вершинам

графа, окрестность которых принадлежит черной области, а белыми — те вершины графа, окрестность которых принадлежит белой области.

Так, на рис. 1, если покрасить всю плоскость в черный и белый цвета, хорды 2–4, 5–14, 7–9, 10–13 (внутренние) будут черными, а хорды 1–12, 3–6, 8–11 (внешние) будут белыми.

Таким образом, любая тройка (граф, обход, вложение) задает хордовую диаграмму, хорды которой разбиты на два семейства.

Составим теперь две хордовые диаграммы D_B и D_W , которые получаются из хордовой диаграммы D удалением белых (соответственно, черных) хорд, и объединением дуг, инцидентных вершине удаленной хорды в одну дугу.

4. МАТРИЦА ПЕРЕСЕЧЕНИЙ ОСНАЩЕННОЙ ХОРДОВОЙ ДИАГРАММЫ

Пусть D — хордовая диаграмма с непустым множеством хорд. Сопоставим ей квадратную матрицу над полем из двух элементов следующим образом. Размер матрицы будет равен количеству хорд в хордовой диаграмме. Перенумеруем хорды диаграммы D произвольным образом (в дальнейшем эта нумерация не будет играть для нас никакой роли). При $i \neq j$ на месте (i, j) нашей матрицы будет стоять индекс инцидентности хорд с номерами i и j , равный 1, если хорды зацеплены, и 0, если хорды не зацеплены. На диагонали на месте (i, i) будет стоять элемент, равный нулю, если хорда имеет первый тип и единице, если хорда имеет второй тип. Обозначим соответствующую матрицу через $A(D)$.

Пусть теперь D — хордовая диаграмма, имеющая хорды первого и второго типов, и пусть D_B и D_W — соответствующие ей «черная» и «белая» хордовые диаграммы. Такое разбиение приводит к двум новым матрицам $A(D_1)$ и $A(D_2)$.

Оказывается, что по этим двум матрицам можно вычислить род белой части поверхности и род черной части поверхности, а именно, имеет место

$$\text{ТЕОРЕМА 3. } 2g(S_B) = \text{corank } A(D_B), \quad 2g(D_W) = \text{corank } A(D_W).$$

Здесь коранг матрицы (corank) — это разность между ее размерностью и ее рангом. Род понимается в приведенном выше смысле, в частности, он может быть полуцелым.

Приведенная выше теорема 3 является следствием известной теоремы Конна – Лемпеля – Соболевой – Тральди, [11, 14, 16], суть которой состоит в следующем.

Пусть имеется двумерный диск, на крае которого (окружности) отмечены точки, представляющие собой концы хорд хордовой диаграммы.

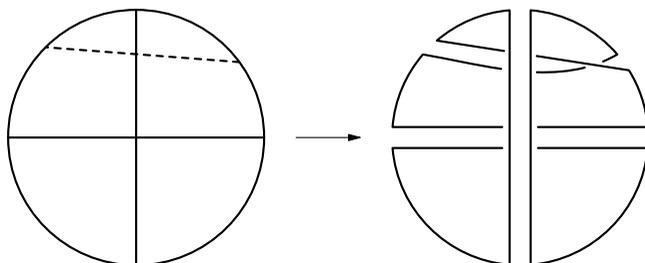


Рис. 4. Хордовая диаграмма и диск с лентами

Приклеим к диску ленты вдоль хорд, причем ленты будут приклеиваться без перекручивания для хорд первого типа, и с перекручиванием для хорд второго типа. В итоге получим двумерное многообразие с краем. Оказывается, что количество компонент края у этого многообразия будет на единицу больше коранга матрицы пересечения соответствующей хордовой диаграммы. На рис. 4 изображена хордовая диаграмма (хорда второго типа изображена пунктирной линией) и соответствующая поверхность.

Диаграмме, изображенной на рис. 4, соответствует следующая матрица

$$\begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Ранг этой матрицы по модулю два полный, т. е. равен трем, а коранг равен нулю. Это соответствует тому, что в правой части рис. 4 мы имеем одну компоненту.

Таким образом, в связи с теоремой 3 наша задача о вложимости оснащенного четырехвалентного графа в поверхность рода g (ориентируемую или неориентируемую) сводится к следующей задаче.

ЗАДАЧА. Пусть дана симметричная матрица M размера $n \times n$ над полем из двух элементов. Каково минимальное значение суммы рангов двух матриц $rank(M_I) + rank(M_J)$, где два подмножества I, J образуют разбиение множества индексов исходной матрицы: $I \sqcup J = \{0, 1, \dots, n\}$, а квадратные матрицы M_I и M_J получаются из матрицы M взятием соответствующих множеств I и J наборов строк и столбцов?

Это минимальное значение отвечает за минимальный род поверхности, в которую данный четырехвалентный граф с крестовой структурой может быть вложен шахматным образом.

Разумеется, эта задача может быть решена прямым перебором 2^{n-1} вариантов, однако, конечно, имеется в виду возможность нахождения ее быстрого (например, полиномиального по n решения).

Как оказывается, быстрое решение такой задачи весьма легко может быть получено явно для случая вложений в сферу (или плоскость), проективную плоскость и бутылку Клейна. Во всех остальных случаях вопрос о быстром решении остается открытым.

Уместно сравнить этот результат с работой Линса, Рихтера и Шанка, [12], в которой случаи плоскости, проективной плоскости и бутылки Клейна также решаются просто, а случай тора — нет. Кроме того, нужно отметить, что с алгоритмической точки зрения проблема распознавания того, в какую поверхность вложим тот или иной граф, является NP-трудной [15].

5. РЕШЕНИЯ ДЛЯ СЛУЧАЯ ПЛОСКОСТИ, ПРОЕКТИВНОЙ ПЛОСКОСТИ И БУТЫЛКИ КЛЕЙНА

Случай \mathbb{R}^2 (S^2). Рассмотрим хордовую диаграмму. Для планарности необходимо, чтобы все хорды имели первый тип: действительно, чтобы сумма рангов двух матриц была равна нулю, на диагонали исходной матрицы не должно быть элементов, равных единице. Пусть это так. Далее нам нужно разбить хорды на 2 семейства таким образом, чтобы хорды из одного семейства были незацеплены (такая диаграмма называется d -диаграммой, [6]). В случае связной диаграммы алгоритм таков: мы рассматриваем произвольную хорду и отправляем ее в первое семейство, затем некоторую зацепленную с ней хорду отправляем во второе семейство, некоторую хорду, зацепленную со второй, отправляем в первое семейство и т. д. Исчерпав все хорды, проверяем, не содержит ли одно из семейств зацепленных хорд.

В случае проективной плоскости мы должны найти хорду с оснащением единица. Далее все хорды с оснащением единица должны быть зацеплены с ней, чтобы ранг соответствующей подматрицы не превышал единицы. После этого два семейства должны быть устроены следующим образом: хорды из первого семейства включают в себя все хорды второго типа, зацепленные между собой, а также хорды с оснащением ноль, которые не зацеплены друг с другом, а также с хордами второго типа. Второе семейство состоит из оставшихся хорд первого типа, попарно незацепленных. Дальнейший алгоритм дословно повторяет алгоритм распознавания d -диаграммы. В случае распознавания вложения в бутылку Клейна нам понадобится следующая очевидная

ЛЕММА 1. Пусть оснащенный граф Γ вложен шахматным образом в бутылку Клейна, и пусть C — обход графа Γ . Тогда либо обход C разбивает бутылку Клейна на два листа Мёбиуса, либо существует хорда второго типа, такая, что обход C' , полученный изменением обхода C в

вершине, соответствующей этой хорде, разбивает бутылку Клейна на два листа Мёбиуса.

После этого нужно устроить разбиение матрицы пересечений для одной из хордовых диаграмм $D_{\Gamma, C}$ или $D_{\Gamma, C'}$ на два семейства, каждое из которых имело бы ранг один. Алгоритм разбиения и проверка дословно повторяют алгоритм распознавания d -диаграммы, только в случае двух хорд второго типа нужно заменить слово «пересечение» на «непересечение» и наоборот. Нужно также поменять инцидентность на графе пересечений для вершин с оснащением один. Случай, когда граф пересечения будет несвязным, легко сводится к проверке каждой из его компонент.

6. ОБ УСЛОВИИ ШАХМАТНОСТИ

ЗАДАЧА. Докажите, что вложение четырехвалентного графа Γ с крестовой структурой в двумерную поверхность S является шахматным, если и только если любой замкнутый путь на этой поверхности, не проходящий через вершины графа и не касающийся его ребер, пересекает его ребра четное число раз.

Приведенное выше условие математически формулируется так: граф представляет собой нулевой класс одномерных гомологий поверхности в поле из двух элементов.

Над любой двумерной поверхностью S , в которую вложен четырехвалентный граф Γ с крестовой структурой, можно рассмотреть двулистное накрытие $\tilde{S} \rightarrow S$, которое строится следующим образом. Каждый замкнутый путь γ на поверхности S , пересекающий образ графа Γ трансверсально накрывается замкнутым путем, если он пересекает образ графа Γ в четном числе точек. В противном случае он накрывается незамкнутым путем. Таким образом, вопрос о шахматных вложениях тесно связан с вопросом о произвольных вложениях. Подробнее см. [13].

Я благодарен Д. П. Ильютко за полезные обсуждения. Выражаю благодарность М. Н. Вялому, указавшему мне на работу [15].

СПИСОК ЛИТЕРАТУРЫ

- [1] В. А. Васильев. *Инварианты первого порядка и когомологии пространств вложений самопересекающихся кривых в \mathbb{R}^n* // Известия РАН. Сер. Мат. Т. 69, №5. 2005. С. 3–52.
- [2] Д. П. Ильютко. *Оснащенные 4-графы: эйлеровы циклы, гауссовы циклы и поворачивающие обходы* // Матем. сбор., т. 202, №9, 2011. С. 53–76.

- [3] Д. П. Ильютко. *Матрицы пересечений эйлеровых циклов 4-валентных графов с крестовой структурой* // Математическое просвещение. Сер. 3, вып. 16. 2012. С. 105–131.
- [4] В. О. Мантуров. *Доказательство гипотезы Васильева о планарности сингулярных зацеплений* // Известия РАН. Т. 69. 2005. С. 169–178.
- [5] В. О. Мантуров. *Вложения оснащенных четырехвалентных графов в двумерные поверхности* // Доклады РАН. Т. 494, №3. 2009. С. 308–310.
- [6] В. О. Мантуров. *Теория узлов*. Москва–Ижевск: РХД. 2005. 512 с.
- [7] В. О. Мантуров. *Четырехвалентные графы с крестовой структурой* // Математическое просвещение. Сер. 3, вып. 15. 2011. С. 128–137.
- [8] В. В. Прасолов. *Элементы комбинаторной и дифференциальной топологии*. М.: МЦНМО, 2004. 352 с.
- [9] G. Cairns, D. Elton. *The planarity problem for signed Gauss words* // Journal of Knot Theory and Its Ramifications. Vol. 2. 1993. P. 359–367.
- [10] G. Cairns, D. Elton, *The planarity problem*. II // Journal of Knot Theory and Its Ramifications. Vol. 5. 1996. P. 137–144.
- [11] M. Cohn and A. Lempel. *Cycle decomposition by disjoint transpositions* // J. Combin. Theory Ser. A. Vol. 13. 1972. P. 83–89.
- [12] S. Lins, B. Richter, H. Schank. *The Gauss Code Problem off the plane* // Aequationes Mathematicae. Vol. 33, no 1. 1987. P. 81–95.
- [13] V. O. Manturov. *Embeddings of four-valent framed graphs into two-surfaces* // The Mathematics of Knots: Theory and Applications. Heidelberg: Springer, 2010. P. 169–198.
- [14] E. Soboleva. *Vassiliev Knot Invariants Coming from Lie Algebras and 4-Invariants* // Journal of Knot Theory and Its Ramifications. Vol. 10, no 1. 2001. P. 161–169.
- [15] C. Thomassen. *The graph genus problem is NP-complete* // J. of Algorithms. Vol. 10. 1989. P. 568–576.
- [16] L. Traldi. *Binary nullity, Euler circuits and interlace polynomials*. 2009. arXiv:math.CO/0903.4405.

Матрицы пересечений эйлеровых циклов 4-валентных графов с крестовой структурой

Д. П. Ильютко*

В настоящей статье мы рассматриваем связанные 4-валентные графы, снабженные крестовой структурой, и обходы на них. Имея крестовую структуру, мы можем определить разные типы обходов: прямые обходы, т. е. мы двигаемся согласно крестовой структуре, и поворачивающие обходы, т. е. в каждой вершине графа мы поворачиваем. Мы предъявляем явную формулу, связывающую матрицы пересечений разных типов обходов на 4-валентных графах с крестовой структурой.

1. ВВЕДЕНИЕ

Рассмотрим сначала следующую задачу, которая играет ключевую роль в наших исследованиях.

Пусть дана хордовая диаграмма, т. е. окружность с конечным множеством пар точек на ней, причем каждая пара содержит разные точки, и разные пары не пересекаются. Удобно каждую пару точек представлять хордой, соединяющей их. Разрежем окружность по всем точкам, пробегающим множество всех пар (хорд). В результате такого разрезания каждая хорда даст четыре точки. Разобьем каждую четверку на две новые пары и соединим точки из одной пары друг с другом. Мы получим набор замкнутых, возможно (само)пересекающихся, кривых. Вопрос состоит в следующем: сколько замкнутых кривых мы получим, более точная формулировка дана в теореме 3.

Частный случай такой проблемы, когда все четверки разбиваются на пары одним фиксированным способом, был впервые рассмотрен Коном и Лемпелом в [14]. Позже эта теорема была несколько раз передоказана и обобщена на общий случай, см. [9, 21, 23–25].

*Работа выполнена при частичной финансовой поддержке гранта РФФИ (проект № 10-01-00748-а), гранта Президента РФ поддержки Ведущих научных школ (проект НШ-3224.2010.1), программы Развитие научного потенциала высшей школы (проект 2.1.1.3704), Программ Научные и научно-педагогические кадры инновационной России (госконтракты 02.740.11.5213 и 14.740.11.0794).

Ответ на поставленную выше проблему дается простой формулой. С каждой хордовой диаграммой можно связать матрицу пересечений, состоящую из нулей и единиц. Внедиагональные элементы этой матрицы отвечают за пересечение/непересечение хорд (0, если не пересекаются, и 1 в противном случае), а диагональные элементы отвечают за тип соединения точек, полученных в результате разрезания окружности, точные определения см. ниже. Оказывается, что число замкнутых кривых равно корангу матрицы пересечений, рассматриваемой над \mathbb{Z}_2 , плюс один (напомним, что коранг равен размерности матрицы минус ее ранг).

Перейдем теперь к 4-валентным графам и задачам, связанными с ними. Понятие 4-валентного графа с крестовой структурой появляется, например, при кодировании узлов плоскими диаграммами. Напомним, что *узел* представляет собой образ гладкого вложения f окружности S^1 в трехмерное евклидово пространство \mathbb{R}^3 . Причем узлы рассматриваются с точностью до естественной эквивалентности: два узла считаются эквивалентными, если один узел мы можем без (само)пересечений продеформировать в другой. Для построения плоской диаграммы узла мы фиксируем некоторую плоскость в пространстве и рассматриваем проекцию узла на нее. Без ограничения общности можно считать, что проекция узла на плоскость представляет собой вложенный конечный 4-валентный граф, являющийся образом гладкого погружения окружности в плоскость. При этом проекция узла обладает дополнительной структурой: четыре исходящих ребра (точнее, полуребра) из каждой вершины графа разбиваются на две пары (противоположных) ребер: ребра одной пары имеют прообразы на S^1 , стыкующиеся в точке, которая при отображении f переходит в вершину графа. Таким образом, мы имеем 4-валентный граф с крестовой структурой.

Узлы удобно также кодировать с помощью *гауссовых диаграмм* [13,17], которые представляют собой окружность со стрелками, снабженными знаками. Для этого надо на окружности S^1 отметить точки, проецирующиеся при отображении f в вершины графа, и соединить точки, проецирующиеся в одну и ту же вершину, стрелкой, при этом стрелку снабдив знаком (мы не будем указывать явно, как направлена стрелка и какой знак она имеет), см. рис. 1. Очевидно, что гауссова диаграмма получается рассмотрением на плоской диаграмме узла эйлерова цикла, который в каждой вершине переходит с ребра на противоположное ребро (*гауссов цикл*). Гауссовы диаграммы применяются также при построении инвариантов конечного порядка и инвариантов Васильева [8, 13, 17].

Рассмотрим обратную задачу. А именно, пусть дан произвольный абстрактный связный 4-валентный граф с крестовой структурой. Верно ли, что существует узел, плоская диаграмма которого совпадает с данным графом? Очевидно, что необходимым и достаточным условием существования

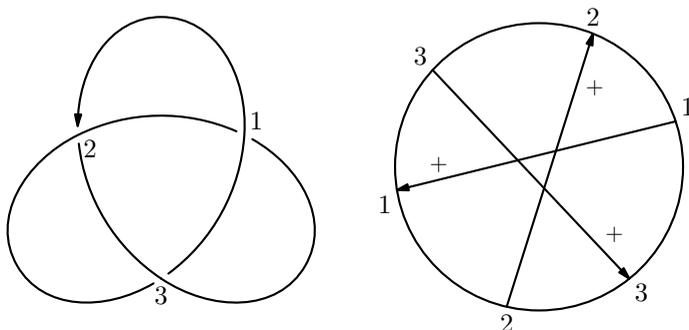


Рис. 1. Гауссова диаграмма трилистника

такого узла является условие вложимости этого графа в плоскость с сохранением крестовой структуры. На рис. 2 изображен 4-валентный граф с крестовой структурой (крестовая структура индуцируется из плоскости), который не вложим в плоскость с сохранением структуры.

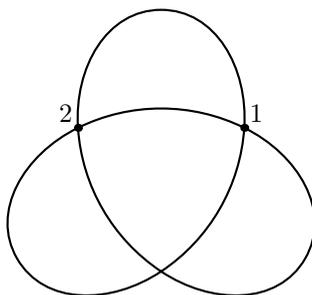


Рис. 2. Невложимый в плоскость 4-валентный граф с крестовой структурой

Для определения планарности 4-валентного графа с крестовой структурой удобно пользоваться *поворачивающим обходом* (эйлеров цикл, который в каждой вершине переходит с ребра на ребро из другой пары), см. [1, 2, 22]. Аналогично гауссовой диаграмме, мы можем построить хордовую диаграмму, т.е. окружность с хордами, соответствующую поворачивающему обходу. Критерий планарности формулируется очень просто: 4-валентный граф с крестовой структурой планарен тогда и только тогда, когда он допускает седловую ориентацию, и хордовая диаграмма произвольного поворачивающего обхода является *d-диаграммой*, т.е. множество всех хорд хордовой диаграммы может быть разбито на два дизъюнктных подмножества, причем хорды из одного множества не зацеплены друг с другом, см. [3, 5, 22]. Две хорды *зацеплены*, если их концы

чередуются при обходе окружности хордовой диаграммы. Существуют также критерии планарности 4-валентного графа с крестовой структурой в терминах гауссовых диаграмм, см. [11, 12].

Если мы хотим обобщить вопрос планарности и рассматривать вопрос о нахождении минимального рода двумерной замкнутой ориентируемой поверхности, в которую может быть вложен заданный 4-валентный граф с крестовой структурой, то подход с помощью поворачивающего обхода тоже более удобен. Существует критерий, дающий ответ на вопрос о минимальности рода, см. [1, 5].

Заметим, что поворачивающий обход существует на любом связном 4-валентном графе с крестовой структурой, и их количество почти всегда больше одного. В то же самое время, гауссов цикл существует не всегда, и если существует, то он единственен. Возникают задачи: найти критерий существования гауссова цикла, и в случае существования понять, как связаны поворачивающие обходы и гауссов цикл. Конечно мы можем ответить на эти вопросы, просто двигаясь вдоль графа согласно крестовой структуре, в каждой вершине мы имеем единственный способ пройти через нее. Если по возвращению в точку отправления мы прошли все ребра графа, то на данном графе существует гауссов цикл. Но этот способ в случае большого количества вершин не очень удобен и не дает явную связь между циклами. В настоящей статье мы даем явную формулу, которая зависит только от матрицы пересечений эйлерова цикла: беря произвольный эйлеров цикл и строя его матрицу пересечений, мы можем понять, имеет ли данный 4-валентный граф с крестовой структурой гауссов цикл, и в случае его существования найти его матрицу пересечений. Используя данную формулу, в последней части нашей работы мы получим интересные факты о симметрических матрицах.

БЛАГОДАРНОСТИ

Автор выражает благодарность за внимание к работе А. Т. Фоменко, В. О. Мантурову, И. М. Никонову и Л. Тральди.

2. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ И ПРЕДВАРИТЕЛЬНЫЕ РЕЗУЛЬТАТЫ

2.1. 4-ГРАФЫ И ЭЙЛЕРОВЫ ЦИКЛЫ

Термин «граф» впервые появился в книге венгерского математика Д. Кёнига в 1936 г., хотя задачи по теории графов восходят еще к Л. Эйлеру (XVIII в.).

Напомним, что *граф* задается множеством вершин и множеством ребер, соединяющих эти вершины, при этом, ребро может соединять одну и ту же вершину (*петля*), и два ребра могут соединять одну и ту же пару вершин

(кратные ребра). Множество вершин графа G обозначается через $V(G)$, а множество ребер — $E(G)$. Каждое ребро можно снабдить ориентацией, в результате мы получим *ориентированный* граф. На протяжении всей статьи все рассматриваемые графы являются *конечными*, т. е. множества вершин и ребер предполагаются конечными.

Графы удобно изображать в виде рисунков, состоящих из точек и линий, соединяющих некоторые из этих точек. При этом точки соответствуют вершинам графа, а соединяющие пары точек линии — ребрам.

На рис. 3 изображены разные графы. На втором графе рисунка 3 мы имеем два кратных ребра, а на третьем графе рисунка 3 мы имеем петлю.

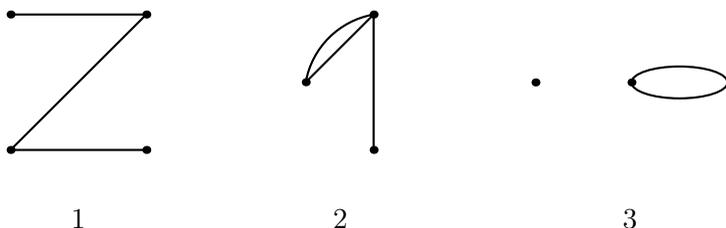


Рис. 3. Графы

Ребро, соединяющее вершины u и v , мы будем записывать в виде $e = uv$ или $e = vu$. В этом случае также говорят, что вершина u (вершина v) *инцидентна* ребру e .

При определении степени вершины удобно считать, что каждое ребро состоит из двух полуребер. Вершина v имеет *степень*, равную k , если v инцидентна k полуребрам. Граф, все вершины которого имеют степень k , называется k -валентным или просто k -графом. *Свободная петля*, т. е. граф без вершин с одним циклическим ребром, рассматривается как k -граф для любого k . На рис. 4 изображены 2-граф и 3-граф, имеющие по четыре вершины.

Чередующаяся последовательность

$$v_1, e_1, v_2, e_2, \dots, e_l, v_{l+1}$$

вершин и ребер такая, что $e_i = v_i v_{i+1}$, $i = 1, \dots, l$, называется *маршрутом*,



Рис. 4. 2-Граф и 3-граф

соединяющим вершины v_1 и v_{l+1} . Маршрут называется *цепью*, если все его ребра различны. Цепь, у которой $v_1 = v_{l+1}$, называется *циклом*. Цикл в графе называется *эйлеровым*, если он содержит все ребра графа. Цикл в графе называется *гамильтоновым*, если он проходит через все вершины графа по одному разу, за исключением первой и последней вершин.

ЗАМЕЧАНИЕ 1. По определению цикл имеет ориентацию. Для неориентированных графов мы почти всегда (если явно не указано другое) отождествляем два цикла, отличающихся ориентацией, т. е. мы рассматриваем неориентированные циклы.

Граф называется *связным*, если любые две его несовпадающие вершины соединены маршрутом.

Хорошо известна следующая

ТЕОРЕМА 1 (Л. ЭЙЛЕР, 1736 г.). *Связный граф имеет эйлеров цикл тогда и только тогда, когда степени всех его вершин четны.*

Пусть H — произвольный связный 4-граф с множеством вершин $V(H)$, и пусть U — эйлеров цикл на H . Опишем связь между двумя эйлеровыми циклами на данном графе H .

Определим *k-преобразование* 4-графов, которое было введено Коцигом [20]. Для каждой вершины $v \in V(H)$ существуют в точности два (неориентированных) цикла P_v и Q_v на U , не имеющих общих ребер, начинающихся и заканчивающихся в вершине v , и каждый из которых содержит по крайней мере по одному ребру. Существует единственный эйлеров цикл, отличный от U , также содержащий циклы P_v и Q_v (если мы зададим произвольную ориентацию на эйлеровом цикле U , то на новом эйлеровом цикле мы двигаемся вдоль P_v согласно ориентации на U , а вдоль Q_v — в противоположном направлении). Обозначим через $U * v$ новый эйлеров цикл, полученный из U . Преобразование $U \mapsto U * v$ называется *k-преобразованием*.

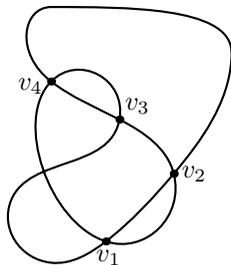


Рис. 5. Граф

ТЕОРЕМА 2 (СМ. [20]). Любые эйлеровы циклы на 4-графе связаны конечной последовательностью k -преобразований.

Мы оставим теорему 2 без доказательства.

УПРАЖНЕНИЕ 1. Рассмотрим граф, изображенный на рис. 5. Найти на нем все эйлеровы циклы и для каждой пары различных эйлеровых циклов найти конечную последовательность k -преобразований, связывающую их.

2.2. ЭЙЛЕРОВЫ ЦИКЛЫ, ЦИКЛИЧЕСКИЕ СЛОВА И ХОРДОВЫЕ ДИАГРАММЫ

Эйлеровы циклы удобно записывать словами над алфавитом, состоящим из вершин данного 4-графа. Дадим необходимые определения.

ОПРЕДЕЛЕНИЕ 1. Пусть $w = x_1x_2 \dots x_{k-1}x_k$ — произвольное слово, т. е. конечная последовательность букв некоторого конечного алфавита. Зеркальный образ слова w — это слово $\tilde{w} = x_kx_{k-1} \dots x_2x_1$. Мы рассматриваем не просто слова, а классы эквивалентности слов, где любое слово из класса, порожденного словом $x_1 \dots x_k$, является или циклической перестановкой $w_i = x_ix_{i+1} \dots x_kx_1 \dots x_{i-1}$, $1 \leq i \leq k$, слова $x_1 \dots x_k$, или зеркальным образом слова w_i . Мы обозначим этот класс через $(x_1 \dots x_k)$ и назовем его *циклическим словом*.

ОПРЕДЕЛЕНИЕ 2. Слово называется *словом с двойным вхождением*, если каждая его буква встречается в нем ровно два раза.

ПРИМЕР 1. Например слово $abcbsa$ является словом с двойным вхождением, а слово $abcsb$ не является словом с двойным вхождением.

Очевидно, что зеркальный образ и циклическая перестановка слова с двойным вхождением являются словами с двойным вхождением. Поэтому имеет смысл говорить о циклическом слове с двойным вхождением.

Каждое циклическое слово с двойным вхождением удобно изображать хордовой диаграммой.

ОПРЕДЕЛЕНИЕ 3. *Хордовая диаграмма* — это 3-граф, состоящий из выбранного неориентированного гамильтонового цикла (*окружность*) и неориентированных ребер (*хорд*), соединяющих точки на окружности.

Представление слова в виде хордовой диаграммы строится следующим образом. Пусть t — произвольное циклическое слово с двойным вхождением. Хордовая диаграмма, соответствующая слову t строится последовательным расположением букв слова t вдоль окружности S^1 , выбором точек на S^1 около каждого появления буквы слова и соединением хордой каждой пары точек, соответствующих двум одинаковым буквам слова. Нетрудно видеть, что мы получаем взаимно однозначное соответствие

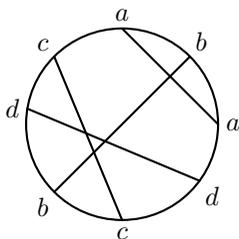


Рис. 6. Хордовая диаграмма слова $(abacdbcd)$

между множеством циклических слов с двойным вхождением и множеством хордовых диаграмм (рассматриваемых с точностью до изоморфизма, переводящего гамильтоновы циклы друг в друга).

ПРИМЕР 2. Рассмотрим слово $m = (abacdbcd)$. Слово m имеет представление с помощью хордовой диаграммы, изображенной на рис. 6.

Определим операцию $*$ на циклических словах с двойным вхождением, которая будет соответствовать k -преобразованию. Пусть $m = (vAvB)$, где A, B — подслова слова m , и буквы принадлежат некоторому конечному алфавиту. Тогда положим $m * v = (v\tilde{A}vB)$, \tilde{A} — зеркальный образ подслова A . На рис. 7 преобразование $m \mapsto m * v$ изображается для хордовых диаграмм (пунктирные дуги хордовых диаграмм содержат концы всех хорд, отличных от v). Для каждого преобразования хордовых диаграмм мы считаем, что только фиксированные фрагменты хордовых диаграмм меняются. Части хордовых диаграмм, не содержащие хорд, участвующих в преобразованиях, изображаются пунктирными дугами.

Пусть U — произвольный эйлеров цикл на 4-графе H с множеством вершин $V(H) = \{v_1, \dots, v_n\}$, которое будет играть роль алфавита. Зададим произвольную ориентацию на U . Двигаясь вдоль U , мы встречаем каждую вершину дважды. Последовательно записывая встречающиеся вершины, мы получим слово с двойным вхождением над $V(H)$.

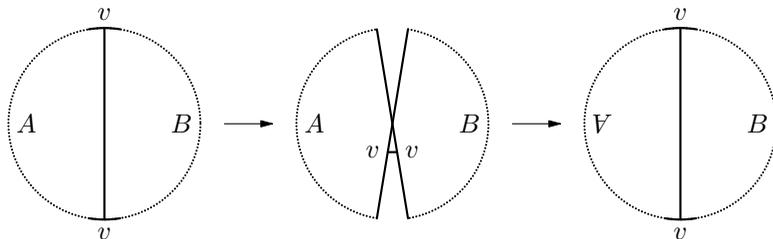


Рис. 7. Операция $*$ на хордовых диаграммах

Следовательно, (неориентированные) эйлеровы циклы кодируются циклическими словами с двойным вхождением. Обозначим соответствующее циклическое слово с двойным вхождением через $m(U)$.

УПРАЖНЕНИЕ 2. Покажите, что $m(U * v) = m(U) * v$, и если мы имеем циклическое слово m с двойным вхождением, то мы можем построить 4-граф, имеющий такой эйлеров цикл U , что $m(U) = m$.

2.3. 4-ГРАФЫ С КРЕСТОВОЙ СТРУКТУРОЙ И ЭЙЛЕРОВЫ ЦИКЛЫ

В данном разделе мы рассмотрим 4-графы с дополнительной структурой.

ОПРЕДЕЛЕНИЕ 4. 4-Граф называется *графом с крестовой структурой*, если в каждой вершине графа четыре исходящих из нее полуребра разбиты на две пары полуребер. Полурёбра из одного семейства называются *противоположными*.

Пусть H — произвольный 4-граф с крестовой структурой, и U — эйлеров цикл на нем. Построим *оснащенное* циклическое слово $m(U)$ с двойным вхождением (соответственно, *оснащенную* хордовую диаграмму), соответствующее эйлерову циклу U . В каждой вершине v графа H мы имеем следующие три возможности прохождения вдоль U (не зависимо от ориентации U) через вершину v .

- 1) Мы переходим с полуребра на противоположное ему полуребро, см. рис. 8 а). Вершина v в этом случае будет называться *гауссовой вершиной для U* , и хорда, соответствующая этой вершине, также будет называться *гауссовой*.
- 2) Мы переходим с полуребра на непротивоположное ему полуребро, причем ориентации противоположных ребер различны, см. рис. 8 б). Вершина v в этом случае будет называться *негауссовой вершиной с оснащением 0 для U* , и хорда, соответствующая этой вершине, также будет называться *негауссовой хордой с оснащением 0*.
- 3) Мы переходим с полуребра на непротивоположное ему полуребро, причем ориентации противоположных ребер совпадают, см. рис. 8 в). Вершина v в этом случае будет называться *негауссовой вершиной с оснащением 1 для U* , и хорда, соответствующая этой вершине, также будет называться *негауссовой хордой с оснащением 1*.

ОПРЕДЕЛЕНИЕ 5. Эйлеров цикл, имеющий только гауссовы вершины, называется *гауссовым циклом*. Эйлеров цикл, содержащий только негауссовы вершины, называется *поворачивающим обходом*, см. [1, 2, 7, 18, 22].

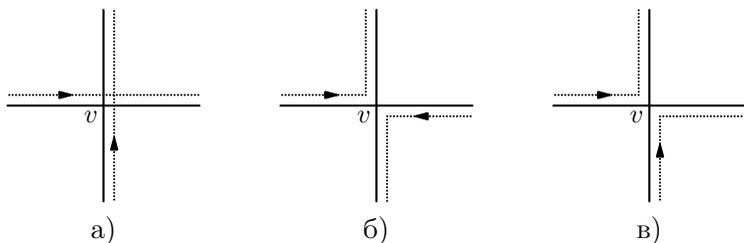


Рис. 8. Переход через вершину

Двигаясь вдоль эйлерова цикла U , мы встречаем каждую вершину графа H дважды. Перейдем к построению *оснащенного* циклического слова $m(U)$ с двойным вхождением, соответствующего эйлерову циклу U . Слова будут рассматриваться над алфавитом $X = V(H) \cup V(H)^{-1} \cup V(H)^G$, где множество $V(H)^{-1}$ состоит из элементов вида v^{-1} для каждой вершины $v \in V(H)$, а множество $V(H)^G$ состоит из элементов вида v^G для каждой вершины $v \in V(H)$. Каждой гауссовой вершине будут соответствовать в $m(U)$ две одинаковые буквы из множества $V(H)^G$, т. е. каждому вхождению соответствующей вершины мы припишем верхний индекс G . Например, $m(U) = (Av^G Bv^G)$, если вершина v является гауссовой. Каждой негауссовой вершине с оснащением 0 будут соответствовать в $m(U)$ две одинаковые буквы из множества $V(H) \cup V(H)^{-1}$, т. е. каждому вхождению соответствующей вершины мы либо ничего не припишем, либо припишем оба раза верхний индекс -1 . Например, $m(U) = (AvBv)$ или $m(U) = (Av^{-1}Bv^{-1})$, если вершина v является негауссовой вершиной с оснащением 0. Каждой негауссовой вершине с оснащением 1 будут соответствовать в $m(U)$ две разные буквы из множества $V(H) \cup V(H)^{-1}$, т. е. двум вхождениям соответствующей вершины мы, произвольным образом, приписываем разные верхние индексы. Например, $m(U) = (Av^{-1}Bv)$ или $m(U) = (AvBv^{-1})$, если вершина v является негауссовой вершиной с оснащением 1 (мы не делаем различия между этими двумя словами). Таким образом, мы рассматриваем не просто оснащенные циклические слова, а классы эквивалентности оснащенных циклических слов, где эквивалентность порождается автоморфизмами алфавита, которые меняют буквы v и v^{-1} местами для некоторой буквы v . Для простоты изложения мы называем эти классы оснащенными циклическими словами.

ЗАМЕЧАНИЕ 2. Построенное оснащенное слово не всегда будет являться словом с двойным вхождением каждой буквы. Мы можем рассмотреть проекцию $\pi: V(H) \cup V(H)^{-1} \cup V(H)^G \rightarrow V(H) \cup V(H)^G$, заданную правилом $v^{\pm 1} \mapsto v$ и $v^G \mapsto v^G$. Образ построенного оснащенного слова при этой проекции является уже словом с двойным вхождением каждой

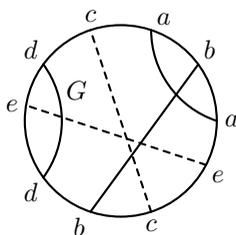


Рис. 9. Оснащенная хордовая диаграмма для $(ab^{-1}acd^Ge^{-1}d^Gb^{-1}c^{-1}e)$

буквы. Мы называем оснащенное слово *словом с двойным вхождением*, если образ слова при проекции π является словом с двойным вхождением.

Изображая оснащенное циклическое слово с двойным вхождением посредством оснащенной хордовой диаграммы, мы будем использовать хорды трех типов: хорды с меткой G для гауссовых вершин, «жирные» хорды без меток для негауссовых вершин с оснащением 0 и пунктирные хорды для негауссовых вершин с оснащением 1.

ПРИМЕР 3. Рассмотрим оснащенное циклическое слово с двойным вхождением $m = (ab^{-1}acd^Ge^{-1}d^Gb^{-1}c^{-1}e)$. Имеем: d — гауссова вершина, a, b — негауссовы вершины с оснащением 0 и c, e — негауссовы вершины с оснащением 1. Соответствующая оснащенная хордовая диаграмма изображена на рис. 9.

Пусть V — произвольное конечное множество. Имея оснащенное циклическое слово m с двойным вхождением (оснащенную хордовую диаграмму) над $V \cup V^{-1} \cup V^G$, мы можем построить 4-граф с крестовой структурой на множестве V , имеющий такой эйлеров цикл U , что оснащенное слово $m(U)$ совпадает с m . Мы сначала построим 4-граф, а затем зададим крестовую структуру, используя тип каждой вершины.

Определим операцию *оснащенная звездочка* на множестве оснащенных циклических слов с двойным вхождением. Мы обозначим эту операцию тем же самым символом $*$.

ЗАМЕЧАНИЕ 3. Мы использовали то же самое обозначение для «простых» циклических слов с двойным вхождением. Далее мы будем рассматривать только оснащенные циклические слова с двойным вхождением и то же самое обозначение не приведет к противоречию.

Сначала мы определим операцию \overline{w} , где w — произвольное подслово (необязательно слово с двойным вхождением) оснащенного циклического слова с двойным вхождением. Пусть $w = x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k}$. Тогда $\overline{w} = \overline{x_k^{\varepsilon_k}} \dots \overline{x_1^{\varepsilon_1}}$, где $\overline{x_l^{\varepsilon_l}} = x_l^{\varepsilon_l}$, если $\varepsilon_l = G$, $\overline{x_l^{\varepsilon_l}} = x_l^{-\varepsilon_l}$, если $\varepsilon_l = \pm 1$.

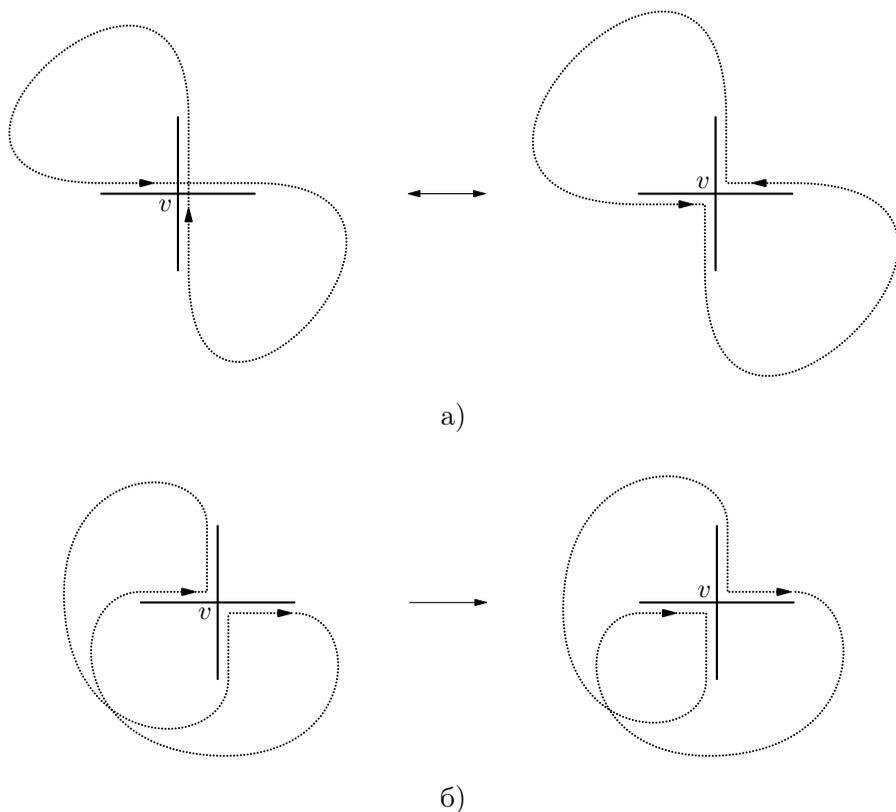


Рис. 10. Операция оснащенная звездочка

Далее, $m = (a^\varepsilon m_1 a^{\varepsilon'} m_2)$ — оснащенное циклическое слово с двойным вхождением. Положим $m * a = (a \bar{m}_1 a m_2)$, если $\varepsilon = \varepsilon' = G$ (рис. 10 а)); $m * a = (a^G \bar{m}_1 a^G m_2)$, если $\varepsilon = \varepsilon' \neq G$ (рис. 10 а)); $m * a = (a \bar{m}_1 a^{-1} m_2)$, если $\varepsilon = -\varepsilon'$ (рис. 10 б)). Таким образом, в результате применения операции оснащенная звездочка к букве a мы получаем: если a являлась гауссовой буквой, то в новом слове она будет негауссовой буквой с оснащением 0; если a являлась негауссовой буквой с оснащением 0 (соотв., 1), то в новом слове она будет гауссовой буквой (соотв., негауссовой буквой с оснащением 1).

Следующие три утверждения мы оставляем в качестве упражнений.

УПРАЖНЕНИЕ 3. Любые два оснащенных циклических слова с двойным вхождением, полученные из 4-графа с крестовой структурой, связаны между собой последовательным применением операции оснащенная звездочка.

УПРАЖНЕНИЕ 4. Каждый 4-граф с крестовой структурой имеет поворачивающий обход.

Очевидно, что существует много поворачивающих обходов и что не каждый 4-граф с крестовой структурой имеет гауссов цикл (если имеет гауссов цикл, то он единствен).

УПРАЖНЕНИЕ 5. Любые два поворачивающих обхода, заданные с помощью оснащенных циклических слов с двойным вхождением, получаются друг из друга последовательностью следующих операций: оснащенная звездочка, примененная к негауссовым буквам с оснащением 1, и $((m * a) * b) * a$, где m — оснащенное циклическое слово с двойным вхождением, a, b — негауссовы буквы с оснащением 0, причем они чередуются в слове m , т. е. $m = (\dots a \dots b \dots a \dots b \dots)$.

3. ГАУССОВЫ ЦИКЛЫ

В данном разделе мы даем явную формулу, позволяющую найти матрицу пересечений гауссова цикла из матрицы пересечений произвольного эйлерова цикла (конечно при условии, что гауссов цикл существует).

3.1. СУЩЕСТВОВАНИЕ ГАУССОВА ЦИКЛА

Нам потребуются два понятия для формулирования критерия существования гауссова цикла: *матрица пересечений* оснащенной хордовой диаграммы (оснащенного циклического слова с двойным вхождением) и *перестройка* множества хорд.

ОПРЕДЕЛЕНИЕ 6. Пусть D — оснащенная хордовая диаграмма, и пусть S^1 — ее окружность. Мы назовем две хорды *зацепленными*, если концы одной хорды лежат в разных связных компонентах множества, полученного из S^1 выбрасыванием концов другой хорды.

ЗАМЕЧАНИЕ 4. Если мы нарисуем хордовую диаграмму и расположим все хорды внутри окружности, то зацепленные хорды будут пересекать друг друга на картинке.

ЗАМЕЧАНИЕ 5. На языке оснащенных циклических слов с двойным вхождением определение зацепленных хорд формулируется следующим образом. Две буквы a, b называются *чередующимися*, если мы их встречаем последовательно $(\dots a^{\alpha_1} \dots b^{\beta_1} \dots a^{\alpha_2} \dots b^{\beta_2} \dots)$ при прочтении слова циклически.

ОПРЕДЕЛЕНИЕ 7. *Матрица пересечений* хордовой диаграммы D с пронумерованными n хордами — это $n \times n$ матрица $A(D) = (a_{ij})$, удовлетворяющая следующим условиям

- 1) элемент a_{ii} равен оснащению хорды с номером i , т. е. или G , или 0, или 1;
- 2) $a_{ij} = 1$, $i \neq j$, если и только если хорды с номерами i и j зацеплены;
- 3) $a_{ij} = 0$, $i \neq j$, если и только если хорды с номерами i и j не зацеплены.

ЗАМЕЧАНИЕ 6. Буква G , фигурирующая в определении матрицы пересечений, — это формальная переменная. В последующих конструкциях она будет указывать на строки и столбцы, которые удаляются. В результате мы будем иметь матрицу, состоящую только из нулей и единиц и рассматриваемую над \mathbb{Z}_2 .

ПРИМЕР 4. Пусть D — оснащенная хордовая диаграмма, изображенная на рис. 9. Пронумеруем все хорды из D : хорда aa имеет номер 1, хорда bb — номер 2 и т. д. Тогда

$$A(D) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & G & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Предположим, что нам дана оснащенная хордовая диаграмма D , все хорды которой имеют оснащение 0 или 1 (без гауссовых хорд).

ОПРЕДЕЛЕНИЕ 8. Определим *перестройку вдоль хорд* хордовой диаграммы D следующим образом. Для каждой хорды, имеющей оснащение 0 (соответственно, 1), мы рисуем параллельную (соответственно, пересекающую) хорду около первоначальной хорды и удаляем дуги окружности между соседними концами, как показано на рис. 11. Незначительным шевелением картинка в \mathbb{R}^2 перестраивается в одномерное многообразие в \mathbb{R}^3 . Это многообразие $M(D)$ и есть *результат перестройки*, см. рис. 12.

Оказывается, число компонент связности многообразия $M(D)$ может быть определено из матрицы пересечений $A(D)$ диаграммы D .

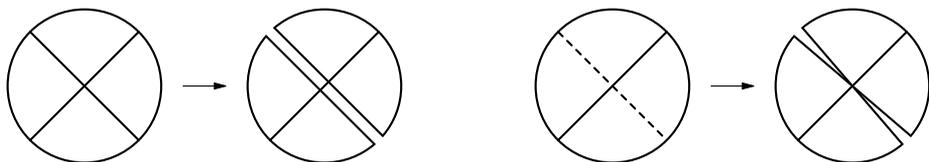


Рис. 11. Перестройка окружности по хордам

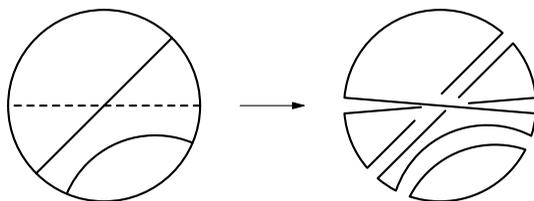


Рис. 12. Многообразие $M(D)$

ТЕОРЕМА 3 (см. [9, 14, 21, 23, 25]). Пусть D — оснащенная хордовая диаграмма, не содержащая гауссовых хорд. Тогда число компонент связности многообразия $M(D)$ равно $\text{corank } A(D) + 1$, где $A(D)$ — матрица пересечений диаграммы D над \mathbb{Z}_2 и коранг corank вычисляется над \mathbb{Z}_2 .

Напомним, что коранг равен размерности матрицы минус ее ранг.

ПРИМЕР 5. Рассмотрим хордовую диаграмму D , изображенную на рис. 13 слева. Совершив перестройку вдоль всех хорд, мы получим многообразие $M(D)$, см. рис. 13 справа. Легко видеть, что число компонент многообразия $M(D)$ равно двум.

С другой стороны мы имеем

$$A(D) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} \quad \text{и} \quad \text{corank } A(D) = 3 - \text{rank } A(D) = 3 - 2 = 1.$$

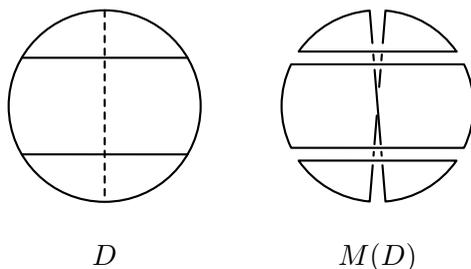


Рис. 13. Хордовая диаграмма D и многообразии $M(D)$

УПРАЖНЕНИЕ 6. Для хордовой диаграммы D , изображенной на рис. 14, найти число компонент связности многообразия $M(D)$, совершив перестройку вдоль всех хорд, и число $\text{corank } A(D) + 1$.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 3. Докажем теорему по индукции, следуя статье [25].

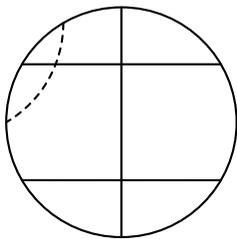


Рис. 14. Оснащенная хордовая диаграмма

База индукции. Пусть оснащенная хордовая диаграмма содержит только одну хорду, и оснащение данной хорды равно 1. Тогда $A(D) = (1)$ и $\text{corank } A(D) + 1 = 1$. Легко видеть, что в результате перестройки вдоль хорды мы получим одну компоненту связности. Таким образом, в данном случае формула имеет место.

Легко также показать по индукции справедливость теоремы для хордовых диаграмм, все хорды которых не зацеплены друг с другом и имеют оснащение 0. Справедливость этого утверждения мы оставляем читателю в качестве упражнения.

Предположение индукции. Пусть утверждение теоремы справедливо для всех оснащенных хордовых диаграмм, количество хорд которых меньше n .

Шаг индукции. Пусть D — оснащенная хордовая диаграмма, содержащая ровно n хорд. Возможны следующие два случая.

(1) Пусть D содержит хорду a с оснащением 1. Рассмотрим оснащенную хордовую диаграмму D' , получающуюся из D применением операции оснащенная звездочка к хорде a и последующим удалением этой хорды, т. е. мы совершили перестройку вдоль a .

Легко видеть, что числа компонент связности многообразий $M(D)$ и $M(D')$ совпадают.

С другой стороны мы имеем (после подходящей нумерации)

$$A(D) = \begin{pmatrix} \mathbf{1} & \mathbf{0}^\top & \mathbf{1}^\top \\ \mathbf{0} & A_0 & A_1 \\ \mathbf{1} & A_1^\top & A_2 \end{pmatrix}, \quad A(D') = \begin{pmatrix} A_0 & A_1 \\ A_1^\top & A_2 + (1) \end{pmatrix},$$

здесь жирные $\mathbf{0}$ и $\mathbf{1}$ указывают на вектор-столбцы, полностью состоящие из 0 и 1 соответственно; (1) — это матрица, полностью состоящая из единиц, и A_i — какие-то матрицы.

Покажем, что коранги матриц $A(D)$ и $A(D')$ совпадают. Применяя элементарные преобразования к строкам матрицы $A(D)$, мы получим

$$A(D) \rightsquigarrow \begin{pmatrix} 1 & \mathbf{0}^\top & \mathbf{1}^\top \\ \mathbf{0} & A_0 & A_1 \\ \mathbf{0} & A_1^\top & A_2 + (1) \end{pmatrix},$$

т. е. $\text{corank } A(D) = \text{corank } A(D')$. Хордовая диаграмма D' содержит $n - 1$ хорд, т. е. для нее утверждение теоремы справедливо. Справедливость утверждения теоремы для D следует из цепочки равенств

$$\begin{aligned} \text{число компонент многообразия } M(D) &= \\ &= \text{число компонент многообразия } M(D') = \\ &= \text{corank } A(D') + 1 = \text{corank } A(D) + 1. \end{aligned}$$

(2) Пусть все хорды оснащенной хордовой диаграммы D имеют оснащение, равное нулю. Если все хорды попарно не зацеплены, то справедливость утверждения для D следует из базы индукции. Пусть хорды a и b зацеплены. Рассмотрим оснащенную хордовую диаграмму D' , получающуюся из D последовательным применением операции оснащенная звездочка к хордам a , b и снова a , и последующим удалением этих хорд, т. е. мы совершили перестройку вдоль a и b .

Доказательство этого случая аналогично доказательству первого случая, мы оставляем его в качестве упражнения.

Пусть D — оснащенная хордовая диаграмма с матрицей пересечений $A(D)$. Построим матрицу $\hat{A}(D)$, выкидывая строки и столбцы матрицы $A(D)$, соответствующие гауссовым хордам.

ТЕОРЕМА 4 ((см. [7, 18])). *Пусть H — 4-граф с крестовой структурой, и пусть U — эйлеров цикл на H . Тогда H имеет гауссов цикл тогда и только тогда, когда $\text{corank}(\hat{A}(D) + E) = 0$, где D — оснащенная хордовая диаграмма, построенная из U , и E — единичная матрица.*

УПРАЖНЕНИЕ 7. Используя теорему 3 и рис. 15, докажите теорему 4.

3.2. ГАУССОВ ЦИКЛ

Пусть H — 4-граф с крестовой структурой, имеющий гауссов цикл, и пусть U — эйлеров цикл на H . Будем считать, что $m(U)$ (соотв., хордовая диаграмма D) не имеет гауссовых вершин (соотв., гауссовых хорд), т. е. U — поворачивающий обход.

ОПРЕДЕЛЕНИЕ 9. Две матрицы $A = (a_{ij})$ и $B = (b_{kl})$ равны с точностью до диагональных элементов, если $a_{ij} = b_{ij}$ при $i \neq j$.

Основной результат статьи — следующая теорема.

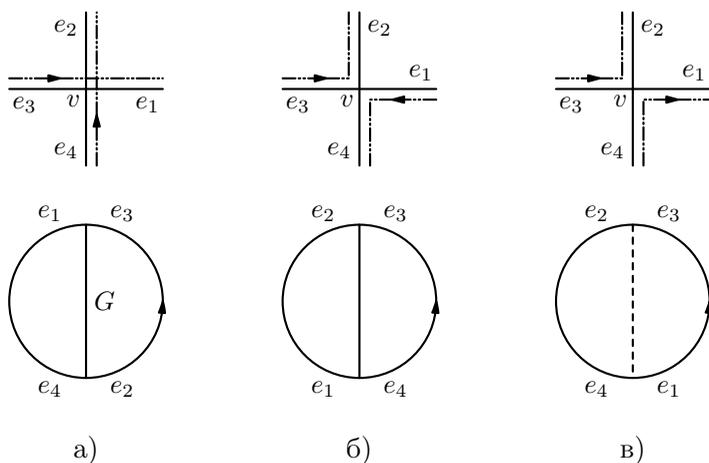


Рис. 15. Структура оснащенной хордовой диаграммы

ТЕОРЕМА 5 ([6]). Матрица пересечений гауссова цикла, рассматриваемая над \mathbb{Z}_2 , с точностью до диагональных элементов равна $(A(D) + E)^{-1}$.

Перед доказательством теоремы мы сформулируем утверждение, на котором базируется доказательство теоремы, в виде упражнения.

УПРАЖНЕНИЕ 8. Рассмотрим две операции, которые мы будем называть *уменьшающими*:

- 1) оснащенная звездочка, примененная к негауссовой хорде с оснащением 0, см. рис. 10 а);
- 2) $t \mapsto (((t*a)*b)*a)$, где t — оснащенное циклическое слово с двойным вхождением, a, b — негауссовы буквы (хорды) с оснащением 1 и они чередуются в t (зацеплены), см. рис. 16.

Докажите, что, применяя эти две операции к диаграмме D , мы за конечное число шагов получим хордовую диаграмму, содержащую только гауссовы хорды.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 5. Пусть $V(H) = \{v_1, \dots, v_n\}$.

Пусть $A(D)$ — матрица пересечений хордовой диаграммы D , не содержащей гауссовых хорд. Будем применять уменьшающие операции. Без ограничения общности можно считать, что уменьшающие операции применяются к хордам с наименьшими номерами в нашей нумерации. Тогда первая уменьшающая операция, примененная к первому элементу, на

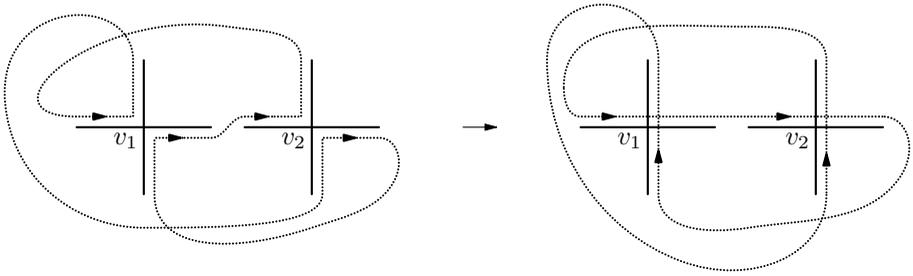


Рис. 16. Уменьшающая операция

языке матриц выглядит следующим образом

$$A(D) = \begin{pmatrix} 0 & \mathbf{0}^\top & \mathbf{1}^\top \\ \mathbf{0} & A_0 & A_1 \\ \mathbf{1} & A_1^\top & A_2 \end{pmatrix} \rightsquigarrow A(D') = \begin{pmatrix} G & \mathbf{0}^\top & \mathbf{1}^\top \\ \mathbf{0} & A_0 & A_1 \\ \mathbf{1} & A_1^\top & A_2 + (1) \end{pmatrix},$$

а вторая, примененная к двум первым элементам, —

$$A(D) = \begin{pmatrix} 1 & 1 & \mathbf{0}^\top & \mathbf{1}^\top & \mathbf{0}^\top & \mathbf{1}^\top \\ 1 & 1 & \mathbf{0}^\top & \mathbf{0}^\top & \mathbf{1}^\top & \mathbf{1}^\top \\ \mathbf{0} & \mathbf{0} & A_0 & A_1 & A_2 & A_3 \\ 1 & \mathbf{0} & A_1^\top & A_4 & A_5 & A_6 \\ \mathbf{0} & 1 & A_2^\top & A_5^\top & A_7 & A_8 \\ 1 & 1 & A_3^\top & A_6^\top & A_8^\top & A_9 \end{pmatrix} \rightsquigarrow \begin{pmatrix} G & 1 & \mathbf{0}^\top & \mathbf{0}^\top & \mathbf{1}^\top & \mathbf{1}^\top \\ 1 & G & \mathbf{0}^\top & \mathbf{1}^\top & \mathbf{0}^\top & \mathbf{1}^\top \\ \mathbf{0} & \mathbf{0} & A_0 & A_1 & A_2 & A_3 \\ \mathbf{0} & 1 & A_1^\top & A_4 & A_5 + (1) & A_6 + (1) \\ 1 & \mathbf{0} & A_2^\top & A_5^\top + (1) & A_7 & A_8 + (1) \\ 1 & 1 & A_3^\top & A_6^\top + (1) & A_8^\top + (1) & A_9 \end{pmatrix}.$$

Мы будем последовательно применять эти операции к хордовой диаграмме D . Наша следующая цель — показать, что после применения уменьшающих операций к оснащенной хордовой диаграмме D , не имеющей гауссовых хорд, мы в итоге получим оснащенную хордовую диаграмму, содержащую только гауссовы хорды и имеющую с точностью до диагональных элементов матрицу $(A(D) + E)^{-1}$ своей матрицей пересечений.

Матрицу $(A(D) + E)^{-1}$ мы будем находить, совершая элементарные преобразования над строками матрицы $B(D) = A(D) + E$ с $\det(A(D) +$

$+E) = 1$. Построим матрицу $(A(D)+E|E)$ размера $n \times 2n$. Обозначим через $\widehat{M}_{ij\dots k}$ матрицу, полученную из матрицы M удалением строк и столбцов с номерами i, j, \dots, k .

Так как $\det B(D) = 1$, то или существует диагональный элемент равный 1, или два таких номера i и j , что $b_{ii} = b_{jj} = 0$, $b_{ij} = b_{ji} = 1$.

В первом случае без ограничения общности можно предположить, что $b_{11} = 1$. Совершая элементарные преобразования над матрицей $B(D)$ с помощью первой строки, получаем

$$\begin{aligned} B(D) = A(D) + E &= \begin{pmatrix} 1 & \mathbf{0}^\top & \mathbf{1}^\top \\ \mathbf{0} & A_0 + E & A_1 \\ \mathbf{1} & A_1^\top & A_2 + E \end{pmatrix} \rightsquigarrow \\ &\rightsquigarrow B'(D) = \begin{pmatrix} 1 & \mathbf{0}^\top & \mathbf{1}^\top \\ \mathbf{0} & A_0 + E & A_1 \\ \mathbf{0} & A_1^\top & A_2 + E + (1) \end{pmatrix} \end{aligned}$$

и

$$\begin{aligned} (B(D)|E) &\rightsquigarrow (B'(D)|E') = \\ &= \left(\begin{array}{ccc|ccc} 1 & \mathbf{0}^\top & \mathbf{1}^\top & 1 & \mathbf{0}^\top & \mathbf{0}^\top \\ \mathbf{0} & A_0 + E & A_1 & \mathbf{0} & E & 0 \\ \mathbf{0} & A_1^\top & A_2 + E + (1) & \mathbf{1} & 0 & E \end{array} \right). \end{aligned}$$

После применения первой уменьшающей операции к хордовой диаграмме D хорда, соответствующая вершине v_1 , становится гауссовой хордой, и пересечения негауссовых хорд определяются матрицей $\widehat{B'(D)}_1$, а другие пересечения определяются первым столбцом матрицы E' (с точностью до диагональных элементов).

Во втором случае без ограничения общности можем предположить, что $b_{11} = b_{22} = 0$, $b_{12} = b_{21} = 1$. Совершая элементарные преобразования с помощью первых двух строк матрицы $B(D)$, мы получим

$$\begin{aligned} B(D) = A(D) + E &= \\ &= \begin{pmatrix} 0 & 1 & \mathbf{0}^\top & \mathbf{1}^\top & \mathbf{0}^\top & \mathbf{1}^\top \\ 1 & 0 & \mathbf{0}^\top & \mathbf{0}^\top & \mathbf{1}^\top & \mathbf{1}^\top \\ \mathbf{0} & \mathbf{0} & A_0 + E & A_1 & A_2 & A_3 \\ \mathbf{1} & \mathbf{0} & A_1^\top & A_4 + E & A_5 & A_6 \\ \mathbf{0} & \mathbf{1} & A_2^\top & A_5^\top & A_7 + E & A_8 \\ \mathbf{1} & \mathbf{1} & A_3^\top & A_6^\top & A_8^\top & A_9 + E \end{pmatrix} \rightsquigarrow \end{aligned}$$

Рассмотрим первый случай. Без ограничения общности считаем, что $r_{11} = 1$. В этом случае мы применим первую уменьшающую операцию. Мы получим

$$\begin{aligned}
 (B'(D)|E') &= \left(\begin{array}{ccc|cc} E & C & & F & 0 \\ 0 & R & & S & E \end{array} \right) = \\
 &= \left(\begin{array}{cccc|cccc} E & C_1 & C_2 & C_3 & F & 0 & 0 & 0 \\ 0 & 1 & \mathbf{0}^\top & \mathbf{1}^\top & S_1 & 1 & \mathbf{0}^\top & \mathbf{0}^\top \\ \mathbf{0} & \mathbf{0} & R_1 & R_2 & S_2 & \mathbf{0} & E & 0 \\ \mathbf{0} & \mathbf{1} & R_2^\top & R_3 & S_3 & \mathbf{0} & 0 & E \end{array} \right) \rightsquigarrow \\
 &\rightsquigarrow \left(\begin{array}{cccc|cccc} E & 0 & C'_2 & C'_3 & F'_1 & F'_2 & 0 & 0 \\ 0 & 1 & \mathbf{0}^\top & \mathbf{1}^\top & S_1 & 1 & \mathbf{0}^\top & \mathbf{0}^\top \\ \mathbf{0} & \mathbf{0} & R_1 & R_2 & S_2 & \mathbf{0} & E & 0 \\ \mathbf{0} & \mathbf{0} & R_2^\top & R_3 + (1) & S'_3 & \mathbf{1} & 0 & E \end{array} \right) = \\
 &= \left(\begin{array}{ccc|cc} E & C' & & F' & 0 \\ 0 & R' & & S' & E \end{array} \right) = (B''(D)|E''),
 \end{aligned}$$

где F' — это $((l+1) \times (l+1))$ -матрица, R' — это симметрическая матрица. Число гауссовых хорд равно $l+1$, пересечения негауссовых хорд определяются матрицей R' , а все оставшиеся пересечения — первыми $l+1$ столбцами матрицы E'' . Второй случай рассматривается аналогично первому.

В конце мы получим матрицу

$$\left(E \mid (A(D) + E)^{-1} \right)$$

и оснащенную хордовую диаграмму только с гауссовыми хордами. Матрица пересечений полученной хордовой диаграммы с точностью до диагональных элементов равна $(A(D) + E)^{-1}$.

Мы доказали теорему для недиагональных элементов, но мы знаем, что на диагонали будут стоять буквы G . \square

ЗАМЕЧАНИЕ 7. Пусть H — произвольный (связный и содержащий хотя бы одну вершину) ориентированный 4-граф, причем в каждую вершину входят и выходят ровно два полуребра (ориентации полуребер, соответствующих одному ребру, совпадают). Легко видеть, что на графе H существует ориентированный эйлеров цикл U . Зададим крестовую структуру на H таким образом, чтобы U являлся поворачивающим обходом на уже новом графе с крестовой структурой, и в каждой вершине пара противоположных полуребер состоит из входящего и исходящего из нее полуребер. Если на полученном ориентированном 4-графе с крестовой структурой существует ориентированный гауссов цикл, то теорема 5 дает формулу для

матрицы пересечений гауссова цикла. Таким образом, последнее утверждение о существовании гауссова цикла является теоремой 3.4 из [19], и, следовательно, теорема 3.4 из [19] является частным случаем теоремы 5.

4. СЛЕДСТВИЯ ИЗ ТЕОРЕМЫ 5

Используя разные критерии планарности 4-графа с крестовой структурой и теорему 5, мы в данном разделе сформулируем интересные факты, касающиеся симметрических матриц. На самом деле не каждая симметрическая матрица является матрицей пересечений некоторого эйлерова цикла [10], но как было показано в [6] аналогичные утверждения можно сформулировать для всех симметрических матриц над полем \mathbb{Z}_2 .

СЛЕДСТВИЕ 1. Пусть U_1 и U_2 — два поворачивающих обхода одного и того же 4-графа с крестовой структурой, и пусть D_1 и D_2 — их оснащенные хордовые диаграммы такие, что $\det(A(D_i) + E) = 1$. Тогда матрицы $(A(D_1) + E)^{-1}$ и $(A(D_2) + E)^{-1}$ совпадают с точностью до диагональных элементов.

ПРИМЕР 6. Рассмотрим 4-граф с крестовой структурой, состоящий из 4 вершин v_i , рис. 5 (структура индуцируется из плоскости). Пусть U_1 и U_2 — два поворачивающих обхода, заданные оснащенные циклическими словами с двойными вхождениями

$$m(U_1) = (v_1 v_4 v_2 v_1^{-1} v_2 v_3 v_4 v_3) \quad \text{и} \quad m(U_2) = (v_1 v_4 v_3 v_4 v_2 v_3 v_1 v_2^{-1}),$$

соответственно. Тогда

$$A(m(U_1)) = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \quad A(m(U_2)) = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Мы получаем

$$(A(m(U_1)) + E)^{-1} = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix},$$

$$(A(m(U_2)) + E)^{-1} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

и

$$A = \begin{pmatrix} G & 0 & 1 & 1 \\ 0 & G & 1 & 1 \\ 1 & 1 & G & 1 \\ 1 & 1 & 1 & G \end{pmatrix}$$

— матрица пересечений гауссова цикла, заданного с помощью слова

$$(v_1 v_4 v_3 v_1 v_2 v_4 v_3 v_2).$$

ОПРЕДЕЛЕНИЕ 10. Оснащенная хордовая диаграмма называется *d-диаграммой* [4], если все ее хорды являются негауссовыми хордами с оснащением 0, и множество всех ее хорд может быть разбито на два дизъюнктных подмножества, причем хорды из одного множества не зацеплены друг с другом.

Следующее следствие сразу следует из критерия планарности 4-графа с крестовой структурой, сформулированного на языке поворачивающих обходов, и из теории атомов, см. [3, 15].

СЛЕДСТВИЕ 2 (В. О. МАНТУРОВ). Пусть D — оснащенная хордовая диаграмма, все хорды которой являются негауссовыми с оснащением 0, и $\det(A(D) + E) = 1$. Если числа $\lambda_1, \dots, \lambda_n \in \mathbb{Z}_2$ таковы, что

$$\det((A(D) + E)^{-1} + \text{diag}(\lambda_1, \dots, \lambda_n)) = 1,$$

то матрица

$$((A(D) + E)^{-1} + \text{diag}(\lambda_1, \dots, \lambda_n))^{-1}$$

имеет единицы на диагонали. Кроме того, если D является *d-диаграммой*, то матрица

$$((A(D) + E)^{-1} + \text{diag}(\lambda_1, \dots, \lambda_n))^{-1}$$

является матрицей пересечений *d-диаграммы*. Здесь через

$$\text{diag}(\lambda_1, \dots, \lambda_n)$$

обозначена диагональная матрица с числами $\lambda_1, \dots, \lambda_n$ на диагонали.

Геометрически первая часть следствия 2 означает следующее. Имея 4-граф H с крестовой структурой и некоторый поворачивающий обход U на нем, мы можем задать ориентацию на H : ориентируем обход U произвольным образом и зададим с помощью него ориентацию на H . Мы скажем, что обход U задает *седловую ориентацию*, если каждая пара противоположных ребер состоит из двух входящих в вершину или двух исходящих из нее полуредер, см. рис. 17. Заметим, что наличие седловой ориентации не зависит от ориентации обхода U . Оказывается, если какой-то поворачивающий обход задает седловую ориентацию на 4-графе с

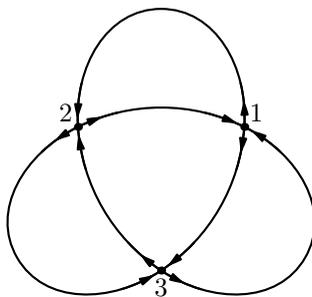


Рис. 17. Седловая ориентация

крестовой структурой, то и любой другой поворачивающий обход тоже будет задавать седловую ориентацию. Вторая часть следствия относится к вопросу планарности. Если у нас имеется планарный 4-граф с крестовой структурой, т. е. вложенный в плоскость граф с сохранением структуры, то все поворачивающие обходы задают d -диаграммы.

Хорошо известно необходимое условие планарности 4-графа с крестовой структурой в терминах матрицы пересечений гауссова цикла.

ТЕОРЕМА 6 (ТЕОРЕМА ГАУССА [16]). Пусть H — 4-граф с крестовой структурой, имеющий гауссов цикл, и пусть D — гауссова диаграмма. Тогда если граф H планарен, то сумма элементов в каждой строке (каждом столбце) матрицы $A(D)$, за исключением диагонального элемента, равна нулю по модулю два.

Отсюда получаем

СЛЕДСТВИЕ 3. Пусть D — d -диаграмма, и $\det(A(D) + E) = 1$. Тогда сумма элементов в каждой строке (каждом столбце) матрицы $(A(D) + E)^{-1}$, за исключением диагонального элемента, равна нулю по модулю два.

СПИСОК ЛИТЕРАТУРЫ

- [1] В. О. Мантуров. Вложения четырехвалентных оснащенных графов в двумерные поверхности // Доклады РАН. Т. 424, №3. 2009. Р. 308–310.
- [2] В. О. Мантуров. Доказательство гипотезы В. А. Васильева о планарности сингулярных зацеплений // Известия РАН: Сер. Мат. Т. 69, №5. 2005. Р. 169–178.
- [3] В. О. Мантуров. Теория узлов. Москва–Ижевск: РХД, 2005.

- [4] В. О. Мантуров. *Скобочная полугруппа узлов* // Мат. Заметки. Т. 67, №4. 2000. P. 449–462.
- [5] В. О. Мантуров. *Четырехвалентные графы с крестовой структурой. Вложения в двумерные поверхности* // Математическое просвещение. Сер. 3, вып. 16. 2012. С. 94–104.
- [6] Д. П. Ильютко. *Оснащенные 4-графы: эйлеровы циклы, гауссовы циклы и поворачивающие обходы* // Матем. сб. Т. 202, №9. 2011. P. 53–76.
- [7] Д. П. Ильютко, В. О. Мантуров. *Граф-зацепления* // Доклады РАН. Т. 428, №5. 2009. P. 591–594.
- [8] D. Bar-Natan. *On the Vassiliev Knot Invariants* // Topology. Vol. 34. 1995. P. 423–472.
- [9] D. Bar-Natan, S. Garoufalidis. *On the Melvin – Morton – Rozansky conjecture* // Inv. Math. Vol. 125. 1996. P. 103–133.
- [10] A. Bouchet. *Circle graph obstructions* // J. Combinatorial Theory, ser. B. Vol. 60. 1994. P. 107–144.
- [11] G. Cairns, D. Elton. *The planarity problem for signed Gauss words* // Journal of Knot Theory and Its Ramifications. Vol. 2. 1993. P. 359–367.
- [12] G. Cairns, D. Elton. *The planarity problem. II* // Journal of Knot Theory and Its Ramifications. Vol. 5. 1996. P. 137–144.
- [13] S. V. Chmutov, S. V. Duzhin, S. K. Lando. *Vassiliev Knot Invariants. I, II, III* // Adv. Sov. Math. Vol. 21. 1994. P. 117–147.
- [14] M. Cohn, A. Lempel. *Cycle decomposition by disjoint transpositions* // J. Combin. Theory, ser. A. Vol. 13. 1972. P. 83–89.
- [15] A. T. Fomenko. *The theory of multidimensional integrable hamiltonian systems (with arbitrary many degrees of freedom). Molecular table of all integrable systems with two degrees of freedom* // Adv. Sov. Math. Vol. 6. 1991. P. 1–35.
- [16] C. F. Gauss *Werke*. Band 8. Göttingen: Teubner. 1900.
- [17] M. Goussarov, M. Polyak, O. Viro. *Finite type invariants of classical and virtual knots* // Topology. Vol. 39. 2000. P. 1045–1068.
- [18] D. P. Ilyutko, V. O. Manturov. *Introduction to graph-link theory* // Journal of Knot Theory and Its Ramifications. Vol. 18. 2009. P. 791–823.

- [19] J. Jonsson. *On the number of Euler trails in directed graphs* // Math. Scand. Vol. 90. 2002. P. 191–214.
- [20] A. Kotzig. *Eulerian lines in finite 4-valent graphs and their transformations* // Theory of Graphs (Proc. Colloq., Tihany, 1966). New York: Academic Press. 1968. P. 219–230.
- [21] G. Moran. *Chords in a circle and linear algebra over $GF(2)$* // J. Combin. Theory, ser. A. Vol. 37. 1984. P. 239–247.
- [22] R. C. Read, P. Rosenstiehl. *On the Gauss crossing problem* // Colloq. Math. Soc. Janos Bolyai. Amsterdam and New-York: North-Holland. 1976. P. 843–876.
- [23] E. Soboleva. *Vassiliev Knot Invariants Coming from Lie Algebras and 4-Invariants* // Journal of Knot Theory and Its Ramifications. Vol. 10. 2001. P. 161–169.
- [24] S. Stahl. *On the product of certain permutations* // Europ. J. Combin. Vol. 8. 1987. P. 69–72.
- [25] L. Traldi *Binary nullity, Euler circuits and interlace polynomials*. 2009. [arXiv:math.CO/0903.4405](https://arxiv.org/abs/math/0903.4405)
- [26] V. G. Turaev *Cobordisms of Words*. 2005. [arXiv: math.CO/0511513v2](https://arxiv.org/abs/math/0511513v2)

Задача Эрдёша – Гинзбурга – Зива и ее окрестности

А. М. Райгородский

1. ВВЕДЕНИЕ

В этой статье мы поговорим об одной из самых красивых задач современной комбинаторики. Ее предложили в далеком 1961 году П. Эрдёш, А. Гинзбург и А. Зив, которым удалось доказать следующее замечательное утверждение.

ТЕОРЕМА 1 (Эрдёш, Гинзбург, Зив, 1961). *Из любого множества $A = \{a_1, \dots, a_{2n-1}\}$, состоящего из целых чисел, можно выбрать n чисел, сумма которых делится на n .*

Разумеется, числа в множестве A из формулировки теоремы не обязаны быть различными. Более того, нам лишь нужно знать, какой остаток от деления на n дают эти числа. Понятно сразу, что в некотором смысле теорема 1 неуплучшаема: величину $2n - 1$ в ней нельзя заменить на $2n - 2$. Действительно, если взять числа

$$a_1 = \dots = a_{n-1} = 0, \quad a_n = \dots = a_{2n-2} = 1,$$

то среди них уже не будет n чисел, сумма которых делится на n .

С одной стороны, теорема 1 послужила отправной точкой для развития целого направления в комбинаторной математике. Науку, которая выросла из нее, принято относить к «аддитивной комбинаторике», т. е. к разделу комбинаторики, в котором изучаются задачи, связанные с отысканием различных множеств чисел, чьи суммы обладают теми или иными интересными свойствами.

С другой стороны, теорема 1 весьма «олимпиадна», и потому ее сразу полюбили популяризаторы математики. По-видимому, особенный всплеск ее популярности пришелся на начало 70-х годов XX века, когда, например, в «Кванте» была опубликована статья с ее доказательством (см. [4]). Позже в «олимпиадной» среде задачу Эрдёша – Гинзбурга – Зива слегка подзабыли, о чем свидетельствует еще одна недавняя статья в том же «Кванте» (см. [5]).

В этой статье нам хочется рассказать о той удивительной науке, которая выросла из теоремы 1 и которую незаслуженно мало знают у нас в стране. Но прежде всего мы изложим одно очень красивое доказательство теоремы, основанное на применении малой теоремы Ферма. Оно не самое простое из многочисленных известных доказательств (см. [4–7]), но для наших целей оно будет исключительно полезно: именно его главная идея ляжет в основу всех дальнейших изысканий.

2. ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1

Ниже мы рассмотрим лишь случай, когда $n = p$, где p — простое число. Переход к общему случаю достаточно прост, и о нем можно прочесть в статье [5]. Поскольку мы собираемся пользоваться малой теоремой Ферма, в первом параграфе этого раздела мы напомним читателю все необходимые сведения из классической арифметики, а также приведем пару утверждений о делимости биномиальных коэффициентов. Во втором параграфе мы изложим доказательство теоремы 1.

2.1. НЕМНОГО ТЕРМИНОЛОГИИ И НЕСКОЛЬКО ВСПОМОГАТЕЛЬНЫХ ФАКТОВ

Выражение « a делится на p » мы часто будем записывать в виде « $a \equiv 0 \pmod{p}$ » (читается « a сравнимо с нулем по модулю p »). Вообще, запись « $a \equiv b \pmod{p}$ » подразумевает, что $b - a$ делится на p , т. е. у чисел a и b одинаковые остатки от деления на p .

Пусть дано множество чисел $A = \{a_1, \dots, a_k\}$. Рассмотрим множество индексов $I = \{i_1, \dots, i_l\} \subseteq \{1, \dots, k\}$. Тогда сумма вида $\sum_{i \in I} a_i$ — это просто $a_{i_1} + \dots + a_{i_l}$.

Количество элементов в данном множестве X обозначим через $|X|$. Под записью

$$\sum_{\substack{I \subseteq \{1, \dots, k\}: \\ |I|=l}} \sum_{i \in I} a_i$$

будем понимать сумму по всем l -элементным подмножествам множества $\{1, \dots, k\}$ уже известных нам сумм $\sum_{i \in I} a_i$. Например,

$$\sum_{\substack{I \subseteq \{1, 2, 3, 4\}: \\ |I|=2}} \sum_{i \in I} a_i = (a_1 + a_2) + (a_1 + a_3) + (a_1 + a_4) + (a_2 + a_3) + (a_2 + a_4) + (a_3 + a_4).$$

В новых терминах теорема Эрдёша – Гинзбурга – Зива звучит так: для любого множества $A = \{a_1, \dots, a_{2p-1}\}$, состоящего из целых чисел,

существует такое множество $I \subset \{1, \dots, 2p-1\}$, что $|I| = p$ и $\sum_{i \in I} a_i \equiv 0 \pmod{p}$.

Хорошо известна следующая теорема.

ТЕОРЕМА 2 (МАЛАЯ ТЕОРЕМА ФЕРМА). Если $a \not\equiv 0 \pmod{p}$, то $a^{p-1} \equiv 1 \pmod{p}$.

Доказательство теоремы 2 можно найти в любой книжке по арифметике или теории чисел. Например, оно есть в книге [3]. Однако мы приведем ниже одно симпатичное рассуждение, которое также доказывает теорему и вместе с тем идейно близко ко всему, о чем пойдет речь дальше.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2. Достаточно показать, что $a^p \equiv a \pmod{p}$, если $a > 0$. Имеем

$$a^p = (1 + 1 + \dots + 1)^p = 1^p + 1^p + \dots + 1^p + \sum \frac{p!}{n_1! \dots n_a!} 1^{n_1} \dots 1^{n_a},$$

где последнее суммирование идет по всем упорядоченным наборам чисел $n_1 < p, \dots, n_a < p$, для которых $n_1 + \dots + n_a = p$. Поскольку число p простое, величина $\frac{p!}{n_1! \dots n_a!}$ делится на p (ведь в знаменателе нет ни одного числа, делящегося на p). Таким образом,

$$a^p \equiv 1^p + 1^p + \dots + 1^p \pmod{p}, \quad a^p \equiv a \pmod{p},$$

и теорема доказана.

Нам потребуются следующие два факта относительно биномиальных коэффициентов.

УТВЕРЖДЕНИЕ 1. Для любого простого числа p выполнено $C_{2p-1}^p \equiv 1 \pmod{p}$.

УТВЕРЖДЕНИЕ 2. Для любого простого числа p и любого $q \in \{1, \dots, p-1\}$ выполнено $C_{2p-1-q}^{p-q} \equiv 0 \pmod{p}$.

Докажем, для примера, утверждение 1; второе утверждение доказывается аналогично.

ДОКАЗАТЕЛЬСТВО УТВЕРЖДЕНИЯ 1. Посмотрим на известное тождество

$$C_{2p}^0 + C_{2p}^1 + \dots + C_{2p}^p + \dots + C_{2p}^{2p} = 4^p.$$

В нем первое и последнее слагаемые равны единице. Остальные слагаемые, кроме C_{2p}^p , имеют вид $C_{2p}^i = \frac{(2p)!}{i!(2p-i)!}$ с $i \neq p$. Ясно, что в каждом из них числитель делится на p^2 , а знаменатель не делится. Значит, $C_{2p}^i \equiv 0 \pmod{p}$, т. е.

$$C_{2p}^0 + C_{2p}^1 + \dots + C_{2p}^p + \dots + C_{2p}^{2p} \equiv 2 + C_{2p}^p \pmod{p}.$$

В то же время по малой теореме Ферма $4^p \equiv 4 \pmod{p}$. Получается, что $C_{2p}^p \equiv 2 \pmod{p}$. Но

$$C_{2p-1}^p = \frac{1}{2} C_{2p}^p \equiv 1 \pmod{p},$$

и утверждение доказано.

Отметим, что в связи с теоремой 2 и утверждениями 1 и 2 очень полезны статьи [1, 2].

2.2. САМО ДОКАЗАТЕЛЬСТВО

Будем работать с переформулировкой теоремы 1, которую мы привели в параграфе 2.1. Предположим, что, вопреки ее утверждению, для любого множества $I \subset \{1, \dots, 2p-1\}$, имеющего p элементов, $\sum_{i \in I} a_i \not\equiv 0 \pmod{p}$.

Тогда по малой теореме Ферма

$$\left(\sum_{i \in I} a_i \right)^{p-1} \equiv 1 \pmod{p}.$$

Следовательно, с учетом утверждения 1

$$S = \sum_{\substack{I \subset \{1, \dots, 2p-1\}: \\ |I|=p}} \left(\sum_{i \in I} a_i \right)^{p-1} \equiv C_{2p-1}^p \equiv 1 \pmod{p}.$$

С другой стороны, раскроем скобки в выражении $\left(\sum_{i \in I} a_i \right)^{p-1}$. Понятно, что каждое слагаемое в результирующей сумме будет иметь вид

$$a_{i_1}^{k_{i_1}} \cdot \dots \cdot a_{i_q}^{k_{i_q}},$$

где $1 \leq q \leq p-1$, $k_{i_1} \geq 1, \dots, k_{i_q} \geq 1$, а $k_{i_1} + \dots + k_{i_q} = p-1$. Значит, можно написать

$$S = \sum_{\substack{I \subset \{1, \dots, 2p-1\}: \\ |I|=p}} \sum a_{i_1}^{k_{i_1}} \cdot \dots \cdot a_{i_q}^{k_{i_q}}.$$

Переставим в последней записи порядки суммирования. Иными словами, сперва зафиксируем произвольное выражение

$$a_{i_1}^{k_{i_1}} \cdot \dots \cdot a_{i_q}^{k_{i_q}},$$

а затем посчитаем, сколько есть множеств $I \subset \{1, \dots, 2p-1\}$ из p элементов, для каждого из которых это выражение могло возникнуть при раскрытии скобок в записи $\left(\sum_{i \in I} a_i \right)^{p-1}$. Нетрудно видеть, что такие множества I должны содержать набор $\{i_1, \dots, i_q\}$ в качестве подмножества,

т. е. их ровно C_{2p-1-q}^{p-q} штук. Ввиду утверждения 2 это количество делится на p . Иначе говоря, каждое слагаемое в сумме S делится на p , а стало быть, $S \equiv 0 \pmod{p}$.

Однако выше, исходя из предположения противного, мы получили $S \equiv 1 \pmod{p}$. Имеем противоречие, и теорема 1 доказана.

3. ПЕРВОЕ ОБОБЩЕНИЕ ЗАДАЧИ ЭРДЁША – ГИНЗБУРГА – ЗИВА: ПРОБЛЕМА КЕМНИЦА

В этом разделе мы расскажем об исключительно красивом «двумерном» аналоге теоремы Эрдёша – Гинзбурга – Зива.

3.1. НЕМНОГО ОБ ИСТОРИИ

В 1983 году А. Кемниц придумал одно очень естественное обобщение задачи Эрдёша – Гинзбурга – Зива. Он предложил вместо целых чисел рассматривать пары целых чисел, которые представляют собой точки на обычной плоскости, имеющие целые координаты.

Действительно, рассмотрим произвольное множество точек $A = \{(a_1, b_1), \dots, (a_f, b_f)\}$. Сложим любые n точек из множества A по координатно. Скажем, что полученная сумма (также являющаяся точкой на плоскости) делится на n , если обе ее координаты делятся на n . Иными словами, полученная при сложении точка должна иметь вид (na, nb) , где $a, b \in \mathbb{Z}$. Вопрос: при каком f мы можем гарантировать наличие в A подмножества мощности n , сумма элементов которого делится на n ?

Нетрудно видеть, что в качестве f нельзя взять $4n - 4$. В самом деле, пусть A содержит $n - 1$ точек $(0, 0)$, столько же точек $(0, 1)$, столько же точек $(1, 0)$ и столько же $(1, 1)$. Очевидно, в A нет n -элементных подмножеств с суммой элементов, делящейся на n .

Кемниц высказал гипотезу: $f = 4n - 3$. Эта гипотеза оказалась весьма «крепким орешком». Для нескольких маленьких значений n ее «вручную» проверили сам Кемниц и Х. Харборт. Затем Н. Алон и М. Дубинер в 1993 году показали, что $f \leq 6n - 5$. В 2000 году Л. Роньяи установил неравенство $f \leq 4n - 2$, и лишь в 2003 году гипотезу «дожал» Х. Райхер.

И Роньяи, и Райхер действовали примерно одинаково, и в основе их рассуждений было далеко идущее обобщение идей, которые мы использовали в параграфе 2.2. Рассуждение Райхера довольно трудное (см. [6]), а рассуждение Роньяи — это, пожалуй, одно из самых изящных рассуждений в комбинаторике. Его-то мы здесь и изложим (опять же, для простых n). Но сперва нам понадобится ряд вспомогательных понятий и фактов.

3.2. ЕЩЕ НЕМНОГО ТЕРМИНОЛОГИИ

Во-первых, мы будем писать $(a_1, b_1) + \dots + (a_k, b_k) \equiv 0 \pmod{p}$, подразумевая, что сумма точек делится на p .

Во-вторых, нам понадобятся многочлены от нескольких переменных. Конечно, все отлично знают, что многочлен — это запись вида $f(x) = a_n x^n + \dots + a_1 x + a_0$. Но это многочлен степени n от одной переменной x . Что же такое, например, многочлен степени n от двух переменных x, y ? Если $n = 0$, то по-прежнему речь идет о произвольной константе. Если $n = 1$, то общий вид многочлена таков: $f(x, y) = a_1 x + a_2 y + a_3$. При $n = 2$ имеем $f(x, y) = a_1 x^2 + a_2 y^2 + a_3 xy + a_4 x + a_5 y + a_6$. И так далее. Иными словами, $f(x, y) = \sum a_{i,j} x^i y^j$, где $a_{i,j} \in \mathbb{R}$, а суммирование идет по некоторым парам натуральных чисел i и j . При этом степень многочлена — это $\max(i + j)$.

Аналогично определяется многочлен произвольного числа переменных:

$$f(x_1, \dots, x_n) = \sum a_{i_1, \dots, i_n} x_1^{i_1} \cdot \dots \cdot x_n^{i_n}.$$

Его степень равна $\max(i_1 + \dots + i_n)$. Степень многочлена f обозначается $\deg f$. Числа $a_{i_1, \dots, i_n} \in \mathbb{R}$ называются коэффициентами многочлена.

Далее, у малой теоремы Ферма есть следующее уточнение: *для любого простого $p > 2$ и любого $k \in \{1, \dots, p - 2\}$ найдется такое число a , что $a^k \not\equiv 0 \pmod{p}$ и $a^k \not\equiv 1 \pmod{p}$* . Смысл уточнения в том, что в малой теореме Ферма нельзя заменить степень $p - 1$ на $k \leq p - 2$. Оставим его читателю в качестве упражнения.

Наконец, совсем легкое упражнение состоит в том, чтобы доказать такое утверждение: *если a взаимно просто с p и x пробегает от 1 до p , то ax тоже пробегает от 1 до p (но, возможно, в ином порядке)*.

3.3. ТЕОРЕМА ВАРНИНГА – ШЕВАЛЛЕ

Имеет место следующий замечательный факт.

ТЕОРЕМА 3 (ВАРНИНГ – ШЕВАЛЛЕ). *Пусть f — многочлен от n переменных с целыми коэффициентами степени строго меньше n . Пусть, далее, p — простое число. Обозначим через N количество различных наборов (x_1, \dots, x_n) , таких, что $x_i \in \{1, \dots, p\}$ для каждого i и $f(x_1, \dots, x_n) \equiv 0 \pmod{p}$. Тогда $N \equiv 0 \pmod{p}$.*

Теорема 3 означает, что число решений сравнения $f(x_1, \dots, x_n) \equiv 0 \pmod{p}$ делится на p , лишь бы было выполнено неравенство $\deg f < n$. Довольно забавный и, на вид, нетривиальный факт.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 3. С учетом малой теоремы Ферма

$$N \equiv \sum_{x_1=1}^p \dots \sum_{x_n=1}^p (1 - f^{p-1}(x_1, \dots, x_n)) \pmod{p}.$$

Значит, достаточно показать, что

$$\sum_{x_1=1}^p \dots \sum_{x_n=1}^p f^{p-1}(x_1, \dots, x_n) \equiv 0 \pmod{p}.$$

При возведении многочлена в степень и раскрытии скобок возникнет сумма выражений вида

$$a_{i_1, \dots, i_n} x_1^{i_1} \cdot \dots \cdot x_n^{i_n},$$

где $a_{i_1, \dots, i_n} \in \mathbb{Z}$, $i_1 + \dots + i_n < n(p-1)$ (ср. §2.2). Следовательно, достаточно убедиться в том, что для любых натуральных i_1, \dots, i_n , удовлетворяющих неравенству $i_1 + \dots + i_n < n(p-1)$, выполнено соотношение

$$S = \sum_{x_1=1}^p \dots \sum_{x_n=1}^p x_1^{i_1} \cdot \dots \cdot x_n^{i_n} \equiv 0 \pmod{p}.$$

Имеем

$$\sum_{x_1=1}^p \dots \sum_{x_n=1}^p x_1^{i_1} \cdot \dots \cdot x_n^{i_n} = \left(\sum_{x_1=1}^p x_1^{i_1} \right) \cdot \dots \cdot \left(\sum_{x_n=1}^p x_n^{i_n} \right).$$

Возможны два случая. В первом случае какое-то i_ν равно нулю. Тогда, очевидно, $S \equiv 0 \pmod{p}$, и теорема доказана.

Во втором случае все i_ν не меньше единицы. Но их сумма строго меньше $n(p-1)$. Значит, какое-то из них строго меньше $p-1$, т. е. оно лежит в пределах от 1 до $p-2$ (и, в частности, $p > 2$). Обозначим его k (ср. уточнение малой теоремы Ферма из параграфа 3.2). Исходя из упомянутого только что уточнения, возьмем то самое a , с которым $a^k \not\equiv 0 \pmod{p}$ и $a^k \not\equiv 1 \pmod{p}$. Тогда

$$a^k \cdot \sum_{x_\nu=1}^p x_\nu^k = \sum_{x_\nu=1}^p (ax_\nu)^k = \sum_{x_\nu=1}^p x_\nu^k.$$

Последнее равенство выполнено ввиду «легкого упражнения», завершающего параграф 3.2. В итоге $\sum_{x_\nu=1}^p x_\nu^k \equiv 0 \pmod{p}$, а стало быть, $S \equiv 0 \pmod{p}$. Теорема доказана.

У доказанной теоремы есть очевидное следствие.

СЛЕДСТВИЕ ИЗ ТЕОРЕМЫ 3. Пусть f — многочлен от n переменных с целыми коэффициентами степени строго меньше n . Пусть, далее, p —

простое число. Если набор (p, \dots, p) удовлетворяет сравнению $f(p, \dots, p) \equiv 0 \pmod{p}$, то найдется и набор (x_1, \dots, x_n) , в котором не все x_i делятся на p и с которым также $f(x_1, \dots, x_n) \equiv 0 \pmod{p}$.

Наконец, имеет место следующее обобщение, доказательство которого мы предоставим читателю.

ОБОБЩЕНИЕ СЛЕДСТВИЯ ИЗ ТЕОРЕМЫ 3. Пусть f_1, \dots, f_m – многочлены от n переменных с целыми коэффициентами, сумма степеней которых строго меньше n . Пусть, далее, p – простое число. Если набор (p, \dots, p) одновременно удовлетворяет всем сравнениям

$$f_1(p, \dots, p) \equiv 0 \pmod{p}, \quad \dots, \quad f_m(p, \dots, p) \equiv 0 \pmod{p},$$

то найдется и набор (x_1, \dots, x_n) , в котором не все x_i делятся на p и с которым также

$$f_1(x_1, \dots, x_n) \equiv 0 \pmod{p}, \quad \dots, \quad f_m(x_1, \dots, x_n) \equiv 0 \pmod{p}.$$

3.4. ОСНОВНАЯ ЛЕММА

Сейчас мы с помощью теоремы Варнинга – Шевалле установим следующий важный факт.

ЛЕММА 1. Пусть p – простое число. Пусть, далее, $(a_1, b_1), \dots, (a_{3p}, b_{3p})$ – произвольные точки с целыми координатами, сумма которых делится на p . Тогда найдется такое множество $I \subset \{1, \dots, 3p\}$, что $|I| = p$ и $\sum_{i \in I} (a_i, b_i) \equiv 0 \pmod{p}$.

ДОКАЗАТЕЛЬСТВО ЛЕММЫ 1. Зафиксируем произвольные точки $(a_1, b_1), \dots, (a_{3p}, b_{3p})$, удовлетворяющие соотношению $\sum_{i=1}^{3p} (a_i, b_i) \equiv 0 \pmod{p}$. Рассмотрим три многочлена

$$f_1(x_1, \dots, x_{3p-1}) = \sum_{i=1}^{3p-1} a_i x_i^{p-1},$$

$$f_2(x_1, \dots, x_{3p-1}) = \sum_{i=1}^{3p-1} b_i x_i^{p-1},$$

$$f_3(x_1, \dots, x_{3p-1}) = \sum_{i=1}^{3p-1} x_i^{p-1}.$$

Эти многочлены зависят от $3p-1$ переменных, и сумма их степеней, равная $3p-3$, строго меньше величины $3p-1$. Более того, набор (p, \dots, p) , очевидно, таков, что на нем все три многочлена принимают значения, делящиеся

на p . Значит, в силу обобщения следствия из теоремы 3, существует набор (x_1, \dots, x_{3p-1}) , в котором не все числа делятся на p и на котором, тем не менее, f_1, f_2, f_3 одновременно обнуляются по модулю p . Пусть J — множество, состоящее из всех индексов $i \in \{1, \dots, 3p-1\} \subset \{1, \dots, 3p\}$, с которыми $x_i \not\equiv 0 \pmod{p}$.

Мы знаем, что $f_1(x_1, \dots, x_n) \equiv 0 \pmod{p}$. Стало быть, с учетом малой теоремы Ферма, имеем

$$\sum_{i=1}^{3p-1} a_i x_i^{p-1} \equiv \sum_{i \in J} a_i x_i^{p-1} \equiv \sum_{i \in J} a_i \equiv 0 \pmod{p}.$$

Аналогично получаем

$$\sum_{i \in J} b_i \equiv 0 \pmod{p},$$

т. е.

$$\sum_{i \in J} (a_i, b_i) \equiv 0 \pmod{p}.$$

Наконец, из соотношения $f_3(x_1, \dots, x_n) \equiv 0 \pmod{p}$ вытекает сравнение $|J| \equiv 0 \pmod{p}$, т. е. либо $|J| = p$ и тогда лемма доказана (полагаем $I = J$), либо $|J| = 2p$. В последнем случае берем $I = \{1, \dots, 3p\} \setminus J$. Мощность множества I равна p , и

$$\sum_{i \in I} (a_i, b_i) = \sum_{i=1}^{3p} (a_i, b_i) - \sum_{i \in J} (a_i, b_i) \equiv 0 \pmod{p}.$$

Лемма доказана.

3.5. ДОКАЗАТЕЛЬСТВО НЕРАВЕНСТВА $f \leq 4p - 2$

Для краткости введем обозначение $m = 4p - 2$. Зафиксируем произвольные m точек $(a_1, b_1), \dots, (a_m, b_m)$. Мы хотим доказать существование такого множества $I \subset \{1, \dots, m\}$, что $|I| = p$ и $\sum_{i \in I} (a_i, b_i) \equiv 0$

\pmod{p} . Предположим, однако, что такого множества нет, т. е. для любого $I \subset \{1, \dots, m\}$, состоящего из p элементов, $\sum_{i \in I} (a_i, b_i) \not\equiv 0 \pmod{p}$. С учетом

леммы 1 можно предположить даже больше: для любого $I \subset \{1, \dots, m\}$, состоящего из p или $3p$ элементов, $\sum_{i \in I} (a_i, b_i) \not\equiv 0 \pmod{p}$. Постараемся

прийти к противоречию.

Обозначим через σ_p многочлен

$$\sigma_p(x_1, \dots, x_n) = \sum_{\substack{I \subset \{1, \dots, n\}: \\ |I|=p}} \prod_{i \in I} x_i.$$

Например,

$$\sigma_2(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4.$$

Положим

$$\begin{aligned} g(x_1, \dots, x_m) = & \\ = & \left(\left(\sum_{i=1}^m a_i x_i \right)^{p-1} - 1 \right) \left(\left(\sum_{i=1}^m b_i x_i \right)^{p-1} - 1 \right) \left(\left(\sum_{i=1}^m x_i \right)^{p-1} - 1 \right) \cdot \\ & \cdot (\sigma_p(x_1, \dots, x_m) - 2). \end{aligned}$$

Будем подставлять в многочлен g произвольные наборы (x_1, \dots, x_m) , состоящие из нулей и единиц. Рассмотрим несколько отдельных случаев.

Пусть $x_1 + \dots + x_m \in \{p, 3p\}$. В этом случае обозначим через I множество всех индексов i , с которыми $x_i = 1$, так что $|I| \in \{p, 3p\}$. Сделанное нами предположение противного означает, что для такого множества I , как и для любого другого аналогичного множества, выполнено $\sum_{i \in I} (a_i, b_i) \not\equiv 0 \pmod{p}$. Следовательно, либо $\sum_{i \in I} a_i \not\equiv 0 \pmod{p}$ и тогда за счет малой теоремы Ферма обнуляется (по модулю p) первая скобка в записи многочлена g , либо $\sum_{i \in I} b_i \not\equiv 0 \pmod{p}$ и тогда обнуляется вторая скобка в записи многочлена g . Иными словами, $g(x_1, \dots, x_m) \equiv 0 \pmod{p}$.

Пусть $x_1 + \dots + x_m = 2p$. В этом случае $\sigma_p(x_1, \dots, x_m) = C_{2p}^p$. Доказывая утверждение 1 (см. §2.1), мы по ходу дела поняли, что $C_{2p}^p \equiv 2 \pmod{p}$. Значит, обнуляется четвертая скобка в записи g , т.е. снова $g(x_1, \dots, x_m) \equiv 0 \pmod{p}$.

Пусть, $x_1 + \dots + x_m \not\equiv 0 \pmod{p}$. В этом случае обнуляется третья скобка, и опять $g(x_1, \dots, x_m) \equiv 0 \pmod{p}$.

Остается лишь случай, когда $x_1 = \dots = x_m = 0$. Здесь уже $g(x_1, \dots, x_m) = 2$.

Теперь представим себе, что мы раскрыли все четыре скобки в записи g . Разумеется, возникнет, как обычно, сумма выражений вида $x_{i_1}^{k_{i_1}} \dots x_{i_r}^{k_{i_r}}$, где $k_{i_1} \geq 1, \dots, k_{i_r} \geq 1$. Формально заменим каждое такое выражение выражением $x_{i_1} \dots x_{i_r}$. Получится новый многочлен g' , значения которого на наборах из нулей и единиц в точности совпадают со значениями исходного многочлена g .

Итак, у нас есть многочлен g' , который обнуляется на всех наборах нулевых и единичных аргументов, кроме набора из одних нулей, на котором его значение равно 2. При этом каждая переменная входит в этот многочлен в степени не выше 1. Читателю предлагается доказать, что тогда

$$g'(x_1, \dots, x_m) = 2 \cdot (1 - x_1) \cdot (1 - x_2) \cdot \dots \cdot (1 - x_m).$$

Ясно, что $\deg g' = m$. В то же время

$$\deg g' \leq \deg g = (p-1) + (p-1) + (p-1) + p = 4p - 3 < 4p - 2 = m.$$

Это и есть искомое противоречие, завершающее доказательство неравенства $f \leq 4p - 2$.

4. ВТОРОЕ ОБОБЩЕНИЕ ЗАДАЧИ ЭРДЁША – ГИНЗБУРГА – ЗИВА

По прочтении всего предшествующего текста сразу возникает вопрос: ну, хорошо, мы изучили наборы целых чисел и пар целых чисел; а почему бы не рассмотреть задачу про наборы последовательностей целых чисел произвольной длины d ? Разумеется, этим много занимались, и ниже мы об этом поговорим.

4.1. ПОСТАНОВКА ЗАДАЧИ

Итак, даны числа n и d . Обозначим через $f(n, d)$ наименьшее f , при котором для любого множества A , состоящего из f последовательностей целых чисел $(a_1^1, \dots, a_d^1), \dots, (a_1^f, \dots, a_d^f)$, найдется такое подмножество $I \subset \{1, \dots, f\}$, что $|I| = n$ и сумма $\sum_{i \in I} (a_1^i, \dots, a_d^i)$ делится на n (по каждой «координате»). Ясно, что $f(n, 1) = 2n - 1$ и $f(n, 2) = 4n - 3$. Что же будет, если $d \geq 3$?

Прежде всего очень легко обобщить примеры, свидетельствовавшие о том, что $f(n, 1) \geq 2n - 1$ и $f(n, 2) \geq 4n - 3$. Для этого надо взять все последовательности из d нулей и единиц и каждую такую последовательность проитерировать $n - 1$ раз. Получится множество A из $f = 2^d(n - 1)$ последовательностей, в котором нет n -элементных подмножеств с суммой элементов, делящейся на n . Иными словами, $f(n, d) \geq 2^d(n - 1) + 1$.

При $d = 1$ и $d = 2$ оценка $f(n, d) \geq 2^d(n - 1) + 1$ оказывалась точной, т. е. удавалось показать, что $f(n, d) = 2^d(n - 1) + 1$. Естественное предположение состоит в том, что последнее равенство выполнено для всех d . Однако и тут нас ожидает сюрприз: уже при $d = 3$ предположение неверно!

Действительно, рассмотрим девять последовательностей

$$\begin{aligned} (2, 1, 2), & \quad (0, 0, 0), & \quad (0, 0, 1), & \quad (0, 1, 0), & \quad (0, 1, 1), \\ (1, 0, 0), & \quad (1, 0, 1), & \quad (1, 1, 2), & \quad (1, 2, 2). \end{aligned}$$

Возьмем каждую из этих последовательностей дважды, в результате чего образуется множество A из восемнадцати последовательностей. Нетрудно убедиться в том, что в A нет трех последовательностей, сумма которых делится на 3. Иными словами, $f(3, 3) \geq 19$. В то же время неравенство $f(n, d) \geq 2^d(n - 1) + 1$ дает лишь оценку $f(3, 3) \geq 17$.

Описанная элементарная конструкция принадлежит Х. Харборту. В 2004 году Х. Элсхольц сумел обобщить ее, доказав в итоге, что $f(n, 3) \geq 9n - 8$ при всех нечетных n (см. [8]).

Видно, что задача становится исключительно трудной. Не ясно даже, каковы предположительные значения величины $f(n, d)$. В следующем параграфе мы перечислим некоторые из известных результатов.

4.2. НЕКОТОРЫЕ ИЗВЕСТНЫЕ РЕЗУЛЬТАТЫ

Прежде всего заметим, что всегда $f(n, d) \leq n^d(n-1) + 1$. В самом деле, пусть A — множество последовательностей, состоящее из $f = n^d + 1$ элементов. Тогда по принципу Дирихле в этом множестве есть две последовательности, сравнимые по модулю n , т. е. такие последовательности (a_1, \dots, a_d) , (b_1, \dots, b_d) , что $a_i \equiv b_i \pmod{n}$ для любого i . Значит, если в A не меньше $n^d(n-1) + 1$ элементов, то в A есть, как минимум, n попарно сравнимых последовательностей. Сумма любых n из них и делится на n .

Разумеется, оценка $f(n, d) \leq n^d(n-1) + 1$ крайне далека от оценки $f(n, d) \geq 2^d(n-1) + 1$. Однако, ввиду результатов Харборта и Элсхольца, описанных в предыдущем параграфе, трудно сказать даже, к какой из этих оценок ближе истинное значение величины $f(n, d)$.

Гораздо больших продвижений к настоящему времени удалось достичь в вопросе уточнения верхней оценки. Так, Алон и Дубинер доказали, что $f(n, d) \leq c(d)n$, где $c(d)$ — некоторая функция, зависящая от d , но не зависящая от n . Понятно, что при больших n (возможно, очень больших) оценка Алона – Дубинера значительно сильнее неравенства $f(n, d) \leq n^d(n-1) + 1$. Тем не менее, $c(d)$ гораздо больше, нежели 2^d , а потому до решения задачи еще крайне далеко (доказано, например, что $c(d) \geq 2^d 1.125^{\lfloor d/3 \rfloor}$).

Впрочем, при n , равном степени двойки, задача решена полностью. В 1973 году Харборт показал (см. [9]), что для любого a выполнено $f(2^a, d) = 2^d(2^a - 1) + 1$.

В остальном, известны лишь частные результаты. Перечислим их:

- ▷ $f(3, 3) = 19$ (Харборт, 1973);
- ▷ $f(3, 4) = 41$ (Дж. Пеллегрини, Т. Браун, Й. Булер, Дж. Бреннер, Кемниц, 1983);
- ▷ $f(3, 5) = 91$ (И. Эдель, С. Ферре, И. Ландъев, Л. Сторм, 2002);
- ▷ $225 \leq f(3, 6) \leq 229$ (Эдель, Ферре, Ландъев, Сторм, 2002);
- ▷ $f(3, 18) \geq 300 \cdot 2^{12}$ (Р. Грехем, П. Франкл, В. Рёдль, 1987);
- ▷ $f(3, d) \geq 2.217389^d$ при достаточно больших d (Эдель, 2004);

- ▷ $f(3, d) \leq 2\frac{3^d}{d}$ (Р. Мешулам, 1995);
- ▷ $f(n, d) \geq 2.08^d$ для нечетных n и достаточно больших d (Элсхольц, 2004).

СПИСОК ЛИТЕРАТУРЫ

- [1] Э.Б. Винберг. *Удивительные арифметические свойства биномиальных коэффициентов* // Математическое просвещение. Третья серия, вып. 12. 2008. С. 33–42.
- [2] Э.Б. Винберг. *Малая теорема Ферма и ее обобщения* // Математическое просвещение. Третья серия, вып. 12. 2008. С. 43–54.
- [3] И.М. Виноградов. *Основы теории чисел*. Москва – Ижевск: НИЦ «Регулярная и хаотическая динамика». 2003.
- [4] *Задачник Кванта. Математика.* // Квант, №9. 1970. С. 49; Квант, №7. 1971. С. 30.
- [5] А. Толпыго. *Об одной забытой задаче* // Квант, №2. 2010. С. 45–49.
- [6] А.М. Райгородский. *Линейно-алгебраический метод в комбинаторике*. М.: МЦНМО. 2007.
- [7] N. Alon, M. Dubiner. *Zero-sum sets of prescribed size* // Combinatorics: Paul Erdős is Eighty. Bolyai Society, Mathematical Studies, Keszthely, Hungary, 1993. P. 33–50.
- [8] C. Elsholtz. *Lower bounds for multidimensional zero sums* // Combinatorica. Vol. 24. 2004. P. 351–358.
- [9] H. Harborth. *Ein Extremalproblem für Gitterpunkte* // J. Reine Angew. Math. Bd. 262/263. 1973. S. 356–360.

Задача часовщика

Е. А. Горин

1. Задача, о которой пойдёт речь, вероятно, принадлежит к математическому фольклору. Она выглядит как безобидный вопрос, с которым «человек с улицы» может обратиться к профессионалу, и услышать в ответ «ну, конечно, конечно», однако, через 2–3 минуты прозвучит что-то, вроде, смущённого «почему-то сразу не получается, но я обязательно, и т. д.»

В своё время Б. Я. Левин рассказал мне, что в такую ситуацию попал Н. И. Ахиезер, которого часовщик после выяснения профессии клиента, спросил, не покажет ли он такое число, которое увеличится в 6 раз, если его последнюю цифру переставить на первое место. Выражаясь несколько более изысканно, требуется указать число в десятичной записи, которое увеличится в 6 раз при простейшей циклической перестановке его цифр (или вращения, если считать цифры расположенными равномерно вдоль окружности).

Пикантность ситуации состоит в том, что такие числа есть, их бесконечно много, но минимальное из них имеет 58 десятичных знаков. Я расскажу об этой задаче и её вариантах.

Вариант этой задачи, в котором 6 меняется на 2 (и 2 указывается в качестве правой десятичной цифры), фигурирует ещё в классической книге С. П. Боброва «Волшебный двурог» (что напомнил мне Ю. А. Брудный), первое издание которой под редакцией И. В. Арнольда вышло в 1948 г. Недавно она была переиздана [1] тиражом 500 экз., но зато теперь доступна в Интернете. Доступна в Интернете и нестареющая брошюра В. Литцмана «Великаны и карлики в мире чисел» [2].

Сравнительно недавно вариант с числом 2 (которое также заранее поставлено справа) был среди прочего детально исследован в заметке [3] (на которую мне указал Б. Н. Кукушкин). В этой заметке используется связь между перестановками цифр и разложением простых дробей в периодические десятичные. Изящное описание связей между разложениями простых дробей в десятичные дано в небольшом эссе, составляющем раздел в [4, п. 23, с. 174], практически с теми же простейшими примерами, что и в [3] (правда, там авторы отступают от способа Гаусса, который использовал общие теоремы Эйлера о сравнениях). Тем, кто в своё время пропустил эту тему, имеет смысл просматривать эти тексты параллельно.

Некоторым из опрошенных, как оказалось, «задача часовщика» известна, однако никто не сказал мне, где она обсуждается в печати (в отличие от задачи, в которой вместо числа 6 фигурирует 2). Например, А. М. Вершик, как мне стало понятно из переписки, давно знает практически всё, о чем я собираюсь рассказать.

Решение этой и близких задач может быть основано исключительно на первообразных корнях и индексах, что при небольших «коэффициентах растяжения» позволяет предъявить алгоритмы получения числа с точной оценкой числа шагов. В некоторых случаях время можно заметно сэкономить, если использовать квадратичный закон взаимности и готовую программу превращения правильной дроби в десятичную, в других — довести дело «до числа» возможно лишь ценой длинных вычислений. Я использую здесь только элементарные факты теории чисел (в частности, квадратичный закон привлекать не обязательно), о которых можно прочесть в классических учебниках, например, в [5] или [6]. Кроме того, почти в каждом номере «Математического просвещения» кто-нибудь по ходу дела непременно объясняет, что такое функция Эйлера φ и зачем она нужна.

Сначала мы введём обозначения, уточним вопрос и посмотрим, до чего можно добраться в более общих случаях.

2. Пусть k и l — натуральные числа, причём, $1 < k < l$ и $l \geq 3$. Число l — основание системы счисления, k — «коэффициент растяжения». В исходной задаче $k = 6$, $l = 10$. Латинские буквы и стандартные комбинации арабских цифр в обычном написании, скажем, 2, 13, и т. п., и без дополнительных пометок используются для обозначения неотрицательных целых чисел. С другой стороны, например, $(12)_7$ изображает натуральное число 9. Впрочем, ниже выражения вроде $(12)_7$ не используются.

Мы будем использовать позиционную систему с основанием l . Цифры в этой системе обозначаются греческими буквами, например, $X = \beta_1\beta_2 \dots \beta_r$. Считается, что первая цифра в искомом решении (не поставленной пока задачи!) не является нулевой. Поэтому для искомого числа $l^{r-1} \leq X < l^r$.

Убирая из записи искомого числа X последнюю цифру, мы получим запись некоторого числа A с $r - 1$ знаками, причём первый знак не меняется. Поэтому $l^{r-2} \leq A < l^{r-1}$.

Пусть b — число, изображаемое цифрой β_r . Тогда число X получает представление $X = Al + b$, и условие задачи *нахождения числа X , которое при вращении увеличивается в k раз*, принимает вид

$$(Al + b)k = bl^{r-1} + A. \quad (1)$$

Из условия (1) и неравенства $A \geq l^{r-2}$ легко вытекает, что $b > k - 1$. Ввиду целочисленности отсюда следует, что $b \geq k$. Итак, $k \leq b < l$. Заметим, что левое неравенство возникает ввиду желания не рассматривать

числа, запись которых *начинается* нулевой цифрой (хотя в ряде других случаев лучше вместо этого фиксировать длину записи). Этим же исключается $l = 2$. Сформулированная задача, как оказывается, имеет бесконечно много решений, которые не трудно описать целиком, но мы, если противное не ясно из контекста, имеем в виду минимальное решение (впрочем, последнюю цифру, вообще говоря, можно изменять, и тогда число изменяется, однако длина записи может изменяться или нет).

3. Положим $t = kl - 1$. Тогда соотношение (1) можно переписать в виде

$$At = (l^{r-1} - k)b. \quad (2)$$

ТЕОРЕМА. *Предположим дополнительно, что $\gcd(b, t) = 1$. Тогда соотношение (2) может выполняться в том и только в том случае, если выполняется сравнение*

$$l^r \equiv 1 \pmod{t}. \quad (3)$$

Сравнение (3) заведомо выполняется, если $r = \varphi(t)$, где φ — функция Эйлера. Минимальному X соответствуют минимальное r и минимальное (допустимое) b .

ДОКАЗАТЕЛЬСТВО. Умножим равенство (2) на l . Тогда получится, что $Atl = (l^r - kl)b$. По условию, число b обратимо по модулю t . Кроме того, $kl = 1 + t$. Таким образом, соотношение (2) влечёт за собой (3). Этот путь легко пройти в обратном направлении.

Тот факт, что значение $r = \varphi(t)$ годится, — следствие теоремы Эйлера, поскольку $\gcd(l, t) = 1$. Утверждение о минимальности вытекает из монотонности по r и b правой части в (2). В любом случае r — делитель порядка группы обратимых элементов кольца $\mathbb{Z}/(t)$, т. е. числа $\varphi(t)$. \square

Условие $\gcd(b, t) = 1$ не очень существенно: достаточно зачеркнуть общий множитель в равенстве (2), и доказательство можно повторить. Однако, формулировка теоремы усложнится, хотя в некоторых примерах ответ может упроститься. С такими примерами мы встретимся уже при составлении небольшой таблицы с $l = 10$.

4. Будем рассматривать (3) в качестве уравнения относительно (натурального) r при фиксированных (натуральных) l и t с условием $\gcd(l, t) = 1$.

По теореме Эйлера, $r = \varphi(t)$ является решением, а каждое меньшее решение — делитель этого.

Это позволяет предъявить алгоритм поиска X с оценкой $\leq \varphi(t)$ числа шагов.

Поясним это на стандартном примере, в котором $l = 10$, $k = b = 2$. Пусть

$$X = \beta_1\beta_2 \dots \beta_{r-1}\beta_r,$$

так что $\beta_r = 2$. Очевидно, что последней цифрой числа $2X$ будет 4. Поэтому $\beta_{r-1} = 4$. Имея эту информацию, мы можем определить β_{r-2} , и т. д. В данном случае $t = 19$, так что $r \leq \varphi(t) = t - 1 = 18$, и процесс остановится быстро (но не очень: фактически в данном случае $r = 18$).

Хотя процесс вычисления r , не говоря уже о вычислении X , если не применять дополнительных средств, может заметно затянуться даже при небольших k , последний пример укладывается в следующую таблицу.

| $l = 10$ | | | | |
|----------|----------|-----|--------------|-----|
| k | b | t | $\varphi(t)$ | r |
| 2 | 2-9 | 19 | 18 | 18 |
| 3 | 3-9 | 29 | 28 | 28 |
| 4 | 4-9 | 39 | 24 | 6 |
| 5 | $\neq 7$ | 49 | 42 | 42 |
| 5 | 7 | 49 | 42 | 6 |
| 6 | 6-9 | 59 | 58 | 58 |
| 7 | 7-9 | 69 | 44 | 22 |
| 8 | 8, 9 | 79 | 78 | 13 |
| 9 | 9 | 89 | 88 | 44 |

Эту таблицу нелишне прокомментировать.

При $k = 2$ и $k = 3$ имеем $t = 19$ и $t = 29$ соответственно. В обоих случаях получаются простые t , так что группы обратимых элементов соответствующих полей $\mathbb{Z}/(t)$ циклические. Для простых < 100 в [6] представлены таблицы *всех* первообразных корней и индексов (по избранному корню; обычно других корней не указывают), т. е. образующих в группах обратимых элементов и показателей степеней образующих, дающих данный класс вычетов. В обоих случаях $l = 10$ оказывается в числе образующих, откуда сразу следует, что в этих двух случаях $r = \varphi(t) = t - 1$.

Для $k = 4$ получается $t = 39 = 3 \cdot 13$. Если $b = 6$ или $b = 9$, то условие $\gcd(b, t) = 1$ *нарушается*, однако это не играет роли, так как 3 является делителем числа $10^r - 1$ при каждом r . Таким образом, при всех b дело сводится к делимости на 13. При простом 13 число $l = 10$ *не попадает* в список первообразных корней. Однако, привлекая дополнительно таблицу индексов, легко довести дело до конца, и выходит, что при $k = 4$ и всех b будет $r = 6$. Глядя на таблицу, появлению такого «универсального» карлика, можно удивиться не меньше, чем появлению великана. Вычисления оказываются совсем коротким (по поводу вычислений см. также следующий раздел), и в качестве наименьшего (при $b = 4$) будет $X =$

102564

(точку в конце мы намеренно не ставим).

Если $k = 5$, то $t = 49 = 7 \cdot 7$. В этом случае группа обратимых элементов снова циклическая (так как порядок кольца вычетов — степень нечётного простого), но $\varphi(t) = 42$. Если $b \neq 7$, то $\gcd(b, t) = 1$. Мы утверждаем, что в этом случае $r = \varphi(t)$. Действительно, при $r < \varphi(t)$ для r фактически оставались бы возможности 6, 14 и 21 (так как r делит $\varphi(t)$). Но эти возможности легко исключаются при помощи сравнения $100 \equiv 2 \pmod{49}$.

Итак, при $b \neq 7$ будет $r = 42$. Простое вычисление показывает, что в случае $b = 7$ будет $r = 6$ и $X =$

142857

Если $k = 6$, то можно дословно повторить рассуждение, касающееся двух первых значений. Однако этот случай в понятном смысле особенный, и мы покажем, как обойтись без таблиц, используя общие соображения (включая квадратичный закон взаимности). Существенно в приводимом ниже рассуждении только то, что t и $(t - 1)/2$ оба простые. Заметим, что X мы предьявим позже.

Случай $r = 2$ легко исключается. Следовательно, остаётся выяснить, что $29 = (t - 1)/2$ не годится в качестве r . Заметим, что при $t = 59$ число квадратичных вычетов (и невычетов) равно 29. Вместе с тем, число образующих в группе обратимых элементов равно $\varphi(58) = 28$. Для каждой из образующих a , по теореме Эйлера, будет $\lambda_{59}(a) = -1$, где λ (с индексом) — символ Лежандра. Удаляя -1 из множества невычетов, мы получим, что остальные невычеты — образующие. Таким образом, остаётся убедиться, что $\lambda_{59}(10) = -1$, и, по модулю квадратичного закона взаимности, дело сводится к элементарной арифметике.

Последние три строчки заполняются аналогично (какой-нибудь из предыдущих), и мы эту процедуру опустим.

5. Поскольку нас интересует наименьшее число, отвечающее данному k , мы будем считать в дальнейшем, что $b = k$.

Правильная дробь k/t имеет чисто периодическое l -ичное разложение, так как $\gcd(l, t) = 1$. Для десятичных разложений это детально обсуждается в [4], и этот случай ничем не отличается от общего. В частности, длина r периода есть как раз наименьшее положительное решение сравнения (3).

Пусть теперь X — искомое число (т. е. число, отвечающее значениям $l = 10$, $k = b = 6$). Имея в виду l -ичное представление, запишем число в каноническом виде, $X = \beta_1\beta_2 \dots \beta_{r-1}\beta_r$. Положим $Y = \beta_r\beta_1 \dots \beta_{r-2}\beta_{r-1}$. Тогда $Y = kX$.

Рассмотрим периодические дроби

$$x = 0.(\beta_1\beta_2 \dots \beta_{r-1}\beta_r) \text{ и } y = 0.(\beta_r\beta_1 \dots \beta_{r-2}\beta_{r-1}).$$

Используя представления x и y в виде сумм геометрических прогрессий и равенство $Y = kX$, легко усмотреть, что $y = kx$. Вместе с тем, из «графических» соображений ясно, что $y = (x + k)/l$. Таким образом,

$$x = k/t, \text{ где } t = kl - 1.$$

Следовательно, для получения X достаточно числитель разделить «уголком» на знаменатель, собрать с сохранением порядка цифры минимального периода и полученную картинку прочесть как запись числа. Кстати, при делении «уголком» число X будет выписываться слева направо (в отличие от описанного выше способа), а процесс остановится в точности тогда, когда повторится остаток (на самом деле это *основная* периодическая последовательность).

В частности, для получения «великана» используется правильная дробь $6/59$. Воспользовавшись, например, вычислительными возможностями онлайн-оракула WolframAlpha, получаем ответ $X =$

101.69491.52542.37288.13559.32203.38983.05084.74576.27118.64406.77966

(здесь точки поставлены для удобства восприятия).

Я благодарю М. Н. Вялого за разнообразную помощь в подготовке этой статьи. Кроме того, я хотел бы подчеркнуть его терпение и тактичность, с которыми он относится к моим текстам.

СПИСОК ЛИТЕРАТУРЫ

- [1] Бобров С.П. *Волшебный двурог*. М.: МЦНМО, 2006.
- [2] Литцман В. *Великаны и карлики в мире чисел*. М.: Физмагиз, 1959.
- [3] Ерошин А.Е. *Периодические десятичные дроби* // Математическое просвещение. Сер. 3, вып. 8. 2004. С. 239–245.
- [4] Радемахер Г., Теплиц О. *Числа и фигуры*. М.: Наука, 1966.
- [5] И.М.Виноградов. *Основы теории чисел*. М.: Гостехиздат, 1953.
- [6] Сушкевич А.К. *Теория чисел*. Харьков: Изд. Харьковского ун-та, 1956.

Дробная форма натурального числа и ее применение в задачах на циклические перестановки цифр

В. И. Войтицкий

1. ВВЕДЕНИЕ

Среди олимпиадных, исследовательских и занимательных задач по теории чисел нередко встречаются арифметические задачи на циклические перестановки цифр. Некоторые из таких задач достаточно легко решаются элементарными школьными методами, а некоторые требуют довольно долгого кропотливого подсчета. В связи с этим встает естественный вопрос, не существует ли какого-то общего подхода, который позволил бы по единому алгоритму достаточно быстро решать задачи на циклические перестановки цифр? Оказывается, такой подход существует. Его описание и применение к решению различных задач является предметом данной работы.

Суть подхода в том, что каждому натуральному числу можно естественным образом поставить в соответствие единственное дробное выражение (дробную форму), которая превращает соотношения между числами, получающимися друг из друга в результате циклических перестановок цифр, в соотношения между числителями соответствующих дробных форм. Аналогичные соотношения для циклических перестановок цифр периода бесконечной дроби известны (см. [1–3]). Основываясь на этой связи, арифметическая задача превращается в задачу решения сравнения по неизвестному модулю. Решая данную задачу и подбирая из простых соображений коэффициенты дробной формы, удастся сравнительно легко решать различные задачи на циклические перестановки цифр в любой p -ичной системе счисления. В статье рассматриваются некоторые обобщения стандартных задач на циклические перестановки цифр и несколько авторских задач, которые решаются предложенным методом. В частности, решается задача отыскания в произвольной p -ичной системе счисления всех нетривиальных *циклических*, т. е. всех таких чисел C , состоящих по крайней мере из двух различных цифр, что любая циклическая перестановка цифр числа

C образует числа, кратные C . Эта задача несколько отличается от известной задачи поиска в десятичной системе счисления всех так называемых циклических чисел $A = \overline{a_1 a_2 \dots a_n}$. Они характеризуются тем, что число $k \cdot A$ для всех натуральных $k \in [1; n]$ образуется из числа A путем циклических перестановок цифр. Циклические числа обладают одним интересным свойством. Если число цифр n кратно двум или трем, то, разбивая число A на два или три блока одинаковой длины и вычисляя сумму полученных чисел, мы всегда будем получать число из повторяющихся девяток (для четырех блоков это уже не верно). Данный результат является следствием так называемых обобщенных теорем Миди́. Оказывается, аналогичное свойство часто остается справедливым для решений многих задач на циклические перестановки цифр в любой p -ичной системе счисления.

2. ДРОБНАЯ ФОРМА НАТУРАЛЬНОГО ЧИСЛА

Для начала введем часто используемые в статье обозначения. Наибольший общий делитель двух чисел a и b будем записывать как (a, b) , p -ичную запись числа A будем обозначать как $A = \overline{a_1 a_2 \dots a_n}$, где цифры $a_i \in \{0, 1, \dots, p-1\}$, период p -ичной дроби будем выделять круглыми скобками. Показатель числа p по модулю m , т. е. такое минимальное натуральное число δ , что $p^\delta \equiv 1 \pmod{m}$, будем обозначать через $\delta = P_m(p)$. Напомним, что $a \equiv b \pmod{m}$ (числа a и b сравнимы по модулю m), если m является делителем числа $a - b$ (будем использовать обозначение $m \mid a - b$).

Со школы всем хорошо известно, что любую обыкновенную несократимую дробь можно единственным образом представить в виде бесконечной периодической десятичной дроби, причем у данной дроби отсутствует предпериод тогда и только тогда, когда знаменатель взаимно прост с числом 10. Аналогичный факт имеет место и в произвольной p -ичной системе счисления (данное утверждение можно найти, например, в [2, с. 74–78]). Приведем его здесь без доказательства.

ТЕОРЕМА 2.1. *Любая несократимая дробь $\frac{r}{m}$, $r \leq m$, $(r, m) = 1$, $r, m \in \mathbb{N}$, представима и притом единственным образом в виде бесконечной p -ичной дроби $\overline{0, b_1 \dots b_k (a_1 \dots a_\delta)}$. Данная дробь имеет вид $\overline{0, (a_1 \dots a_\delta)}$ (предпериод отсутствует) тогда и только тогда, когда $(m, p) = 1$, при этом $\delta = P_m(p)$. Если $(m, p) = 1$, то цифра $a_1 > 0$ тогда и только тогда, когда $pr > m$.*

На сформулированную теорему можно посмотреть с другой стороны. Пусть нам дано произвольное натуральное число $A = \overline{a_1 \dots a_n}$. Тогда

несложно видеть, что имеет место равенство

$$\frac{\overline{a_1 \dots a_n}}{p^n - 1} = 0, (\overline{a_1 \dots a_n}) = \frac{r}{m}, \quad (1)$$

где последняя дробь является несократимой. Отсюда для числа A получаем единственное представление

$$A = \overline{a_1 \dots a_n} = \frac{r(p^n - 1)}{m}, \quad (2)$$

которое назовем *дробной формой* n -значного числа A .

Согласно теореме 2.1 для дробной формы выполняются соотношения $r \leq m$, $(r, m) = 1$, $(p, m) = 1$. Несложно заметить что числам, состоящим только из одной повторяющейся цифры, соответствует дробная форма с $m \mid p - 1$. Этот случай является тривиальным и в задачах на циклические перестановки цифр легко может быть проверен отдельно. Далее будем рассматривать ситуацию, когда $m \nmid p - 1$, т. е. по меньшей мере $m > 1$.

Следует также оговориться, что согласно традиции число $A = \overline{a_1 \dots a_n}$ считается n -значным, если $a_1 > 0$. Далее, если не оговорено противное, будем искать именно такие числа, им соответствует условие на дробную форму $pr > m$. Отказываясь от него, можно по тому же алгоритму работать с числами, имеющими в начале p -ичной записи один или несколько нулей.

Исходя из соотношения (1), легко заметить интересную деталь. Если числу $A = \overline{a_1 \dots a_n}$ соответствует дробная форма $\frac{r(p^n - 1)}{m}$, то числу $B = \overline{a_1 \dots a_n a_1 \dots a_n}$ соответствует дробная форма $\frac{r(p^{2n} - 1)}{m}$. Обобщая эту закономерность, получаем следующее утверждение.

ТЕОРЕМА 2.2. Пусть число $B = \overline{a_1 \dots a_n}$ имеет дробную форму $\frac{r(p^n - 1)}{m}$. Тогда натуральное число $s = n/\delta$, где $\delta = P_m(p)$, определяет число повторяющихся блоков цифр $A = \overline{a_1 \dots a_\delta}$ в записи $\overline{a_1 \dots a_n}$, т. е. $\overline{a_1 \dots a_n} = \overline{a_1 \dots a_\delta a_1 \dots a_\delta \dots a_1 \dots a_\delta}$ тогда и только тогда, когда $\overline{a_1 \dots a_n} = \frac{r(p^{s\delta} - 1)}{m}$.

ДОКАЗАТЕЛЬСТВО. Имеем $B = \overline{a_1 \dots a_n} = \frac{r(p^{s\delta} - 1)}{m}$, тогда и только тогда, когда $B = \frac{r(p^\delta - 1)}{m}(p^{\delta(s-1)} + p^{\delta(s-2)} + \dots + 1) = Ap^{\delta(s-1)} + Ap^{\delta(s-2)} + \dots + A = \overline{a_1 \dots a_\delta a_1 \dots a_\delta \dots a_1 \dots a_\delta}$.

Известно (см., например, [1, с. 208] и [2, с. 178–182]), что бесконечные периодические дроби, образованные циклическими перестановками цифр периода, являются обыкновенными дробями с одинаковыми знаменателями,

причем их числители связаны друг с другом определенными соотношениями. Отсюда получаем такой результат.

ТЕОРЕМА 2.3. Пусть число $A_1 = \overline{a_1 \dots a_n}$ имеет дробную форму $\frac{r_1(p^{\delta s} - 1)}{m}$. Тогда все натуральные числа, получающиеся в результате циклической перестановки цифр числа A_1 имеют дробную форму

$$A_i = \overline{a_i \dots a_n a_1 \dots a_{i-1}} = \frac{r_i(p^{\delta s} - 1)}{m}, \quad i = 1, 2, \dots, n, \quad (3)$$

где $r_i \equiv r_1 p^{i-1} \pmod{m}$, $r_i \leq m$, $(r_i, m) = 1$.

ДОКАЗАТЕЛЬСТВО. По определению дробной формы имеем $\frac{r_1}{m} = \frac{0, (a_1 \dots a_n)}{m}$. Отсюда $\frac{r_1}{m} p^{i-1} = \frac{0, (a_1 \dots a_{i-1}, (a_i \dots a_{i-1}))}{m}$, следовательно $\frac{0, (a_i \dots a_{i-1})}{m} = \frac{r_1 p^{i-1} - m \overline{a_1 \dots a_{i-1}}}{m}$. С другой стороны, если соотношение (3) определяет дробную форму, то $\frac{0, (a_i \dots a_{i-1})}{m} = \frac{r_i}{m}$, где $r_i \leq m$, $(r_i, m) = 1$. Поскольку равны левые части, то равны и правые части, т.е. $r_i = r_1 p^{i-1} - m \overline{a_1 \dots a_{i-1}}$, отсюда получаем, что $r_i \equiv r_1 p^{i-1} \pmod{m}$.

Сформулированных выше теорем достаточно, чтобы решить многие арифметические задачи на циклические перестановки цифр. При этом ключевой идеей поиска является отыскание не самих чисел, а их дробных форм.

3. ТЕОРЕМА МИДИ И ЦИКЛИЧЕСКИЕ ЧИСЛА

Еще в 1836 году французский математик Е. Миди доказал интересную теорему, которая утверждает, что если несократимая дробь содержит в десятичном периоде четное число цифр и знаменатель является степенью простого числа, отличного от 2 и 5, то сумма первой и второй половины цифр периода всегда дает число, составленное из одних девяток. Например, $1/13 = 0, (076923)$, $076 + 923 = 999$.

До начала 21 века этот результат мало интересовал математиков, однако, совсем недавно в период с 2003 по 2007 гг. были получены далеко идущие обобщения этого результата (см., например, [5, 6, 8, 9]). Оказалось, что если $r = 1$, m — простое число и число цифр в периоде десятичной дроби $1/m$ кратно трем, т.е. $\delta = 3k$, то сумма трех частей цифр периода равной длины всегда дает число из девяток. Для четырех блоков цифр это свойство, вообще говоря, не выполняется, мы можем констатировать лишь тот факт, что полученная сумма кратна числу из девяток. В [6], однако, доказано, что если m является простым числом Мерсенна, т.е. $m = 2^l - 1$,

где число l — простое, то, разбивая период дроби $1/m$ на l блоков равной длины, всегда получается число из девяток.

В статьях [8] и [5] доказано обобщение этого интересного свойства для двух или трех блоков цифр в произвольной p -ичной системе счисления. В частности, из результатов этих работ следует такое утверждение.

ТЕОРЕМА 3.1. *Обозначим через $M_d(p)$ множество p -ичных чисел $\overline{a_1 a_2 \dots a_{d\kappa}}$, таких что сумма чисел*

$$\overline{a_1 a_2 \dots a_\kappa} + \overline{a_{\kappa+1} a_{\kappa+2} \dots a_{2\kappa}} + \dots + \overline{a_{d(\kappa-1)+1} a_{d(\kappa-1)+2} \dots a_{d\kappa}} = \underbrace{(p-1)(p-1) \dots (p-1)}_{\kappa \text{ цифр}}.$$

Пусть в p -ичной системе счисления обыкновенная несократимая дробь $r/m = \overline{0, (a_1 a_2 \dots a_\delta)}$ имеет четное число цифр $\delta = 2\kappa$ в периоде и число t является степенью простого числа, отличного от делителей p , либо $(m, p^\kappa - 1) = 1$. Тогда имеет место свойство $\frac{r(p^\delta - 1)}{m} = \overline{a_1 a_2 \dots a_\delta} \in M_2(p)$.

Если t является простым числом, отличным от делителей p , и $\delta = 3\kappa$, $r = 1$ или $r = 2$, то $\frac{r(p^\delta - 1)}{m} = \overline{a_1 a_2 \dots a_\delta} \in M_3(p)$. При $r = 3$ результат верен для всех простых t , которые дополнительно не равны трем и семи.

Отметим, что сформулированные условия являются лишь достаточными, т. е. можно найти дробные формы, не удовлетворяющие условиям теоремы, которые, однако, принадлежат одному из множеств $M_d(p)$ ($d \geq 2$). Для дробных форм с $r \geq 4$ или $d \geq 3$ в общем случае установлена лишь кратность моноцифровому числу $(p-1) \dots (p-1)$. При применении теоремы 3.1 следует иметь ввиду, что в случае $pr \leq m$ в начале числа следует поставить несколько нулей так, чтобы количество цифр в числе совпадало с длиной периода обыкновенной дроби.

Особый интерес представляют дробные формы вида

$$A = \frac{p^{m-1} - 1}{m}, \tag{4}$$

где m — простое, причем $\delta = P_m(p) = m - 1$ (повторяющиеся блоки чисел здесь не учитываем). Несложно доказать, что такие и только такие дробные формы задают в p -ичной системе счисления все циклические числа (см., например, [7]). Число $A = \overline{a_1 a_2 \dots a_n}$ ($n = m - 1$) называется *циклическим числом*, если для всех натуральных $k \in [1; n]$ числа $k \cdot A$ образуются из числа A путем циклических перестановок цифр (здесь допускаем, что число A может иметь в начале несколько нулей).

В силу теоремы 3.1 любое циклическое число принадлежит классам $M_2(p)$ или $M_3(p)$ как только число $m - 1$ кратно двум или трем. При умножении циклических чисел на знаменатель m образуются числа, составленные из цифры $p - 1$. Вообще, при умножении циклического числа A на любые «не очень большие» числа k получаются либо числа, в середине которых есть блок $(p - 1) \dots (p - 1)$, либо циклические перестановки цифр числа A . Динамика цифровой структуры чисел $k \cdot A$ с ростом k до настоящего времени не рассматривалась.

Остановимся более подробно на привычном случае $p = 10$. До сих пор остается открытым вопрос: бесконечно или нет количество простых m таких, что $P_m(10) = m - 1$ (т. е. неизвестно бесконечно или нет множество десятичных циклических чисел). Этому свойству удовлетворяют многие (но далеко не все) простые числа. Например, $P_{13}(10) = 6$, поэтому $m = 13$ не удовлетворяет данному свойству. Среди $m < 200$ знаменателями дробных форм циклических чисел являются следующие m :

7, 17, 19, 23, 29, 47, 59, 61, 97, 109, 113, 131, 149, 167, 179, 181, 193.

Первым трем значениям m соответствуют числа

142857, 0588235294117647, 052631578947368421.

Очевидно, единственным $(m - 1)$ -значным циклическим числом в десятичной системе счисления является замечательное число 142857, остальные числа содержат вначале один или несколько нулей. Ниже будет доказано, что это же число является единственным нетривиальным базисным циклидом в десятичной системе. Число 142857 хорошо известно любителям занимательной арифметики. Много его интересных свойств можно найти в книге [8, с. 179–183]. Например, равенства $142 + 657 = 999$ и $14 + 28 + 57 = 99$ подтверждают теорему 3.1. Далее, имеем сумму $1 + 4 + 2 + 8 + 5 + 7 = 27$, при этом сумма всех циклических перестановок числа 142857 равна 2999997. Число 142857 является числом Капрекара, что выражается свойством

$$142857^2 = 020408122449 = (20408 + 122449)^2.$$

4. РЕШЕНИЕ НЕКОТОРЫХ АРИФМЕТИЧЕСКИХ ЗАДАЧ

Задача 4.1. Пусть k, l и t — данные натуральные числа. В p -ичной системе счисления найти все числа $\overline{a_1 a_2 \dots a_n}$, такие что $\overline{a_1 a_2 \dots a_n} \cdot k = \overline{a_l \dots a_n \dots a_{l-1}} \cdot t$.

РЕШЕНИЕ (АЛГОРИТМ). Задача сводится к отысканию дробных форм $\frac{r_1(p^{\delta_s} - 1)}{m}$ и $\frac{r_l(p^{\delta_s} - 1)}{m}$, таких что

$$\begin{cases} 1. (r_1, m) = (r_l, m) = 1, \\ 2. r_1 \leq m, r_l \leq m, \\ 3. pr_1 > m, pr_l > m, \\ 4. kr_1 = tr_l, r_l \equiv r_1 p^{l-1} \pmod{m}. \end{cases}$$

Из условия 4 следует, что $kr_1 \equiv tr_l p^{l-1} \pmod{m}$. В силу 1 отсюда имеем $k \equiv t p^{l-1} \pmod{m}$ или $m \mid t p^{l-1} - k$. С помощью простого перебора легко найти все $m \geq 1$, которые взаимно просты с p и делят число $t p^{l-1} - k$. Их может быть лишь конечное число. Зная знаменатель m , мы находим n в виде δs , где $\delta = P_m(p)$, $s \in \mathbb{N}$. Чтобы закончить решение, необходимо перебрать все числа r_1 от 1 до m такие, что $(r_1, m) = (r_l, m) = 1$, $r_1 \leq m$, $kr_1 \leq tm$, $pr_1 > m$, $kpr_1 > tm$. Таких чисел может быть также не больше конечного числа. Представляя теперь все получающиеся формы в виде натуральных чисел, получаем окончательное решение задачи. Условие 3 можно опустить, если допускать числа с нулями в начале. \square

Частные случаи задачи 4.1 рассматривались в [11, с. 518–519], а также в [4, с. 17–18]. Решим несколько конкретных задач такого вида.

ЗАДАЧА 4.2. *Найти все десятичные числа $\overline{a_1 a_2 \dots a_n}$ такие, что $\overline{a_1 a_2 \dots a_n} \cdot 3 = \overline{a_2 \dots a_n a_1}$.*

РЕШЕНИЕ. В искомым дробных формах знаменатель m должен являться делителем числа $10^{2-1} - 3 = 7$, т.е. $m = 7$ или $m = 1$. Последний случай является тривиальным, поскольку соответствует числам $9 \dots 9$, которые, очевидно, не удовлетворяют условию задачи. Для $m = 7$ имеем $P_7(10) = 6$, поэтому искомые числа имеют вид $\frac{r_1(10^{6s} - 1)}{7}$. Условиям 1–4 удовлетворяют лишь $r_1 \in \{1, 2\}$ (при больших r_1 будем иметь: $3r_1 > 7$).

Таким образом, решениями данной задачи являются: циклическое число 142857 , его циклическая перестановка 285714 , а также все числа вида $\underbrace{142857 \dots 142857}_{6s \text{ цифр}}, \underbrace{285714 \dots 285714}_{6s \text{ цифр}}$, где $s \in \mathbb{N}$. \square

ЗАДАЧА 4.3. *Найти все десятичные числа $\overline{a_1 a_2 \dots a_n}$ такие, что $\overline{a_1 a_2 \dots a_n} = \overline{a_2 \dots a_n a_1} \cdot 2$.*

РЕШЕНИЕ. В искомым дробных формах знаменатель m должен являться делителем числа $2 \cdot 10^{2-1} - 1 = 19$, поскольку это число простое, то остается лишь одно нетривиальное значение для знаменателя дробной формы — это $m = 19$. Имеем $P_{19}(10) = 18$, поэтому искомые числа имеют вид $A_i = \frac{r_1(10^{18s} - 1)}{19}$. Условиям 1–4 удовлетворяют все четные r_1 из промежутка $[4; 18]$ или $r_1 = 2r$, $r = 2, 3, \dots, 9$.

Для наглядности приведем ответ для $r_1 = 4$, $s = 1$:

$$A_1 = 210526315789473684 = 105263157894736842 \cdot 2.$$

Знаменателем дробной формы является $m = 19$, поэтому всеми возможными ответами данной задачи являются циклические перестановки десятичного циклического числа $A_3 = 052631578947368421$. Проиллюстрируем на примере данного ответа выполнение теоремы 3.1. С помощью непосредственной проверки убеждаемся, что каждое $A_i \in M_2(10)$. При этом $A_i \in M_3(10)$, если соответствующее $r_i \leq 4$. Например, при $r_1 = 4$ имеем $210526315 + 789473684 = 999999999$, $210526 + 315789 + 473684 = 999999$, $210 + 526 + 315 + 789 + 473 + 684 = 2997$. Однако уже при $r_i = 5$ получаем $263157894 + 736842105 = 999999999$, но $263157 + 894736 + 842105 = 1999998$. Заметим, что теорема 3.1 гарантирует выполнение свойства $A_i \in M_3(10)$ для $r_i \leq 3$. \square

Рассмотрим еще несколько авторских задач на циклические перестановки цифр.

ЗАДАЧА 4.4. *Найти все десятичные числа $A = \overline{a_1 a_2 \dots a_n}$ такие, что*

$$\overline{a_1 a_2 \dots a_n} + \overline{a_2 \dots a_n a_1} = \underbrace{\overline{bb \dots b}}_{n \text{ цифр}}$$

РЕШЕНИЕ. Несложно найти некоторые частные решения данной задачи. Именно, если b — четное число, тогда задача имеет тривиальное решение $A = \frac{b}{2} \cdot \frac{10^n - 1}{9}$ — число, состоящее из n цифр $b/2$. Если $n = 2$, то решениями являются все двузначные числа $A = \overline{a_1 a_2}$, для которых $a_1 + a_2 = b$. Оказывается, что с точностью до повторяющихся блоков цифр мы описали все решения поставленной задачи. Чтобы доказать этот факт, будем использовать метод дробных форм. Пусть $A = \frac{r_1(10^{\delta s} - 1)}{m}$, тогда задача сводится к уравнению

$$r_1 \cdot \frac{10^{\delta s} - 1}{m} + r_2 \cdot \frac{10^{\delta s} - 1}{m} = b \cdot \frac{10^{\delta s} - 1}{9}.$$

Из него заключаем, что $r_2 = \frac{bm}{9} - r_1$. С другой стороны, известно, что $r_2 \equiv \equiv 10r_1 \pmod{m}$. Следовательно $bm \equiv 99r_1 \pmod{m}$, $m \mid 99r_1$. Поскольку m взаимно просто с r_1 , то $m \mid 99$. Показатель δ любого делителя числа 99 равен 1 либо 2, т. е. решениями поставленной задачи являются одно- либо двузначные числа, а также все числа, получающиеся из них в результате повторов одинакового блока цифр. Для двузначного числа соотношение $a_1 + a_2 = b$, очевидно, следует из равенства $10a_1 + a_2 + 10a_2 + a_1 = 10b + b$. Что и требовалось доказать. \square

Аналогично решается задача $\overline{a_1 a_2 \dots a_n} + \overline{a_2 \dots a_n a_1} + \overline{a_3 \dots a_n a_1 a_2} = \overline{bb \dots b}$. Она может иметь тривиальные решения $A = \frac{b}{3} \cdot \frac{10^n - 1}{9}$, а также решения, состоящие из повторяющихся блоков цифр $\overline{a_1 a_2 a_3}$, где $a_1 + a_2 + a_3 = b$. Например, $234234 + 342342 + 423423 = 999999$, поскольку $2 + 3 + 4 = 9$.

ЗАДАЧА 4.5. Найдти все десятичные числа $\overline{a_1 a_2 \dots a_n}$ такие, что $\overline{a_1 a_2 \dots a_n} + \overline{a_2 \dots a_n a_1} = \overline{a_3 \dots a_1 a_2}$.

РЕШЕНИЕ. Будем искать дробную форму числа $\overline{a_1 a_2 \dots a_n}$ в виде $\frac{r_1(10^{\delta s} - 1)}{m}$. Тогда $\overline{a_2 \dots a_n a_1} = \frac{r_2(10^{\delta s} - 1)}{m}$, $\overline{a_3 \dots a_n a_1 a_2} = \frac{r_3(10^{\delta s} - 1)}{m}$. Условие задачи сводится к тому, что $r_1 + r_2 = r_3$.

По свойствам дробных форм имеем $r_1 \cdot 10 \equiv r_2 \pmod{m}$ и $r_1 \cdot 10^2 \equiv r_3 \pmod{m}$. Отсюда

$$r_1 \cdot 10^2 \equiv r_1 + r_2 \equiv r_1 + r_1 \cdot 10 \pmod{m}.$$

Поскольку $(r_1, m) = 1$, то $10^2 \equiv 1 + 10 \pmod{m}$, $89 \equiv 0 \pmod{m}$. Так как 89 является простым числом, то $m = 89$ (тривиальный случай $m = 1$, очевидно, не подходит). Известно, что $P_{89}(10) = 44$, отсюда решения задачи имеют вид $\frac{r_1(10^{44s} - 1)}{89}$. Установим теперь, какие значения может принимать r_1 .

В силу условия $10r_1 > m$ имеем $r_1 \in \{9, 10, \dots, 87, 88\}$.

Если $r_1 \in [9, 17]$, тогда $r_2 = 10r_1 - 89$. В силу условий $10r_2 > m$ и $r_3 < m$ должны выполняться неравенства

$$r_2 = 10r_1 - 89 > 8, \quad r_3 = 11r_1 - 89 < 89.$$

Им удовлетворяют натуральные $r_1 \in [10, 16]$.

Если $r_1 \in [18, 26]$, тогда $r_2 = 10r_1 - 178$. Имеем неравенства

$$r_2 = 10r_1 - 178 > 8, \quad r_3 = 11r_1 - 178 < 89.$$

Им удовлетворяют натуральные $r_1 \in [19, 24]$.

Если $r_1 \in [27, 35]$, тогда $r_2 = 10r_1 - 267$. Имеем неравенства

$$r_2 = 10r_1 - 267 > 8, \quad r_3 = 11r_1 - 267 < 89.$$

Им удовлетворяют натуральные $r_1 \in [28, 32]$.

Аналогичным образом можно показать, что условиям $10r_2 > m$ и $r_3 < m$ удовлетворяют также натуральные r_1 из промежутков $[37, 40]$, $[46, 48]$ и $r_1 \in \{55, 56, 64\}$. Таким образом, все подходящие значения r_1 найдены, а значит найдены и все возможные искомые числа. При $r_1 = 10$ и $s = 1$ получаем следующее равенство:

$$\begin{aligned}
&11235955056179775280898876404494382022471910 + \\
&12359550561797752808988764044943820224719101 = \\
&23595505617977528089887640449438202247191011.
\end{aligned}$$

Удивительно, что меньших десятичных чисел с таким свойством не существует (за исключением чисел, начинающихся с цифры ноль)! Поскольку число $m = 89$ является простым и показатель $\delta = 44$ кратен двум, то все решения задачи принадлежат множеству $M_2(10)$. \square

Аналогичным методом решаются и другие задачи на циклические перестановки цифр. Например, можно приравнивать два одночлена одинаковой степени от чисел, отличающихся друг от друга циклическими перестановками цифр. В частности, можно рассмотреть такую задачу: $\overline{a_1 \dots a_n}^2 = \overline{a_2 \dots a_1} \cdot \overline{a_3 \dots a_2}$. Для решения подобных задач можно составлять компьютерные программы.

5. ЗАДАЧА О НАХОЖДЕНИИ ВСЕХ НЕТРИВИАЛЬНЫХ p -ИЧНЫХ ЦИКЛИДОВ

ОПРЕДЕЛЕНИЕ 5.1. Натуральное число C будем называть p -ичным циклидом, если p -ичная запись этого числа $C = \overline{a_1 a_2 \dots a_n}$ такова, что любая циклическая перестановка цифр образует в точности n -значное число $\overline{a_i a_{i+1} \dots a_{i-1}}$, которое кратно C . Очевидно, что все моноцифровые числа являются циклидами, которые мы будем называть тривиальными. Если же в числе C имеются хотя бы две различные цифры, то такой циклид назовем нетривиальным.

Отметим, что формально данному определению удовлетворяют упоминаемые выше циклические числа (см. пункт 3). Однако при простых $m > p$ числа $(10^{m-1} - 1)/m$ не являются $(m - 1)$ -значными. Поэтому среди циклических чисел нетривиальными p -ичными циклидами будут являться лишь те, значность которых не превосходит $p - 1$ (циклиды с нулями в начале не рассматриваем в силу их бесконечного количества). Ниже будет показано, что множество нетривиальных циклидов может быть пустым, состоять из циклических чисел или иметь более сложную структуру в зависимости от p .

Итак, рассмотрим дробную форму нетривиального циклида $C = \frac{r_1(p^{\delta s} - 1)}{m}$. Любая циклическая перестановка цифр данного числа образует число $D = \frac{r_i(p^{\delta s} - 1)}{m}$, $i = 1, 2, \dots, \delta$. Согласно определению должно выполняться свойство $C \mid D$, откуда следует, что $r_1 \mid r_i$ или $\text{НОД}\{r_i\} = r_1$.

Условие нетривиальности будет выполнено, если m не является делителем числа $p - 1$. Очевидно, циклидами являются все дробные формы, в которых $r_1 = 1$. Если предположить, что $r_1 = g > 1$, тогда число g обязано быть делителем каждой цифры циклида $C = \overline{a_1 a_2 \dots a_{\delta s}}$. Действительно, в доказательстве теоремы 2.3 установлено, что $r_i = r_1 p^{i-1} - m \overline{a_1 \dots a_{i-1}}$, $i = 1, 2, \dots, \delta$. Отсюда получаем цепочку равенств

$$\begin{aligned} r_2 &= pr_1 - ma_1, & r_3 &= pr_2 - ma_2, \\ r_4 &= pr_3 - ma_3, & \dots & r_n = pr_{n-1} - ma_{n-1}. \end{aligned}$$

Поскольку каждое из чисел r_i кратно $r_1 = g$ и $(m, r_i) = 1$, то каждая цифра a_i кратна g . Следовательно $g \mid \text{НОД}\{a_i\}$. Допустим, мы нашли циклид $C = \frac{g(p^{\delta s} - 1)}{m} = \overline{a_1 a_2 \dots a_{\delta s}}$. Тогда в силу доказанного $\overline{a_1 a_2 \dots a_{\delta s}} = \frac{(ga'_1)(ga'_2) \dots (ga'_{\delta s})}{m} = g \cdot \overline{a'_1 a'_2 \dots a'_{\delta s}}$. Отсюда следует, что число $C' = \frac{(p^{\delta s} - 1)}{m} = \overline{a'_1 a'_2 \dots a'_{\delta s}}$ также является циклидом.

Таким образом, найден алгоритм поиска всех возможных нетривиальных p -ичных циклидов.

ТЕОРЕМА 5.1. *Все нетривиальные p -ичные циклиды следует искать среди чисел $C = \frac{p^{\delta s} - 1}{m}$, где m не делит $p - 1$, $(m, p) = 1$ и $m < p$ (ищем в точности δs -значные числа). Если получаемые по этой формуле числа $C = \overline{a_1 a_2 \dots a_{\delta s}}$ таковы, что существуют натуральные числа $g \in \{2, \dots, p - 1\}$ такие, что $g \cdot \max\{a_i\} < p$, то циклидами являются также числа $C' = \frac{g(p^{\delta s} - 1)}{m}$.*

Несложно заметить, что в 2-ичной, 3-ичной, 4-ичной, 6-ичной системах нетривиальных циклидов не существует! Покажем, чему равны нетривиальные базисные циклиды (при $s = 1$) в других системах счисления.

При $p = 5$ единственным допустимым знаменателем дробной формы является $m = 3$. Отсюда $C_3^5 = \frac{5^2 - 1}{3} = \overline{8}_{10} = \overline{13}_5$, $D = \overline{31}_5 = \overline{16}_{10} = 2C_3^5$ (верхний индекс здесь и далее означает основание системы счисления, а нижний — знаменатель дробной формы). Поскольку $3 \cdot 2 > 5$, то все $g > 1$ не удовлетворяют свойству $g \cdot \max\{a_i\} < 5$. Аналогично $g > 1$ не подходят при $p = 7, 8, 9, 10$.

При $p = 7$ имеем $m_1 = 4, m_2 = 5$. Отсюда

$$C_4^7 = \frac{7^2 - 1}{4} = \overline{12}_{10} = \overline{15}_7, \quad C_5^7 = \frac{7^4 - 1}{5} = \overline{480}_{10} = \overline{1254}_7.$$

При $p = 8$ имеем $m_1 = 3, m_2 = 5$. Отсюда

$$C_3^8 = \frac{8^2 - 1}{3} = \overline{21}_{10} = \overline{25}_8, \quad C_5^8 = \frac{8^4 - 1}{5} = \overline{819}_{10} = \overline{1463}_8.$$

При $p = 9$ имеем $m_1 = 5$, $m_2 = 7$. Отсюда

$$C_5^9 = \frac{9^2 - 1}{5} = \overline{16}_{10} = \overline{17}_9, \quad C_7^9 = \frac{9^3 - 1}{7} = \overline{104}_{10} = \overline{125}_9.$$

При $p = 10$ имеем $m = 7$, т. е. единственным нетривиальным циклидом в десятичной системе счисления является упоминавшееся ранее циклическое число $C_7^{10} = \frac{10^6 - 1}{7} = \overline{142857}_{10}$.

При $p = 11$ имеем 6 различных нетривиальных базисных циклидов, им соответствуют знаменатели дробных форм $m_1 = 3$, $m_2 = 4$, $m_3 = 6$, $m_4 = 7$, $m_5 = 8$ ($g = 1$), $m_6 = 8$ ($g = 2$), $m_7 = 9$. Отсюда

$$\begin{aligned} C_3^{11} &= \frac{11^2 - 1}{3} = \overline{40}_{10} = \overline{37}_{11}, & C_4^{11} &= \frac{11^2 - 1}{4} = \overline{30}_{10} = \overline{28}_{11}, \\ C_6^{11} &= \frac{11^2 - 1}{6} = \overline{20}_{10} = \overline{19}_{11}, & C_7^{11} &= \frac{11^3 - 1}{7} = \overline{190}_{10} = \overline{163}_{11}, \\ C_8^{11} &= \frac{11^2 - 1}{8} = \overline{15}_{10} = \overline{14}_{11}, & (C_8^{11})' &= \frac{2(11^2 - 1)}{8} = \overline{30}_{10} = \overline{28}_{11}, \\ C_9^{11} &= \frac{11^6 - 1}{9} = \overline{196840}_{10} = \overline{124986}_{11}. \end{aligned}$$

Проверка того, что все приведенные выше числа являются циклидами, является хорошим упражнением на перевод чисел из одной системы счисления в другую. Естественно, можно искать нетривиальные циклиды для больших p . По-видимому, они будут существовать, причем в среднем их количество с ростом p будет расти.

Заметим, что сумма двух или трех частей цифр циклида зачастую дает число $\overline{(p-1) \dots (p-1)}$. Это всегда так, если знаменатель дробной формы является простым числом. Если же знаменатель является составным, то данное свойство в случае трех блоков цифр как правило не выполняется, например, $\overline{124986}_{11} \neq \overline{12}_{11} + \overline{49}_{11} + \overline{86}_{11}$. При этом, примеры показывают, что в случае двух блоков свойство выполняется довольно часто (даже если знаменатель не удовлетворяет теореме 3.1). Например, в 13-ичной системе счисления имеем циклид $C_{10}^{13} = \frac{13^4 - 1}{10} = \overline{2856}_{10} = \overline{13(11)9}_{13}$, для которого $\overline{13}_{13} + \overline{(11)9}_{13} = \overline{(12)(12)}_{13}$, хотя 10 не является степенью простого числа и $(10, 13^2 - 1) = 2 \neq 1$. В то же время для циклида $C_8^{13} = \frac{13^2 - 1}{8} = \overline{21}_{10} = \overline{18}_{13}$ сумма $1 + 8 \neq \overline{(12)}_{13}$, аналогично для $C_8^{11} = \overline{14}_{11}$ имеем $1 + 4 \neq \overline{(10)}_{11}$.

ТЕОРЕМА 5.2. Пусть $C = \frac{g(p^\delta - 1)}{m}$ является циклидом, где $\delta = 2k$, $(m, p-1) = 1$. Тогда $C \in M_2(p)$ как только t или k являются нечетными числами.

ДОКАЗАТЕЛЬСТВО. Согласно теореме 3.1 условие $(m, p^\kappa - 1) = 1$ является достаточным для выполнения свойства $C \in M_2(p)$. Пусть $(m, p^\kappa - 1) = a$, тогда в силу $(m, p - 1) = 1$ имеем $(m, P) = a$, где $P = p^{\kappa-1} + p^{\kappa-2} + \dots + p + 1$. Поскольку число $\delta = 2\kappa = P_m(10)$, то $p^\kappa \equiv -1 \pmod{m}$, т. е. $m \mid p^\kappa + 1$. Отсюда $a \mid p^\kappa + 1$. С другой стороны, $a \mid p^\kappa - 1$, из чего заключаем, что $a \mid (p^\kappa + 1) - (p^\kappa - 1) = 2$, т. е. $a = 1, 2$. Очевидно, $a \neq 2$, если m — нечетное число. Аналогично $a \neq 2$, если m — четное, но P — нечетное. Последнее выполнено, если κ — нечетное. Действительно, поскольку C — циклид, то выполнено условие $(m, p) = 1$, откуда p — нечетное. Тогда P — также нечетное число, как сумма нечетного количества κ нечетных чисел p^i , $i = 0, 1, \dots, \kappa - 1$.

Из теоремы следует, что если выполнено $(m, p - 1) \neq 1$ либо m и κ — четные, то возможно $C \notin M_2(p)$. Эти свойства не являются достаточными, поскольку $C_{10}^{13} \in M_2(p)$. Формулировка условия, которое гарантировало бы, что $C \notin M_2(p)$ или $C \notin M_3(p)$ остается открытым вопросом как для циклидов, так и для периода произвольной p -ичной дроби r/m . Отметим, что для дробной формы $(10^\delta - 1)/m$ необходимые и достаточные условия ее принадлежности к классу $M_2(10)$ найдены в [9]. Было бы интересно узнать о наличии у нетривиальных p -ичных циклидов других интересных свойств. Тут имеется открытое поле для деятельности.

СПИСОК ЛИТЕРАТУРЫ

- [1] Бухштаб А.А. *Теория чисел*. М.: Просвещение, 1966.
- [2] Радемахер Г., Теплиц О. *Числа и фигуры (опыты математического мышления)*. М.: ГИФМЛ, 1962.
- [3] Хассе Г. *Лекции по теории чисел*. М.: Из-во иностранной литературы, 1953.
- [4] Шклярский Д.О., Ченцов Н.Н., Яглом И.М. *Избранные задачи и теоремы элементарной математики: арифметика и алгебра*. М.: Наука, 1977.
- [5] Gil J.B., Weiner M.D. *On Cyclic Numbers and an Extension of Midy's Theorem*. arXiv:math/0605347v1 (12 May 2006).
- [6] Gupta A., Sury B. *Decimal Expansion of $1/p$ and Subgroup Sums // Integers: Electronic Journal of Combinatorial Number Theory*, Vol. 5, 2005.
- [7] Guttman S. *On Cyclic Numbers // Amer. Math. Monthly*, Vol. 44, 1934. P. 159–166.
- [8] Lewittes J. *Midy's Theorem for Periodic Decimals*. arXiv:math/0605182v1 (7 May 2006).

- [9] Martin H.W. *Generalizations of Midy's Theorem on Repeating Decimals* // *Integers: Electronic Journal of Combinatorial Number Theory*, Vol. 7, 2007.
- [10] Well D. *The Penguin Book of Curious and Interesting Numbers*. Penguin Books, 1986.
- [11] Yiu P. *Recreational Mathematics*. Florida Atlantic University Press, 2003.

Войтицкий Виктор Иванович, к.ф.-м. н., ассистент кафедры математического анализа Таврического национального университета им. В. И. Вернадского (Симферополь, АР Крым, Украина)

Почтовый адрес: Таврический национальный университет им. В. И. Вернадского, просп. Акад. В. И. Вернадского, 4, Симферополь, 95007, Украина

EMAIL: victor.voytitsky@gmail.com

Еще раз о точке Фейербаха

П. А. Кожевников

Знаменитая теорема Фейербаха гласит, что в любом треугольнике окружность девяти точек¹⁾ касается вписанной окружности.²⁾ Точка касания окружности девяти точек и вписанной окружности называется *точкой Фейербаха*. В этой заметке предлагается геометрическое доказательство теоремы Фейербаха, которое дает возможность описать точку Фейербаха и, в частности, получить отличное от авторского геометрическое решение задачи 8 из задачного раздела «Математического просвещения», вып. 14, 2010 г. (авторское решение приведено в статье [1]).

ЛЕММА САВАЯМЫ (ЛЕММА О СЕГМЕНТЕ) И ТЕОРЕМА О ЛУНОЧКАХ

Начнем со следующего утверждения, которое оказывается полезным во многих геометрических сюжетах с касающимися окружностями.

ТЕОРЕМА 1 (ЛЕММА САВАЯМЫ). Пусть B, C, X, Y — точки на окружности Ω , а окружность ω касается окружности Ω и касается прямых BX и CY в точках K и L . Тогда прямая KL проходит через центр вписанной окружности либо одной из невписанных окружностей треугольника BCY (а также треугольников BCX, XYB, XYC).

Доказательство этой теоремы можно найти, например, в статье [3]. Некоторые варианты конфигурации из теоремы 1 показаны на рис. 1.

Следующую теорему сформулировал И. Богданов.

ТЕОРЕМА 2 (О ЛУНОЧКАХ³⁾). Пусть зафиксированы точки B и C , окружность Ω , проходящая через B и C , а также дуга Γ некоторой окружности, имеющая концами точки B и C . На дуге Γ выбирается

¹⁾Окружность девяти точек — это окружность, которая проходит через середины сторон, основания высот и середины отрезков, соединяющие вершины треугольника с его ортоцентром.

²⁾Окружность девяти точек касается также невписанных окружностей треугольника.

³⁾В некотором смысле утверждение теоремы 2 эквивалентно теореме о сегменте из статьи [2]. Кроме предложенной конфигурации можно рассматривать другие, например, со случаем внешнего касания окружностей.

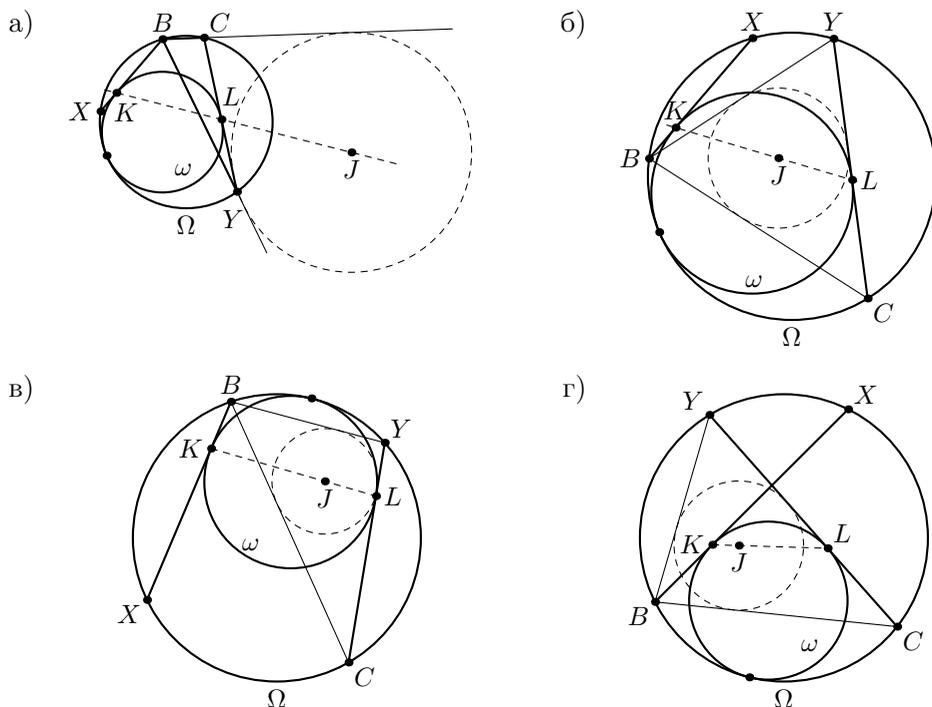


Рис. 1.

некоторая точка A . Обозначим через γ окружность, вписанную в треугольник ABC , и через r — ее радиус. Пусть прямые AB и AC пересекают вторично Ω в точках X и Y соответственно. Пусть ω — окружность, вписанная в угол BAC , которая касается Ω в точке T , касается отрезков BX и CY соответственно в точках K и L , и такая, что ровно один из отрезков AT и XY пересекает прямую BC ⁴⁾ (см. рис. 2), r_ω — радиус окружности ω . Тогда отношение радиусов $\frac{r}{r_\omega}$ не зависит от выбора точки A на дуге Γ .

ДОКАЗАТЕЛЬСТВО.⁵⁾ Пусть I_ω — центр окружности ω , I — центр окружности γ ; I_ω и I лежат на биссектрисе угла BAC . Заметим, что углы $\angle(AB, AC)$, $\angle(AB, AI)$, $\angle(AB, KL)$ и $\angle(KL, KI_\omega)$ ⁶⁾ постоянны. Теперь

⁴⁾ Если отказаться от последнего условия, то ω , возможно, неоднозначно определена.

⁵⁾ Идея излагаемого здесь доказательства принадлежит Н. Белухову; некоторые изменения и упрощения произошли в процессе занятия с командой России на международной олимпиаде школьников 2010 г.

⁶⁾ Здесь и далее $\angle(a, b)$ обозначает угол от прямой a до прямой b , отсчитываемый против часовой стрелки.

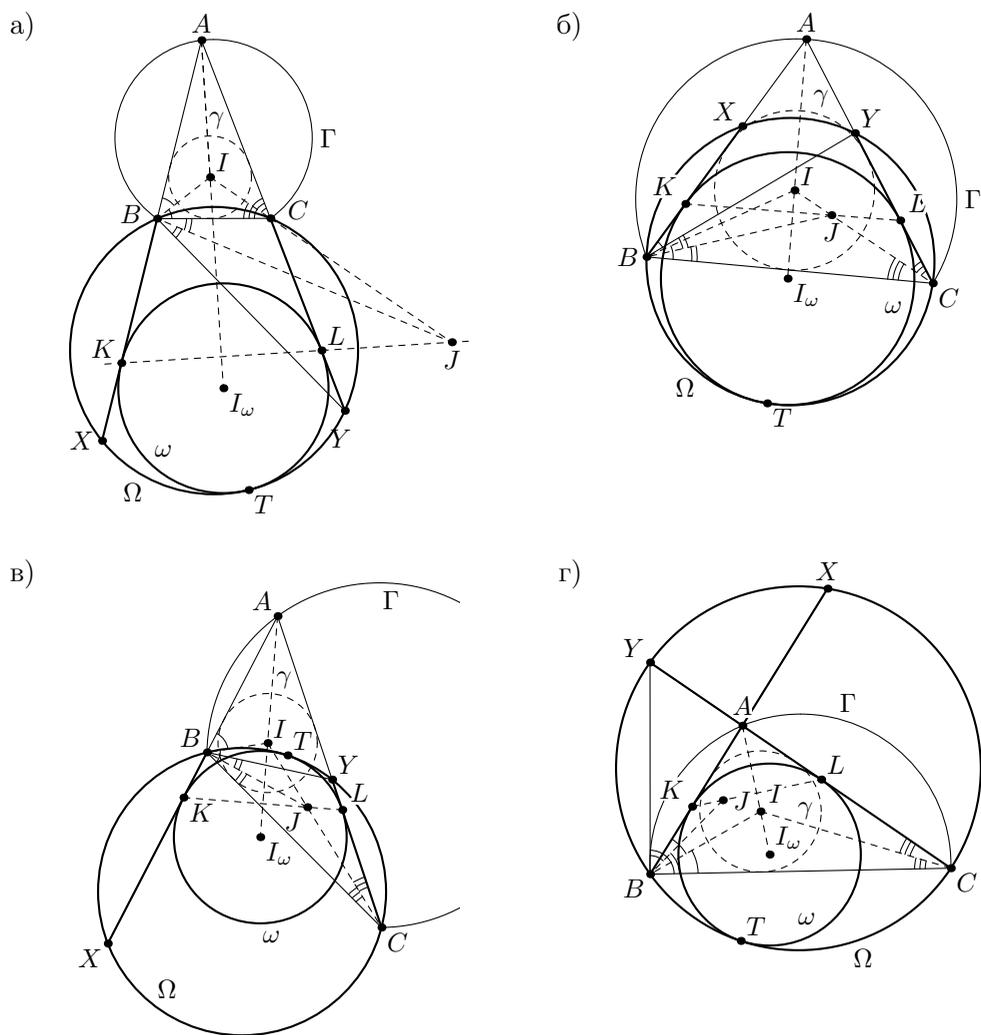


Рис. 2.

достаточно доказать, что $\angle(KL, KI)$ постоянный. Действительно, тогда для двух различных положений точки A на дуге Γ существует преобразование подобия, совмещающее четверки точек A, K, I_ω, I , значит, отношение $\frac{r}{r_\omega} = \frac{AI}{AI_\omega}$ для двух различных положений точки A одно и то же.

Прямые BI и CI – биссектрисы углов треугольника ABC . Пусть $J = CI \cap KL$, тогда по теореме 1 J – центр вписанной или невписанной окружности треугольника BCY . Подсчет углов (с учетом $KL \perp AI$) дает $\angle(CI, KL) = \angle(BI, BA)$, то есть $\angle(JI, JK) = \angle(BI, BK)$, значит точки

I, J, K, B лежат на одной окружности, откуда $\angle(KL, KI) = \angle(KJ, KI) = \angle(BJ, BI)$. Но угол $\angle(BY, BA)$ постоянный, а следовательно и угол $\angle(BJ, BI)$ между биссектрисами углов YBC и ABC постоянный. \square

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ ФЕЙЕРБАХА

Теперь можно дать следующее доказательство теоремы Фейербаха.⁷⁾

Пусть H — ортоцентр треугольника ABC , Γ — дуга BAC окружности, описанной около треугольника ABC , Ω — окружность (BHC) . Как нетрудно видеть, $\angle(BA, CA) = \angle(CH, BH)$, это означает что Γ и Ω имеют равные радиусы, и при отражении относительно BC дуга Γ переходит в дугу окружности Ω .

В обозначениях теоремы 2 рассмотрим окружность ω (рис. 2). Из теоремы 2 следует, что отношение радиусов $\frac{r}{r_\omega}$ постоянно. Поэтому достаточно рассмотреть частный случай $AB = AC$. Если $AB = AC$, то картинка симметрична относительно серединного перпендикуляра к BC ; в таком случае окружность γ касается отрезка BC в его середине M , а окружность ω касается дуги BC в ее середине N . Из симметрии окружностей (ABC) и Ω относительно BC имеем $AM = MN$. Гомотетия с центром A , переводящая M в N , очевидно, переводит γ в ω , поэтому $\frac{r}{r_\omega} = \frac{AM}{AN} = \frac{1}{2}$.

Возвращаясь к общему случаю, имеем $\frac{r}{r_\omega} = \frac{1}{2}$. Это означает, что гомотетия h с центром A и коэффициентом $\frac{1}{2}$ переводит окружность ω в окружность γ . Гомотетия h переводит окружность Ω , проходящую через B, C, H , в окружность, проходящую через середины отрезков AB, AC, AH , то есть в окружность девяти точек треугольника ABC . При гомотетии касание окружностей сохраняется, поэтому γ и окружность девяти точек касаются. \square

ОПИСАНИЕ ТОЧКИ ФЕЙЕРБАХА

С помощью следующей теоремы мы решим задачу 8 «Математического просвещения» из вып. 14, хотя рассматриваемая здесь конструкция интересна сама по себе.

ТЕОРЕМА 3. Пусть окружности Ω и ω касаются внутренним образом в точке T . Из точек B и C окружности ω проведены соответственно касательные BK и CL к окружности ω ($K, L \in \omega$). Пусть

⁷⁾Используя соответствующую конфигурацию теоремы о луночках так же можно доказать, что вневписанные окружности касаются окружности девяти точек.

$S = BC \cap KL$ (см. рис. 3). Тогда прямая ST проходит через середину дуги BC окружности Ω (если $KL \parallel BC$, то T — середина дуги BC).⁸⁾

ДОКАЗАТЕЛЬСТВО. Достаточно доказать, что TS — это биссектриса (внутренняя или внешняя — в зависимости от конфигурации) угла BTC , то есть, что $\frac{SB}{SC} = \frac{BT}{CT}$.

Применяя теорему Менелая к треугольнику, образованному прямыми BC , BK и CL , с секущей KL , и используя равенство длин касательных к ω , проведенных из одной точки, получаем: $\frac{SB}{SC} = \frac{BK}{CL}$.

Пусть D и E — вторые точки пересечения прямых TB и TC с ω . При гомотетии с центром T , переводящей ω в Ω , точки D и E перейдут соответственно в B и C , значит $DE \parallel BC$. Поэтому $\frac{BD}{CE} = \frac{BT}{CT}$. Отсюда $\frac{SB^2}{SC^2} = \frac{BK^2}{CL^2} = \frac{BD \cdot BT}{CE \cdot CT} = \frac{BT^2}{CT^2}$, то есть $\frac{SB}{SC} = \frac{BT}{CT}$, что и требовалось.⁹⁾ \square

ЗАДАЧА. В треугольнике ABC точки A_1, B_1, C_1 — точки касания сторон BC, CA, AB со вписанной окружностью соответственно, A_0, B_0, C_0 — середины сторон BC, CA, AB соответственно. Пусть $C' = A_0B_0 \cap A_1B_1$, $A' = B_0C_0 \cap B_1C_1$, $B' = C_0A_0 \cap C_1A_1$. Докажите, что A_1A' , B_1B' и C_1C' пересекаются в точке Фейербаха.

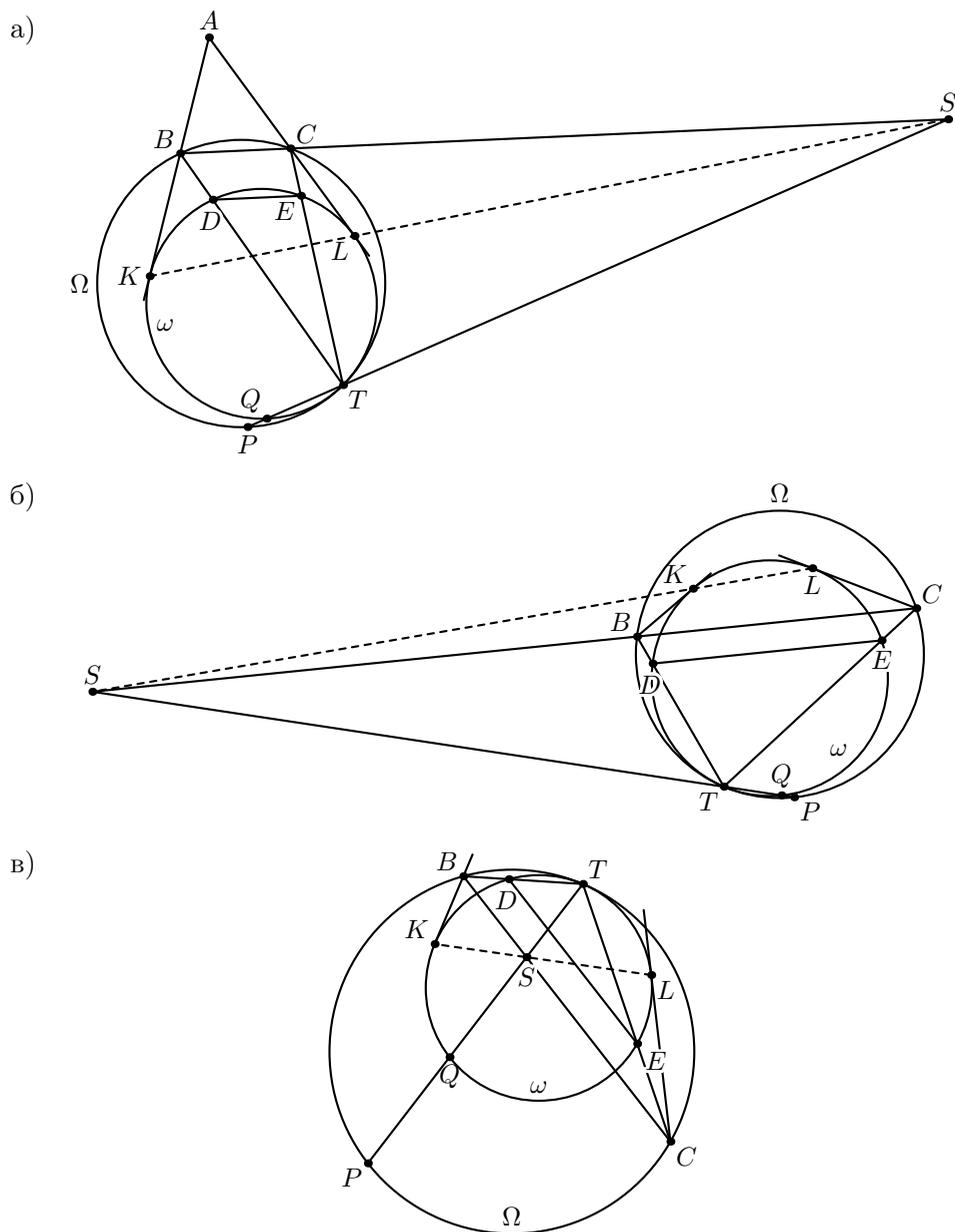
РЕШЕНИЕ. Докажем, что A_1F проходит через A' , где F — точка Фейербаха. Аналогично доказывается, что B_1F и C_1F проходят через B' и C' соответственно, откуда следует утверждение задачи.

Используем обозначения из теоремы 2.

Если $KL \parallel BC$, то $AB = AC$, и утверждение очевидно из симметрии.

⁸⁾ Частный случай этой теоремы, когда точка пересечения BK и CL лежит на окружности Ω — это задача И. Ф. Шарыгина, предлагавшаяся на соровской олимпиаде.

⁹⁾ Приведем построение, из которого следует другое доказательство теоремы 3. Пусть изначально дана окружность ω с центром O и точки B и C вне ее. Пусть из B проведены касательные BK_1 и BK_2 , а из C — касательные BL_1 и BL_2 ($K_1, K_2, L_1, L_2 \in \omega$). Положим $S = K_1L_1 \cap K_2L_2$, $R = K_1L_2 \cap K_2L_1$, $Z = K_1K_2 \cap L_1L_2$. Тогда тройка точек S, R, Z автополярна относительно ω (то есть для любой точки из этой тройки прямая, проходящая через две другие, является ее полярной). Как известно, точки R, B, S, C лежат на одной прямой, причем эта четверка точек — гармоническая. Пусть ZO пересекает ω в точках Q_1 и Q_2 . Касательные к ω , проведенные в Q_1 и Q_2 , параллельны BC , так как $ZO \perp SR$. Пусть Q_1R и Q_2R пересекают вторично ω соответственно в точках T_1 и T_2 . Тогда T_1Q_2 и T_2Q_1 пересекаются в точке, лежащей на полярной точки R и на полярной точки Z , то есть в точке S . Центральное проектирование с центром T_1 переводит четверку R, B, S, C в гармоническую четверку точек Q_1, D, Q_2, E окружности ω . Так как Q_1Q_2 — диаметр, то $Q_1Q_2 \perp DE \parallel BC$. Это означает, что существует гомотетия с центром T_1 , переводящая треугольник T_1DE в треугольник T_1BC , а окружность ω — в окружность Ω , описанную вокруг треугольника T_1BC и касающуюся ω . Эта гомотетия переводит Q_2 в середину дуги BC окружности Ω , значит S, T_1, Q_2 и середина дуги BC лежат на одной прямой.



Пусть $S = KL \cap BC$. По теореме 3 прямая ST пересекает вторично Ω в точке P — середине дуги BC . Касательная к Ω , проведенная в P , параллельна BC . Пусть ST пересекает вторично ω в точке Q (см. рис. 3). При гомотетии с центром T , переводящей Ω в ω , точка P переходит в Q , поэтому касательная к ω , проведенная в Q , также параллельна BC .

Теперь, как и выше в доказательстве теоремы Фейербаха, применим гомотетию h с центром в точке A и коэффициентом $\frac{1}{2}$. При этой гомотетии ω переходит во вписанную окружность γ , причем точка Q переходит в A_1 (касательные к ω и γ в точках Q и A_1 параллельны). При гомотетии h прямая BC переходит в прямую B_0C_0 , прямая KL — в прямую B_1C_1 , поэтому точка $S = BC \cap KL$ переходит в $A' = B_0C_0 \cap B_1C_1$. Как мы видели в доказательстве теоремы Фейербаха, h переводит T в F . Так как прямая QT проходит через точку S , то прямая A_1F проходит через точку A' , что и требовалось доказать. \square

СПИСОК ЛИТЕРАТУРЫ

- [1] Ивлев Ф. *Несколько прямых, проходящих через точку Фейербаха* // Математическое Просвещение. Сер. 3, вып. 15. 2011. С. 219–228.
- [2] Протасов В. *Вокруг теоремы Фейербаха* // Квант. №9. 1992. С. 51–58.
- [3] Протасов В. *Касающиеся окружности: от Тебо до Фейербаха* // Квант. №4. 2008. С. 10–15.

О формуле Брахмагупты в геометрии Лобачевского

А. Д. Медных*

1. ВВЕДЕНИЕ

Из школьного курса всем хорошо известна формула Герона, выражающая площадь треугольника S через длины его сторон a , b и c . Представим ее в следующем виде

$$S^2 = (p - a)(p - b)(p - c)p, \quad (1)$$

где $p = \frac{a + b + c}{2}$ — полупериметр треугольника.

Индийский математик и астроном Брахмагупта (VII век) нашел удивительное обобщение этой формулы для четырехугольника, вписанного в окружность. В этом случае она имеет вид

$$S^2 = (p - a)(p - b)(p - c)(p - d), \quad (2)$$

где a , b , c , d — стороны четырехугольника, а $p = \frac{a + b + c + d}{2}$ — его полупериметр.

Отметим еще один важный вклад Брахмагупты в развитие математики. Он впервые ввел в рассмотрение число 0.

Формула (1), очевидно, является частным случаем формулы (2) при $d = 0$. Доказательство формулы Брахмагупты можно найти в книге Я. П. Понарина [1, с. 90].

Дальнейшие обобщения формул Герона и Брахмагупты на случай произвольных n -угольников, вписанных в окружность можно найти в замечательной работе И. Х. Сабитова [2]. Там же содержится обзор близких результатов, полученных другими авторами. Отметим, что вписанные многоугольники, рассматриваемые в [2], не обязательно являются выпуклыми.

*Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (код проекта 09-01-00255) и грантом АВЦП развития научного потенциала Высшей школы (проект №2.1.1/3707) и грантом поддержки ведущих научных школ НШ-6613.2010.1

Они могут допускать самопересечение сторон. В частности, площадь вписанного четырехугольника с самопересечениями является корнем некоторого биквадратного уравнения, коэффициенты которого — целочисленные полиномы от длин сторон a, b, c, d . В данной статье мы будем рассматривать только выпуклые четырехугольники без самопересечений.

Перейдем теперь к геометрии Лобачевского или, что то же самое, к гиперболической геометрии. Элементарные сведения из гиперболической геометрии приведены в книгах [3] и [4]. Все результаты настоящей работы сформулированы для плоскости Лобачевского с гауссовой кривизной равной $k = -1$.

В последнее время появилось много работ, посвященных неевклидовым аналогам теорем из классической евклидовой геометрии. Эти результаты, во многом, стали возможны благодаря использованию современных компьютеров, способных выполнять сложные символьные вычисления с тригонометрическими формулами. Общие сведения о неевклидовых многоугольниках, вписанных в окружность, можно найти в статьях [5] и [6]. В частности, в [5] показано, что вписанный n -угольник однозначно, с точностью до изометрии, определяется длинами своих сторон. В работе [6] установлено, что среди всех гиперболических многоугольников с заданными длинами сторон, наибольшую площадь имеет многоугольник, вписанный в окружность, орицикл или эквидистанту.

Классические теоремы из евклидовой геометрии могут допускать несколько различных вариантов их обобщений в гиперболической геометрии. Это справедливо, в частности, и для формулы Герона. На плоскости Лобачевского она имеет три следующих аналога.

ТЕОРЕМА 1. *Площадь S гиперболического треугольника со сторонами a, b и c находится по одной из трех следующих формул:*

$$\operatorname{tg}^2 \frac{S}{4} = \operatorname{th} \frac{p-a}{2} \operatorname{th} \frac{p-b}{2} \operatorname{th} \frac{p-c}{2} \operatorname{th} \frac{p}{2}, \quad (3)$$

$$\sin^2 \frac{S}{2} = \frac{\operatorname{sh}(p-a) \operatorname{sh}(p-b) \operatorname{sh}(p-c) \operatorname{sh} p}{4 \operatorname{ch}^2 \frac{a}{2} \operatorname{ch}^2 \frac{b}{2} \operatorname{ch}^2 \frac{c}{2}}, \quad (4)$$

$$\sin^2 \frac{S}{4} = \frac{\operatorname{sh} \frac{p-a}{2} \operatorname{sh} \frac{p-b}{2} \operatorname{sh} \frac{p-c}{2} \operatorname{sh} \frac{p}{2}}{\operatorname{ch} \frac{a}{2} \operatorname{ch} \frac{b}{2} \operatorname{ch} \frac{c}{2}}, \quad (5)$$

где $p = \frac{a+b+c}{2}$ — полупериметр треугольника.

Формулы (3) и (4) можно найти в книге [3, с. 36], а формула (5) получается извлечением квадратного корня из их произведения.

Цель настоящей работы — найти аналоги приведенных формул для площади гиперболического четырехугольника, вписанного в окружность,

орицикл или эквидистанту. Тем самым будут установлены три различных варианта классической формулы Брахмагупты для плоскости Лобачевского.

Развитый здесь подход, без сомнения, может быть использован для установления подобных теорем в сферической геометрии.

2. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ ИЗ ЕВКЛИДОВОЙ И ГИПЕРБОЛИЧЕСКОЙ ГЕОМЕТРИЙ

Напомним несколько хорошо известных фактов о четырехугольниках, вписанных в окружность.

Евклидов четырехугольник с внутренними углами A, B, C, D является вписанным в окружность тогда и только тогда, когда выполняется равенство $A + C = B + D = \pi$. Доказательство этого утверждения можно найти в [1, с. 52].

В то же время, в геометрии Лобачевского указанное свойство записывается еще более просто. Следуя Ф. В. Петрову [7], будем называть гиперболический четырехугольник *вписанным*, если он вписан в окружность, орицикл или эквидистанту. Все необходимые определения содержатся в работе [7], где, в частности, получен следующий результат.

ПРЕДЛОЖЕНИЕ 2. *Гиперболический четырехугольник с внутренними углами A, B, C, D является вписанным тогда и только тогда, когда выполняется равенство*

$$A + C = B + D.$$

Поскольку сумма углов в любом гиперболическом четырехугольнике меньше 2π , для вписанного четырехугольника всегда имеем неравенство $A + C = B + D < \pi$.

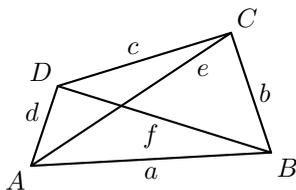


Рис. 1.

Предположим теперь, что углы четырехугольника неизвестны, а длины его сторон и диагоналей, изображенные на рис. 1, равны a, b, c, d, e, f . Тогда необходимые и достаточные условия для евклидова четырехугольника быть вписанным в окружность выражаются равенством $ef = ac + bd$.

Это утверждение хорошо известно как теорема Птолемея (см., например, [1, с. 61]).

Аналогичные условия для гиперболического четырехугольника получены в работе [8]. В терминах длин сторон они выражаются следующим вариантом теоремы Птолемея.

ПРЕДЛОЖЕНИЕ 3. *Гиперболический четырехугольник с длинами сторон a, b, c, d и диагоналями e, f является вписанным тогда и только тогда, когда выполняется равенство*

$$\operatorname{sh} \frac{e}{2} \operatorname{sh} \frac{f}{2} = \operatorname{sh} \frac{a}{2} \operatorname{sh} \frac{c}{2} + \operatorname{sh} \frac{b}{2} \operatorname{sh} \frac{d}{2}.$$

Важным дополнением к теореме Птолемея служит следующее свойство вписанного четырехугольника на евклидовой плоскости. Длины его сторон и диагоналей связаны соотношением

$$\frac{e}{f} = \frac{ad + bc}{ab + cd}. \quad (6)$$

(См. [1, с. 62].) Вместе с теоремой Птолемея указанное равенство позволяет выразить длины диагоналей четырехугольника через длины его сторон.

В работе [9] замечено, что основные соотношения между длинами сторон и диагоналями вписанного евклидова многоугольника остаются справедливыми и в гиперболической геометрии. Для их формулировки, как правило, достаточно во всех формулах заменить длину стороны a на величину $s(a) = \operatorname{sh} \frac{a}{2}$. В частности, соотношение (6) записывается следующим образом.

ПРЕДЛОЖЕНИЕ 4. *Длины сторон и диагонали вписанного гиперболического четырехугольника связаны соотношением*

$$\frac{s(e)}{s(f)} = \frac{s(a)s(d) + s(b)s(c)}{s(a)s(b) + s(c)s(d)}.$$

Из предложений 3 и 4 находятся следующие формулы для длин диагоналей вписанного гиперболического четырехугольника

$$s^2(e) = \frac{s(a)s(d) + s(b)s(c)}{s(a)s(b) + s(c)s(d)} (s(a)s(c) + s(b)s(d)), \quad (7)$$

$$s^2(f) = \frac{s(a)s(b) + s(c)s(d)}{s(a)s(d) + s(b)s(c)} (s(a)s(c) + s(b)s(d)). \quad (8)$$

Важно отметить, что полученные формулы верны также в евклидовой и сферической геометриях, если в качестве $s(a)$ взять функции $s(a) = a$ и $s(a) = \sin \frac{a}{2}$ соответственно.

Сформулированные утверждения потребуются нам ниже для доказательства теоремы Брахмагупты для гиперболического четырехугольника.

3. ФОРМУЛИРОВКИ ТЕОРЕМЫ БРАХМАГУПТЫ И ЕЕ СЛЕДСТВИЯ

В этом параграфе мы рассмотрим три формулировки теоремы Брахмагупты для гиперболического четырехугольника. Они являются аналогами соответствующих утверждений теоремы 1 для треугольника. Кроме того, будут получены два следствия из указанных теорем. Одно из них устанавливает верхнюю и нижнюю оценки на площадь вписанного четырехугольника через длины его сторон, а второе выражает площадь одновременно вписанного и описанного четырехугольника.

Аналог формулы (3) имеет следующий вид.

ТЕОРЕМА 5. *Площадь S вписанного гиперболического четырехугольника со сторонами a, b, c и d находится по формуле*

$$\operatorname{tg}^2 \frac{S}{4} = \frac{1}{1-\varepsilon} \operatorname{th} \frac{p-a}{2} \operatorname{th} \frac{p-b}{2} \operatorname{th} \frac{p-c}{2} \operatorname{th} \frac{p-d}{2},$$

$$\text{где } \varepsilon = \frac{\operatorname{sh} \frac{a}{2} \operatorname{sh} \frac{b}{2} \operatorname{sh} \frac{c}{2} \operatorname{sh} \frac{d}{2}}{\operatorname{ch} \frac{p-a}{2} \operatorname{ch} \frac{p-b}{2} \operatorname{ch} \frac{p-c}{2} \operatorname{ch} \frac{p-d}{2}}, \quad a p = \frac{a+b+c+d}{2}.$$

Отметим, что при $d = 0$ число ε обращается в ноль и мы снова имеем формулу (3). Формула (4) для случая четырехугольника переписывается в виде следующей теоремы.

ТЕОРЕМА 6. *Площадь S вписанного гиперболического четырехугольника со сторонами a, b, c и d находится по формуле*

$$\sin^2 \frac{S}{2} = \frac{\operatorname{sh}(p-a) \operatorname{sh}(p-b) \operatorname{sh}(p-c) \operatorname{sh}(p-d)}{4 \operatorname{ch}^2 \frac{a}{2} \operatorname{ch}^2 \frac{b}{2} \operatorname{ch}^2 \frac{c}{2} \operatorname{ch}^2 \frac{d}{2}} (1-\varepsilon),$$

где p и ε — те же, что и в теореме 5.

Заметим, что при перемножении формул площади, приведенных в теоремах 5 и 6, величины $1-\varepsilon$ взаимно сокращаются. После извлечения квадратного корня из полученного произведения приходим к следующему утверждению. Оно является прямым аналогом формулы (5).

ТЕОРЕМА 7. *Площадь S вписанного гиперболического четырехугольника со сторонами a, b, c и d находится по формуле*

$$\sin^2 \frac{S}{4} = \frac{\operatorname{sh} \frac{p-a}{2} \operatorname{sh} \frac{p-b}{2} \operatorname{sh} \frac{p-c}{2} \operatorname{sh} \frac{p-d}{2}}{\operatorname{ch} \frac{a}{2} \operatorname{ch} \frac{b}{2} \operatorname{ch} \frac{c}{2} \operatorname{ch} \frac{d}{2}},$$

$$\text{где } p = \frac{a+b+c+d}{2}.$$

Из формулировки теоремы 5 непосредственно заключаем, что при $a, b, c, d \neq 0$ имеют место неравенства $\frac{1}{1-\varepsilon} > 0$ и $\varepsilon > 0$. Откуда $0 < \varepsilon < 1$. Учитывая это обстоятельство, получим приведенное ниже следствие из теорем 5 и 6.

СЛЕДСТВИЕ 8. Для невырожденного гиперболического четырехугольника со сторонами $a, b, c, d \neq 0$ имеют место следующие неравенства

$$\begin{aligned} \operatorname{tg}^2 \frac{S}{4} &> \operatorname{th} \frac{p-a}{2} \operatorname{th} \frac{p-b}{2} \operatorname{th} \frac{p-c}{2} \operatorname{th} \frac{p-d}{2}, \\ \sin^2 \frac{S}{2} &< \frac{\operatorname{sh}(p-a) \operatorname{sh}(p-b) \operatorname{sh}(p-c) \operatorname{sh}(p-d)}{4 \operatorname{ch}^2 \frac{a}{2} \operatorname{ch}^2 \frac{b}{2} \operatorname{ch}^2 \frac{c}{2} \operatorname{ch}^2 \frac{d}{2}}. \end{aligned}$$

Четырехугольник, описанный около окружности, очевидно, удовлетворяет следующему свойству

$$a + c = b + d = (-|-) + (-||-) + (-|||-) + (-\circ-).$$

(См. рис. 2.) В этом случае, $p - a = c, p - b = d, p - c = a, p - d = b$.

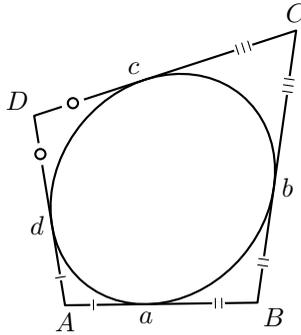


Рис. 2.

Это позволяет установить следующее интересное следствие из теоремы 7.

СЛЕДСТВИЕ 9. Пусть гиперболический четырехугольник со сторонами a, b, c и d является одновременно вписанным и описанным. Тогда его площадь S находится по формуле

$$\sin^2 \frac{S}{4} = \operatorname{th} \frac{a}{2} \operatorname{th} \frac{b}{2} \operatorname{th} \frac{c}{2} \operatorname{th} \frac{d}{2}.$$

Классический аналог этой теоремы хорошо известен [1, с. 91]. Если евклидов четырехугольник является одновременно вписанным и описанным, то его площадь определяется равенством $S^2 = abcd$.

4. ДОКАЗАТЕЛЬСТВО ТЕОРЕМ БРАХМАГУПТЫ ДЛЯ ГИПЕРБОЛИЧЕСКОГО ЧЕТЫРЕХУГОЛЬНИКА

Рассмотрим вписанный гиперболический четырехугольник, длины сторон которого и углы указаны на рис. 1. Обозначим через S площадь этого четырехугольника. Тогда по классической формуле Гаусса – Бонне имеем

$$S = 2\pi - A - B - C - D.$$

Выразим величину $\sin^2 \frac{S}{4}$ через длины сторон a, b, c и d . Учитывая равенство $A + C = B + D$ (см. предложение 2), получим

$$2 \sin^2 \frac{S}{4} = 1 - \cos \frac{S}{2} = 1 - \cos(\pi - (A + C)) = 1 + \cos(A + C).$$

Откуда

$$\sin^2 \frac{S}{4} = \frac{1 + \cos A \cos C - \sin A \sin C}{2}. \quad (9)$$

Покажем, что величины $\cos A, \cos C$, а также произведение $\sin A \sin C$ выражаются через элементарные функции от длин сторон, и найдем эти выражения в явном виде.

Прежде всего, выразим $\cos A$ через длины сторон a, b, c, d . Для этого воспользуемся теоремой косинусов для гиперболического треугольника ABD :

$$\operatorname{ch} f = \operatorname{ch} a \operatorname{ch} d - \operatorname{sh} a \operatorname{sh} d \cos A.$$

Откуда

$$\cos A = \frac{\operatorname{ch} a \operatorname{ch} d - \operatorname{ch} f}{\operatorname{sh} a \operatorname{sh} d}. \quad (10)$$

Поскольку $\operatorname{ch} f = 2s^2(f) + 1$, а также $\operatorname{ch} a = 2s^2(a) + 1$ и $\operatorname{ch} d = 2s^2(d) + 1$, мы можем воспользоваться формулами (8) и (10) для нахождения $\cos A$ через a, b, c и d .

Поручая необходимые упрощения компьютеру, получим

$$\begin{aligned} \cos A &= \frac{(2s^2(a) + 1)(2s^2(d) + 1) - (2s^2(f) + 1)}{2s(a) \operatorname{ch} \frac{a}{2} \cdot 2s(d) \operatorname{ch} \frac{d}{2}} = \\ &= \frac{s^2(a) - s^2(b) - s^2(c) + s^2(d) + 2s(a)s(b)s(c)s(d) + 2s^2(a)s^2(d)}{2(s(a)s(d) + s(b)s(c)) \operatorname{ch} \frac{a}{2} \operatorname{ch} \frac{d}{2}}. \quad (11) \end{aligned}$$

Аналогично устанавливается формула

$$\cos C = \frac{-s^2(a) + s^2(b) + s^2(c) - s^2(d) + 2s(a)s(b)s(c)s(d) + 2s^2(b)s^2(c)}{2(s(a)s(d) + s(b)s(c)) \operatorname{ch} \frac{b}{2} \operatorname{ch} \frac{c}{2}}. \quad (12)$$

Извлекая положительный квадратный корень из выражения

$$\sin^2 A \sin^2 C = (1 - \cos^2 A)(1 - \cos^2 C),$$

где $\cos A$ и $\cos C$ найдены по формулам (11) и (12), имеем

$$\begin{aligned} & \sin A \sin C = \\ & 4 \operatorname{ch} \frac{a+b-c-d}{4} \operatorname{ch} \frac{a-b+c-d}{4} \operatorname{ch} \frac{a-b-c+d}{4} \operatorname{ch} \frac{a+b+c+d}{4} \\ & \operatorname{sh} \frac{-a+b+c+d}{4} \operatorname{sh} \frac{a-b+c+d}{4} \operatorname{sh} \frac{a+b-c+d}{4} \operatorname{sh} \frac{a+b+c-d}{4} / \quad (13) \\ & ((\operatorname{sh} \frac{a}{2} \operatorname{sh} \frac{d}{2} + \operatorname{sh} \frac{b}{2} \operatorname{sh} \frac{c}{2})^2 \operatorname{ch} \frac{a}{2} \operatorname{ch} \frac{b}{2} \operatorname{ch} \frac{c}{2} \operatorname{ch} \frac{d}{2}). \end{aligned}$$

Подставляя формулы (11), (12) и (13) в (9), после упрощений на компьютере получим

$$\sin^2 \frac{S}{4} = \frac{\operatorname{sh} \frac{-a+b+c+d}{4} \operatorname{sh} \frac{a-b+c+d}{4} \operatorname{sh} \frac{a+b-c+d}{4} \operatorname{sh} \frac{a+b+c-d}{4}}{\operatorname{ch} \frac{a}{2} \operatorname{ch} \frac{b}{2} \operatorname{ch} \frac{c}{2} \operatorname{ch} \frac{d}{2}}. \quad (14)$$

Это доказывает теорему 7.

Аналогично, замечая, что $2 \cos^2 \frac{S}{4} = 1 + \cos \frac{S}{2} = 1 - \cos(A + C)$, имеем

$$\cos^2 \frac{S}{4} = \frac{\operatorname{ch} \frac{a+b-c-d}{4} \operatorname{ch} \frac{a-b+c-d}{4} \operatorname{ch} \frac{a-b-c+d}{4} \operatorname{ch} \frac{a+b+c+d}{4}}{\operatorname{ch} \frac{a}{2} \operatorname{ch} \frac{b}{2} \operatorname{ch} \frac{c}{2} \operatorname{ch} \frac{d}{2}}. \quad (15)$$

Доказательство следующей леммы представляет из себя легкое упражнение для компьютера.

ЛЕММА 10. *Величина*

$$Q = \frac{\operatorname{ch} \frac{a+b-c-d}{4} \operatorname{ch} \frac{a-b+c-d}{4} \operatorname{ch} \frac{a-b-c+d}{4} \operatorname{ch} \frac{a+b+c+d}{4}}{\operatorname{ch} \frac{-a+b+c+d}{4} \operatorname{ch} \frac{a-b+c+d}{4} \operatorname{ch} \frac{a+b-c+d}{4} \operatorname{ch} \frac{a+b+c-d}{4}}$$

представима в виде $Q = 1 - \varepsilon$, где

$$\varepsilon = \frac{\operatorname{sh} \frac{a}{2} \operatorname{sh} \frac{b}{2} \operatorname{sh} \frac{c}{2} \operatorname{sh} \frac{d}{2}}{\operatorname{ch} \frac{p-a}{2} \operatorname{ch} \frac{p-b}{2} \operatorname{ch} \frac{p-c}{2} \operatorname{ch} \frac{p-d}{2}}, \quad a p = \frac{a+b+c+d}{2}.$$

Взяв учетверенное произведение формул (14) и (15), имеем

$$\sin^2 \frac{S}{2} = \frac{\operatorname{sh} \frac{-a+b+c+d}{2} \operatorname{sh} \frac{a-b+c+d}{2} \operatorname{sh} \frac{a+b-c+d}{2} \operatorname{sh} \frac{a+b+c-d}{2}}{4 \operatorname{ch}^2 \frac{a}{2} \operatorname{ch}^2 \frac{b}{2} \operatorname{ch}^2 \frac{c}{2} \operatorname{ch}^2 \frac{d}{2}} \cdot Q, \quad (16)$$

где Q то же, что и в лемме 10.

Из формулы (16), пользуясь леммой 10 и очевидными тождеством $p - a = \frac{-a+b+c+d}{2}$, получим утверждение теоремы 6.

Аналогично, поделив (14) на (15), имеем

$$\operatorname{tg}^2 \frac{S}{4} = \frac{\operatorname{sh} \frac{-a+b+c+d}{4} \operatorname{sh} \frac{a-b+c+d}{4} \operatorname{sh} \frac{a+b-c+d}{4} \operatorname{sh} \frac{a+b+c-d}{4}}{\operatorname{ch} \frac{a+b-c-d}{4} \operatorname{ch} \frac{a-b+c-d}{4} \operatorname{ch} \frac{a-b-c+d}{4} \operatorname{ch} \frac{a+b+c+d}{4}}. \quad (17)$$

Откуда, еще раз применяя лемму 10, установим справедливость теоремы 5.

СПИСОК ЛИТЕРАТУРЫ

- [1] Понарин Я. П. *Элементарная геометрия. Т.1. Планиметрия*. М.: МЦНМО. 2004. 312 с.
- [2] Сабитов И. Х. *Решение циклических многоугольников // Математическое просвещение. Третья серия. Вып. 14. 2010. С. 149–154.*
- [3] Прасолов В. В. *Геометрия Лобачевского*. 3-е изд. М.: МЦНМО. 2004. 88 с.
- [4] Алексеевский Д. В., Винберг Э. Б., Солодовников А. С. *Геометрия пространств постоянной кривизны // Итоги науки и техники. Современные проблемы математики. Фундаментальные направления. М.: ВИНТИ. Т. 29. 1988. С. 1–146.*
- [5] Walter R. *Polygons in hyperbolic geometry 1: Rigidity and inversion of the n-inequality*. 2010. arXiv:1008.3404v1 [math.MG]
- [6] Walter R. *Polygons in hyperbolic geometry 2: Maximality of area*. 2010. arXiv:1008.3821v1 [math.MG]
- [7] Петров Ф. В. *Вписанные четырехугольники и трапеции в абсолютной геометрии // Математическое просвещение. Третья серия. Вып. 13. 2009. С. 149–154.*
- [8] Valentine J. E. *An analogue of Ptolemy's theorem and its converse in hyperbolic geometry // Pacific J. Math. Vol. 34. 1970. P. 817–825.*
- [9] Ren Guo, Nilgün Sönmez. *Cyclic polygons in classical geometry // Comptes rendus de l'Academie bulgare des Sciences. Vol. 64, no. 2. 2011. P. 185–194. arXiv:1009.2970v1 [math.MG].*

Преподавание математики

Стохастический анализ в задачах

А. Гасников Е. Черноусова Т. Нагапетян О. Федько

Курсы «Теория вероятностей», «Случайные процессы», «Математическая статистика» читаются студентам ФУПМ МФТИ вот уже более 30 лет. Во многом эти курсы сформировались под влиянием и при самом непосредственном участии профессора Андрея Александровича Натана (06.02.1918 – 09.01.2009) [40].

На данный момент уже выпущены пособия по материалам прочитанных курсов, написанные А. А. Натаном в соавторстве с учениками (ныне лекторами по этим дисциплинам) доцентами С. А. Гузом и О. Г. Горбачевым.

Натан А.А., Горбачев О.Г., Гуз С.А. Теория вероятностей: Учебное пособие. — М.: МЗ Пресс — МФТИ, 2007. — 253 с.

Натан А.А., Горбачев О.Г., Гуз С.А. Основы теории случайных процессов: Учебное пособие. — М.: МЗ Пресс — М.: МФТИ, 2003. — 165 с.

Натан А.А., Горбачев О.Г., Гуз С.А. Математическая статистика: Учебное пособие. — М.: МЗ Пресс — М.: МФТИ, 2004. — 156 с.

Пособия получили положительные отзывы специалистов. Однако, как отмечал Андрей Александрович, пособия представляют собой лишь запись (конспект) курса лекций, и содержат мало разобранных примеров. Ввиду вышесказанного кафедра Математических основ управления ФУПМ, которую долгие годы возглавлял Андрей Александрович, решила подготовить настоящую статью, в основу которой положены задачи (в том числе повышенной сложности), предлагавшиеся в разные годы, в основном студентам ФУПМ, на различных семинарах, сдачах заданий и экзаменах. Главными отличительными особенностями являются: а) широкий спектр представленного материала, б) отражение ряда современных течений и в) нацеленность на приложения. При работе над задачами в 2010 г. было решено организовать учебно-методический кафедральный семинар

«Стохастический анализ в задачах» [38]. На этом семинаре обсуждаются важные вопросы, как правило, не входящие в обязательную программу цикла стохастических дисциплин.

Отметим несколько важных современных течений, нашедших отражения в виде докладов на этом семинаре и в виде задач: понятие равновесия макросистемы = эргодическая теорема + явление концентрации меры (Пуанкаре – Леви – Мильман – Громов – Талагран), стохастические транспортные (компьютерные) сети при термодинамическом предельном переходе, вероятностные методы в комбинаторике и теории чисел, вероятностные и рандомизированные алгоритмы.

Задачи специально подбирались таким образом, чтобы с одной стороны часть из них была доступна продвинутым школьникам старших классов, а с другой стороны — отражали основной инструментарий и наиболее важные современные приложения вероятностных методов. Некоторые задачи трудны, и их решение предполагает серьёзное самостоятельное исследование (такие задачи помечены звёздочкой). Причём понимание условий ряда таких задач, в свою очередь, требует значительных усилий. Наконец, имеется пара задач, полные решения которых авторам не известны.

От читателей предполагается знакомство с азами теории вероятностей, случайных процессов и математической статистики, например, в объёме замечательной книги [12]. Рекомендуем также ознакомиться с материалами [24, 36, 44], содержащими много интересных вероятностных задач.

Авторы благодарны О. Г. Горбачеву и С. А. Гузу за ряд ценных замечаний, а также М. Н. Вялому и А. Х. Шеню, способствовавшим улучшению первоначальной версии текста. Работа выполнена при поддержке Лаборатории структурных методов анализа данных в предсказательном моделировании, МФТИ, грант правительства РФ дог. 11 11.G34.31.0073.

НЕРАВЕНСТВО ЧЕБЫШЁВА И ЗАКОН БОЛЬШИХ ЧИСЕЛ

ЗАДАЧА (О ВЫБОРАХ). В некотором городе прошел второй тур выборов. Выбор был между двумя кандидатами А и В (графы «против всех» на этих выборах не было). Сколько человек надо опросить на выходе с избирательных участков, чтобы, исходя из ответов, можно было определить долю проголосовавших за кандидата А с точностью 0.01 и с вероятностью не меньшей 0.95.

ЗАДАЧА (О КОЛИЧЕСТВЕ ЭКЗАМЕНАЦИОННЫХ БИЛЕТОВ). В некотором вузе проходит экзамен. Количество экзаменационных билетов $N \gg 1$. Перед экзаменационной аудиторией выстроилась очередь из студентов, которые не знают чему равно N . Согласно этой очереди студенты вызываются на экзамен (второй студент заходит в аудиторию, после того

как из нее выйдет первый и т. д.). Каждый студент с равной вероятностью может выбрать любой из N билетов (в независимости от других студентов). Проэкзаменованные студенты, выходя из аудитории, сообщают оставшейся очереди номера своих билетов. Оцените (сверху) сколько студентов должно быть проэкзаменовано, чтобы оставшаяся к этому моменту очередь смогла оценить число экзаменационных билетов с точностью 5% с вероятностью не меньшей 0.95.

ЗАДАЧА (ИЗОГНУТАЯ ИГЛА БЮФФОНА). Любопытный студент швейного техникума решил повторить опыты Бюффона по бросанию иглы (студент хочет оценить число π). Для этого он подготовил горизонтально расположенный лист бумаги, разлинованный параллельными прямыми так, что расстояние между соседними прямыми равно 1. Однако в распоряжении студента оказалось только погнутая иголка. Иголка имеет форму кочерги, но студент не имеет точного представления о том, как именно погнута иголка. Ему известно лишь то, что длина погнутой иголки равна 2. Студент «случайно» и независимо бросил погнутую иголку 1 000 000 раз и посчитал суммарное число пересечений, учитывая кратность. Помогите студенту оценить число π : а) с помощью неравенства Чебышёва; б*) с помощью з.б.ч. (закона больших чисел) и неравенств о вероятностях больших уклонений; в) с помощью ц.п.т. (центральной предельной теоремы) и оценок скорости сходимости в ц.п.т., например, с помощью неравенства Берри – Эссена или более точных аппроксимаций.

ЗАДАЧА (МЕТОД МОНТЕ-КАРЛО). Предложите эффективный способ вычисления с заданной точностью ε и с заданной доверительной вероятностью γ интеграла:

$$J = \int_{[0, 1]^m} f(\vec{x}) d\vec{x}.$$

Считайте, что $|f(\vec{x})| \leq 1$ для всех $\vec{x} \in [0, 1]^m$.

ПОЯСНЕНИЕ. Введём случайный m -вектор $\vec{X} \in R([0, 1]^m)$ и с.в.

$$\xi = f(\vec{X}).$$

Тогда $M\xi = \int_{[0, 1]^m} f(\vec{x}) d\vec{x} = J$. Поэтому получаем оценку интеграла

$\bar{J}_n = \frac{1}{n} \sum_{k=1}^n f(\vec{x}^k)$, где $\vec{x}^k, k = 1, \dots, n$ – повторная выборка значений случайного вектора \vec{X} (т. е. все $\vec{x}^k, k = 1, \dots, n$ – независимы и одинаково распределены, так же как и вектор \vec{X}). В задаче требуется оценить сверху число n ($n \gg m$), начиная с которого $P(|J - \bar{J}_n| \leq \varepsilon) \geq \gamma$.

ЗАДАЧА (ТЕОРЕМА ШЕННОНА – МАКМИЛЛАН ИЛИ ОСНОВНАЯ ТЕОРЕМА ТЕОРИИ КОДИРОВАНИЯ). Пусть буква X — дискретная с.в., принимающая значения из алфавита (x_1, \dots, x_m) с вероятностями (p_1, \dots, p_m) . Имеется случайный текст из $n \gg 1$ букв X (предполагается, что буквы в тексте не зависимы друг от друга). Общее количество таких текстов $2^{n \log m}$. Поэтому можно закодировать все эти слова, используя $n \log m$ бит. Однако, используя то обстоятельство, что (p_1, \dots, p_m) — в общем случае неравномерное распределение, предложите лучший способ кодирования, основанный на усиленном законе больших чисел.

УКАЗАНИЕ. Пусть $\Omega = \{\omega : \omega = (X_1, X_2, \dots, X_n), X_i \in 1, 2, \dots, m\}$ — пространство элементарных исходов. Вероятность появления слова $\omega = (X_1, X_2, \dots, X_n)$ равна $p(\omega) = p_{X_1} \cdot \dots \cdot p_{X_n}$. Покажите, что по закону больших чисел (простое следствие неравенства Чебышёва):

$$-\frac{1}{n} \log p(\omega) = -\frac{1}{n} \sum_{i=1}^n \log p_{X_i} \xrightarrow[n \rightarrow \infty]{P} -\sum_{i=1}^m p_i \log p_i \stackrel{\text{def}}{=} H(\vec{p}).$$

Текст ω будем называть δ -типичным, если

$$2^{-n(H(\vec{p})+\delta)} < p(\omega) < 2^{-n(H(\vec{p})-\delta)}.$$

Покажите, что

1. Существует не более $2^{n(H(\vec{p})+\delta)}$ типичных текстов.
2. Для $n > n(\varepsilon, \delta)$ существует по крайней мере $(1 - \varepsilon) 2^{n(H(\vec{p})-\delta)}$ типичных текстов.
3. Множество нетипичных текстов имеет вероятность $\leq \varepsilon$.

Таким образом, можно осуществить эффективное кодирование данных, используя все двоичные последовательности длины $n(H(\vec{p}) + \delta)$, чтобы закодировать все δ -типичные тексты и отбросить нетипичные. Вероятность ошибки при таком кодировании будет не больше ε . Обратное, любой код, использующий двоичные последовательности длины $n(H(\vec{p}) - \delta)$, имеет асимптотически не исчезающую вероятность ошибки, стремящуюся к единице при $n \rightarrow \infty$.

Функцию $H(\vec{p})$, которую можно проинтерпретировать как меру количества информации (в битах на передаваемый символ) в случайном тексте, называют *энтропией*. Величина $nH(\vec{p})$ характеризует меру неопределённости случайного текста. Ясно, что для $(p_1, \dots, p_m) = (1/m, \dots, 1/m)$ энтропия максимальна, $H(\vec{p}) = \log m$, и эффективное кодирование невозможно.

ЛИНЕЙНОСТЬ МАТЕМАТИЧЕСКОГО ОЖИДАНИЯ

Задача (о лифте). На первом этаже семнадцатизэтажного общежития в лифт вошли десять человек. Предполагая, что каждый из вошедших (независимо от остальных) может с равной вероятностью жить на любом из шестнадцати этажей (со 2-го по 17-й), найдите математическое ожидание числа остановок лифта.

УКАЗАНИЕ. Попробовать ввести случайные величины, принимающие значения 1 и 0 (то есть индикатор некоторого события), так чтобы вопрос задачи сводился к нахождению математического ожидания суммы эти случайных величин.

Задача (о посадке космического корабля). Поверхность некоторой шарообразной планеты состоит из океана и суши (множество мелких островков). Суша (измеримое по Лебегу множество) занимает больше половины площади планеты. На планету хочет совершить посадку космический корабль, сконструированный так, что концы всех шести его ножек лежат на поверхности планеты. Посадка окажется успешной, если не меньше четырёх ножек из шести окажутся на суше. Возможна ли успешная посадка корабля на планету?

УКАЗАНИЕ. Обратим внимание на то, что ответ не зависит от того, какое именно множество представляет собой суша, и как располагаются шесть ножек корабля, на которые он совершает посадку. Эта задача, на первый взгляд, не имеет ничего общего с теорией вероятностей. Однако метод её решения базируется на введении вероятностных объектов и использовании двух простых фактов: 1) линейности математического ожидания (независимость слагаемых не нужна), 2) если математическое ожидание с.в. больше какого-то числа, то существует исход (точнее говоря, исходы, вероятностная мера которых больше нуля) такой, что с.в. принимает на этом исходе значение больше упомянутого числа).

Задача (парадокс бросания симметричной монетки). Симметричную монету независимо бросили n раз. Результат бросания записали в виде последовательности нулей и единиц. Покажите, что с вероятностью, стремящейся к единице при $n \rightarrow \infty$, длина максимальной подпоследовательности из подряд идущих единиц лежит в промежутке

$$(\log \sqrt{n}, \log n^2).$$

ПАРАДОКСЫ

Задача (о теннисных матчах). Юноша собирается сыграть три теннисных матча со своими родителями, и он должен победить два раза подряд. Порядок матчей может быть следующим отец-мать-отец,

мать-отец-мать. Юноше нужно решить, какой порядок для него предпочтительней, учитывая, что отец играет лучше матери.

ЗАДАЧА (ПАРАДОКС ТРАНЗИТИВНОСТИ). Будем говорить, что случайная величина X больше по вероятности случайной величины Y , если $P(X > Y) > P(X \leq Y)$. Пусть известно, что для случайных величин X, Y, Z, W выполнена следующая цепочка равенств:

$$P(X > Y) = P(Y > Z) = P(Z > W) = \alpha > 1/2.$$

Верно ли, что X больше по вероятности W и почему?

ЗАДАЧА (ПАРАДОКС С. БАНАХА). В двух спичечных коробках имеется по n спичек. На каждом шаге наугад выбирается коробок, и из него удаляется (используется) одна спичка. Найти вероятность того, что в момент, когда один из коробков опустеет, в другом останется k спичек.

ЗАДАЧА (ИГРА У. ПЕННИ, 1969). Алиса и Билл играют в игру: они бросают монету до тех пор, пока не встретится РРО или РОО (Р — решка, О — орёл). Если первой появится последовательность РРО, выигрывает Алиса, если РОО — Билл. Покажите, что игра не будет честной. Алиса будет выигрывать примерно вдвое чаще Билла!

ЗАДАЧА «СТО ЗАКЛЮЧЁННЫХ». В коридоре находятся 100 человек, у каждого свой номер (от 1 до 100). Их по одному заводят в комнату, в которой находится комод со 100 выдвижными ящиками. В ящики случайным образом разложены карточки с номерами (от 1 до 100). Каждому разрешается заглянуть в не более чем 50 ящиков. Цель каждого — определить, в каком ящике находится его номер. Общаться и передавать друг другу информацию запрещается. Предложите стратегию, которая с вероятностью не меньшей 0.3 (в предположении, что все 100! способов распределения карточек по ящикам равновероятны) приведёт к выигрышу всей команды. Команда выигрывает, если все 100 участников верно определили ящик с карточкой своего номера.

СТРАТЕГИЯ. Каждый человек первым открывает ящик под его номером, вторым — под номером, который указан на карточке, лежащей в ящике, открытом перед этим и т. д. Среднее число циклов длины r в случайной перестановке есть $1/r$ (покажите, используя, например, задачу «про предельные меры»). Тогда среднее число циклов длины большей $n/2$ есть $\sum_{k=n/2}^n 1/k$. Это и есть вероятность существования цикла длины большей $n/2$. Поэтому вероятность успеха команды есть $1 - \sum_{k=51}^{100} 1/k \approx 0.31$.

Если же просто произвольно открывать ящики, то вероятность успеха будет $2^{-100} \approx 8 \cdot 10^{-31}$. В случае, когда карточки разложены не случайным

образом, то следует сделать случайной нумерацию ящиков, и далее следовать старой стратегии.

С деталями можно познакомиться, например, здесь [45, р. 176].

ЗАДАЧА (О ШЛЯПАХ; Тод ЭБЕРТ, 1998). А) Трёх игроков отводят в комнату, где на них надевают (случайно и независимо) белые и чёрные шляпы. Каждый видит цвет других шляп и должен написать на бумажке одно из трёх слов: «белый», «чёрный», «пас» (не советуясь с другими и не показывая им свою бумажку). Команда выигрывает, если хотя бы один из игроков назвал правильный цвет своей шляпы и ни один не назвал неправильного. Как им сговориться, чтобы увеличить шансы. Б*) Решите эту же задачу, если игроков $n = 2^m - 1$ ($m \in \mathbb{N}$).

ЗАМЕЧАНИЕ. Как ни странно, вероятность выигрыша можно сделать достаточно большой. Скажем, для семи игроков есть стратегия, успешная в семи из восьми случаев (и связано это с так называемым кодом Хэмминга).

ЗАДАЧА (ПАРАДОКС ВРЕМЕНИ ОЖИДАНИЯ). Автобусы прибывают на остановку в соответствии с пуассоновским процессом с параметром $\lambda > 0$. Вы приходите на остановку в фиксированный момент времени (скажем, в полдень). Каково математическое ожидание времени, в течение которого вы ждёте автобуса?

* * * * *

Большое число вероятностных парадоксов собрано в книге [29].

УСЛОВНЫЕ ВЕРОЯТНОСТИ

ЗАДАЧА (О САМОЛЁТЕ). В самолёте n мест. Есть n пассажиров, выстроившихся друг за другом в очередь. Во главе очереди — «заяц». У всех кроме «зайца» есть билет, на котором указан номер посадочного места. Так как «заяц» входит первым, он случайным образом занимает некоторое место. Каждый следующий пассажир, входящий в салон самолёта, действует по такому принципу: если его место свободно, то садится на него, если занято, то занимает с равной вероятностью любое свободное. Найдите вероятность того, что последний пассажир сядет на своё место.

УКАЗАНИЕ. Попробовать решить задачу для $n = 2, 3, 4, \dots$ и понять, что происходит для любого n .

ЗАДАЧА (О НЕСИММЕТРИЧНОЙ МОНЕТКЕ). 1) Имеется несимметричная монетка. Несимметричность монетки заключается в том, что либо орёл выпадает в два раза чаще решки; либо наоборот (априорно (до проведения опытов) оба варианта считаются равновероятными). Монетку бросили 10 раз. Орёл выпал 7 раз. Определите апостериорную вероятность

того, что орёл выпадает в два раза чаще решки (апостериорная вероятность считается с учётом проведённых опытов (иначе говоря, это просто условная вероятность)).

2) Определите апостериорную вероятность того, что орёл выпадает не менее, чем в два раза чаще решки. Если несимметричность монетки заключается в том, что либо орёл выпадает не менее, чем в два раза чаще решки; либо наоборот (априорно оба варианта считаются равновероятными).

УКАЗАНИЕ. Условие 2) задачи можно понимать, например, следующим образом. Рассмотрим два события

$$A = \{p \in R [0, 1/3]\} \quad \text{и} \quad \bar{A} = \{p \in R [2/3, 1]\},$$

где p — вероятность выпадения орла, запись $p \in R [0, 1/3]$ означает, что с.в. p имеет равномерное распределение на отрезке $[0, 1/3]$. По условию $P(A) = P(\bar{A}) = 1/2$. Нужно найти $P(\bar{A} \mid r_{10} = 7)$, где $r_{10} \in Bi(p, 10)$. Заметим, что

$$\begin{aligned} P(r_{10} = 7 \mid \bar{A}) &= \int_{2/3}^1 P(r_{10} = 7 \mid p) P(dp \mid \bar{A}) = 3 \int_{2/3}^1 P(r_{10} = 7 \mid p) dp = \\ &= 3C_{10}^7 \int_{2/3}^1 p^7(1-p)^3 dp \approx 0.144. \end{aligned}$$

ВЕРОЯТНОСТНЫЙ МЕТОД

ЗАДАЧА (О ТУРНИРЕ). На турнир приехало n игроков. Каждая пара игроков, согласно регламенту турнира, должна провести одну встречу (ничьих быть не может). Пусть

$$C_n^k \cdot (1 - 2^{-k})^{n-k} < 1.$$

Докажите, что тогда игроки могли сыграть так, что для каждого множества из k игроков найдётся игрок, который побеждает их всех.

УКАЗАНИЕ. Введите на множестве всех турниров равномерную меру, т. е. считайте, что все $2^{C_n^2}$ турниров равновероятны. Введите событие A_K , состоящее в том, что не существует игрока, побеждающего всех игроков из множества K . Докажите, что $P\left(\bigcup_{K \subset \{1, \dots, n\}, |K|=k} A_K\right) \leq C_n^k \cdot (1 - 2^{-k})^{n-k}$.

Следовательно, $P\left(\overline{\bigcup_{K \subset \{1, \dots, n\}, |K|=k} A_K}\right) > 0$.

ЗАДАЧА (О ЧИСЛАХ РАМСЕЯ). Покажите, что можно так раскрасить в два цвета ребра полного графа с n вершинами (т. е. графа без петель, в котором любые две различные вершины соединены одним ребром), что любой его полный подграф с m вершинами, где $2C_n^m \left(\frac{1}{2}\right)^{C_m^2} < 1$, имеет рёбра разного цвета.

ЗАДАЧА (ТЕОРЕМА ЭРДЁША – КО – РАДО). Семейство множеств Φ называется пересекающимся, если для любых двух множеств $A, B \in \Phi$ выполняется условие $A \cap B \neq \emptyset$. Пусть $n \geq 2k$ и семейство Φ является пересекающимся семейством k -элементных подмножеств множества $\{0, 1, 2, \dots, n-1\}$. Покажите, что число множеств в семействе Φ удовлетворяет неравенству

$$|\Phi| \leq C_{n-1}^{k-1} = \frac{(n-1)!}{(k-1)!(n-k)!}.$$

ЗАДАЧА (О ЛАМПОЧКАХ). Рассмотрим матрицу $n \times n$, составленную из лампочек, каждая из которых либо включена ($a_{ij} = 1$), либо выключена ($a_{ij} = -1$). Предположим, что для каждой строки и каждого столбца имеется переключатель, поворот которого ($x_i = -1$ для строки i и $y_j = -1$ для столбца j) переключает все лампочки в соответствующей линии: с «вкл.» на «выкл.» и с «выкл.» на «вкл.». Тогда для любой начальной конфигурации лампочек можно установить такое положение переключателей, что разность между числом включённых и выключенных лампочек будет не меньше $(\sqrt{2/\pi} + o(1))n^{3/2}$.

УКАЗАНИЕ. Пусть y_1, \dots, y_n – независимые одинаково распределённые с.в. с законом распределения

$$y_j = \begin{cases} 1, & p = 1/2, \\ -1, & p = 1/2. \end{cases}$$

Введите с.в. $R_i = \sum_{j=1}^n a_{ij}y_j$, $i = 1, \dots, n$ и $R = \sum_{j=1}^n |R_j|$. Покажите, что с.в. R_i , $i = 1, \dots, n$ распределены также, как с.в. $S_n = \sum_{j=1}^n y_j$. Покажите

далее, что $E(|R_i|) = E(|S_n|) = (\sqrt{2\pi} + o(1))\sqrt{n}$ (можно получить точную формулу для $E(|S_n|)$ из комбинаторных соображений, а затем воспользоваться формулой Стирлинга, однако, более простым вариантом является применение ц.п.т. к $S_n = \sum_{j=1}^n y_j$). Далее следует выбирать с.в. x_1, \dots, x_n так, что $x_i R_i \stackrel{\text{н.н.}}{=} |R_i|$, $i = 1, \dots, n$.

Для дополнительного знакомства с вероятностным методом можно рекомендовать книги [1, 28, 35].

МАРКОВСКИЕ ПРОЦЕССЫ

ЗАДАЧА (ИГРА В ОРЛЯНКУ). Пусть имеются два натуральных числа A и B . Есть два игрока, у которых начальные капиталы равны соответственно A и B рублей. Они играют в орлянку: если выпал орёл (с вероятностью p) второй игрок платит первому рубль, если решка — наоборот. Найдите вероятности разорения игроков. Найдите среднюю продолжительность игры.

ЗАДАЧА (ОБ ОЧЕРЕДИ ЗА БУЛОЧКАМИ). В буфете за булочками выстроилась очередь из $2n$ человек. Каждый человек в очереди хочет купить ровно одну булочку. Одна булочка стоит 10 рублей 50 копеек. У половины людей в очереди имеется монетки достоинством 50 копеек, а у половины не имеется. У продавца изначально нет копеечной сдачи. Какова вероятность, что продавец всегда сможет дать сдачу? Считайте, что все способы расстановки людей в очереди равновероятны.

ЗАДАЧА О РАЗБОРЧИВОЙ НЕВЕСТЕ (ГАРДНЕР – ДЫНКИН, 1965). В аудитории находится невеста, которая хочет выбрать себе жениха. За дверью выстроилась очередь из $N \gg 1$ женихов. Относительно любых двух женихов невеста может сделать вывод, какой из них для неё предпочтительнее. Таким образом, невеста задаёт на множестве женихов отношение порядка (естественно считать, что если A предпочтительнее B , а B предпочтительнее C , то A предпочтительнее C). Предположим, что все $N!$ вариантов очередей равновероятны и невеста об этом знает (равно, как и число N). Женихи запускаются в аудиторию по очереди. Невеста видит каждого из них в первый раз! Если на каком-то женихе невеста остановится (сделает свой выбор), то оставшаяся очередь расходиться. Невеста хочет выбрать наилучшего жениха (исследуя k -го по очереди жениха, невеста лишь может сравнить его со всеми предыдущими, которых она уже просмотрела и пропустила).

Оцените (при $N \rightarrow \infty$) вероятность того, что невесте удастся выбрать наилучшего жениха, если она придерживается следующей стратегии: посмотреть (пропустить) первых по очереди $\lfloor N/e \rfloor$ кандидатов и затем выбрать первого кандидата, который лучше всех предыдущих (впрочем, такого кандидата может и не оказаться, тогда, очевидно, невеста не смогла выбрать наилучшего жениха).

Эта задача уже неоднократно предлагалась школьникам, см., например, брошюру [13].

Отметим, также брошюру [31], вышедшую в этой же серии и посвящённую тому, как «с помощью случайных блужданий» можно численно решать задачу Дирихле для уравнения Лапласа (и других полуэллиптических уравнений).

ЗАДАЧА (МОДЕЛЬ ЭРЕНФЕСТОВ)*. Рядом стоят две собаки с номерами 1 и 2. На собаках как-то расположились $M = 2n \gg 1$ блох. Скажем, в начальный момент все блохи собрались на собаке с номером 1. На каждом шаге случайно и независимо от предыстории определяется блоха (с вероятностью $1/M$ будет выбрана любая из блох), которая перепрыгивает на другую собаку. Микросостояние системы есть способ распределения M различных блох по двум различным собакам. Макросостояние системы есть способ распределения M одинаковых блох между двумя различными собаками. Микросостояний будет 2^M , а макросостояний $M + 1$. Очевидно, макросостояние можно задавать числом блох на первой собаке.

Покажите, что существует такое $T = O(M)$, что для любого $m \geq T$

$$P \left(\frac{|n_1(m) - n_2(m)|}{M} \leq \frac{3}{\sqrt{M}} \right) \geq 0.99,$$

где $n_1(m)$ — число блох на первой собаке на шаге m , а $n_2(m)$ — на второй (случайные величины). Т. е. относительная разность числа блох на собаках будет иметь порядок малости $O(1/\sqrt{M})$ на больших временах ($T \geq 2M$).

ЗАМЕЧАНИЕ. Обозначим через

$$\begin{aligned} \tau(k) &= \inf \{m \in \mathbb{Z}, m \geq 0 : n_1(m) = k\}, \\ \sigma(k) &= \inf \{m \in \mathbb{Z}, m > 0 : n_1(m) = k, n_1(0) = k\} \end{aligned}$$

времена соответственно первого попадания и первого возвращения в состояние k . Тогда

а) $E\sigma(k) = 2^M \frac{k!(M-k)!}{M!}$, и, в частности, среднее время возвращения в нулевое состояние $E\sigma(0) = 2^M$, где $E\sigma(k)$ — математическое ожидание времени первого возвращения в состояние k , если $n_1(0) = k$, $k = 0, \dots, n$;

б) $E_n\tau(0) = \frac{1}{M} 2^M (1 + o(M))$, где $E_n\tau(0)$ — математическое ожидание времени первого попадания в состояние 0, если $n_1(0) = n$;

в) $E_0\tau(n) = n \ln n + n + O(1)$, где $E_0\tau(n)$ — математическое ожидание времени первого попадания в состояние n , если $n_1(0) = 0$.

На примере этой модели можно говорить о том, что в макросистемах возврат к неравновесным макросостояниям вполне допустим, но происходить это может только через очень большое время (*циклы Пуанкаре*), так что нам может не хватить отведённого времени, чтобы это заметить (*парадокс Цермело*). Напомним, что описанный выше случайный процесс обратим во времени. Однако наблюдается необратимая динамика относительной разности числа блох на собаках (*парадокс Лошмидта*). Но в таком случае можно удивляться также и тому, что газ, собранный в начальный момент в одной половине сосуда, с течением времени равномерно распределится по сосуду [16].

ЗАДАЧА (ВИЛЬФРЕДО ПАРЕТО, «КИНЕТИКА СОЦИАЛЬНОГО НЕРАВЕНСТВА»)*. В городе живёт $M = 2n \gg 1$ (например, 10 000) пронумерованных жителей. У каждого i -го жителя есть в начальный (нулевой) момент времени целое (неотрицательное) количество рублей $s_i(0)$ (монетами, достоинством в один рубль). Со временем пронумерованные жители (количество которых не изменяется, также как и суммарное количество рублей) случайно разыгрывают своё имущество. В каждый момент времени $t = 1, 2, 3, \dots$ случайно и независимо от предыстории формируются n пар (все $M!/2^n$ возможных наборов пар равновероятны). В каждой паре с вероятностью $1/2$ житель с большим номером отдаёт 1 рубль (если, конечно, он не банкрот) жителю с меньшим номером, и с вероятностью $1/2$ наоборот. Пусть $c_s(t)$ — доля жителей города, имеющих ровно s рублей в момент времени t (заметим, что $c_s(t)$ — случайная величина). Пусть $S = \sum_{i=1}^M s_i(0)$, $\bar{s} = S/M$. Покажите, что для любого $0 \leq q \leq S$ найдутся такие $\lambda_q, T_q = O(M)$, что для любого $t \geq T_q$

$$P \left(\left| \frac{c_s(t)}{C e^{-s/\bar{s}}} - 1 \right| \leq \frac{\lambda_q}{\sqrt{M}}, s = 0, \dots, q \right) \geq 0.99,$$

где C определяется из условия нормировки: $\sum_{s=0}^S C e^{-s/\bar{s}} = 1$, т. е. $C \approx \bar{s}^{-1}$.

ЗАМЕЧАНИЕ. Скорость сходимости оценивается сверху, исходя из оценок в доказательстве эргодической теоремы для однородных марковских цепей с конечным числом состояний. Как показывают численные эксперименты, оценка $O(M)$ точная. Так, если в городе 10 000 жителей и единица времени — день, то при начальном «социальном равенстве» с вероятностью, близкой к единице, через 20–30 лет установится «социальное неравенство». Оказывается (см. также модель Эренфестов), что оценка скорости сходимости $O(\text{poly}(M))$ характерна для большинства макросистем. Отмеченное выше обстоятельство хорошо известно специалистам по имитационному моделированию, как Markov chain Monte Carlo revolution.

Эта задача в упрощённом виде предлагалась школьникам в [6].

ЗАДАЧА (MARKOV CHAIN MONTE CARLO REVOLUTION и СОСТОЯТЕЛЬНОСТЬ ОЦЕНОК МАКСИМАЛЬНОГО ПРАВДОПОДОБИЯ [42])* . В руки опытных криптографов попало закодированное письмо (10 000 символов). Чтобы это письмо прочитать нужно его декодировать. Для этого берётся стохастическая матрица переходных вероятностей $P = \|p_{ij}\|$ (линейный размер которой определяется числом возможных символов — букв, знаков препинания и т. п. в языке, на котором до шифрования было написано письмо — этот язык известен и далее будет называться базовым), в которой p_{ij} отвечает за вероятность появления символа с номером

j сразу после символа под номером i . Такая матрица может быть идентифицирована с помощью статистического анализа какого-нибудь большого текста, скажем, «Войны и мира» Л. Н. Толстого.

Пусть способ (де)шифрования (подстановочный шифр) определяется некоторой неизвестной дешифрующей функцией \bar{f} — преобразование (перестановка) множества кодовых букв во множество символов базового языка.

В качестве «начального приближения» выбирается какая-то функция f , например, полученная исходя из легко осуществимого частотного анализа. Далее рассчитывается вероятность выпадения полученного закодированного текста \vec{x} , сгенерированного при заданной функции f (функция правдоподобия):

$$L(\vec{x}; f) = \prod_k p_{f(x_k), f(x_{k+1})}. \quad (*)$$

Случайно выбираются два аргумента у функции f и значения функции при этих аргументах меняются местами. Если в результате получилась такая f^* , что $L(\vec{x}; f^*) \geq L(\vec{x}; f)$, то $f := f^*$, иначе независимо бросается монетка с вероятностью выпадения орла $p = L(\vec{x}; f^*)/L(\vec{x}; f)$, и если выпадает орёл, то $f := f^*$, иначе $f := f$. Далее процедура повторяется (в качестве f выбирается функция, полученная на предыдущем шаге).

Объясните, почему предложенный алгоритм после некоторого числа итераций с большой вероятностью и с хорошей точностью восстанавливает дешифрующую функцию \bar{f} ? Почему сходимость оказывается такой быстрой (0.01 сек. на современном PC)?

ЗАМЕЧАНИЕ. Приведенный алгоритм является частным случаем более общего алгоритма Метрополиса: для того чтобы сгенерировать требуемое дискретное распределение вероятностей (нормировка распределения на единицу несущественна), строится неразложимая марковская цепь с сильно разреженной матрицей переходных вероятностей, (единственным) стационарным распределением которой будет требуемое распределение. По эргодической теореме для марковских цепей, это означает, что после некоторого числа шагов построенной марковской цепи «получится» (независимо от начального распределения) распределение вероятностей близкое к стационарному, т.е. требуемому. Поскольку матрица переходных вероятностей сильно разрежена, то эволюция, согласно описанной марковской динамике, вычислительно малозатратна. Осталось заметить (см., например, предыдущие две задачи), что при довольно естественных предположениях марковская цепь может крайне быстро «выходить» на своё стационарное распределение [48]. Собственно, одним из революционных направлений последних десятилетий при построении эффективных алгоритмов стало использование только что отмеченного

факта (возможности потенциально быстрой сходимости в эргодической теореме для марковских процессов). В качестве другого нетривиального и интересного примера укажем вероятностные алгоритмы (работающие быстрее известных детерминированных) поиска центра тяжести выпуклого множества и его объёма [41] (одна из работ в этом направлении была удостоена премии Фалкерсона — аналога Нобелевской премии в области Computer Science).

Обратим также внимание, что школьники могли познакомиться с этой темой на примере задачи тасования карт (сколько раз надо «перемешивать» колоду, чтобы все возможные перестановки были практически равновероятны) из выступления Андрея Окунькова в ЛШСМ-2010 [25].

Для лучшего понимания происходящего в условиях задачи, отметим, что одним из самых универсальных способов получения асимптотически наилучших оценок неизвестных параметров по выборке является метод наибольшего правдоподобия. Напомним вкратце в чем он заключается. Пусть имеется выборка из распределения, зависящего от неизвестного параметра — в нашем случае выборкой \vec{x} из 10 000 элементов будет письмо, а неизвестным «параметром» будет функция f (хотя наш параметр может принимать много значений, но все-таки конечное число). Далее считается вероятность (или плотность вероятности в случае непрерывных распределений) $L(\vec{x}; f)$ того что выпадет данный \vec{x} при условии, что значения параметра f . Если посмотреть на распределение $L(\vec{x}; f)$, как на распределение в пространстве параметров (\vec{x} — зафиксирован), то при большом объёме выборки (размерности \vec{x}) при естественных условиях это распределение концентрируется в малой окрестности наиболее вероятного значения

$$f(\vec{x}) = \underset{f}{\text{Argmax}} L(\vec{x}; f),$$

которое «асимптотически» совпадает с искомым значением \bar{f} .

ЗАДАЧА (ВЕТВЯЩИЙСЯ ПРОЦЕСС). В колонию зайцев внесли зайца с необычным геном. Обозначим через p_k вероятность того, что в потомстве этого зайца ровно k зайчат унаследуют этот ген ($k = 0, 1, 2, \dots$). Это же распределение вероятностей характеризует всех последующих потомков, унаследовавших необычный ген. Будем считать, что каждый заяц даёт потомство один раз в жизни в возрасте одного года (как раз в этом возрасте находился самый первый заяц с необычным геном в момент попадания в колонию).

Обозначим через $G(z)$ — производящую функцию распределения

$$p_k, k = 0, 1, 2, \dots, \text{ т. е. } G(z) = \sum_{k=0}^{\infty} p_k z^k.$$

Пусть X_n — количество зайцев в возрасте одного года с необычным геном спустя n лет после попадания в колонию первого такого зайца. Производящую функцию с.в. X_n обозначим $\Pi_n(z) = M(z^{X_n})$.

1. Получите уравнение, связывающее $\Pi_{n+1}(z)$ с $\Pi_n(z)$ посредством $G(z)$.

УКАЗАНИЕ. Покажите, что $M(z^{X_{n+1}} | X_n) = [G(z)]^{X_n}$. Затем возьмите математическое ожидание от обеих частей равенства.

2. Покажите, что вероятность вырождения гена $q_n = P(X_k = 0; k \geq n)$ равна $\Pi_n(0)$. Существует ли предел $q = \lim_{n \rightarrow \infty} q_n$? Если существует, то найдите его.

УКАЗАНИЕ. Легко видеть, что функция $G(z)$ выпуклая. Уравнение $z = G(z)$ имеет два корня: один в любом случае равен 1, другой $q \leq 1$. Если $\nu = G'(1) > 1$, то $q < 1$. Если $\nu \leq 1$, то $q = 1$.

Подробнее с ветвящимися процессами можно познакомиться, например, по лекционным курсам [4, 8].

Задача (ЗАМКНУТАЯ СЕТЬ, ТЕОРЕМА ГОРДОНА – НЬЮЭЛЛА)*. Рассматривается (следуя [5]) транспортная сеть, в которой между N станциями курсируют M такси. Клиенты прибывают в i -й узел в соответствии с пуассоновским потоком с параметром $\lambda_i > 0$ ($i = 1, \dots, N$). Если в момент прибытия в i -й узел там есть такси, клиент забирает его и с вероятностью $p_{ij} \geq 0$ направляется в j -й узел, по прибытии в который покидает сеть. Такси остаётся ждать в узле прибытия нового клиента. Времена перемещений из узла в узел — независимые случайные величины, имеющие показательное распределение с параметром $\nu_{ij} > 0$ для пары узлов (i, j) . Если в момент прихода клиента в узел там нет такси, клиент сразу покидает узел. Считая $p_{ij} = N^{-1}$, $\lambda_i = \lambda$, $\nu_{ij} = \nu$, покажите, что вероятность того, что клиент, поступивший в узел (в установившемся (стационарном) режиме работы сети), получит отказ, равна

$$P_{\text{отказа}}(N, M) = \sum_{k=0}^M \frac{C_{N-2+k}^k \rho^{M-k}}{(M-k)!} \bigg/ \sum_{k=0}^M \frac{C_{N-1+k}^k \rho^{M-k}}{(M-k)!}, \quad \rho = N\lambda/\nu.$$

Методом перевала покажите справедливость следующей асимптотики при $N \rightarrow \infty$:

$$P_{\text{отказа}}(N, rN) = 1 - \frac{2r}{\lambda/\nu + r + 1 + \sqrt{(\lambda/\nu + r + 1)^2 - 4\lambda r/\nu}} + O\left(\frac{1}{N}\right).$$

Метод перевала — очень полезный инструмент исследования асимптотик интегралов по параметру. Подробное изложение метода перевала имеется, например, в [32].

* * * * *

Недавно вышел современный учебник по марковским случайным процессам, который мы рекомендуем заинтересовавшимся в этой теме читателям [18].

ВЕРОЯТНОСТНЫЕ АЛГОРИТМЫ И ВЕРОЯТНОСТНЫЙ АНАЛИЗ АЛГОРИТМОВ

ЗАДАЧА (О СЛОЖНОСТИ В СРЕДНЕМ ВЫСТРОЙ СОРТИРОВКИ МАССИВА). Дан случайным образом приготовленный массив длины n (все $n!$ возможных порядков равновероятны). Покажите, что сложность в среднем алгоритма сортировки этого массива Quicksort есть $O(n \ln n)$. Верно ли, что сложность в худшем случае при этом есть $O(n^2)$?

ЗАДАЧА (ОБ УПАКОВКЕ). Рассмотрим (следуя [21]) NP-полную задачу

$$\sum_{j=1}^n x_j \rightarrow \max;$$

$$x_j \in \{0, 1\}, j = 1, \dots, n; \quad \sum_{j=1}^n a_{ij} x_j \leq 1, i = 1, \dots, m \quad (*)$$

$$(a_{ij} \in \{0, 1\}, i = 1, \dots, m, j = 1, \dots, n).$$

Булев вектор \vec{x} длины n будем называть допустимым, если он удовлетворяет системе (*). Обозначим через $T(j)$ множество всех допустимых булевых векторов для системы (*) с $n - j$ нулевыми последними компонентами и через \vec{e}_j — вектор длины n с единичной j -й компонентой и с остальными нулевыми компонентами.

Рассмотрим алгоритм: 1) строим множество допустимых решений $T(j)$ на основе множества $T(j - 1)$, пытаясь добавить вектор \vec{e}_j ко всем булевым векторам $T(j - 1)$; 2) среди $|T(n)|$ допустимых булевых векторов ищем «наилучший».

А) Покажите, что сложность описанного алгоритма составляет $O(|T(n)mn|)$. При каких $a_{ij} \in \{0, 1\}$ алгоритм будет работать экспоненциально долго?

Б) Оцените сложность в среднем $E(|T(n)|)mn$, т.е. математическое ожидание времени работы алгоритма, если с.в. $\{a_{ij}\}_{i,j=1}^{m,n}$ — независимые и одинаково распределенные по закону Бернулли $Be(p)$ ($mp^2 \geq \ln n$).

УКАЗАНИЕ К Б). Пусть $k > 0$. Положим: $\vec{x}_{j_1, \dots, j_k}$ — вектор с единицами на позициях $\{j_1, \dots, j_k\}$ и $n - k$ нулями; p_{ki} — вероятность выполнения i -го неравенства системы (*) для $\vec{x}_{j_1, \dots, j_k}$; P_k — вероятность того, что \vec{x}^k — допустимое решение (покажите, что p_{ki} и P_k не зависят от набора $\{j_1, \dots, j_k\}$).

Докажите, что $p_{ki} \leq (1 - p^2)^{k-1} \leq e^{-p^2(k-1)}$, $P_k \leq e^{-mp^2(k-1)}$ и

$$E(|T(n)|) = \sum_{k=0}^n C_n^k P_k < 1 + n + n \sum_{k=2}^n e^{(k-1)(\ln n - mp^2)}.$$

ЗАДАЧА (СРАВНЕНИЕ СТРОК)*. Требуется сравнить две битовые строки a , b , затратив как можно меньше операций. Основная идея — сравнивать не сами строки, а функции от них; скажем, сравнивать $a \bmod p$ и $b \bmod p$, для некоторого простого числа p .

ОПИСАНИЕ АЛГОРИТМА СРАВНЕНИЯ СТРОК:

1. Пусть $|a| = |b| = n$, $N = n^2 \log_2 n^2$.
2. Выбираем случайное простое число p из интервала $[2, \dots, N]$.
3. Выдать «да», если $a \bmod p = b \bmod p$ (т. е. $(a - b) \equiv 0 \pmod{p}$), иначе выдать «нет».

Покажите, что этот алгоритм является вероятностным алгоритмом с односторонней ошибкой и вероятностью ошибки $O(1/n)$. То есть

$$P\{\text{«да»} \mid a = b\} = 1,$$

$$P\{\text{«да»} \mid a \neq b\} = O(1/n).$$

При этом необходимое количество сравнений равно $O(\log_2 n)$.

ЗАДАЧА (ИНТЕРАКТИВНЫЕ ДОКАЗАТЕЛЬСТВА, ИЗОМОРФИЗМ ГРАФОВ). Алисе известен изоморфизм φ графов G_0 и G_1 . Она хочет убедить Боба в том, что графы G_0 и G_1 изоморфны, не сообщив Бобу «никакой информации» об изоморфизме φ .¹⁾ Алиса посылает Бобу граф, который получается некоторой случайной перестановкой вершин ψ из графов G_0, G_1 , т. е. $H = \psi(G_a)$, где $a \in \{0, 1\}$ выбирается равномерно. Боб просит сообщить ему изоморфизм между G_b и H , где $b \in \{0, 1\}$ также выбирается равномерно. При $a = b$ Алиса посылает ψ , иначе — $\psi\varphi^{1-2b}$. Таких партий разыгрывается N штук, случайные величины в разных партиях независимы (ψ в каждой партии генерируется заново). Если φ — действительно изоморфизм $G_0 \sim G_1$, то все проверки Боба будут положительны. Покажите, что если φ не является изоморфизмом G_0 и G_1 , то с вероятностью 2^{-N} хотя бы одна проверка обнаружит это, т. е. Боб получит перестановку, которая не является изоморфизмом H и G_b .

ЗАМЕЧАНИЕ. Этот задача поучительна с точки зрения «криптографического фокуса»: Алиса убедила Боба в $G_0 \sim G_1$ так и не огласив самого изоморфизма φ . Если φ — это пароль, диалог можно вести даже в открытую, что служит примером системы с нулевым разглашением.

¹⁾Мы не приводим точных определений — в задаче они не используются.

Обратим внимание, что школьники могли познакомиться с тематикой нескольких последних задач из выступления А. А. Разборова в ЛШСМ-2011 [27].

ЗАДАЧА (АДАПТИВНЫЕ ПРАВИЛА [46])*. Имеется два «одноруких бандита» (так называют игровые автоматы с ручкой, дёргая за которую получаем случайный выигрыш). Вероятность выиграть на первом автомате $p_1 > 0$, а на втором $p_2 > 0$. Обе вероятности неизвестны. Игрок может в любом порядке $n \gg 1$ раз дёргать за ручки «одноруких бандитов». Стратегией игрока является выбор ручки на каждом шаге, в зависимости от результатов всех предыдущих шагов, так чтобы суммарный выигрыш был бы максимальным. Приведите асимптотически оптимальную стратегию игрока.

Решите предыдущую задачу, если выигрыш есть случайная величина с распределением из экспоненциального семейства, зависящего от неизвестного параметра θ (определение см. в [22]). Хотя значения θ_1 и θ_2 (для 1-го и 2-го игрового автомата) неизвестны, но, не ограничивая общности, считайте, что $\theta_1 \neq \theta_2$. Выигрыш является суммой выигрышей во всех розыгрышах.

ЗАДАЧА (УСТОЙЧИВЫЕ СИСТЕМЫ БОЛЬШОЙ РАЗМЕРНОСТИ; В.И.ОПОЙЦЕВ, 1985 [26]). Из курсов функционального анализа и вычислительной математики хорошо известно, что если спектральный радиус матрицы $A = \|a_{ij}\|_{i,j=1}^n$ меньше единицы: $\rho(A) < 1$, то итерационный процесс $\vec{x}^{n+1} = A\vec{x}^n + \vec{b}$ независимо от начальной точки \vec{x}^0 , сходится к единственному решению уравнения $\vec{x}^* = A\vec{x}^* + \vec{b}$.

Если $\|A\| = \max_i \sum_j |a_{ij}| < 1$, то и $\rho(A) < 1$. Обратное, конечно же, неверно. Предположим, что существует такое маленькое $\varepsilon > 0$, что

$$\frac{1}{n} \sum_{i,j} |a_{ij}| < 1 - \varepsilon. \quad (S)$$

Очевидно, что отсюда тем более не следует $\rho(A) < 1$. Тем не менее, введя на множестве матриц, удовлетворяющих условию (S), равномерную меру, покажите, что относительная мера тех матриц (удовлетворяющих условию (S)), для которых спектральный радиус не меньше единицы, стремится к нулю с ростом n (ε — фиксировано и от n не зависит).

УКАЗАНИЯ. 1. Покажите, что при доказательстве можно ограничиться матрицами с неотрицательными элементами.

2. Покажите, что, не ограничивая общности, можно также считать, что в определении множества S стоит не неравенство, а равенство. Так определённое множество матриц будем называть SE.

3. Положите, например, $a_{ij} \in \text{Exp}(n/(1 - \varepsilon))$ — независимые одинаково распределённые с.в., и покажите, что при $n \rightarrow \infty$ распределение элементов случайной матрицы $A = \|a_{ij}\|_{i,j=1}^n$ будет сходиться к равномерному распределению на SE.

4. Покажите, введя обозначение $P_n = P(\|A\| \geq 1) \geq P(\rho(A) \geq 1)$ и используя неравенство Чебышёва, что

$$P_n \leq nP\left(\sum_j a_{1j} \geq 1\right) \leq \frac{n}{\varepsilon^4} M \left[\left(\sum_j a_{1j} - (1 - \varepsilon)\right)^4 \right] = O\left(\frac{1}{n}\right) \xrightarrow{n \rightarrow \infty} 0.$$

В качестве дополнительной литературы по вероятностным алгоритмам и вероятностному анализу алгоритмов можно рекомендовать книги [20, 49].

ГЕОМЕТРИЧЕСКИЕ ВЕРОЯТНОСТИ

ЗАДАЧА (СРЕДНЯЯ ПЛОЩАДЬ ПОВЕРХНОСТИ И ИНТЕГРАЛЬНАЯ ГЕОМЕТРИЯ). Покажите, что средняя площадь ортогональной проекции куба с ребром единица на случайную плоскость равна $3/2$.

УКАЗАНИЕ. Обозначим через S_k величину k -мерного объёма ортогональной проекции рассматриваемой области в \mathbb{R}^n на случайную k -мерную плоскость, или, что то же самое, среднее значение (усреднённое по всем k -мерным плоскостям, предполагаемым равновероятными) площади ортогональной k -мерным проекции области. Оказывается, что S_k также равны средним значениям (усреднённым по поверхности рассматриваемой области) симметрических функций от главных кривизн поверхности, и участвуют в (удивительной) формуле для объёма h -окрестности этой области:

$$V(h) = V_0 + V_1 h + V_2 h^2 + \dots + V_n h^n,$$

где V_0 — объём области; V_1 — $(n - 1)$ -мерный объём границы области; число V_k пропорционально S_k и выражается через средние значения от произведений k главных кривизн. В случае $n = 3$, из главных кривизн k_1 и k_2 в каждой точке можно составить *среднюю кривизну* $k_1 + k_2$ и *гауссову кривизну* $K = k_1 k_2$. В этом случае объём h -окрестности получается $V(h) = V_0 + V_1 h + V_2 h^2 + V_3 h^3$, где V_2 пропорционально интегралу от средней кривизны по всей поверхности, а V_3 — от гауссовой:

$$V_3 = \frac{4}{3} \pi \iint K \, dS.$$

Например, для сферы радиуса R

$$V(h) = \frac{4}{3} \pi \cdot (R + h)^3 = \frac{4}{3} \pi R^3 + h \cdot (4\pi R^2) + h^2(4\pi R) + \frac{4}{3} \pi h^3.$$

Здесь

$$k_1 = k_2 = 1/R, \quad k_1 + k_2 = 2/R, \quad k_1 k_2 = 1/R^2, \quad \iint (k_1 + k_2) dS = 8\pi R,$$

$$\iint (k_1 k_2) dS = 4\pi \quad (\text{формула Гаусса – Бонне}).$$

Коэффициент V_3 не зависит от деталей области, а зависит только от *эйлеровой характеристики* поверхности рассматриваемой области. Это обстоятельство привело Г. Вейля к созданию теории характеристических классов и чисел, обобщающих формулу Гаусса – Бонне.

По-видимому, первым эту задачу решил предложить школьникам В. И. Арнольд [2].

ЗАДАЧА (ПРИНЦИП КОНЦЕНТРАЦИИ ПЛОЩАДИ СФЕРЫ; А. ПУАНКАРЕ, 1911). Покажите, что если в многомерном шаре задано равномерное распределение вероятностей и согласно этому распределению вероятностей сгенерированы два случайных вектора, то с вероятностью, близкой к единице, концы этих векторов будут лежать почти на границе шара и эти два случайных вектора будут почти ортогональны.

УКАЗАНИЕ. Нетривиально второе утверждение (про ортогональность). Для того чтобы его установить, покажите, что доля от площади всей сферы S_r^n (радиуса r), которую занимает площадь сегмента, проектирующегося в отрезок $[a, b]$, скажем, оси x_1 , равна

$$P[a, b] = \int_a^b \left(1 - (x/r)^2\right)^{\frac{n-3}{2}} dx \bigg/ \int_{-r}^r \left(1 - (x/r)^2\right)^{\frac{n-3}{2}} dx.$$

Фиксируя $r = 1$ и устремляя n к бесконечности, получите,

$$P[-\delta, \delta] \sim 1 - \sqrt{\pi/2} \exp(-\delta^2 n/2).$$

В статистической физике $\sum_{i=1}^n V_i^2 = \frac{2E_n}{m} \sim n$. Поэтому если известно, что вектор скоростей молекул газа равномерно распределён по поверхности постоянной энергии, то для того чтобы найти (следуя Максвеллу) распределение компонент вектора скорости, скажем V_1 , нужно осуществить термодинамический скейлинг $n \rightarrow \infty$, $r = \sigma n^{1/2} \rightarrow \infty$

$$P[a, b] = \frac{\int_a^b \exp\left(-\frac{x^2}{2\sigma^2}\right) dx}{\int_{-\infty}^{\infty} \exp\left(-\frac{x^2}{2\sigma^2}\right) dx} = \frac{1}{\sqrt{2\pi\sigma^2}} \int_a^b \exp\left(-\frac{x^2}{2\sigma^2}\right) dx.$$

Таким образом, получаем нормальный закон распределения Максвелла в статистической физике.

Задача (ИЗОПЕРИМЕТРИЧЕСКОЕ НЕРАВЕНСТВО И ПРИНЦИП КОНЦЕНТРАЦИИ МЕРЫ; П. ЛЕВИ, 1919)*. Число μ_f называют медианой функции f , если

$$\mu(\vec{x} \in S_1^n : f(\vec{x}) \geq \mu_f) \geq 1/2 \text{ и } \mu(\vec{x} \in S_1^n : f(\vec{x}) \leq \mu_f) \geq 1/2,$$

где $\mu(d\vec{x})$ — равномерная мера на единичной сфере S_1^n в \mathbb{R}^n . Пусть A — измеримое (борелевское) множество на сфере S_1^n . Через A_δ будем обозначать δ -окрестность множества A на сфере S_1^n . Предположим теперь, что в некотором царстве, расположенном на S_1^3 , царь предложил царице Дидоне построить огород с заданной длиной забора. Царица хочет, чтобы её огород при заданном периметре имел наибольшую площадь. Таким образом, царице надо решить изопериметрическую задачу (такие задачи обычно рассматриваются в курсах вариационного исчисления). Решение этой задачи хорошо известно — «круглый огород». Для нас же полезно, рассмотрение двойственной задачи, имеющей такое же решение: при заданной площади огорода спроектировать его так, чтобы он имел наименьшую длину забора, его ограждающего. Используя решение этой задачи, покажите, что если $\mu(A) \geq 1/2$, то

$$\mu(A_\delta) \geq 1 - \sqrt{\pi/2} \exp(-\delta^2 n/2).$$

Пусть теперь на S_1^n задана функция с модулем непрерывности

$$\omega_f(\delta) = \sup \{ |f(\vec{x}) - f(\vec{y})| : \rho(\vec{x}, \vec{y}) \leq \delta, \vec{x}, \vec{y} \in S_1^n \}.$$

Тогда

$$\mu(\vec{x} \in S_1^n : |f(\vec{x}) - \mu_f| \geq \omega_f(\delta)) \leq \sqrt{\pi/2} \exp(-\delta^2 n/2).$$

Можно показать, что при весьма естественных условиях медиана асимптотически близка к среднему значению (математическому ожиданию). Аналогичное неравенство можно получить (М. Талагран, 1994), например, для модели случайных графов (Эрдёша – Реньи) и исследовать плотную концентрацию около среднего значения различные функций на случайных графов: число независимости, хроматическое число и т. п.

Задача (ИЗОПЕРИМЕТРИЧЕСКОЕ НЕРАВЕНСТВО ТАЛАГРАНА И ЕГО ПРИЛОЖЕНИЯ; М. ТАЛАГРАН, 1996 [43])* . а) Пусть заданы множества $\Omega_i, i = 1, \dots, n$, элементарных исходов. На этих множествах заданы вероятностные меры $P_i, i = 1, \dots, n$. Положим

$$\Omega = \prod_{i=1}^n \Omega_i, \quad P = \prod_{i=1}^n P_i.$$

Введём взвешенную метрику Хэмминга:

$$d_\alpha(\vec{x}, \vec{y}) = \sum_{x_i \neq y_i} \alpha_i / \sqrt{\sum_{i=1}^n \alpha_i^2}$$

и определим $d_\alpha(\vec{x}, A) = \min_{\vec{y} \in A} d_\alpha(\vec{x}, \vec{y})$, $\rho(\vec{x}, A) = \sup_{\vec{\alpha} \in \mathbb{R}^n} d_\alpha(\vec{x}, A)$. Пусть $A \subset \Omega$. Определим t -окрестность ($t \geq 0$) множества A по формуле

$$A_t = \{\vec{x} \in \Omega : \rho(\vec{x}, A) \leq t\}.$$

Покажите, что тогда справедливо следующее неравенство:

$$P(A)(1 - P(A_t)) \leq \exp(-t^2/4).$$

б) Пусть в сельском районе, имеющем форму квадрата со стороной 1, находится n домов ($n \gg 1$), размерами которых можно пренебречь по сравнению с линейным размером района. Будем считать, что при строительстве домов застройщик случайно (согласно равномерному распределению $R[0, 1]^2$) и независимо выбирал их местоположения. Почтальону необходимо обойти все n домов ровно по одному разу (от любого дома почтальон может направиться к любому другому по прямой). Обозначим через TSP длину кратчайшего из таких путей (кратчайший гамильтонов путь). Используя п. а), покажите, что найдутся такие постоянные $c > 0$ и $\beta > 0$, не зависящие от n , что

$$P(|TSP - E[TSP]| \geq t) \leq \exp(-t^2/(4c)), \quad \text{где } E[TSP] \sim \beta\sqrt{n}.$$

в) Пусть в условиях п. б) требуется построить систему дорог минимальной суммарной длины *SteinerTree*, по которой можно было бы добраться из любого дома в любой другой (дерево Штейнера с минимальной суммарной длиной рёбер). Получите неравенство о плотной концентрации с.в. *SteinerTree* в окрестности своего математического ожидания, аналогичное неравенству п. б). Как себя асимптотически ведёт $E[SteinerTree]$ при $n \rightarrow \infty$?

ЗАДАЧА (ПЕРКОЛЯЦИЯ, [37])* . В квадратном пруду (со стороной равной 1) выросли (случайным образом) $N \gg 1$ цветков лотоса, имеющих форму круга радиуса $r > 0$. Назовём r_N радиусом перколяции, если с вероятностью не меньшей 0.99 не любящий воду жук сможет переползти по цветкам лотоса с северного берега на южный, не замочившись.

Покажите, что $r_N \sim C/\sqrt{N}$. Оцените C .

Для более глубокого погружения в геометрическую теорию вероятностей можно рекомендовать следующие книги [14, 19, 47].

ПРИМЕНЕНИЕ ВЕРОЯТНОСТНЫХ МЕТОДОВ В ТЕОРИИ ЧИСЕЛ

ЗАДАЧА (ТЕОРЕМА ГАУССА – ГИЛЬДЕНА – ВИМАНА – КУЗЬМИНА [3, 17, 44]). Каждое число из промежутка $\Omega = [0, 1)$ может быть разложено в цепную дробь (вообще говоря, бесконечную). Цепные дроби играют важную роль, например, в различных вычислениях (поскольку позволяют строить в определённом смысле наилучшие приближения иррациональных чисел рациональными), в теории динамических систем (КАМ теории). Для рациональных чисел такие дроби конечны, для квадратичных иррациональностей – периодические (см. пример ниже, в котором период равен 1):

$$\frac{\sqrt{5} - 1}{2} = \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}} = \frac{1}{1 + \frac{1}{1 + \dots}}.$$

Покажите, что, несмотря на приведённый выше пример, для почти всех (в равномерной мере) точек $\omega \in [0, 1)$ и любого натурального m

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n I_m(a_k(\omega)) = \frac{1}{\ln 2} \ln \left(1 + \frac{1}{m(m+2)} \right), \quad I_m(a_k) = \begin{cases} 1, & a_k = m, \\ 0, & a_k \neq m. \end{cases}$$

УКАЗАНИЕ. Покажите, что преобразование $T: [0, 1) \rightarrow [0, 1)$

$$T\omega = \begin{cases} \left\{ \frac{1}{\omega} \right\}, & \omega \in (0, 1), \\ 0, & \omega = 0, \end{cases}$$

где $\{5.8\} = 0.8$ – дробная часть числа, сохраняет меру Гаусса

$$P(A) = \frac{1}{\ln 2} \int_A \frac{dx}{1+x}, \quad \text{где } A \in \Xi \text{ – } \sigma\text{-алгебре борелевских множеств на } \Omega;$$

т. е. покажите, что $P(T^{-1}A) = P(A)$.

Рассмотрите случайный процесс (в дискретном времени) $X_k(\omega) = x_m(T^k\omega)$, где

$$x_m(\omega) = \begin{cases} 1, & \omega^{-1} \in [m, m+1), \\ 0, & \omega^{-1} \in (1, m) \cup [m+1, \infty). \end{cases}$$

Покажите, что случайный процесс X_k – стационарный в узком смысле. В предположении, что этот процесс эргодичен по математическому ожиданию:

$$\frac{1}{n} \sum_{k=1}^n X_k(\omega) \xrightarrow[n \rightarrow \infty]{\text{п.н.}} M X_k(\omega) = \text{const},$$

найдите искомый предел.

Задача (КАМ ТЕОРИЯ [30]). Число α из отрезка $[0, 1]$ назовём нормально приближаемым рациональными числами, если найдутся $c, \varepsilon > 0$ такие, что при любом натуральном q

$$\min_{p \in \mathbb{Z}} \left| \alpha - \frac{p}{q} \right| \geq \frac{c}{q^{2+\varepsilon}}.$$

Используя лемму Бореля – Кантелли докажите, что множество нормально приближаемых чисел на отрезка $[0, 1]$ имеет лебегову меру 1.

УКАЗАНИЕ. Зафиксируем $c, \varepsilon > 0$ и рассмотрим множество

$$A_q = \left\{ \alpha \in [0, 1] : \min_{p \in \mathbb{Z}} \left| \alpha - \frac{p}{q} \right| < \frac{c}{q^{2+\varepsilon}} \right\}.$$

Покажите, что $\mu(A_q) \leq 2c/q^{1+\varepsilon}$. Таким образом, ряд $\sum_q \mu(A_q)$ сходится.

В силу леммы Бореля – Кантелли отсюда следует нужное утверждение.

Заметим, что эта задача пришла из теории динамических систем на двумерном торе. Подобного же рода задачи возникают и в КАМ теории.

В связи с полученным результатом, будет интересно заметить [33], что существует такая бесконечная последовательность q_k и соответствующая ей последовательность p_k , что

$$\left| \alpha - \frac{p_k}{q_k} \right| < \frac{1}{\sqrt{5}} \frac{1}{q_k^2}.$$

В теории цепных дробей показывается, что последовательность p_k/q_k будет подпоследовательностью последовательности подходящих дробей для числа α . Заметим также, что константу $1/\sqrt{5}$ в неравенстве уменьшить нельзя.

Задача (СТАТИСТИКА ТЕОРЕТИКО-ЧИСЛОВЫХ ФУНКЦИЙ). Довольно часто вероятностные соображения (например, независимость) используются в теории чисел не совсем строго, но зато весьма часто они позволяют угадать правильный ответ. Поясним сказанное, пожалуй, наиболее популярным примером из книги [17].

Пусть A — некоторое множество положительных целых чисел. Обозначим через $A(n)$ количество тех его элементов, которые содержатся среди первых n чисел натурального ряда. Если существует предел $\lim_{n \rightarrow \infty} A(n)/n = P(A)$, то он называется плотностью A . К сожалению, вероятностная мера $P(A)$ не является вполне аддитивной (счётно-аддитивной).

Рассмотрим целые числа, делящиеся на простое число p . Плотность множества таких чисел, очевидно, равна $1/p$. Возьмём теперь множество целых чисел, которые делятся одновременно на p и q (q — другое простое число). Делимость на p и q эквивалентна делимости на pq , и, следовательно, плотность нового множества равна $1/pq$. Так как $1/pq = (1/p) \cdot (1/q)$, то мы можем истолковать это так: «события», заключающиеся в делимости

на p и q , независимы. Это, конечно, выполняется для любого количества простых чисел.

Поставим теперь задачу посчитать долю несократимых дробей или, другими словами, «вероятность» несократимости дроби (фиксируется знаменатель дроби n , а затем случайно, с равной вероятностью $1/n$ выбирается любое число от 1 до n в качестве числителя, и подсчитывается доля случаев, в которых полученная дробь оказывалась несократимой) в следующем смысле (здесь и далее индекс p может пробегать только простые числа):

$$\begin{aligned} \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \frac{\#\{k < n : \text{НОД}(n, k) = 1\}}{n} &= \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \frac{\varphi(n)}{n} = \\ &= \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \prod_p \left(1 - \frac{\rho_p(n)}{p}\right), \end{aligned}$$

где $\varphi(n)$ — функция Эйлера, $\rho_p(n) = \begin{cases} 1, & n \text{ делится на } p, \\ 0, & \text{иначе.} \end{cases}$

Согласно введённому выше определению плотности:

$$M \left\{ \prod_{p \leq p_k} \left(1 - \frac{\rho_p(n)}{p}\right) \right\} = \prod_{p \leq p_k} M \left\{ \left(1 - \frac{\rho_p(n)}{p}\right) \right\} = \prod_{p \leq p_k} \left(1 - \frac{1}{p^2}\right).$$

С учётом этого хочется написать следующее:

$$\begin{aligned} \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N \frac{\varphi(n)}{n} &= M \left\{ \frac{\varphi(n)}{n} \right\} = M \left\{ \prod_p \left(1 - \frac{\rho_p(n)}{p}\right) \right\} \stackrel{?}{=} \\ &\stackrel{?}{=} \prod_p M \left\{ \left(1 - \frac{\rho_p(n)}{p}\right) \right\} = \prod_p \left(1 - \frac{1}{p^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}. \end{aligned}$$

Будь введённая вероятностная мера, по которой считается это математическое ожидание, счётно-аддитивной, то можно было бы поставить точку, получив ответ. Однако, это не так. Хотя ответ мы и получили правильный, но приведённое выше рассуждение не может считаться доказательством. Впрочем, часто вероятностные рассуждения удаётся пополнить, используя их в качестве основы. Так в разобранным нами примере все сводится к обоснованию равенства «?».

Легко понять, что полученный ответ несёт определённую информацию о статистических свойствах функции Эйлера.

В теории чисел такого типа задачи занимают крайне важное место. Достаточно сказать, что гипотеза Римана «на миллион» о распределении

нетривиальных нулей дзета-функции Римана $\zeta(z)$ равносильна следующему свойству функции Мёбиуса $\mu(n)$:

$$\left| \sum_{n=1}^N \mu(n) \right| \leq \sqrt{N} \quad (\text{Олдыжко – Ризель}).$$

Что в свою очередь (Х. М. Эдвардс) в определённом смысле «завязано» на случайность последовательности $\{\mu(n)\}_{n \in \mathbb{N}}$.

Используя указанный выше формализм, найдите долю чисел натурального ряда, свободных от квадратов, т. е. не делящихся на квадрат любого простого числа.

По-видимому, первым эту задачу решился предложить школьникам около десяти лет назад В. И. Арнольд. В заключение заметим, что применение вероятностных соображений в теории чисел продолжает привлекать ведущих математиков и по сей день (см., например, выступление Я. Г. Сина на семинаре «Глобус» [39]).

ЗАДАЧА (ПРЕДЕЛЬНЫЕ МЕРЫ; А. М. ВЕРШИК и ДР., 1977 [9, 11])*. В качестве множества элементарных исходов рассматривается группа всевозможных подстановок (перестановок) S_n (симметрическая группа), $n \gg \gg 1$. В этой группе $n!$ элементов. Припишем каждой подстановке одинаковую вероятность $1/n!$.

А) Покажите, что математическое ожидание числа циклов есть $\approx \ln n$.

Б) В каком смысле нормированные длины циклов случайной подстановки убывают со скоростью геометрической прогрессии со знаменателем e^{-1} ?

В) Положим $\rho_n(a) = |\{g \in S_n : n_{\max}(g) \leq an\}|/n!$, где $n_{\max}(g)$ — длина максимального цикла в подстановке g . Покажите, что $\rho_n(a)$ удовлетворяет уравнению Дикмана – Гончарова (40-е годы XX века):

$$\rho_n(a) = \int_0^a \rho_n\left(\frac{a}{1-t}\right) dt.$$

Г) Покажите, что, начиная с некоторого большого числа N , 99% натуральных чисел n , больших, чем N , обладают свойством

$$n^{0.99} < p_1 \cdot \dots \cdot p_{11}, \quad n = p_1 \cdot \dots \cdot p_{m(n)}, \quad p_1 \geq p_2 \geq \dots \geq p_{m(n)}, \quad p_i \text{ — простые.}$$

Иначе говоря, у основной части (99%) натуральных чисел основная часть (99%) числа есть произведение наибольших простых делителей. Число 11 возникло из-за того, что мы выбрали 99% и 99%.

УКАЗАНИЕ. Решение задач всех пунктов сводится (технически весьма нетривиально!) к задаче о «ломании палки». Отрезок $[0, 1]$ делится

(«ломается») случайно с равномерной вероятностью. Левый отрезок фиксируем, а правый ломается аналогичным образом и т. д.

Обратим внимание, что школьники могли познакомиться с этой темой из выступления А. М. Вершика в ЛШСМ-2008 [10].

ЭЛЕМЕНТЫ МАТЕМАТИЧЕСКОЙ СТАТИСТИКИ

ЗАДАЧА (КРИТЕРИЙ СОГЛАСИЯ КОЛМОГОРОВА). Пусть $\vec{X} = (X_1, X_2, \dots, X_n)$ — простая выборка объёма n из распределения $F(x)$. Покажите, что для непрерывных распределений $F(x)$ распределение статистики $D_n(\vec{X}) = \sup_{x \in \mathbb{R}} |F_n(x; \vec{X}) - F(x)|$ не зависит от $F(x)$. Здесь $F_n(x; \vec{X})$ обозначает эмпирическую функцию распределения:

$$F_n(x; \vec{X}) = \frac{\mu_n(x)}{n} = \frac{1}{n} \sum_{k=1}^n I_k(x),$$

где $\mu_n(x) = |\{j : X_j < x\}|$, $I_k(x) = \begin{cases} 1, & X_k < x, \\ 0, & X_k \geq x. \end{cases}$

В действительности, подобный результат будет справедлив и для широкого класса статистик $G(F_n, F)$ (т. е. измеримых функционалов) от $F_n(x; \vec{X})$.

УКАЗАНИЕ. Положим по определению

$$F^{-1}(u) = \inf \{ \xi : F(\xi) = u \} = \min \{ \xi : F(\xi) = u \} \quad \text{для } u \in [0, 1],$$

где последнее равенство имеет место в силу непрерывности $F(x)$. Понятно, что это отнюдь не единственный способ выбора однозначной функции из, вообще говоря, многозначного отображения $F^{-1}(u)$, однако именно такое определение окажется наиболее полезным в дальнейшем. Положим $u = F(x)$, тогда u пробегает как минимум все точки интервала $(0, 1)$ (а как максимум — отрезка $[0, 1]$), когда x пробегает \mathbb{R} . Делая замену $u = F(x)$ и используя определение $F^{-1}(u)$, получим

$$D_n(\vec{X}) = \max_{u \in [0, 1]} |F_n(F^{-1}(u); \vec{X}) - u|.$$

Далее имеем

$$F_n(F^{-1}(u)) = \frac{1}{n} \sum_{k=1}^n \theta(F^{-1}(u) - X_k).$$

Остается показать эквивалентность событий

$$\{F^{-1}(u) - X_k \leq 0\} \sim \{u - F(X_k) \leq 0\}.$$

Сделайте это, завершив, тем самым, доказательство сформулированного утверждения.

ЗАДАЧА (РАСПРЕДЕЛЕНИЕ КОШИ). На плоскости на расстоянии $a > 0$ (неизвестный параметр) от детектирующей прямой располагается радиоактивный источник, который излучает вспышками равновероятно по любому направлению в этой плоскости. Пусть $\vec{x} = (x_1, \dots, x_n)$ — вектор координат вспышек, регистрируемых детектором. Требуется построить по такой простой выборке состоятельную оценку координаты проекции источника на детектирующую прямую.

ЗАДАЧА (ОЦЕНКА ПАРАМЕТРА С ПОМОЩЬЮ ЭРГОДИЧЕСКОЙ ТЕОРЕМЫ). В модели Блэка – Шоулса – Мертона эволюция цены акции описывается геометрическим броуновским движением

$$S(t) = S(0) \exp(at + \sigma W(t)),$$

где $W(t)$ — винеровский процесс ($\sigma > 0$). С помощью эргодической теоремы для случайных процессов оцените неизвестный параметр a , если известна реализация процесса $S(t)$ на достаточно длинном временном отрезке $[0, T]$. Предложите способ оценки неизвестного параметра σ .

ЗАДАЧА (КРИТЕРИЙ НЕЙМАНА – ПИРСОНА). В результате эксперимента получена простая выборка \vec{x} , относительно которой имеются две простые гипотезы:

$$H_0 : \vec{x} \in L(\vec{x} | H_0) \quad \text{и} \quad H_1 : \vec{x} \in L(\vec{x} | H_1).$$

С уровнем значимости $\alpha > 0$ постройте наиболее мощный критерий проверки гипотезы H_0 против альтернативы H_1 , т. е. найдите такую функцию $\varphi(\vec{x})$ (решающее правило — вероятность, с которой следует принимать гипотезу H_1 , если выпал \vec{x}), что

$$P(H_0 | H_1) = \int_{\Omega} (1 - \varphi(\vec{x})) L(\vec{x} | H_1) d\vec{x} \rightarrow \min_{0 \leq \varphi(\cdot) \leq 1}$$

$$P(H_1 | H_0) = \int_{\Omega} \varphi(\vec{x}) L(\vec{x} | H_0) d\vec{x} = \alpha.$$

Покажите, что решение этой задачи — наиболее мощное решающее правило (Неймана – Пирсона) — имеет вид

$$\varphi(\vec{x}) = \begin{cases} 1, & \Lambda(\vec{x}) > \bar{\Lambda} \\ p(\vec{x}), & \Lambda(\vec{x}) = \bar{\Lambda}, \\ 0, & \Lambda(\vec{x}) < \bar{\Lambda} \end{cases}, \quad \text{где } \Lambda(\vec{x}) = \frac{L(\vec{x} | H_1)}{L(\vec{x} | H_0)},$$

$\bar{\Lambda}$ и $0 \leq p(\vec{x}) \leq 1$ следует определять из условия (ошибкой первого рода):

$$P(H_1 | H_0) = \int_{\{\vec{x}: \Lambda(\vec{x}) > \bar{\Lambda}\}} L(\vec{x} | H_0) d\vec{x} + \int_{\{\vec{x}: \Lambda(\vec{x}) = \bar{\Lambda}\}} p(\vec{x}) L(\vec{x} | H_0) d\vec{x} = \alpha. \quad (*)$$

Причём $\bar{\Lambda}$ определяется единственным образом, а от того, как выбирать $p(\vec{x})$, удовлетворяющее (*), не зависит ошибка второго рода:

$$P(H_0 | H_1) = \int_{\{\vec{x}: \Lambda(\vec{x}) < \bar{\Lambda}\}} L(\vec{x} | H_1) d\vec{x} + \int_{\{\vec{x}: \Lambda(\vec{x}) = \bar{\Lambda}\}} (1 - p(\vec{x})) L(\vec{x} | H_1) d\vec{x} = \beta.$$

УКАЗАНИЕ. Воспользуйтесь методом множителей Лагранжа [23].

ЗАДАЧА (О НАИБОЛЕЕ МОЩНОМ КРИТЕРИИ ДЛЯ ОЦЕНКИ СТУДЕНТОВ). Опытный преподаватель математической статистики знает, что к нему на экзамен могут приходиться два типа студентов: знающие предмет и не знающие предмет. Причём, ввиду всяких случайных факторов (не выспался, переволновался, воспользовался шпаргалкой) впечатление, которое студент производит на экзаменатора, — случайная величина. Для знающих студентов она имеет пуассоновское распределение с параметром 200, а для не знающих — с параметром 100. Преподаватель ставит только две оценки: «зачёт» и «незачёт». Философия преподавателя такова: «пусть лучше я поставлю «зачёт» студенту, который этого не заслуживает, нежели поставлю «незачёт» знающему материал студенту». Предложите, как следует действовать преподавателю (какую оценку ставить в зависимости от впечатления (целое неотрицательное число), которое на него производит студент), если он допускает, что с вероятностью не большей 0.1 можно ошибиться и поставить не знающему студенту «зачёт».

ЗАДАЧА (ОЦЕНКА ВЕРОЯТНОСТИ ПЕРЕОБУЧЕНИЯ). Пусть x_1, \dots, x_l — простая выборка из распределения с функцией распределения $F(x)$. Элементами этой выборки x_i могут быть, например, векторы. Пусть $\alpha \in \Omega$ — некоторый абстрактный параметр, $0 \leq R(x, \alpha) \leq a$ — некоторая функция, измеримая при всех $\alpha \in \Omega$ относительно меры $F(x)$. Далее

$$M(\alpha) = MR(x, \alpha) = \int R(x, \alpha) dF(x), \quad M_{\text{эмп}}(\alpha) = \frac{1}{l} \sum_{i=1}^l R(x_i, \alpha).$$

Рассмотрим систему событий S вида $A(\alpha, c) = \{x : R(x, \alpha) \geq c\}$ для всевозможных значений $\alpha \in \Omega$ и c .

Обозначим через $\Delta^S(x_1, \dots, x_l)$ число (бинарных) решающих правил класса S , по-разному классифицирующих объекты заданной выборки. Выборке x_1, \dots, x_l и конкретному $A(\alpha, c)$ ставится в соответствие последовательность нулей и единиц по правилу: $x_i \in A(\alpha, c) \Rightarrow 1, x_i \notin A(\alpha, c) \Rightarrow 0$.

Разным $A(\alpha, c)$ могут соответствовать как разные, так и одинаковые последовательности нулей и единиц. Очевидно, что $\Delta^S(x_1, \dots, x_l)$ есть число различных последовательностей нулей и единиц, построенных по семейству $\{A(\alpha, c)\}_{\alpha \in \Omega, c}$. Очевидно также, что $\Delta^S(x_1, \dots, x_l) \leq 2^l$.

Введём функцию роста $M^S(l) = \max \Delta^S(x_1, \dots, x_l)$, где максимум берётся по всем последовательностям (x_1, \dots, x_l) длины l . Покажите, что

$$P \left\{ \sup_{\alpha \in \Omega} |M(\alpha) - M_{\text{эмп}}(\alpha)| > \varepsilon \right\} \leq 6M^S(2l) \exp \left[-\frac{\varepsilon^2(l-1)}{4a^2} \right].$$

ЗАМЕЧАНИЕ. Заметим, что для любой системы событий S имеет место:

$$M^S(l) = 2^l \text{ или } M^S(l) \leq \sum_{i=0}^{n-1} C_l^i,$$

т. е. $M^S(l) = O(l^{n_0})$ для некоторого $n_0 \in \mathbb{N}$.

Минимально возможное значение n_0 принято называть размерностью Вапника – Червоненкиса (VC-размерность). Однако А. Я. Червоненкис предлагает (в учебном пособии [34]) называть её комбинаторной размерностью S . Так, например, для множества всевозможных линейных решающих правил в пространстве размерности n комбинаторная размерность равна $n_0 = n + 1$. Если $M^S(l) = 2^l$, то говорят, что комбинаторная размерность бесконечна. Для рассматриваемого в задаче случая достаточным условием конечности комбинаторной размерности, как следствие равномерной сходимости с ростом объёма выборки $M_{\text{эмп}}(\alpha)$ к $M(\alpha)$, является условие, что Ω – компакт, $R(x, \alpha)$ непрерывна по α , $|R(x, \alpha)| < K(x)$, где $\int K(x) dx < \infty$.

Для более глубоко знакомства с методами математической статистики можно рекомендовать [7, 15, 22].

СПИСОК ЛИТЕРАТУРЫ

- [1] Алон Н., Спенсер Дж. *Вероятностный метод*. М.: Бином, 2006.
- [2] Арнольд В.И. *Математическое понимание природы*. М.: МЦНМО, 2011.
- [3] Арнольд В.И. *Цепные дроби*. М.: МЦНМО, 2001.
- [4] Афанасьев В.И. *Случайные блуждания и ветвящиеся процессы*. Лекционные курсы НОЦ, вып. 6. М.: МИАН, 2008.
<http://www.mi.ras.ru/index.php?c=lectures>

- [5] Афанасьева Л.Г. *Очерки исследования операций*. М.: Изд-во механико-математического факультета МГУ, 2007.
- [6] Богданов К.Ю. *Прогулки с физикой*. Б-ка «Квант», вып. 98. М.: Бюро Квантум, 2006; глава 18.
- [7] Боровков А.А. *Математическая статистика*. М.: ФИЗМАТЛИТ, 2007.
- [8] Ватутин В.А. *Ветвящиеся процессы и их применение*. М.: МИАН, Лекционные курсы НОЦ, вып. 8, 2008.
- [9] Вершик А.М. *Асимптотическое распределение разложений натуральных чисел на простые делители* // ДАН, 1986. Т. 289, №2. С. 269–272.
- [10] Вершик А.М. *А что будет, если n очень большое?* Лекция 1. Дубна, 2008.
<http://www.mathnet.ru/PresentFiles/231/v231.pdf>,
<http://www.mathnet.ru/php/presentation.phtml?presentid=231>
- [11] Вершик А.М., Шмидт А.А. *Предельные меры, возникающие в асимптотической теории симметрических групп* // ТВП, Т. 22. №1. 1977. С. 72-88; Т. 23. №1. 1978. С. 42-54.
- [12] Гнеденко Б.В. *Курс теории вероятностей*. М.: Едиториал УРСС, 2005.
- [13] Гусейн-Заде С.М. *Разборчивая невеста*. М.: МЦНМО, Б-ка «Математическое просвещение», вып. 25, 2003.
- [14] Зорич А.В. *Математический анализ задач естествознания*. М.: МЦНМО, 2008. С. 48-56.
- [15] Ивченко Г.И., Медведев Ю.И. *Введение в математическую статистику*. М.: Издательство ЛКИ, 2010.
- [16] Кац М. *Вероятность и смежные вопросы в физике*. М.: Мир, 1965.
- [17] Кац М. *Статистическая независимость в теории вероятностей, анализе и теории чисел*. М.: ИЛ, 1963.
- [18] Кельберт М. Я., Сухов Ю. М. *Вероятность и статистика в примерах и задачах*. Т. 2. М.: МЦНМО, 2010.
- [19] Кендалл М., Моран П. *Геометрические вероятности*. М.: Наука, 1972.
- [20] Кормен Т., Лейзерсон Ч., Ривест Р., Штайн Ш. *Алгоритмы. Построение и анализ*. М.: Изд-во Вильямс, 2005.

- [21] Кузюрин Н.Н., Фомин С.А. *Эффективные алгоритмы и сложность вычислений*. М.: МФТИ, 2007.
- [22] Лагутин М.Б. *Наглядная математическая статистика*. М.: Бином, 2009.
- [23] Магарил-Ильяев М.А., Тихомиров В.М. *Выпуклый анализ*. М.: Едиториал УРСС, 2011.
- [24] Мальшев В.А. *Кратчайшее введение в современные вероятностные модели*. М.: Изд-во мехмата МГУ, 2009.
<http://mech.math.msu.su/~malyshev/Malyshev/Lectures/course.pdf>
- [25] А.Ю. Окуньков. *Легко ли заблудиться в группе?* Дубна, 2010.
<http://www.mathnet.ru/php/presentation.phtml?presentid=3491>
- [26] Опойцев В.И. *Устойчивые системы большой размерности* // АиТ, №6. 1986. С. 43-49.
- [27] Разборов А.А. *Теория сложности вычислений*. Лекция 3. Дубна, 2011.
<http://www.mathnet.ru/php/presentation.phtml?presentid=3645>
- [28] Райгородский А.М. *Вероятность и алгебра в комбинаторике*. М.: МЦНМО, 2008.
- [29] Секей Г. *Парадоксы в теории вероятностей и математической статистике*. Москва – Ижевск: РХД, 2002.
- [30] Синай Я.Г. *Основы эргодической теории*. М.: ФАЗИС, 1996.
- [31] Сосинский А.Б. *Мыльные плёнки и случайные блуждания*. М.: МЦНМО, Б-ка «Математическое просвещение», вып. 6, 2000.
- [32] Федорюк М.В. *Метод перевала*. М.: УРСС, 2010.
- [33] Хинчин А.Я. *Ценные дроби*. М.: УРСС, 2004.
- [34] Червоненкис А.Я. *Компьютерный анализ данных*. М.: Яндекс, 2009.
- [35] Шень А. *Вероятностные доказательства* // Квант, №6. 2009. С. 11–15.
- [36] Шень А. *Вероятность: примеры и задачи*. М.: МЦНМО, 2008.
<http://www.mcsme.ru/free-books/shen/shen-probability.pdf>
- [37] Эфрос А.Л. *Физика и геометрия беспорядка*. Б-ка «Квант», вып. 19. М.: Наука, 1982.
- [38] <http://dame.mipt.ru/studyandscience/stohanaliz.html>

- [39] <http://erb-files.narod.ru/#GLOBUS>
- [40] <http://www.mou.mipt.ru/natan.html>
- [41] Annual IEEE Symposium on Foundations of Computer Science, 1 – 51.
Например, <http://theory.stanford.edu/focs2010/>
- [42] Diaconis P. *The Markov chain Monte Carlo revolution* // Bulletin (New Series) of the AMS. 2009. V. 49. №2. P. 179-205.
<http://www-stat.stanford.edu/~cgates/PERSI/papers/MCMCRev.pdf>
- [43] Dubhashi D.P., Panconesi A. *Concentration of measure for the analysis of randomized algorithms*. Cambridge University Press, 2009.
- [44] Durrett R. *Probability: Theory and examples*. Pacific Grove CA: Wadsworth, 1991.
http://www.math.duke.edu/~rtd/PTE/PTE4_Jan2010.pdf
- [45] Flajolet P., Sedgewick R. *Analytic combinatorics*. Cambridge University Press, 2008. <http://algo.inria.fr/flajolet/Publications/book.pdf>
- [46] Lai T., Robbins H. *Asymptotically efficient adaptive allocation rules* // Advances in Applied Mathematics. V. 6. 1985. P. 41–22.
- [47] Ledoux M. *Concentration of measure phenomenon*. Providence, RI, Amer. Math. Soc., 2001 (Math. Surveys Monogr. V. 89).
- [48] Montenegro R., Tetali P. *Mathematical aspects of mixing times in Markov chains*. 2006.
<http://people.math.gatech.edu/~tetali/PUBLIS/survey.pdf>
- [49] Motwani R., Raghavan P. *Randomized algorithms*. Cambridge Univ. Press, 1995.

Конкурсы и олимпиады

Студенческие олимпиады мехмата МГУ 2010 – 2011 гг.*

И. В. Аржанцев В. И. Богачёв А. И. Гарбер
А. А. Заславский В. Ю. Протасов[†] А. Б. Скопенков[‡]

Мы приводим задачи заключительных туров олимпиад мехмата МГУ 2010 и 2011 годов, а также математического боя между командой преподавателей и командой первокурсников на мехмате МГУ (вместе с указаниями, решениями и комментариями).¹⁾ Заключительный тур 2011 года был совмещен с универсиадой-2011, поэтому в нем приняли участие студенты из ВШЭ, МФТИ и СПбГУ. Введение и задачи прошлых олимпиад приведены в [1, 2]. Имена победителей приведены в конце заметки.

Мы благодарим механико-математический факультет МГУ, попечительский совет мехмата МГУ и компанию «Атон» за награждение победителей всемехматовской олимпиады 2011 и поддержку командирования команды мехмата на международную олимпиаду ИМС. Научно-методическое обеспечение универсиад – всемехматовских олимпиад еще нуждается в финансовой поддержке.

*Обновляемая версия: <http://mccme.ru/circles/oim/stolymp/mechm1011.pdf>

[†]Поддержан фондом «Династия».

[‡]Поддержан грантом фонда Саймонса.

¹⁾Вот кто предложил задачи и приведенные решения (предложивший не обязательно является автором): И. Аржанцев (2010-2,3), В. Богачёв (2010-1, 2011-3,5, МБ-2, МБ-5), В. Брагин (2010-5), С. Гайфуллин (2010-3), А. Гарбер (МБ-4, 2011-5), И. Григорьев (2011-2, МБ-1), А. Ефимов (МБ-4), А. Заславский (2010-4, МБ-3), Ф. Ивлев (МБ-6), А. Клячко (МБ-7), С. Ландо (МБ-8), Н. Назаренко (МБ-6), Ф. Петров (2011-5), А. Пешнин (2010-3), В. Протасов (2011-1,4, МБ-6), А. Райгородский (2010-5), А. Скопенков (МБ-1, МБ-7, МБ-8). Задачи 2011-4 и 2011-5 взяты из книг. Все варианты составлены В. И. Богачёвым.

ВСЕМЕХМАТОВСКАЯ СТУДЕНЧЕСКАЯ ОЛИМПИАДА 2010 ГОДА

2010-1. Пусть $f: [0, 1] \rightarrow [0, 1]$ и $g: [0, 1] \rightarrow [0, 1]$ – непрерывные функции, для которых $f(g(x)) = g(f(x))$ при любом $x \in [0, 1]$. Предположим, что g непрерывно дифференцируема на $(0, 1)$ и $g'(x) \leq 1$ для $x \in (0, 1)$. Докажите, что существует точка $t \in [0, 1]$, для которой $f(t) = g(t) = t$.

2010-2. Даны векторы $v_1, \dots, v_n \in \mathbb{R}^k$. Обозначим через (v_1, \dots, v_n) матрицу размера $k \times n$, образованную их координатами. Докажите, что существует m и $w_1, \dots, w_n \in \mathbb{R}^m$ со следующими двумя условиями:

- (i) $(w_1, \dots, w_n)(v_1, \dots, v_n)^T = 0 \in \mathbb{R}^{mk}$;
(ii) для любого l и любых элементов $u_1, \dots, u_n \in \mathbb{R}^l$ таких, что

$$(u_1, \dots, u_n)(v_1, \dots, v_n)^T = 0 \in \mathbb{R}^{lk},$$

существует линейное отображение $T: \mathbb{R}^m \rightarrow \mathbb{R}^l$, для которого $T(w_i) = u_i$ при любом $i = 1, \dots, n$.

2010-3. Пусть $A = (a_{ij})$ – квадратная матрица размера $n \times n$ с вещественными элементами. Предположим, что для любого подмножества $I \subseteq \{1, \dots, n\}$ и матрицы $A_I := (a_{ks})_{k,s \in I}$ выполнено $A_I^n = 0$. Докажите, что матрицу A можно сделать верхнетреугольной с нулями на главной диагонали конечным числом следующих преобразований: сначала переставляются две строки в матрице, а потом переставляются два столбца с такими же номерами.

2010-4. Дана пирамида $SABC$. Рассмотрим сферы X , вписанные в трехгранный угол с вершиной S . Найти ГМТ пересечения трех плоскостей, касательных к X , проходящих через прямые AB , BC и CA , соответственно, и не содержащих грани пирамиды. (S, A, B, C фиксированы, а X меняется.)

2010-5. Для каких

- (a) нечетных n (b) четных n

можно покрасить вершины n -мерного куба в n цветов так, что для любой вершины ее n соседей имеют разные цвета?

ВСЕМЕХМАТОВСКАЯ СТУДЕНЧЕСКАЯ ОЛИМПИАДА 2011 ГОДА

2011-1. Функция $f: (0, 1) \rightarrow (0, +\infty)$ обладает следующим свойством:

$$\frac{f(x)}{f(y)} \leq 1 + \frac{x}{y} \quad \text{для всех } x, y \in (0, 1).$$

Докажите, что существует конечный предел $\lim_{x \rightarrow 0} f(x)$.

2011-2. Пусть G — связный (неориентированный) граф с n вершинами $1, 2, \dots, n$, $n \geq 3$. Для каждой пары ребер ij , jk (имеющих общую вершину) возьмем циклы (ijk) и (ikj) . Докажите, что взятые циклы порождают всю подгруппу четных перестановок.

(Напомним, что циклом (abc) называется перестановка множества $\{1, 2, \dots, n\}$, переводящая a в b , b в c , c в a и каждый другой элемент в себя.)

2011-3. Непрерывная функция $h : [1, +\infty) \rightarrow [1, +\infty)$ строго возрастает и сюръективна. Докажите, что

$$\int_1^{+\infty} \frac{h(t)}{t^2} dt = 1 + \int_1^{+\infty} \frac{1}{h^{-1}(s)} ds,$$

если хотя бы один интеграл конечен.

2011-4. Пусть M, N и A — различные внутренние точки шара в трехмерном пространстве, ограниченного сферой Σ . Прямые AM и AN перпендикулярны диаметру сферы Σ , проходящему через A . Две различные сферы Σ_1 и Σ_2 касаются сферы Σ и проходят через M, N, A . Докажите, что радиус сферы Σ равен сумме радиусов сфер Σ_1 и Σ_2 .

2011-5. Пусть A — матрица $n \times n$ с вещественными элементами. Матрица $H = (A + A^T)/2$ положительно определена. Докажите, что $\det H \leq \leq \det A$.

ЗАДАЧИ МАТЕМАТИЧЕСКОГО БОЯ

МБ-1. При каких $N > 1$ и $K > 1$ циклы $(1, 2, \dots, N)$ и $(N, N + 1, \dots, N + K - 1)$ порождают всю группу перестановок $(N + K - 1)$ -элементного множества?

МБ-2. Существует ли непостоянная функция $f : [0, 1] \rightarrow \mathbb{R}$, имеющая конечную производную в каждой точке, равную нулю на некотором всюду плотном множестве?

МБ-3. Эллипс с фокусами F_1 и F_2 касается изнутри в двух точках окружности с центром O и радиусом r . Докажите, что эксцентриситет эллипса равен OF_1/r .

МБ-4. Пусть x_i, y_i — вещественные числа, где $i \in \mathbb{Z}/(2r + 1)\mathbb{Z}$, $r \geq 1$. Предположим, что

$$\sum_{i=1}^{2r+1} x_i = \sum_{i=1}^{2r+1} y_i = 0 \quad \text{и} \quad \Delta_{i,j} := x_i y_j - x_j y_i \geq 0 \quad \text{при} \quad j \in \{i + 1, \dots, i + r\}.$$

Тогда

$$3 \sum_{\substack{1 \leq i \leq r, \\ r+1 \leq j \leq 2r, \\ j \in \{i+1, \dots, i+r\}}} \Delta_{i,j} \leq \sum_{\substack{1 \leq i \leq 2r+1, \\ j \in \{i+1, \dots, i+r\}}} \Delta_{i,j}.$$

(На матбое предлагалась эта задача для $r = 8$.)

МБ-5. Существует ли такой многочлен P с целыми коэффициентами, что $|P(x) - 10^{-1}| < 10^{-4}$ для всех $x \in [2/25; 3/25]$?

МБ-6. На плоскости даны ограниченный выпуклый многоугольник и треугольник. Каждая из прямых, содержащих стороны треугольника, делит площадь многоугольника пополам. Докажите, что площадь треугольника не превосходит четверти площади многоугольника.

МБ-7. Докажите, что если n взаимно просто с $\varphi(n)$, то любая группа из n элементов является циклической. Здесь $\varphi(n)$ — количество чисел от 1 до n , взаимно простых с n .

МБ-8. На сфере заданы конечное семейство A непересекающихся окружностей и семейство B из такого же количества непересекающихся окружностей. Обязательно ли существуют два многогранника $f, g \subset \mathbb{R}^3$, гомеоморфных сфере, для которых $f \cap g$ есть объединение замкнутых несамопересекающихся ломаных, образующее семейство A на f и семейство B на g ?

ПРИМЕЧАНИЯ. Окружности в семействах *не занумерованы*. Здесь многогранником называется его *поверхность*, а не внутренность. Многогранники f и g *несамопересекающиеся* и *не обязательно выпуклые*. Многогранник называется *гомеоморфным сфере*, если любая замкнутая ломаная, лежащая на его поверхности, разбивает многогранник на две части. Подразумевается теоретико-множественное пересечение $f \cap g$, никаких условий трансверсальности не накладываемся. Объединение $f \cap g$ замкнутых несамопересекающихся ломаных *образует* семейство A на f , если существует взаимно однозначное соответствие между связными компонентами дополнения $f - (f \cap g) = f - g$ и связными компонентами дополнения $S^2 - A$, при котором две компоненты в $f - g$ примыкают к окружности из $f \cap g$ тогда и только тогда, когда соответствующие компоненты в $S^2 - A$ примыкают к окружности из A .

РЕШЕНИЯ И КОММЕНТАРИИ К ВСЕМЕХМАТОВСКОЙ ОЛИМПИАДЕ 2010 ГОДА

2010-1. Если $g(a) = a$ и $g(b) = b$, $a \leq b$, то $g(s) = s$ при всех $s \in [a, b]$, ибо если $g(s) < s$, то $g(b) < b$ при $b > s$ из-за $g' \leq 1$. Так как $f(g) = g(f)$, то $f([a, b]) \subset [a, b]$, значит, существует $t \in [a, b]$ с $f(t) = t$.

2010-2. Условие $x(v_1, \dots, v_n)^T = 0 \in \mathbb{R}^k$ на вектор-строку $x \in \mathbb{R}^n$ является системой линейных уравнений с матрицей $(v_1, \dots, v_n)^T$. Возьмем векторы-столбцы $w_1, \dots, w_n \in \mathbb{R}^m$, для которых строки матрицы (w_1, \dots, w_n) порождают пространство решений этой системы. Тогда условия (i) и (ii), очевидно, выполнены. (Для доказательства свойства (ii) заметим, что условие « $T(w_i) = u_i$ для любого $i = 1, 2, \dots, n$ » равносильно условию

$$\langle (u_1, \dots, u_n) = T'(w_1, \dots, w_n) \rangle$$

на $(l \times m)$ -матрицу T' линейного отображения T .)

Замечание. Переход от матрицы системы к матрице ее некоторого фундаментального набора решений (т.е. от набора v_1, \dots, v_n к набору w_1, \dots, w_n) научно называют *линейным преобразованием Гейла*, см., например [6].

Авторская формулировка. Пусть v_1, \dots, v_n — элементы векторного пространства V . Докажите, что найдутся такое векторное пространство W и такие элементы $w_1, \dots, w_n \in W$, что

$$(i) v_1 \otimes w_1 + \dots + v_n \otimes w_n = 0 \text{ в } V \otimes W;$$

(ii) для любого векторного пространства U и любых элементов $u_1, \dots, u_n \in U$, для которых $v_1 \otimes u_1 + \dots + v_n \otimes u_n = 0$ в $V \otimes U$, найдется такое линейное отображение $\varphi : W \rightarrow U$, что $\varphi(w_i) = u_i$, $i = 1, \dots, n$.

Авторское решение. Можно считать, что $V = \langle v_1, \dots, v_n \rangle$. Рассмотрим линейное пространство W_1 с базисом e_1, \dots, e_n , и вложим в него сопряженное пространство V^* :

$$\iota : V^* \rightarrow W_1, \quad l \mapsto l(v_1)e_1 + \dots + l(v_n)e_n.$$

Рассмотрим факторпространство $W := W_1/\iota(V^*)$ и проекцию $p : W_1 \rightarrow W$. Положим $w_i := p(e_i)$. Для того, чтобы проверить свойство (i), достаточно заметить, что условие $v_1 \otimes w_1 + \dots + v_n \otimes w_n = 0$ в $V \otimes W$ равносильно тому, что $l(v_1)w_1 + \dots + l(v_n)w_n = 0$ в W для любой функции $l \in V^*$. Для проверки свойства (ii) определим линейное отображение $\psi : W_1 \rightarrow U$ условиями $\psi(e_i) = u_i$. Чтобы проверить, что отображение ψ индуцирует отображение $\varphi : W \rightarrow U$, достаточно показать, что $\psi(\iota(V^*)) = 0$. Последнее следует из того, что $v_1 \otimes u_1 + \dots + v_n \otimes u_n = 0$ в $V \otimes U$.

2010-3. По матрице A построим ориентированный граф на n вершинах, в котором стрелка от вершины i в вершину j проведена в точности тогда, когда $a_{ij} \neq 0$. Достаточно показать, что в этом графе нет ориентированных циклов. Воспользуемся индукцией по n . Пусть ориентированный цикл есть. Тогда по предположению индукции он имеет длину n . Наличие стрелки вне этого цикла приводит к ориентированному циклу меньшей длины. Значит, наш граф является простым ориентированным циклом, и тогда определитель матрицы A отличен от нуля, противоречие.

2010-4. *Ответ.* Гипербола, лежащая в плоскости, перпендикулярной ABC и проходящей через прямую точек, равноудаленных от граней трехгранного угла $SABC$. Фокусы гиперболы — точки пересечения касательных к сфере в этой плоскости с ABC .

Решение. Рассмотрим сначала плоский аналог задачи. Пусть к окружности, вписанной в угол POQ , проведены из точек P, Q касательные, отличные от сторон угла. Тогда, если R — точка пересечения этих касательных, то нетрудно видеть, что $|PR - QR| = |PO - QO|$. Следовательно, при изменении радиуса окружности точка R будет двигаться по гиперболе с фокусами P, Q , проходящей через O .

Возвращаясь к исходной задаче, заметим, что полюс плоскости ABC относительно вписанной сферы, вершина трехгранного угла и точка пересечения вторых касательных плоскостей лежат на одной прямой, причем точка пересечения этой прямой с плоскостью ABC будет для этих трех точек четвертой гармонической. Значит, если множество полюсов — коника, то и множество точек пересечения тоже. Но все полюса лежат в плоскости, проходящей через линию центров сфер и перпендикулярной ABC . Таким образом, задача свелась к плоскому аналогу, и мы получаем приведенный выше ответ. Отметим также, что это рассуждение обобщается на любую размерность.

2010-5. (а) *Ответ.* Ни при каких.

Решение. Возьмем все вершины, среди координат которых две единицы и $n - 2$ нуля, а также вершину со всеми нулевыми координатами. Всего взято $C_n^2 + 1$ вершин. Среди любых $[n/2] + 1$ вершин есть две, соединенные ребром. Значит, необходимое для такой раскраски число цветов не меньше $[(C_n^2 + 1)/([n/2])] = n + 1$.

(b) *Ответ.* При $n = 2^k$.

Доказательство необходимости. Из каждой вершины первого или второго цвета выходит ровно одно ребро, соединяющее вершины первого и второго цвета. Количество таких ребер равно как количеству вершин первого цвета, так и количеству вершин второго цвета. Поэтому всех цветов поровну. Тогда 2^n делится на n . Значит, $n = 2^k$.

Построение примера раскраски для $n = 2^k$. Занумеруем цвета упорядоченными наборами из нулей и единиц длины k . Покрасим вершину

$$(a_1, a_2, \dots, a_n), \quad \text{где } a_s \in \{0, 1\} \quad \text{в цвет } a_1\bar{1} \oplus a_2\bar{2} \oplus \dots \oplus a_n\bar{n},$$

где \bar{s} — набор, соответствующий двоичной записи числа s и \oplus — сумма по модулю 2 (фактически суммируются наборы \bar{s} , для которых $a_s = 1$).

Докажем, что такая раскраска удовлетворяет условиям задачи. Рассмотрим вершину (a_1, a_2, \dots, a_n) . Предположим, что ее соседи $(a_1, a_2,$

$\dots, a_i \oplus 1, \dots, a_n)$ и $(a_1, a_2, \dots, a_j \oplus 1, \dots, a_n)$ имеют одинаковый цвет. Тогда

$$a_1 \bar{1} \oplus a_2 \bar{2} \oplus \dots \oplus a_n \bar{n} \oplus \bar{i} = a_1 \bar{1} \oplus a_2 \bar{2} \oplus \dots \oplus a_n \bar{n} \oplus \bar{j}.$$

Поэтому $\bar{i} = \bar{j}$. Значит, $i = j$. Таким образом, предъявленная раскраска удовлетворяет условию задачи.

РЕШЕНИЯ И КОММЕНТАРИИ К ВСЕМЕХМАТОВСКОЙ ОЛИМПИАДЕ 2011 ГОДА

2011-1. Фиксируем произвольное $y \in (0, 1)$. Для любого $x \in (0, y)$ имеем $f(x) \leq (1 + \frac{x}{y}) f(y) \leq 2 f(y)$. Следовательно, функция $f(x)$ ограничена на интервале $(0, y)$. Если она не имеет предела при $x \rightarrow 0$, то найдутся последовательности $\{a_k\}$ и $\{b_k\}$, стремящиеся к нулю, для которых существуют пределы $a := \lim_{k \rightarrow \infty} f(a_k) \neq \lim_{k \rightarrow \infty} f(b_k) =: b$. Фиксируем произвольное n . Для любого k имеем $f(a_k) \leq (1 + \frac{a_k}{b_n}) f(b_n)$. В пределе при $k \rightarrow \infty$ получаем $a \leq f(b_n)$, что в пределе при $n \rightarrow \infty$ дает $a \leq b$. Аналогично $b \leq a$, откуда $a = b$, что противоречит предположению.

2011-2. Достаточно доказать утверждение для деревьев. Для дерева оно доказывается по индукции с отбрасыванием висячей вершины. Другое решение приведено в [5].

2011-3. *Первое решение.* Если функция h непрерывно дифференцируема на $[1, R]$ и строго возрастает, то замена $t = h^{-1}(s)$ и интегрирование по частям дают

$$\int_1^R \frac{1}{h^{-1}(s)} ds = \int_1^{h^{-1}(R)} \frac{h'(t)}{t} dt = \int_1^{h^{-1}(R)} \frac{h(t)}{t^2} dt - 1 + \frac{R}{h^{-1}(R)}. \quad (1)$$

Это равенство остается в силе и без предположения о непрерывной дифференцируемости, ибо можно взять гладкие возрастающие функции

$$h_n(t) = \int_0^1 h\left(t + \frac{s}{n}\right) \varrho(s) ds,$$

где ϱ — гладкая функция с носителем в $[0, 1]$ и единичным интегралом, причем при $t > T$ мы полагаем $h(t) = h(T)$. Эти функции равномерно сходятся к h на $[1, R]$, строго возрастают, причем $h_n^{-1}(s) \rightarrow h^{-1}(s)$ при $s \in (0, T]$ (при фиксированном $s \in (0, T]$ значения $h_n^{-1}(s)$ определены при достаточно больших n). В самом деле, если $h_{n_k}^{-1}(s) \rightarrow y$, то $s = h_{n_k}(h_{n_k}^{-1}(s)) \rightarrow h(y)$, т. е. $y = h^{-1}(s)$. Тем самым (1) верно при наших условиях.

Если интеграл от функции $h(t)/t^2$ конечен, то найдется последовательность $t_n \rightarrow \infty$, для которой $h(t_n)/t_n \rightarrow 0$. Значит, $R_n = h(t_n) \rightarrow \infty$,

$R_n/h^{-1}(R_n) \rightarrow 0$, откуда следует доказываемое. Это же верно, если интеграл от функции $1/h^{-1}(s)$ конечен.

Второе решение. Пусть интеграл от функции $f(s) = 1/h^{-1}(s)$ конечен. Тогда интеграл от f по $[1, +\infty)$ равен площади под графиком f . Последняя по теореме Фубини равна интегралу по $t \in (0, 1)$ от длины множества

$$P_t = \{u \geq 1: f(u) \leq t\} = [1, h(t^{-1})],$$

ибо $f(1) = 1$, $f(u) \rightarrow 0$ при $u \rightarrow \infty$. Длина множества P_t равна $h(t^{-1}) - 1$. Наконец, замена $u = t^{-1}$ дает

$$\int_0^1 h(t^{-1}) dt = \int_1^\infty h(u)u^{-2} du.$$

Аналогично рассматривается случай, когда интеграл от функции $h(t)t^{-2}$ конечен.

2011-4. Пусть O – центр внешней сферы, а O_1, O_2 – центры внутренних сфер, M_1, M_2 – точки касания (M_i лежит на сфере с центром O_i , $i = 1, 2$). Из условия следует, что отрезок OA перпендикулярен плоскости, содержащей общие точки двух внутренних сфер, а значит, параллелен прямой O_1O_2 . Проведем сечение плоскостью, проходящей через точки O, O_1, O_2 . Эта плоскость содержит точки касания M_1, M_2 и точку A . Получаем две окружности с центрами O_1, O_2 , пересекающиеся в точке A и касающиеся изнутри в точках M_1, M_2 окружности с центром O . Надо доказать, что радиус R внешней окружности равна сумме радиусов $R_1 + R_2$ внутренних.

Обозначим $f(X) := XO_1 - XO_2$. Пусть B – вторая точка пересечения внутренних окружностей. Возьмем на прямой OA точку C такую, что O_1O_2AC – равнобедренная трапеция. Тогда O_1BO_2C – параллелограмм, откуда $CO_1 = R_2, CO_2 = R_1$, следовательно, $f(C) = CO_1 - CO_2 = R_2 - R_1$. Из касания окружностей заключаем, что $OO_1 + R_1 = OO_2 + R_2 = R$, откуда $f(O) = OO_1 - OO_2 = R_2 - R_1$. Так как функция $f(X)$ строго монотонна на прямой OA , то уравнение $f(C) = R_2 - R_1$ имеет не более одного решения $C \in OA$. Поэтому $C = O$, откуда $OO_1 = R_2$, и значит $R_2 + R_1 = R$.

Примечание. Центр большой окружности в сечении – это так называемая «точка двух велосипедистов» для двух маленьких окружностей [7]. У этой точки масса интересных свойств (только на международной олимпиаде школьников задачи, в которых эта точка так или иначе фигурировала, появлялись, как минимум, трижды).

2011-5. *Первое решение.* Так как H положительно определена, то $H = D^2$ для некоторой положительно определенной матрицы D . Обозначим $W := (A - A^t)/2$. Тогда $A = H + W = D(I + D^{-1}WD^{-1})D$. Так как W

кососимметрическая, то и $C := D^{-1}WD^{-1}$ кососимметрическая. Поэтому утверждение задачи вытекает из следующей леммы.

ЛЕММА. *Если вещественная матрица C кососимметрическая, то $\det(E + C) \geq 1$, где E — единичная матрица.*

Доказательство. Собственные числа матрицы C разбиваются на пары $(it, -it)$ с вещественными t . Для каждого из таких t имеем $(1 + it)(1 - it) \geq 1$. Перемножая по всем t (с учетом кратности) получаем требуемое. \square

Второе решение. Будем рассматривать матрицы A и H как матрицы квадратичных форм \mathcal{A} и \mathcal{H} , соответственно. В силу положительной определенности матрицы H существует базис, в котором форма \mathcal{H} имеет единичную матрицу E , то есть $E = C^T H C$ для некоторой невырожденной матрицы C . Матрица формы \mathcal{A} в этом базисе имеет вид $B = C^T A C$. Так как $\det H = (\det C)^{-2}$ и $\det A = \det B(\det C)^{-2}$, то достаточно доказать, что $\det B \geq 1$.

Так как $H = \frac{A + A^T}{2}$, то $E = \frac{B + B^T}{2}$. Поэтому матрица B представляется в виде $B = E + B'$, где B' — кососимметрическая матрица. Собственные значения матрицы B' чисто мнимые. Значит, собственные значения матрицы B имеют вид $1 + ti$, причем комплексные собственные значения разбиваются на пары сопряженных $1 \pm ti$, произведение которых равно $1 + t^2 > 1$. Определитель матрицы B равен произведению ее собственных значений, которые равны 1 или разбиваются на пары, произведение в которых больше 1. То есть $\det B \geq 1$.

Набросок третьего решения (оно встречалось в работах многих студентов). Приводим H к диагональному виду. Далее A представляется в виде суммы H и кососимметрической. Далее определитель A расписываем через сумму по перестановкам (обобщенным диагоналям). Объединяем перестановки в группы с одинаковыми неподвижными элементами. Тогда произведение соответствующих диагональных элементов матрицы H будет умножаться на минор кососимметрической матрицы, который неотрицателен. А для тождественной перестановки будет как раз $\det H$.

Набросок четвертого решения. Доказываем по индукции для неотрицательно определенной матрицы H . Приводим H к диагональному виду. Далее $\det A$ и $\det H$ линейно зависят от диагонального элемента a_{11} и коэффициент в $\det A$ не меньше по предположению индукции. Значит, достаточно доказать для $a_{11} = 0$. Аналогично, достаточно рассмотреть случай когда все диагональные элементы матрицы A равны нулю. Так как H диагональна, то в этом случае $H = 0$ и A кососимметрична. А определитель кососимметрической матрицы неотрицателен, что легко видеть из ее канонического вида.

ориентированная площадь параллелограмма, построенного на векторах \mathbf{a}_p и \mathbf{a}_q . Известно, что $\sum_{i=1}^{2r+1} \mathbf{a}_i = \mathbf{0}$ и направления векторов идут против часовой стрелки, причем если мы проведем прямую через ненулевой вектор \mathbf{a}_i , то векторы $\mathbf{a}_{i+1}, \dots, \mathbf{a}_{i+r}$ окажутся по одну сторону от нее, а векторы $\mathbf{a}_{i-1}, \dots, \mathbf{a}_{i-r}$ — по другую (это как раз условие неотрицательности $\Delta_{i,j}$ при $j = i + 1, \dots, i + r$). Отметим, что в каждой из частей данного неравенства записана сумма некоторых неотрицательных площадей $\Delta_{p,q}$ и функция ориентированной площади $S(\mathbf{u}, \mathbf{v})$ от пары векторов билинейна и кососимметрична.

Теперь перейдем к решению задачи по индукции по r . База индукции $r = 1$, тогда вектора три и утверждение проверяется непосредственно. Пусть $r > 1$. Возможны три случая:

(1) Среди данных векторов есть нулевой $\mathbf{a}_{i_0} = \mathbf{0}$ и $i_0 \neq 2r + 1$. Тогда удалим этот вектор, а векторы \mathbf{a}_{i_0+r} и \mathbf{a}_{i_0-r} заменим на их сумму. В получившемся наборе будет $2r - 1$ вектор, которые удовлетворяют условию задачи. При этом левая часть неравенства не изменилась, так как пара векторов \mathbf{a}_{i_0+r} и \mathbf{a}_{i_0-r} не разделялась ни одной прямой с направлением \mathbf{a}_i при $i \neq i_0$. Правая часть неравенства не увеличилась, так как в ней пропало слагаемое вида Δ_{i_0+r, i_0+r+1} , а все остальные слагаемые, в которых участвовали векторы \mathbf{a}_{i_0+r} или \mathbf{a}_{i_0-r} , сгруппировались по парам благодаря билинейности ориентированной площади.

(2) Найдется такое $i_0 \neq r + 1, 2r + 1$, что векторы \mathbf{a}_{i_0} и \mathbf{a}_{i_0+r} противоположно направлены. Тогда заменим один из этих векторов на их сумму, а второй \mathbf{x} на нулевой; опять же векторов стало $2r - 1$ и все условия задачи будут выполнены. При этом левая часть неравенства уменьшится на $3|S(\mathbf{x}, \mathbf{a}_{i_0} + \mathbf{a}_{i_0+1} + \dots + \mathbf{a}_{i_0+r})|$, а правая на $4|S(\mathbf{x}, \mathbf{a}_{i_0} + \mathbf{a}_{i_0+1} + \dots + \mathbf{a}_{i_0+r})|$, то есть разность правой и левой частей не увеличилась и мы перешли к случаю (1).

(3) Любые два вектора \mathbf{a}_i и \mathbf{a}_j при $i, j \neq 2r + 1$ линейно независимы. Начнем двигать конец вектора \mathbf{a}_{2r} вдоль вектора \mathbf{a}_r и соответственно уменьшать вектор \mathbf{a}_r , сохраняя нулевую сумму всех векторов, пока условие попарной линейной независимости сохраняется. Это условие нарушится либо если вектор \mathbf{a}_r станет нулевым (случай (1)), либо когда вектор \mathbf{a}_{2r} станет противоположно направлен вектору \mathbf{a}_{r-1} (случай (2)). Поэтому осталось показать, что при таком движении разность правой и левой частей не увеличивается. Пусть мы изменили каждый из двух векторов на вектор \mathbf{y} , тогда левая часть уменьшилась на $3|S(\mathbf{y}, \mathbf{a}_r + \mathbf{a}_{r+1} + \dots + \mathbf{a}_{2r})|$, а правая на $4|S(\mathbf{y}, \mathbf{a}_r + \mathbf{a}_{r+1} + \dots + \mathbf{a}_{2r})|$, то есть нужная разность не увеличилась.

Таким образом, утверждение индукции доказано.

Примечания. Отношение эти сумм не только не меньше 3, но и не больше 4. Константа 3 экстремальна, 4 — нет. Эта задача возникла из одной проблемы об исключительных наборах в производных категориях торических стеков Фано.

МБ-5. Ответ: да, существует. Можно взять $P(x) = ((10x - 1)^5 + 1)/10$. Легко проверить, что этот многочлен удовлетворяет условию.

Примечание. Придумать решение можно так. Ищем P в виде $Q/10$, где Q удовлетворяет условию $|Q(x) - 1| < 0.001$ и коэффициенты многочлена Q делятся на 10. Многочлен Q ищем в виде $Q(x) = (10x - 1)^n$ с нечетным n . Условие на x запишем в виде $|10x - 1| < 0.2$. Поэтому достаточно взять n таким, что $(0.2)^n < 0.001$.

МБ-6. Пусть M — данный многоугольник площади S_M , $A_1A_2A_3$ — данный треугольник площади S . Из условия следует, что каждая вершина треугольника лежит внутри M .

(Действительно, предположим, напротив, что некоторая вершина A_1 лежит вне многоугольника. Тогда ввиду выпуклости многоугольника прямые A_1A_2 и A_1A_3 делят его на три части. По условию площади двух «крайних» из этих частей равны половине площади многоугольника. Следовательно, площадь «средней» части равна нулю. Противоречие.)

Для $i = 1, 2, 3$ обозначим через S_i площадь пересечения многоугольника с углом, вертикальным к углу A_i треугольника, а через q_i обозначим площадь пересечения M с бесконечной фигурой, ограниченной стороной треугольника, противоположной вершине A_i , и продолжениями двух других сторон. Так как и A_1A_2 , и A_1A_3 делят площадь многоугольника M пополам, то $S_i = S + q_i \geq S$. Поэтому $S_M \geq S + S_1 + S_2 + S_3 \geq 4S$.

Примечания. Оценка $1/4$ не точна. Аналог утверждения задачи несправедлив для невыпуклых фигур. В решении нужна выпуклость, чтобы треугольник лежал внутри фигуры. Для невыпуклых он может не пересекаться с фигурой вовсе. На этом основан следующий *контрпример к аналогу задачи 6 для невыпуклых фигур*, придуманный В. Ю. Протасовым.

Возьмем правильный семиугольник $A_1 \dots A_7$. Убрав сторону A_1A_7 , получим шестизвенную ломаную. Каждая из прямых A_1A_4 , A_2A_5 и A_4A_7 делит периметр этой ломаной пополам. Заменим каждую сторону данной ломаной узкой прямоугольной полоской ширины $h > 0$. Получаем невыпуклый 14-угольник M (это шестизвенная «ломаная», «каждая сторона которой имеет толщину»). При $h \rightarrow 0$ площадь 14-угольника M стремится к нулю, а отношения, в которых каждая из прямых A_1A_4 , A_2A_5 и A_4A_7 делит площадь 14-угольника M , стремятся к $1/2$. Поэтому образы этих прямых при малом параллельном переносе делят площадь 14-угольника M пополам. При этом переносе площадь S треугольника, образованного

этими прямыми, изменится мало. Поэтому при малых h эта площадь будет больше площади 14-угольника M .

МБ-7. См. [3].

МБ-8. Авторам неизвестно решение этой задачи. Ср. [8].

ИНФОРМАЦИЯ О ПОБЕДИТЕЛЯХ

Вот призы заключительных туров: Антропов А. (2011), Ардинарцев Н. (2011), Балицкий А. (2011), Бажов И. (2010 и 2011), Бердников А. (2011), Брагин В. (2010), Горинов Е. (2010 и 2011), Григорьев С. (2010 и 2011), Девятков Р. (2010), Ивлев Ф. (2011), Калачев Г. (2011), Карпучин М. (2010), Карпушин В. (2010), Климовицкий И. (2011), Клочков Е. (2011), Мищенко П. (2011), Мокин В. (2011), Наумов В. (2010), Немиро В. (2011), Облакова А. (2010), Омеляненко В. (2011), Плосконосов А. (2011), Руденко Д. (2011), Савчик А. (2010), Тыщук К. (2011), Царьков О. (2011), Шмаров В. (2010 и 2011).

Составы команд на международную олимпиаду:

2010: Арутюнов В. (3-я премия), Бажов И. (1-я премия), Брагин В. (не участвовал ввиду отсутствия загранпаспорта), Горинов Е. (1-я премия), Девятков Р. (1-я премия), Шмаров В. (1-я премия).

2011: Бердников А. (1-я премия), Горинов Е. (1-я премия), Ивлев Ф. (2-я премия), Мокин В. (2-я премия), Облакова А. (3-я премия), Омеляненко В. (1-я премия), Царьков О. (3-я премия), Шмаров В. (1-я премия). Не участвовали по техническим причинам (отсутствие загранпаспорта или своевременной связи): Григорьев С., Антропов А., Калачев Г., Брагин В.

В неофициальном командном зачете команда заняла II место в 2010 году и VI место в 2011 году. Руководители команды М. П. Заплетин, К. В. Семенов и Н. А. Толмачев.

Матбой состоялся в день Пифагора 30.11.2010. Он организован студенческим советом во главе с А. Поповым. В команде первокурсников участвовали А. Бердников, Ф. Ивлев, Н. Медведь, А. Менщиков, В. Моксин и В. Омеляненко, а в команде преподавателей — А. Гайфуллин, С. Гайфуллин, А. Гарбер, В. Галатенко и О. Герман. Жюри: А. Скопенков и Н. Толмачев. Победила команда первокурсников.

Подробнее см. <http://www.universe.msu.ru>.

СПИСОК ЛИТЕРАТУРЫ

- [1] И. В. Аржанцев, В. И. Богачёв, А. А. Заславский, В. Ю. Протасов, А. М. Райгородский, А. Б. Скопенков. *Студенческие олимпиады мехмата МГУ // Математическое просвещение*. Сер. 3, вып. 14, 2010. С. 225–234.

- [2] В. И. Богачев, А. М. Райгородский, А. Б. Скопенков, Н. А. Толмачев. *Студенческие олимпиады и межкафедральный семинар на мехмате Московского государственного университета* // Математическое просвещение. Сер. 3, вып. 12, 2008. С. 205–222.
- [3] В. Брагин, А. Клячко, А. Скопенков. *Когда любая группа из n элементов циклическая?* 2011. arXiv:1108.5406v2.
- [4] И. Григорьев. *Порождение перестановок «восьмеркой»*. http://www.mcsme.ru/mmks/dec10/grigoryev_report.pdf (осторожно, там имеется ошибка!)
- [5] И. Григорьев. *Порождение перестановок циклами длины 3*. Неопубликованная рукопись.
- [6] T. Oda, H.S. Park. *Linear Gale transforms and Gel'fand-Kapranov-Zelevinskij decompositions* // Tohoku Math. J. (2) 43 (1991), no. 3, 375–399.
- [7] В. Ю. Протасов. *О двух велосипедистах и вишневого косточке* // Квант, 2008, №3. С. 41–45.
- [8] A. Rukhovich. *On intersection of two embedded spheres in 3-space*. 2010. arXiv:1012.0925v5.

И. В. Аржанцев, механико-математический факультет Московского государственного университета.

Email: arjantse@mcsme.ru

В. И. Богачёв, механико-математический факультет Московского государственного университета.

Email: vibogachev@yandex.ru

А. И. Гарбер, механико-математический факультет Московского государственного университета.

Email: alexeyigorevich@rambler.ru

А. А. Заславский, Центральный экономико-математический институт.

Email: zaslavsky@mcsme.ru

В. Ю. Протасов, механико-математический факультет Московского государственного университета.

Email: v-protassov@yandex.ru

А. Б. Скопенков, механико-математический факультет Московского государственного университета, Независимый московский университет, Московский институт открытого образования.

Email: skopenko@mcsme.ru

Инфо: <http://dfgm.math.msu.su/files/skopenkov/PAPERSCI.pdf>

Отклик на статью В. О. Мантурова

А. Б. Скопенков

В методической заметке [3] (разосланной в августе 2010 г. В. О. Мантурову и десятку других специалистов) приводятся четкая формулировка и короткое доказательство основного результата работы [1]. Доказательство по сути не отличается от приведенного в [1, 2]. Однако ввиду красоты и важности результата читателю может быть интересно короткое доказательство, освобожденное от ненужных деталей, с добавлением простых задач, поясняющих основную идею.

СПИСОК ЛИТЕРАТУРЫ

- [1] В. О. Мантуров. *Доказательство гипотезы Васильева о планарности сингулярных зацеплений* // Известия РАН. Т. 69. 2005. С. 169–178.
- [2] В. О. Мантуров. *Четырехвалентные графы с крестовой структурой* // Математическое просвещение. Сер. 3, вып. 15. 2011. С. 128–137.
- [3] А. Скопенков. *Вложения в плоскость графов с вершинами степени 4*. 2010. arXiv:1008.4940v1 <http://arxiv.org/abs/1008.4940>

Отклики на задачный раздел «Математического просвещения»

А. Б. Скопенков: В подписи к задаче 2008–3 следует заменить «А. Скопенков» на «А. Канель-Белов». Действительно, я не являюсь автором этого утверждения (трудно представить себе, чтобы оно было неизвестно до 1993 г., когда я предложил эту задачу на математический бой). Предложил эту задачу в задачник «Мат. Просвещения» А. Канель-Белов.

А. Ю. Эвнин: Задача 2011–2 была опубликована в отделе «Задачи» журнала «Математика в школе» под номером 3053 (решение этой задачи напечатано в №5 за 1987 г.). Размышления над этой задачей привели меня к более общим результатам, которые содержатся в моей статье [1] (частично эти результаты были опубликованы и в журнале «Математика в школе»).

СПИСОК ЛИТЕРАТУРЫ

- [1] А.Ю.Эвнин. *Период суммы двух периодических функций* // Вестник ЮУрГУ. Серия «Математика, физика, химия». №2, вып.5. 2005. С. 56–61. Сокр. эл. вариант:
http://pdf.vestnik.susu.ac.ru/mpc/05/08m056_Evnin_view.pdf

Задачный раздел

В этом разделе вниманию читателей предлагается подборка задач разной степени сложности, в основном трудных. 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.

В скобках после условия задачи приводится фамилия автора (уточнения со стороны читателей приветствуются).

1. Найти первообразную $\int \frac{x^2 dx}{(x \sin(x) + \cos(x))^2}$.
2. В Черноморске во время обсуждения вопроса о том, когда же наконец Черноморск объявят вольным городом, сложилась занятная ситуация. Все черноморцы разбились на партии, а все партии на фракции так, что: 1) существует партия, в которой объединились все n жителей города; 2) каждая партия состояла ровно из двух непересекающихся фракций; 3) каждая фракция численностью более одного человека считала себя партией. Каждый житель города платит членский взнос (1 руб.) в каждой партии, членом которой является. Как им надо было организовать, чтобы сумма взносов была: а) максимальной; б) минимальной? (*Д. В. Дерягин*)
3. Пусть у функции, определенной на отрезке [или на прямой], в каждой точке этого отрезка [прямой] есть конечный предел (не обязательно совпадающий со значением в точке). Насколько такая функция может отличаться от непрерывной? Более точно, каким может быть множество точек разрыва у такой функции? (*М. Прасолов*)
4. Ограничена ли последовательность $\{a_n\}$, заданная рекуррентно: $a_1 = 1$, $a_2 = x$, $a_{n+1} = (a_{n-1} \cdot a_n - 1)/a_{n-1}$, если $1 < x < 2$? (*К. Н. Игнатьев*)
5. Двумерная фигура в четырёхмерном пространстве имеет площадь S . Ее проекция на первые две координаты имеет площадь S_1 , а проекция на последние две координаты имеет площадь S_2 . Докажите, что $S \geq S_1 + S_2$. (*неравенство Виртингера*)

6. Дана инъекция $F: \mathbb{N} \rightarrow \mathbb{N}$. Когда из нее извлекается функциональный корень, т.е. существует отображение $G: \mathbb{N} \rightarrow \mathbb{N}$ такое, что $G \circ G = F$? Когда множество функциональных корней конечно? Ответ дать в терминах строения множества двусторонних орбит элементов. *Двусторонняя орбита* элемента x — это множество элементов вида $\{f^k(x)\}_{k \in \mathbb{Z}}$. (Н. Николов, Б. Станков)
7. В единичный шар вписано тело T , все ребра которого имеют длину не более 10^{-3} , а площадь его поверхности больше 10^3 . Докажите, что у него не менее 10^9 граней. (А. Я. Белов)
8. Даны два подмножества \mathbb{Z}_2^n — A и B . Известно, что $|A| + |B| > 2^k$. Докажите, что $|A + B| \geq 2^k$. ($A + B$ — это сумма Минковского двух множеств.) (Д. Фон-Дер-Флаас)
9. В алфавите Анчурского языка есть лишь три буквы: A , B и C . Два разных слова обозначают одно и то же понятие, если одно из них может быть получено из другого с помощью следующих операций, которые можно проводить в любой последовательности и в любых количествах:
- в любом месте слова можно заменять друг на друга следующие комбинации букв: ABA на BAB , ACA на CAC или BC на CB (и наоборот).
 - из любого места можно выкидывать две одинаковые буквы, идущие подряд, а также в любое место можно вставлять две одинаковые буквы.
- Конечное или бесконечное количество понятий можно выразить с помощью этого языка? Если конечное, то сколько?
 - Тот же вопрос, если замена BC на CB запрещена, однако разрешена замена BCB на CBC .
 - Тот же вопрос, если в алфавите две буквы A и B , свойство 2 сохраняется и из любого места можно выкидывать $(AB)^n$ и в любое место это вставлять.
- (В. О. Бугаенко)
10. Дан выпуклый n -угольник. Двое по-очереди проводят его стороны или диагонали. Запрещается проводить отрезок, имеющий общую точку с ранее проведенными (в том числе и общий конец). Проигрывает тот, кому некуда ходить. При каких n выигрывает начинающий?
11. При каких натуральных n число $\frac{3^n - 1}{2}$ есть квадрат целого числа? (Э. Б. Винберг)

12. а) Куб $n \times n \times n$ разбит на n^3 единичных кубиков, каждый раскрашен в один из трех цветов. Докажите, что найдется одноцветный путь, соединяющий противоположные грани большого кубика. Соседними считаются кубики имеющие хотя бы одну общую точку.
(Теорема Лебега о покрытиях)
- б) k -мерный куб $n \times n \cdots \times n$ разбит на n^k единичных кубиков, каждый раскрашен в один из l цветов. Докажите, что найдется связный кластер объема $C(k)n^{k+1-l}$.
(Г. В. Кондаков, А. Я. Белов)

Решения задач из предыдущих выпусков

7.6. УСЛОВИЕ. Ломаная L проходит по поверхности куба $n \times n \times n$, разбитой на квадратные клетки со стороной 1, и делит эту поверхность на две части — черную и белую. Вершины L находятся в центрах клеток, а звенья параллельны ребрам куба. При каких n площадь белой части может быть не равна площади черной?

ОТВЕТ: при $n = 1$ площадь белой части обязательно равна площади черной, а при любом $n > 1$ — нет.

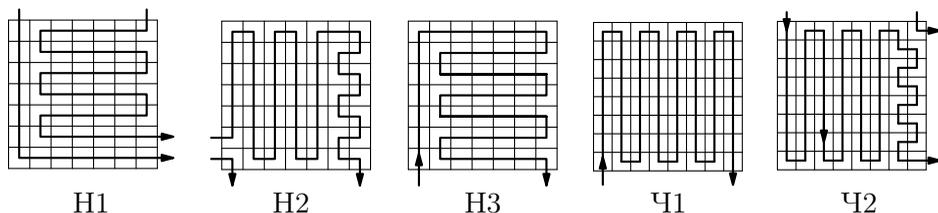
РЕШЕНИЕ. Сначала рассмотрим случай $n = 1$. Пусть ломаная, проходящая через середины всех граней, разбивает поверхность куба на две части Б и Ч. Заметим, что если часть Б или Ч содержит угол, то она содержит и три четвертинки граней, к нему примыкающих. Поэтому при $n = 1$ достаточно показать, что Б и Ч содержат ровно по 4 угла. Пусть какая-то часть содержит не 4 вершины. Тогда без ограничения общности можно считать, что часть Ч содержит ≤ 3 вершин.

Заметим, что ломаная L , удовлетворяющая условиям задачи, может пересечь ребро куба не более одного раза, а дуга, соединяющая точки одной компоненты, пересечена L четное число раз, поэтому ребро, соединяющее соседние вершины одной компоненты, не пересечено L . Пусть K — набор вершин одной компоненты (Б или Ч). Тогда он реберно связанный, ибо дугу C , соединяющую две такие вершины и не пересекающую L , можно непрерывно продеформировать в реберный путь внутри своей компоненты. В самом деле, пересечение открытой части Ч без границы с гранью куба есть либо вся грань, либо ее четвертинка с открытым участком границы, либо ее дополнение с открытым участком границы. В последних двух случаях это пересечение стягивается по себе на реберный каркас куба, а в первом случае оно стягивается при выбрасывании любой внутренней точки. Значит, стягивается и каждая часть с несколькими выброшенными точками (их можно выбрать не на C). Стягивание происходит вместе со всеми обитателями, в том числе и дугой C .

Имеется три возможности: Ч содержит одну вершину куба, две вершины куба (соединенные ребром) или же три вершины куба (соединенные парой перпендикулярных ребер). Легко видеть, что для каждого из этих случаев существует грань куба, через середину которой ломаная, охваты-

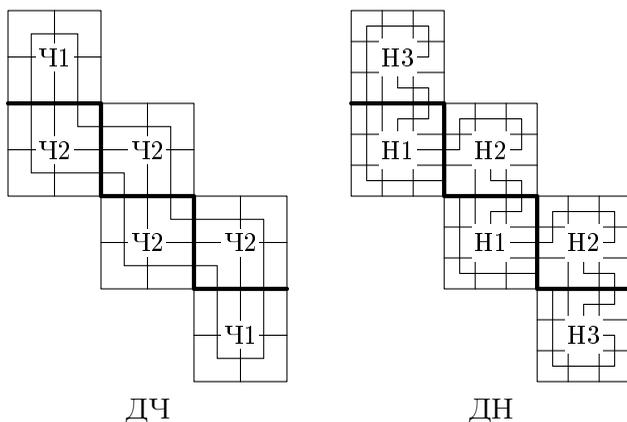
вающая выбранные вершины куба, не проходит. Следовательно, части Б и Ч содержат по 4 угла куба и равны по площади. Случай $n = 1$ разобран.

Теперь мы построим для каждого $n > 1$ пример замкнутой ломаной, проходящей через середины всех единичных квадратиков, расположенных на сторонах куба. Пример строится отдельно для четного и нечетного $n > 1$. На рисунках Н1, Н2, Н3, Ч1, Ч2 указано несколько способов провести ломаную через середины всех единичных квадратиков одной грани куба.



Примеры легко обобщаются на случай любого четного/нечетного числа $n \geq 2$ (предполагается, что читатель может это легко проверить).

- 1) Пусть $2 \mid n$. Последовательно соединяя картинки Ч1 и Ч2, как указано на картинке ДЧ, мы получаем замкнутую ломаную, проходящую через середины всех единичных квадратиков, расположенных на сторонах куба.
- 2) Пусть $2 \nmid n$. Последовательно соединяя картинки Н1, Н2 и Н3, как указано на картинке ДН, мы получаем замкнутую ломаную, проходящую через середины всех единичных квадратиков, расположенных на сторонах куба.



Заметим, что в каждом из указанных примеров построенная ломаная не пересекает границ развертки куба. Следовательно, по формуле Пика площадь, ограничиваемая ломаной, равна числу граничных вершин (их $6n^2$) пополам плюс число внутренних вершин (их нет) минус один. Таким

образом, в каждом из построенных примеров ломаная ограничивает фигуру площади $3n^2 - 1$. Откуда дополнение к ней имеет площадь $3n^2 + 1$. Таким образом, для всех $n \geq 2$ мы показали, что замкнутая ломаная может разбивать куб $n \times n \times n$ на две части разной площади, проходя через середины всех единичных квадратиков, расположенных на гранях куба.

(А. В. Петухов)

12.1. УСЛОВИЕ. Найти предел: $\lim_{x \rightarrow 0} \frac{\sin \operatorname{tg}(x) - \operatorname{tg} \sin(x)}{\arcsin \operatorname{arctg}(x) - \operatorname{arctg} \arcsin(x)}$.

РЕШЕНИЕ. Обозначим $\sin(\operatorname{tg}(x)) := f(x)$, $\operatorname{tg}(\sin(x)) := g(x)$. Требуется найти предел

$$\lim_{x \rightarrow 0} \frac{f(x) - g(x)}{g^{(-1)}(x) - f^{(-1)}(x)}.$$

Заметим, что f , g , $f^{(-1)}$ и $g^{(-1)}$ являются бесконечно дифференцируемыми функциями в окрестности нуля и все они сохраняют 0. Также заметим, что $\lim_{x \rightarrow 0} \frac{f(x)}{x} = 1$. То же самое верно для функций g , $f^{(-1)}$ и $g^{(-1)}$.

Пусть у функции $h(x) = g^{(-1)}(x) - f^{(-1)}(x)$ первые $k - 1$ производных в нуле являются нулями, а k -я производная нулем не является. Тогда

$$\lim_{x \rightarrow 0} \frac{g^{(-1)}(x) - f^{(-1)}(x)}{x^k} = \frac{\overbrace{h^{(k)} \cdots'}(0)}{k!}.$$

Вместо x подставим $f(x)$. Получим

$$\lim_{x \rightarrow 0} \frac{g^{(-1)}(f(x)) - f^{(-1)}(f(x))}{(f(x))^k} = \frac{\overbrace{h^{(k)} \cdots'}(0)}{k!}.$$

Следовательно,

$$\lim_{x \rightarrow 0} \frac{g^{(-1)}(x) - f^{(-1)}(x)}{g^{(-1)}(f(x)) - x} = 1.$$

Из того, что $\lim_{x \rightarrow 0} f^{(-1)}(x) = 1$, следует, что

$$\lim_{x \rightarrow 0} \frac{f^{(-1)}(f(x)) - f^{(-1)}(g(x))}{f(x) - g(x)} = 1.$$

Введем обозначение $f^{(-1)}(g(x)) = s(x)$. Тогда задача сводится к нахождению предела

$$\lim_{x \rightarrow 0} \frac{x - s(x)}{s^{(-1)}(x) - x}.$$

Если $s(x)$ в окрестности нуля разлагается в ряд Тейлора как

$$x + ax^k + \dots,$$

то ряд Тейлора функции $s^{(-1)}(x)$ имеет вид

$$x - ax^k + \dots$$

Следовательно, предел отношения числителя к знаменателю равен 1.

ЗАМЕЧАНИЕ. В. И. Арнольд очень любил с помощью этой задачи выявлять аналитическую культуру. Большинство студентов много раз применяло правило Лопиталья, вместо того, чтобы получить содержательное решение. (Н. Кудык)

12.3. УСЛОВИЕ. Вершины A и B графа G назовем *эквивалентными*, если существует такая последовательность вершин $A = A_0, A_1, \dots, A_n = B$, что любые две соседние вершины A_i и A_{i+1} можно соединить k путями без общих промежуточных вершин. Докажите, что любые две эквивалентные вершины можно соединить k путями без общих ребер.

ПЕРВОЕ РЕШЕНИЕ. Припишем ребрам исходного графа G пропускные способности, равные единице. Получаем взвешенный граф Γ . Из условия задачи следует, что никакой (реберный) разрез величины $k - 1$ не разбивает вершины A_i и A_{i+1} для любого i , а, значит, то же самое справедливо для вершин A_0 и A_n . Остается применить теорему Форда – Фалкерсона к графу Γ , источнику $u = A_0$ и стоку $w = A_n$. Формулировку теоремы Форда – Фалкерсона см. в статье М. Вялого и В. Гурвича на с. 82.

(А. Я. Белов)

ВТОРОЕ РЕШЕНИЕ. Преобразуем граф G следующим образом. Отметим на каждом ребре по точке, удублируем каждую вершину G (кроме A_0 и A_{n+1}) k раз и, если набор ребер имеет общую вершину, то соединим попарно соответствующие точки между собой и с дублями соответствующей вершины графа G . Легко видеть, что выбрасывание $k - 1$ вершины оставляет какие-то дубли A_i и A_{i+1} в одной связной компоненте, а значит и вершины A_0 и A_{n+1} . Остается применить теорему Менгера (см., например, статью А. Б. Скопенкова в этом выпуске, с. 48–49). (Г. Р. Челноков)

12.7. УСЛОВИЕ. а) Может ли определитель 10×10 матрицы с коэффициентами $0, \pm 1$ превосходить 2007? б) (Задача на исследование.) Оцените максимально возможный определитель для матрицы $n \times n$ с коэффициентами $0, \pm 1$.

РЕШЕНИЕ. Ответ в пункте а) положительный. Рассмотрим матрицу

$$A = \begin{pmatrix} H_8 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

где $H_8 = H_2^{\otimes 3}$ — матрица Адамара типа Сильвестра, а

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Столбцы (и строки) матрицы H_8 попарно ортогональны. Это легко проверить, если заметить, что при индексации строк и столбцов матрицы H_8 векторами из трехмерного пространства \mathbb{F}_2^3 над полем из двух элементов матричные элементы H_8 записываются как $H_8(u, v) = (-1)^{u \cdot v}$ ($u \cdot v$ — скалярное произведение над полем из двух элементов). Скалярное произведение столбцов H_8 записывается тогда как

$$\sum_{u \in \mathbb{F}_2^3} (-1)^{u \cdot v_1} (-1)^{u \cdot v_2} = \sum_{u \in \mathbb{F}_2^3} (-1)^{u \cdot (v_1 + v_2)}$$

и равно 0 при $v_1 \neq v_2$.

Итак, получаем

$$\det A = \det H_8 = (\sqrt{8})^8 = 2^{12} > 2007.$$

Пункт б) является очень трудной комбинаторной проблемой. Неравенство Адамара утверждает, что определитель матрицы (объем параллелепипеда) не превышает произведения евклидовых норм столбцов (длин ребер). Матрицы Адамара — это ± 1 -матрицы, достигающие эту границу. Матрицы Адамара могут существовать лишь для порядков 1, 2, $4n$ и известная гипотеза утверждает, что матрицы Адамара существуют для всех таких порядков. Эта гипотеза считается очень трудной и остается открытой с 1893 года. Наименьший порядок, кратный 4, для которого неизвестна матрица Адамара, равен 668. (М. Н. Вялый)

14.9. УСЛОВИЕ. Докажите, что при игре «Жизнь» а) в квадрате 2010×2010 ; б) на бесконечной плоскости найдется конфигурация без прообраза.¹⁾

РЕШЕНИЕ. А) Количество различных конфигураций квадрата конечно, и некоторые конфигурации «склеиваются» под действием шаблона, т. е. переходят в одну. (Например, конфигурации из одной и нуля черных точек.) Но тогда множество конфигураций следующего поколения имеет меньше элементов, чем множество всех конфигураций, и, тем самым, не может совпадать с ним.

¹⁾ Конвеевская игра «Жизнь» заключается в следующем: в некоторых клетках решетки стоит по фишке, а некоторые клетки пусты. Фишка, имеющая меньше двух соседей, умирает от одиночества, а имеющая больше трех соседей — от перенаселенности. На пустом поле, имеющем ровно три соседние фишки, рождается новая фишка. Клетки соседствуют по общим сторонам или общим вершинам. Состояния всех клеток меняются одновременно.

Идея решения п. б) состоит в использовании вместе с соображениями из доказательства п. а) того факта, что граница большой области имеет длину, много меньшую площади.

Рассмотрим квадратную область площади S . Число N способов отметить черные и белые вершины равно 2^S .

ОСНОВНАЯ ЛЕММА. *Существуют такие p, q , что при всех S «почти все» конфигурации разбиваются на серии, каждая из которых содержит по 2^{pS} конфигураций, и все конфигурации из одной серии склеиваются в следующем поколении.*

Выражение «почти все» означает, что количество конфигураций, не покрытых сериями, не превосходит $N \cdot 2^{qS}$.

Покажем, как из этого утверждения получить результат п. б).

Пусть $t = \min(p, q)$. Тогда при любой фиксированной раскраске границы квадрата число конфигураций в следующем поколении будет не более, чем $N \cdot 2^{-tS}$.

С другой стороны, имеется $4d\sqrt{S}$ способов осуществить раскраску границы квадрата ширины d , поэтому число возможных конфигураций в следующем поколении, отвечающих всем окраскам границы, не превосходит $N \cdot 2^{4d\sqrt{S}-tS}$, что при больших S меньше N , и доказательство завершает принцип Дирихле.

Перейдем к доказательству основной леммы. Прежде всего заметим, что конфигурации, состоящие из белого квадрата со стороной $2d + 1$ и из такого же квадрата с центральной черной клеткой, склеиваются в следующем поколении при любом «бордюре».

Поэтому достаточно показать, что если квадрат достаточно большой, то существуют такие p, q , что почти все (кроме, может быть, 2^{-qN}) раскрасок содержат не менее, чем pS конфигураций описанного выше вида.

Разрежем квадрат площади S на квадратики со стороной $2d + 1$. Обозначим каждую раскраску такого квадратики своей буквой (всего букв $2^{(2d+1)^2}$, общая раскраска кодируется словом длины $S/(2d + 1)^2$).

Тогда требуемое утверждение вытекает из следующей леммы (которая представляет собой частный случай закона больших чисел):

ЛЕММА. *Для любого $w > 0$ существует $t > 1$ такое, что относительное число выборов f сортов из n элементов, где количество элементов некоторого сорта лежит вне интервала $((1 - w)n/f, (1 + w)n/f)$, меньше, чем t^{-n} .*

ДОКАЗАТЕЛЬСТВО ЛЕММЫ. Будем уравнивать количества элементов из тех или иных сортов поэтапно. Отметим, что число возможных способов выбрать элементы из f сортов не превосходит n^f , что для любого $t > 1$

меньше, чем t^n (если n достаточно большое). Поэтому этим числом можно пренебречь.

Теперь покажем, что отношение числа выборок с описанным в лемме свойством к числу выборок с одинаковым числом предметов каждого сорта менее, чем t^{-n} . В самом деле, возьмем два сорта, отношения количеств в которых лежит вне интервала $(1 - w, 1 + w)$. Отношение числа этих выборок из двух сортов и равномерной выборки не больше $((1 - w)/4)^n$. Это можно установить с помощью формулы Стирлинга: $n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$.

ЗАМЕЧАНИЕ. По сути дела мы доказали более общий результат о том, что локально неоднозначная эволюция системы клеточных автоматов в пространстве имеет конфигурации без прообраза.

(А. Я. Белов, И. А. Иванов-Погодаев, А. С. Малистов)

Подготовка оригинал-макета: L^AT_EX2 ϵ ,
МЕТАРОСТ, М. Н. Вялый

Издательство Московского Центра
непрерывного математического
образования
119002, Москва, Большой Власьевский пер., 11. Тел. (499) 241 74 83

Отпечатано с готовых диапозитивов в ППП «Типография „Наука“».
121099, Москва, Шубинский пер., д. 6.

Подписано в печать 01.03.12. Формат 70×100/16. Бумага офсетная. Печать
офсетная. Печ. л. 15. Тираж 1000 экз. Заказ №