Московский государственный университет имени М. В. Ломоносова

Федеральное агентство правительственной связи и информации при Президенте Российской Федерации

Академия криптографии Российской Федерации

# Московский университет и развитие криптографии в России

Материалы конференции в МГУ 17–18 октября 2002 г.

**Сопредседатели конференции:**

Садовничий В. А. — ректор МГУ;
Шерстюк В. П. — первый зам. секретаря СБ РФ;
Матюхин В. Г. — генеральный директор ФАПСИ;
Андреев Н. Н. — президент АК РФ.

**Оргкомитет конференции:**

Михалев А. В. — председатель;
Носов В. А. — отв. секретарь;
Сачков В. Н. — АК РФ;
Чубариков В. Н. — МГУ;
Емельянов Г. В. — МГУ;
Применко Э. А. — МГУ;
Ященко В. В. — МГУ;
Крюкова Т. В. — МГУ;
Черепнев М. А. — МГУ;
Панкратьев А. Е.- МГУ;
Аносов В. Д. — ФАПСИ;
Логинов Ю. В. — ФАПСИ;
Федюкин М. В. — ФАПСИ;
Коваленко А. П. — ИКСИ.

**Программный комитет конференции:**

Сачков В. Н. — председатель;
Солодовников В. И. — отв. секретарь;
Нестеренко Ю. В. — МГУ;
Сидельников В. М. — МГУ;
Голованов П. Н. — ИКСИ;
Кузьмин А. С. — ФАПСИ;
Балакин Г. В. — ФАПСИ;
Зубков А. М. — РАН;
Ященко В. В. — МГУ;
Чечета С. И. — ИКСИ.

# Содержание

# Приветствие генерального директора ФАПСИ участникам конференции

## Уважаемые сотрудники и выпускники Московского государственного университета! Уважаемые коллеги!

Криптография — область человеческих знаний, насчитывающая в своей истории не одно тысячелетие. Несмотря на то, что при создании и анализе шифров издавна использовались математические методы, только качественный скачок, произошедший в ее развитии в сороковые годы прошлого века, позволил говорить о криптографии как о науке.

Именно в это время на механико-математическом факультете Московского государственного университета было создано отделение, на котором началась подготовка специалистов-криптографов. Поэтому можно смело утверждать, что становление и развитие криптографической науки в России происходило под определяющим влиянием научных идей, рожденных в МГУ.

Федеральное агентство правительственной связи и информации при Президенте Российской Федерации является головной организацией в России в области разработки криптографических средств защиты информации. Нам удается успешно справляться с поставленными задачами во многом благодаря труду и знаниям выпускников Московского государственного университета. По самым скромным подсчетам за время существования Федерального агентства в нем работало более пятисот выпускников МГУ.

Трудно переоценить вклад, который они внесли в развитие отечественной криптографической науки. За прошедшие 50 лет из стен Московского университета вышла целая плеяда ярких талантливых ученых-криптографов, многие из которых стали кандидатами и докторами наук, лауреатами Государственных и Ленинских премий СССР, Государственных премий Российской Федерации. Именно им можно в значительной мере поставить в заслугу то, что Россия сохраняет паритет в области развития криптографии с наиболее развитыми странами мира.

Надо сказать, что в нашу работу свой весомый вклад вносят не только математики, но и физики, лингвисты, экономисты и представители других многочисленных специальностей, которым учат в вашем Университете. Однако, помня о том, что наша конференция посвящена роли университета в развитии криптографии в России, считаю необходимым немного рассказать о сегодняшнем взаимодействии ФАПСИ и МГУ именно в этой области.

Необходимо сказать, что ректор Московского государственного университета Виктор Антонович Садовничий уделяет большое внимание проблемам информационной безопасности. Благодаря его инициативе организована сегодняшняя конференция, значителен его вклад как члена Научного совета при Совете Безопасности Российской Федерации в работу секции по информационной безопасности этого совета.

Благодаря поддержке Виктора Антоновича подписано соглашение о научно-техническом сотрудничестве между Московским государственным университетом и ФАПСИ. В рамках этого соглашения осуществляется взаимодействие в области исследования сложных математических проблем современной криптографии а также по другим направлениям информационной безопасности, включая компьютерную безопасность.

Основная роль в проведении исследований по криптографической тематике принадлежит Лаборатории МГУ по математическим проблемам криптографии. С момента создания в 1989 году лабораторией был проведен широкий спектр научных исследований по теории кодирования, теории сложности, теоретико-числовым криптографическим приложениям, приложениям к криптографическим методам защиты банковской информации, теории булевых функций и ряду других направлений.

Значительный импульс расширению тематики исследований был придан созданием в Университете в 1999 году кафедры информационной безопасности.

Расширилось сотрудничество в области компьютерной безопасности. В настоящее время в Московском университете проводятся работы, направленные на создание методов и средств динамического мониторинга локальных вычислительных сетей, предупреждение компьютерного нападения на информационные объекты, разработку средств тестирования защищенного программного обеспечения и ряд других.

Новым направлением сотрудничества стали работы в области квантовых коммуникаций и квантовых вычислений. Данное направление, с моей точки зрения, является весьма перспективным.

Важную роль для апробации научных идей и полученных результатов играет межведомственный междисциплинарный семинар по научным проблемам информационной безопасности, начавший свою работу в 2000 году и сразу завоевавший большой авторитет в ФАПСИ.

Сегодня нам предстоит познакомиться с наиболее интересными результатами в области криптографии, полученными в Московском государственном университете, Российской академии наук, ФАПСИ и Академии криптографии.

Еще раз хотел бы поблагодарить ректора МГУ Виктора Антоновича Садовничего за инициативу проведения этой конференции. Надеюсь, что научные связи между МГУ и ФАПСИ и впредь будут крепнуть и развиваться.

Желаю всем участникам конференции плодотворной работы, взаимного обогащения новыми научными идеями и замыслами.

Благодарю за внимание.

# Приветствие президента РАН участникам конференции

## Уважаемые коллеги!
## Уважаемые представители отечественной криптографической науки!

В настоящее время криптография стала одним из источников развития нескольких наукоемких и ресурсоемких областей техники и технологии. Из 52 позиций Перечня критических технологий, утвержденного 30 марта 2002 года Президентом Российской Федерации Владимиром Владимировичем Путиным, 6 позиций так или иначе связаны с реализацией криптографических задач и методов. Естественно, что для развития этих технологий в России необходимы серьезные продвижения в некоторых направлениях фундаментальной науки. При этом задачи криптографии, а в более широком плане — задачи обеспечения информационной безопасности России, лежат в основе целого ряда проблем и в естественных, и в технических, и в гуманитарных, и в социальных науках.

Именно поэтому сегодня мы собрались в Московском государственном университете им. М. В. Ломоносова — признанном лидере российской науки и образования, который способен для решения крупных междисциплинарных проблем собрать «в единый кулак» потенциал ученых из разных научных направлений. Это проявилось, в частности, и в развитии отечественной криптографии.

Становление криптографии как науки пришлось на вторую половину XX века при активном участии выпускников МГУ. Назову лишь несколько наиболее ярких имен — академик Колмогоров Андрей Николаевич, члены-корреспонденты Марков Андрей Андреевич, Гельфонд Александр Осипович, Козлов Владимир Яковлевич, вице-президент Академии криптографии РФ Сачков Владимир Николаевич.

Качественный скачок в развитии отечественной криптографии произошел в 90-е годы XX века. В 1991 году несколько членов Российской академии наук — в основном, выпускников МГУ — выступили с инициативой создания Академии криптографии Российской Федерации. Это академики РАН Котельников Владимир Александрович, Прохоров Юрий Васильевич, члены-корреспонденты РАН Козлов Владимир Яковлевич, Севастьянов Борис Александрович, Левин Владимир Константинович. Российская Академия наук поддержала это предложение и 5 июня 1992 года Указом Президента Российской Федерации Академия криптографии была создана. За прошедшие 10 лет Академия криптографии стала ведущим научным центром в области криптографических исследований в России.

Желаю всем участникам конференции успешной и плодотворной работы!

# Криптография как один из источников развития математики

В. А. Садовничий, В. А. Носов, В. В. Ященко

## Уважаемые коллеги!

Любое общество не может гармонично развиваться без производства информации, ее накопления и обмена информацией. С другой стороны, в обществе всегда была и есть необходимость разграничивать круг лиц, для которых предназначена та или иная информация. Поэтому возникла и стала интенсивно развиваться криптография — наука о способах сокрытия информации от непосвященных лиц. Фактически криптография — ровесница письменности. Она в своем развитии прошла через этапы «криптография как искусство» и «криптография как ремесло» к этапу «криптография как наука». Последний этап начался совсем недавно — в сороковые годы двадцатого века. В это время почти одновременно два выдающихся ученых — Владимир Александрович Котельников в России и Клод Шеннон в США — заложили теоретико-информационные основы криптографии. Однако криптография, став наукой, продолжает оставаться и искусством, и ремеслом, поэтому в ней и в настоящее время присутствует больше практических наблюдений и рекомендаций, чем строгих теорем, что существенно отличает криптографию от математики. Но и математика, и криптография всегда развивались в тесном взаимодействии, взаимно обогащая друг друга. В настоящем докладе мы обсудим основную проблематику современной открытой криптографии, более подробное освещение она найдет в других докладах конференции. Следует подчеркнуть, что слова «открытая криптография» мы употребляем условно в смысле «открытые научные исследования в интересах криптографии». Криптография как наука едина, но в настоящее время одни научные направления в ней могут плодотворно развиваться только в открытом режиме, как составная часть соответствующих математических направлений, в то время как другие направления, слишком тесно связанные с приложениями, должны развиваться только в закрытом режиме в специализированных организациях.

Главная функция криптографии — защита информации. Длительное время криптография во всех странах развивалась под эгидой ведомств, отвечающих за безопасность связи и информации, и во многом представляла собой набор практических способов и рецептов защиты информации. С развитием средств связи — телеграфа, телефона, радио — менялся характер криптографии, а с началом применения электронных средств передачи информации задачи криптографии усложнились и расширились. В настоящее время, когда компьютерные технологии получили массовое распространение, проблематика криптографии преобразилась и пополнилась многочисленными задачами, которые не связаны непосредственно с засекречиванием информации. Перечислим некоторые из них: разработка систем электронной цифровой подписи, протоколов выборов, подписания контракта и идентификации удаленных пользователей, методов защиты от навязывания ложных сообщений и систем электронных платежей.

Поэтому и значение криптографии в жизни общества продолжает возрастать. Недаром Дэвид Кан, автор фундаментального труда «Взломщики кодов», сказал: «Великая держава — это страна, которая владеет ядерными технологиями, ракетной техникой и криптографией». С этим нельзя не согласиться. А вот что сказал Ривест — один из соавторов системы шифра RSA: «Криптография является повивальной бабкой всех компьютерных наук». Еще более сильно выразились авторы фундаментального труда «Абстрактная прикладная алгебра» Р. Лидл и Г. Пильц — «Современная криптография может быть охарактеризована и как важная многомиллионодолларовая проблема, и как раздел прикладной математики». Они имеют в виду проблему получения доказуемых и адекватных нижних оценок стойкости шифров и, в частности, шифров с открытым ключом. В математическом плане это один из частных случаев фундаментальной проблемы нижних оценок сложности алгоритмов.

Как уже отмечалось, глубокое понимание математического характера криптографии началось с работ К. Шеннона. Его основополагающая работа «Математическая теория криптографии» в секретном варианте была выполнена в 1945 году, а рассекречена и опубликована в США в 1949 году. В 1963 году по инициативе Андрея Николаевича Колмогорова сборник работ К. Шеннона был издан и на русском языке с предисловием Андрея Николаевича. В 60-х годах были рассекречены и опубликованы результаты исследований немецкой шифрмашины «Энигма» и связанные с этим результаты по решению уравнений в подстановках. В 70-х годах была опубликована революционная работа молодых американских ученых У. Диффи и М. Хеллмана «Новые направления в криптографии». С этого момента наблюдается лавинообразный рост числа публикаций по криптографии. Причины этого разнообразны. С одной стороны — постоянное расширение областей применения криптографии, о чем мы уже говорили. С другой стороны — новизна и привлекательность для ученых математических моделей и задач, которые возникают из потребностей криптографии. И наконец — именно в этот период формируются все атрибуты криптографии, как науки: возникают направления и научные школы со своей внутренней логикой развития, появляются специализированные международные журналы, закрепляется практика ежегодного проведения международных конференций.

Следует подчеркнуть, что формирование криптографии как науки проходило во второй половине XX-го века при определяющем влиянии математики. Вместе с тем криптография является наукой, использующей достижения и многих других наук. Например, результаты таких наук, как физика, теория связи, науки кибернетического цикла находят использование в криптографии и, с другой стороны, задачи и результаты криптографии влияют на проблематику этих наук. В последние годы ряд криптографических идей и методов стал ядром новых междисциплинарных научных направлений, связанных с обеспечением информационной безопасности. В эту орбиту оказались вовлечены и юридические, и гуманитарные, и социальные науки.

Однако математический аппарат продолжает оставаться основным в криптографии. Ведь не случайно в многовековую историю криптографии вписано много имен видных математиков. Приведем лишь несколько наиболее ярких примеров.

**Аристотель** (384–322 до н. э.), древнегреческий ученый, участник Академии Платона, учитель Александра Македонского, охватил почти все доступные в то время знания. Перед математикой его заслуга состоит в том, что он дал первое систематическое изложение логики и теории доказательств. В криптографии известен как автор способа вскрытия шифра «сцитала».

**Кардано Джероламо** (1501–1576), итальянский математик. С его именем в математике связывают формулу Кардано для решения неполных кубических уравнений, он ввел мнимые корни уравнений. В криптографии Кардано известен изобретением шифра, называемого «решеткой Кардано».

**Виет Франсуа** (1540–1603), французский математик. Он известен тем, что ввел в алгебру буквенные обозначения как для неизвестных величин, так и для коэффициентов. Его «формула Виета» связывает коэффициенты уравнения с его корнями. В криптографии Виет известен успешной дешифровальной работой при дворе короля Генриха IV.

**Валлис Джон** (1616–1703). Английский математик, один из основателей Лондонского математического общества. Внес значительный вклад в развитие интегрального исчисления. Валлис также успешно занимался дешифровальной работой.

**Эйлер Леонард** (1707–1783), швейцарский математик, большую часть жизни провел в России. Внес существенный вклад во все разделы математического анализа. Принимал участие в разработке российских государственных шифров.

**Тьюринг Алан** (1912–1954), английский математик, член Лондонского королевского общества. Выполнил цикл работ по математической логике и вычислительной математике. Автор формализации понятия алгоритма в виде абстрактной вычислительной машины (машины Тьюринга). Принимал непосредственное участие в дешифровании немецкой шифровальной машины Enigma. Автор концепции построения специализированной вычислительной машины для перебора ключей.

**Шеннон Клод Эльвуд** (1916–2001). В 1963 году Андрей Николаевич Колмогоров, представляя читателям русский перевод сборника работ К. Шеннона, писал в предисловии: «В наш век возрастающей дифференциации человеческих знаний Клод Шеннон является исключительным примером соединения глубины отвлеченной математической мысли с широким и в то же время совершенно конкретным пониманием больших проблем техники. Его в равной мере можно считать одним из первых математиков и одним из первых инженеров последних десятилетий.».

Поскольку о вкладе выпускников МГУ в развитие отечественной криптографии у нас запланирован отдельный доклад, здесь мы назовем лишь три имени.

**Марков Андрей Андреевич** (1903–1979). Разработал теорию нормальных алгоритмов, называемых теперь алгоритмами Маркова, и доказал алгоритмическую неразрешимость некоторых задач алгебры, в частности, неразрешимость проблемы тождества слов в конечно определенных полугруппах. Он имеет многочисленные работы в области криптографии. Наиболее известна «теорема Маркова», которая классифицирует шифры, не распространяющие искажения.

**Гельфонд Александр Осипович** (1906–1968). Выпускник МГУ 1927 года. Решил седьмую проблему Гильберта о трансцендентности степени алгебраического числа в иррациональной алгебраической степени. Занимался решением многих криптографических задач, в частности, задачи дискретного логарифмирования.

**Колмогоров Андрей Николаевич** (1903–1987). Выпускник МГУ 1925 года. Внес существенный вклад во многие разделы математики. В криптографии нашли применение его работы по теории информации и теории вероятностей, в частности, его критерии случайности последовательностей.

Остановимся теперь коротко на тех направлениях математики, которые испытывали наибольшее влияние задач криптографии и в которых имеется много результатов с «криптографическими корнями».

**Алгебра.** Здесь в первую очередь следует назвать теорию конечных групп и особенно теорию групп подстановок, теорию конечных полей и особенно теорию уравнений над конечными полями, теорию рекуррентных последовательностей на алгебраических структурах, теорию универсальных алгебр.

**Теория вероятностей.** Теория вероятностей во многом возникла как прикладная наука. В связи с потребностями криптографии дополнительный стимул для развития получили теории случайных последовательностей и процессов, исследования по изучению свойств «случайных» комбинаторных объектов.

**Комбинаторный анализ.** Данная наука во многом развивалась в интересах криптографических приложений. Особенно это касается перечислительных проблем, связанных с подстановками, латинскими квадратами, дискретными функциями. Не случайно фундаментальный двухтомный труд по комбинаторике был написан в 1915 году английским майором Макмагоном.

**Теория чисел.** В настоящее время здесь наблюдается подлинный бум в связи с широким распространением криптографических идей Диффи и Хеллмана, а также криптографической схемы RSA. Только благодаря криптографии любые продвижения в таких теоретико-числовых задачах, как «задача факторизации», «задача дискретного логарифмирования», «задача проверки простоты», теперь выплескиваются даже на газетные полосы.

**Теория информации.** Даже само создание теории информации во многом обязано криптографии. Основополагающие работы К. Шеннона по криптографии и теории информации выполнены практически одновременно. И в своем дальнейшем развитии теория информации постоянно подпитывается проблематикой криптографии.

**Теория кодирования.** Основоположником теории кодирования также является К. Шеннон. Многие постановки задач в теории кодирования близки постановкам задач в криптографии, поэтому в криптографии широко применяются методы и результаты теории кодирования.

**Дискретная математика.** Данное направление получило развитие во многом благодаря потребностям компьютерных наук и криптографии. В частности, это относится к теории булевых функций, функций многозначной логики и теории автоматов. Именно с их помощью чаще всего описываются преобразования информации, реализуемые в шифраторах. Поэтому задачи анализа шифров являются одним из источников задач для дискретной математики.

**Компьютерные науки.** Началом данному направлению послужили идеи по формализации процесса алгоритмического вычисления и построению специализированной вычислительной машины для дешифрования. Данные идеи оказались плодотворными и при разработке современных суперкомпьютеров. Для большинства суперкомпьютеров, разработанных в XX-м веке, основным заказчиком и потребителем была криптография.

Более подробно хочется остановиться на двух направлениях, которые возникли под влиянием задач криптографии в последние 10–15 лет.

Направление «сложность алгоритмов и вычислений» — одно из направлений в компьютерных науках — сразу после своего возникновения получило криптографическую окраску. Теоретико-сложностной подход к оценке стойкости криптосистем широко применяется наряду с теоретико-информационным. Когда под влиянием идей Диффи и Хеллмана стали разрабатываться многочисленные криптографические протоколы, теоретико-сложностной подход стал основным для их изучения. Осмысление

различных криптографических протоколов и методов их построения привело в 1985–1986 гг. к появлению двух плодотворных математических моделей — интерактивной системы доказательства и доказательства с нулевым разглашением. На основе этих моделей в математической логике и теории сложности в настоящее время разрабатывается математический аппарат, наиболее адекватно отражающий проблематику «новой криптографии».

Идея использовать в интересах криптографии законы квантового мира давно витала в воздухе. Но лишь в последние годы она приобретает реальные очертания в виде концепций квантовых коммуникаций и квантовых вычислений. Разработка этих концепций потребовала объединения усилий высококвалифицированных специалистов из разных направлений — криптографов, физиков, математиков, компьютерщиков. Такой коллектив уже два года работает и в Москве, в нем — ученые из МГУ, ФАПСИ, РАН, Академии криптографии. Реализация идей квантового компьютера и квантовых коммуникаций приведет к революционным изменениям в ряде областей науки и техники и может серьезно повлиять на состояние безопасности страны, в частности, информационной безопасности.

В заключение еще раз вернемся к мысли о том, что в настоящее время регулярно проводятся международные криптографические конференции. Одна из наиболее авторитетных конференций по криптографии — Eurocrypt. График проведения этой конференции составлен уже до 2005 года. Так, в 2003 году Eurocrypt проводит Польша, а в 2004 году — Швейцария. Многие европейские страны уже проводили у себя конференцию Eurocrypt. Сегодня на нашей конференции естественно поставить вопрос о приглашении конференции Eurocrypt в Россию. Это послужит дополнительным импульсом для консолидации российских ученых, которые проводят открытые научные исследования в интересах криптографии. Хотелось бы и нашу конференцию проводить ежегодно, сделав ее полномасштабной: с секционными докладами и охватом всех математических проблем информационной безопасности. Думаю, что все участники конференции поддержат эти предложения и мы попросим бюро нашего Оргкомитета продолжить работу и в будущем.

# Краткий исторический очерк развития криптографии

В. А. Носов

## 1 Введение

В настоящее время нет недостатка в материалах по истории криптографии — достаточно заглянуть на соответствующие сайты Интернет. В данном очерке делается попытка проследить историю криптографии и присутствия в ней математиков. Основное внимание уделено не именам и датам, а развитию криптографических идей и участию в этом процессе математиков.

## 2 Криптография древнего периода

Криптография возникла вместе с письменностью. В исторических документах древних цивилизаций Индии, Египта, Месопотамии имеются сведения о системах и способах составления шифрованного письма. Так, в древнеиндийских рукописях содержится изложение 64-х способов преобразования текста. Среди них написание знаков не по порядку, а вразброс по некоторому правилу. Многие из приводимых способов следует рассматривать как криптографические, т. е. обеспечивающие секретность переписки. Приведена система замены букв. Упоминается, что тайнопись является одним их 64-х искусств, которым следует владеть как мужчинам, так и женщинам.

Более достоверные сведения о применяемых системах шифров относятся к периоду возникновения государств древней Греции. В Спарте в V–VI веке до нашей эры существовала хорошо развитая криптография. К этому времени относятся описания двух известных приборов для шифрования — Сцитала и таблица Энея, которые осуществляют перестановку букв в тексте и замену букв открытого текста отрезками на прямой. Эней в сочинении «Об обороне укрепленных мест» описывает так называемый «книжный шифр». Полибий описывает систему шифра, называемую «квадрат Полибия», представляющую собой замену каждой буквы парой чисел — координатами буквы в квадрате $5 \times 5$, в котором написаны буквы алфавита. Юлий Цезарь в книге «Записки о галльской войне» описывает шифр, в котором буквы заменяются в соответствии с подстановкой, в которой каждая буква сдвинута на три позиции вправо.

В математике этого периода накапливается материал, относящийся к началам арифметики и геометрии. В этот период появляются правила вычисления площади треугольника и трапеции, объемы пирамиды с квадратным основанием, правила решения простейших квадратных уравнений, теорема Пифагора и формула для суммы арифметической прогрессии.

Потребителями криптографии в этот период являются структуры административной и религиозной власти. Плутарх сообщает, что жрецы хранили тексты прорицателей в зашифрованном виде.

Э. Шюре в книге «Великие посвященные» сообщает, что «с великим трудом и большой ценой добыл Платон один из манускриптов Пифагора, который никогда не записывал свое эзотерическое учение иначе, как тайными знаками и под различными символами». Там же отмечается, что Аристотель получил от Платона шифрованный текст Пифагора. Платону принадлежит метод доказательства «от противного», а Аристотель заложил основы теории логического вывода и теории доказательств. Аристотелю приписывается метод дешифрования шифра сцитала.

## 3 Криптография арабского мира

В период расцвета арабских государств (VIII век н. э.) криптография получила новое развитие. Слово «шифр» арабского происхождения, так же как и слово «цифра». В 855 году появляется «Книга о большом стремлении человека разгадать загадки древней письменности», в которой приводятся описания систем шифров, в том числе и с применением нескольких шифралфавитов. В 1412 году издается 14-томная энциклопедия, содержащая обзор всех научных сведений — «Шауба аль-Аша». Составитель ее Шехаб аль Кашканди. В данной энциклопедии содержится раздел о криптографии, в котором приводятся описания всех известных способов шифрования. В этом разделе имеется упоминание о криптоанализе системы шифра, который основан на частотных характеристиках открытого и шифрованного текста. Приводится частота встречаемости букв арабского языка на основе изучения текста Корана.

Что касается математики арабского мира, то следует упомянуть следующие выдающиеся достижения. Сочинение Мухаммеда бен Муса аль-Хорезми (IX век) по правилам арифметики в позиционной системе счисления, от названия которого появились два термина «алгебра» и «алгоритм». Трактат по тригонометрическим функциям Аль-Баттани (IX век). Вычисление числа «пи» с 17 десятичными знаками (ок. 1427) аль Каши, сотрудником Улугбека.

## 4 Криптография в эпоху Возрождения (XIV–XVI вв.)

До эпохи Возрождения имеется мало сведений о применяемых шифрах. Известен ряд значковых шифров, при котором буквы открытого текста заменяются на специальные знаки. Таким является шифр Карла Великого (780–814 г.). Известен так называемый «еврейский шифр», в котором замена букв осуществляется по подстановке, в которой нижняя строка образуется так: алфавит разбивается на две половины. Буквы второй половины пишутся под буквами первой половины в обратном порядке. Аналогично поступают с остальными буквами.

В эпоху Возрождения в итальянских городах-государствах стали расцветать науки и ремесла. Шифры применяются не только государственной или церковной властью, но и учеными для защиты приоритета научных открытий (Галилей). В XIV веке появляется книга Чикко Симонетти, сотрудника канцелярии папской курии. В этой книге описаны шифры замены, в которых гласным буквам ставятся в соответствие несколько знаков с целью выравнивания частот букв в шифртексте. Дано описание лозунгового шифра, в котором замена букв определяется так: под алфавитом пишутся различные буквы лозунга в порядке появления, а затем буквы, не появившиеся в лозунге. В XV веке появляется книга Габриэля де Лавинда, секретаря Папы Клементия XII, «Трактат о шифрах», в которой дается описание шифра пропорциональной замены. Шифр обеспечивает замену букв несколькими символами, пропорционально встречаемости букв в открытом тексте. Дается рекомендация заменять имена, должности, географические названия специальными знаками.В этот период в Милане применяется шифр, названный «Миланский ключ», представляющий собой значковый шифр пропорциональной замены.

В 1466 году Леон Альберти, знаменитый архитектор и философ представил трактат о шифрах в папскую канцелярию. В трактате рассматриваются различные способы шифрования, в том числе маскировка открытого текста в некотором вспомогательном тексте. Работа завершается собственным шифром, который он назвал «шифр, достойный королей». Это был многоалфавитный шифр, реализованный в виде шифровального диска.

Суть заключается в том, что в данном шифре используется несколько замен в соответствии с ключом. Позднее Альберти изобрел код с перешифровкой. Данное изобретение значительно опередило свое время, поскольку данный тип шифра стал применяться в странах Европы лишь 400 лет спустя.

В 1518 году в развитии криптографии был сделан новый шаг благодаря появлению в Германии первой печатной книги по криптографии. Аббат Иоганнес Тритемий, настоятель монастыря в Вюрцбурге, написал книгу «Полиграфия», в которой дается описание ряда шифров. Один из них развивает идею многоалфавитной замены. Шифрование осуществляется так: Заготавливается таблица замены, в которой первая строка есть алфавит, вторая строка есть алфавит, сдвинутый на один шаг и т. д. При шифровании первая буква открытого текста заменяется на букву, стоящую в первой строке, вторая буква — на букву, стоящую во второй строке и т. д. В 1553 году в Италии вышла небольшая книга «Шифр синьора Белазо». Об авторе Джованни Белазо известно мало. Его вклад заключается

в следующем. Он предложил использовать слово или группу слов, назвав это «паролем», выписывая его над (под) открытым текстом. Буква пароля означает номер применяемой замены к букве открытого текста. В начале XVI века Маттео Арженти, криптограф папской канцелярии изобрел код, представляющий собой шифр замены, в котором заменяются буквы, слоги, слова и целые фразы. Необходимым количеством словарных величин в коде считалось 1200. В это же время появляется и числовой код.

Следующий шаг в развитии криптографии был сделан Джованни Порта, известным итальянским естествоиспытателем. В 1563 году он написал книгу «О тайной переписке», в которой приводится описание всех известных систем шифров. Дается также описание биграммного шифра, в котором осуществляется замена пар букв. Порта предвосхитил то, что называют «методом вероятного слова» и приводит примеры списков вероятных слов из различных областей. Примерно в то же время итальянский математик и философ Джероламо Кардано, автор многочисленных книг по различным вопросам написал книгу «О тонкостях», в которой имеется часть, посвященная криптографии. Его вклад содержит два предложения. Первое — использовать открытый текст в качестве ключа. Второе — он предложил шифр, называемый ныне «Решетка Кардано». Кроме данных предложений Кардано дает «доказательство» стойкости шифров, основанное на подсчете числа ключей.

В том же XVI веке был сделан еще существенный шаг в развитии криптографии. Блез Виженер, французский посол в Риме, познакомился там с трудами по криптографии и в 1585 году написал книгу «Трактат о шифрах», в которой он излагает основы криптографии. Ему принадлежит мысль «Все вещи в мире представляют собой шифр. Вся природа является просто шифром и секретным письмом». Эту мысль повторил позднее Блез Паскаль и в наше время Норберт Винер. Предложение Виженера во многом развивает идею Кардано о применении открытого или шифрованного текста в качестве ключа.

Прогресс в математике в этот период характеризуется трудами Леонардо Фибоначчи, в которых излагается арифметика, алгебра и геометрия. Для вычислений используется сходимость геометрической прогрессии. Н. Орем установил расходимость гармонического ряда, строгое доказательство этого появится только в XVII веке. Кардано при решении уравнений третьей степени вводит отрицательные и мнимые корни и устанавливает известную «формулу Кардано». Алгебра получает развитие у Ф. Виета, который установил связь коэффициентов алгебраических уравнений и корней (формула Виета). Он же начал использовать буквенные обозначения для коэффициентов уравнений, до него это использовалось лишь для корней. Ф. Виет привлекался к дешифровальной работе при дворе Генриха IV и успешно дешифровал переписку испанского короля Филиппа II. Отметим, что великий ученый и художник эпохи Возрождения Леонардо да Винчи (1452–1519) владел криптографией и пользовался ею, в частности, в своих рукописях.

# 5 Криптография в XVII–XVIII веках

XVII век называют эрой «черных кабинетов», поскольку в этот период создаются дешифровальные службы. Так, в Англии Оливер Кромвель создает «Интеллиженс сервис» — разведывательную службу, в которой появляется дешифровальное отделение. В середине XVII века к дешифровальной работе привлекается известный математик Джон Валлис (1616–1703). Он является автором фундаментального труда «Арифметика бесконечного» (1655). Хорошо известна «формула Валлиса», дающая представление числа «пи» в виде бесконечного произведения. Во Франции при Людовике XIV по предложению кадинала Ришелье создается дешифровальное отделение, которое возглавил Антуан Россиньоль. Россиньолю принадлежит доктрина: стойкость военного шифра должна быть такой, чтобы обеспечить секретность донесения в течение срока, необходимого для выполнения приказа. Стойкость дипломатического шифра должна обеспечивать секретность в течение нескольких десятков лет. Сам Ришелье оставил след в криптографии благодаря известному «шифру Ришелье», который представляет собой шифр перестановки, при котором открытый текст разбивается на отрезки, а внутри каждого отрезка буквы переставляются в соответствии с фиксированной перестановкой.

Россиньоль разработал дипломатический шифр, представляющий собой слогово-словарный код на 600 величин.

В Германии в это время также создается дешифровальное отделение, которое возглавляет граф Гронсфельд. Ему принадлежит усовершенствование шифра Виженера, заключающееся в том, что вместо буквенного лозунга применяется цифровой, а значение цифры в лозунге означает число ша-

гов, на которое надо сдвинуть букву открытого текста вправо по алфавиту в стандартной записи. Данный шифр получил широкое распространение благодаря простоте применения. Таким образом, дешифровальные подразделения становятся обычным делом. Что касается шифров, то в этот период применяются, в основном, коды различной степени сложности. Из других шифров следует упомянуть «масонский шифр», представляющий собой оригинальный значковый шифр, в котором из написания алфавита на двух крестах — прямом и косом — извлекались знаки для замены букв. Наполеон во время своих походов использовал шифры, являющиеся вариантами шифра Россиньоля и представляющие собой код на 200 шифрвеличин.

Криптография в России развивалась по пути христианских стран. Датой появления криптографической службы следует считать 1549 год (царствование Ивана IV), с момента образования «посольского приказа», в котором имелось «цифирное отделение». Используемые шифры — такие же как в западных странах — значковые, замены, перестановки. Петр I полностью реорганизовал криптографическую службу, создав «Посольскую канцелярию». В это время применяются для шифрования коды, как приложения к «цифирным азбукам». В знаменитом «деле царевича Алексея» в обвинительных материалах фигурировали и «цифирные азбуки».

Математика XVII–XVIII века получает существенное и качественно новое развитие. Н. Бурбаки называют этот период «героической эпохой». Назовем только некоторых авторов открытий. Изобретатель логарифмов — Дж. Непер, шотландский математик, его «Описание удивительной таблицы логарифмов» было издано в 1614 году. Декарт Рене, французский математик, заложил основы аналитической геометрии. Его фундаментальный труд «Геометрия» вышел в 1637 году.

Блез Паскаль (1623–1662), французский физик и математик. Получил ряд результатов по комбинаторике («треугольник Паскаля») и геометрии («теорема Паскаля»). Открыл метод доказательства по индукции.

Ньютон Исаак (1643–1727) — английский физик и математик и Готфрид Лейбниц (1646–1716) — немецкий философ и математик разработали дифференциальное и интегральное исчисление. Не имеется данных о привлечении этих математиков к шифровальной работе, но есть данные о том, что некоторые их них владели криптографией (Паскаль, Ньютон, Лейбниц). Увлекался криптографией и знаменитый английский философ Ф. Бекон (1561–1626), которому принадлежит идея двоичного кодирования.

Якоб Бернулли (1654–1705), швейцарский математик, заложил основы теории вероятностей, ему принадлежит известная теорема Бернулли, являющаяся важным частным случаем закона больших чисел. Его книга «Искусство предположений» вышла в 1713 году.

Для развития математики в России большую роль сыграла «Арифметика» Магницкого Л. Ф., изданная в 1703 году, которую М. В. Ломоносов назвал «вратами учености». Она представляла собой свод математических сведений на тот период.

К дешифровальной работе в России был привлечен известный математик Христиан Гольбах (1690–1764), приехавший в Россию в 1725 году. В 1727 году в Россию приезжает Леонард Эйлер (1707–1783), который принимал участие в разработке шифров. Ему принадлежат исследования по перечислению и построению латинских квадратов, т. е. шифров многоалфавитной замены. В области математики Эйлер существенно обогатил все разделы математического анализа и заложил основы новых математических дисциплин (теория чисел, вариационное исчисление, уравнения с частными производными, теория функций комплексного переменного). Дешифровальной работой занимался Франц Эпинус (1724–1802), в России с 1757 года, известный математик и физик, изучавший математическими методами электромагнитные явления.

Таким образом, в XVII–XVIII веках в математике закладываются основы аппарата, применяемого в криптографии для анализа шифров и дешифрования. Основным средством для шифрования становятся коды.

## 6 Криптография в XIX веке

В 1819 году во Франции выходит энциклопедия, в которой приведены известные к тому времени системы шифров и методы дешифрования простейших шифров. В 1844 году С. Морзе изобрел телеграф. В России телеграф был изобретен П. Ф. Шиллингом в 1832 году. Шиллингу также принадлежит изобретение биграммного шифра. В Англии изобретение биграммного шифра приписывается министру почт при королеве Виктории Леону Плейферу. Изобретение телеграфа оказало существенное влияние

на криптографию. Сразу же был опубликован коммерческий код под названием «Словарь для тайной корреспонденции; приспособлен для применения на электромагнитном телеграфе Морзе». Развитие коммерческих кодов повлияло и на развитие дипломатических кодов. Специалисты в области шифрованной связи пришли к пониманию, что необходима иерархия в шифрованной связи. Для каждого уровня иерархии требуется своя система шифра. Возрастание скорости передачи потребовало возрастания скорости шифрования. Появляются различные механические устройства для зашифрования. Среди них шифратор Т. Джефферсона и шифратор Ч. Уитстона. Устройство Уитстона демонстрировалось на парижской выставке 1876 года. Отметим, что в викторианской Англии к дешифровальной работе был привлечен математик Ч. Беббидж, известный изобретением вычислительной машины.

В 1863 году офицер прусской армии майор Фридрих Казисский опубликовал книгу под названием «Искусство тайнописи и дешифрования», в которой новым вкладом в криптографию было изложение метода вскрытия многоалфавитного шифра с повторяющимся лозунгом на примере шифра Виженера, который ранее считался недешифруемым. Казисский предложил метод статистического определения числа букв в лозунге, который основан на следующей идее: повторяемость букв в лозунге вместе с повторяемостью букв в открытом тексте дает повторяемость букв в шифрованном тексте. Автор пришел к выводу, что расстояние между повторениями в шифртексте будут равны или кратны периоду лозунга, т. е. его длине. После определения длины лозунга шифртекст разбивается на отрезки, равные длине лозунга, и исходная задача сводится к дешифрованию простой замены. Данный метод дешифрования стал называться «методом Казисского».

В 1883 году появился крупный научный труд под названием «Военная криптография», его автор Огюст Кергоффс, преподаватель иностранных языков и математики во Франции. В данной книге проводится сравнительный анализ шифров. Задача автора — сформулировать требования к шифрам, применительно к использованию новых средств связи. Он делает вывод, что практический интерес представляют те шифры, которые остаются стойкими при интенсивной переписке.

Другой его вывод: только криптоаналитики могут судить о качестве шифра. Кергоффс впервые делает различие между секретностью шифрсистемы и секретностью ключа. И вводит требование секретности по ключу и не требует секретности системы. Это требование сохраняет свое значение и в современной криптографии.

Важное событие в криптографии было связано с именем французского офицера Э. Базери, который отрицательно относился к официальным шифрам и предложил несколько собственных систем шифров. Одна из них — это по сути шифратор Джефферсона.

Военное руководство отказалось его использовать, сославшись на то, что нет гарантий стойкости этого шифра. В 1901 году Э. Базери издал книгу «Раскрытые секретные шифры», в которой показана возможность дешифрования «Великого шифра Россиньоля».

С 80-х годов XIX века криптография во всех ведущих государствах считается наукой и ее изучают в военных академиях. Для шифрования применяются коды с перешифровкой. Созданы и используются механические устройства для шифрования. Нет свидетельств, относящихся к данному периоду, о привлечении крупных математиков для криптографической работы.

Математика XIX века характеризуется революционными открытиями, ломающими привычные представления. В первую очередь следует назвать открытие Н. И. Лобачевским неевклидовой геометрии. Его сочинение « О началах геометрии » было напечатано в журнале «Казанский вестник» в 1829 году. Сходные результаты были получены Я. Больяи в 1832 году. Больцано Б. и позднее Вейерштрасс К. строят пример непрерывной функции, не имеющей конечной производной ни в одной точке. Но это является только началом открытий патологических явлений в математике.

Г. Кантор разработал теорию бесконечных множеств и открыл первые парадоксы теории множеств. Затем аналогичные парадоксы были открыты Бурали-Форти, Ришаром, Расселом. Сложившуюся ситуацию называют «кризисом математики». Знаменитый математик А. Пуанкаре в одном из мемуаров спрашивает: «Как интуиция может обмануть нас до такой степени?». Такое положение дел подтолкнуло к изучению оснований математики, развитию формальных языков и аксиоматического метода. Началась арифметизация математики, т. е. применялся метод, при котором рассуждение о математических объектах сводится к рассуждению о натуральных числах. Начала формироваться новая математическая дисциплина — метаматематика, которая, по Д. Гильберту, исследует математические доказательства финитными методами.

На математическом конгрессе 1900 года в Париже известный немецкий математик Д. Гильберт, формулируя актуальные проблемы математики, на место № 2 в списке проблем ставит вопрос о непротиворечивости арифметики, а на место № 1 проблему Кантора о мощности континуума.

Заметим, что под № 8 в списке проблем Д. Гильберта стоит проблема простых чисел, в которой, в частности, цитируется гипотеза Римана о распределении нулей дзета-функции Римана. Данная проблема, как показали современные исследования, имеет важное значение для криптографии в связи с построением алгоритмов факторизации чисел.

## 7 Криптография в XX веке

XX век — век двух мировых войн, век научно-технического прогресса, век социальных потрясений и передела государственных границ. В этом веке криптография стала электромеханической, затем электронной. Это означает, что основными средствами передачи информации стали электромеханические и электронные устройства. Это преобразило всю криптографию, поскольку расширились возможности доступа к шифрованному тексту и появились возможности влияния на открытый текст.

Поскольку главным шифрсредством во время первой мировой войны были коды, которые не удавалось сохранить от компрометации, то участники военных действий взаимно читали переписку друг друга. В полевых условиях применялись: решетка Кардано (Германия и Австро-Венгрия), шифр Плейфер (Англия), шифр двойной перестановки (Франция), шифр гаммирования цифровой гаммой (Россия). С применением шифров связан ряд трагических событий, из которых упомянем лишь разгром двух русских армий — Ранненкампа и Самсонова в Восточной Пруссии в августе 1914 года, которое произошло из-за плохой организации шифрсвязи и вынужденной связи между этими армиями по радио без всякого шифра.

Война преобразила криптографию. В связи с применением радио для управления войсками расширились возможности добычи шифртекста. В этот период получили развитие методы дешифрования, основанные на парах открытых и шифрованных текстов, на шифртекстах, полученных на одном ключе, на использовании вероятных ключей. Находкой для криптографов было использование в качестве лозунгов пословиц, поговорок, патриотических призывов. В математическом плане получили развитие вероятностно-статистические методы, использующие частоту знаков, биграмм, триграмм и т. д.

Другое новшество этого периода — появление специализации в криптографической деятельности. Появляются группы по дешифрованию кодов и по дешифрованию полевых шифров, по добыче перехвата, по обработке информации, полученной из открытых и агентурных источников и т. д.

Между мировыми войнами появляются во всех ведущих странах электромеханические шифраторы. Они были двух типов — на коммутационных дисках или роторах и на цевочных дисках. Примером первого типа является известная шифрмашина «Энигма», которой были оснащены германские сухопутные войска. Примером второго типа является американская шифрмашина М-209. Коммутационный диск представляет собой полый диск с нанесенными с двух сторон контактами, соответствующими алфавитам открытого и шифрованного текста, причем они соединены между собой по некоторой подстановке, называемой коммутацией диска. Эта коммутация определяет замену букв в начальном угловом положении. При изменении углового положения диска изменяется соответствующая замена на сопряженную подстановку. Шифратор представляет собой устройство из коммутационных дисков и механизма изменения их угловых положений. Шифратор «Энигма» состоял из 4-х коммутационных дисков, которые изменяли свои угловые положения по принципу «счетчика». Она имела несколько модификаций. Одну идею в криптографическом отношении можно считать революционной — каждый диск дважды участвовал в шифровании, что усложняло анализ шифра. Шифрмашина М-209 состояла из 6 колес размера 26, 25, 23, 21, 19, 17, каждое из которых имело выступы и по окружности. Эта 6-мерная комбинация выступов (их число 64) с помощью механического устройства превращалась в число, на которое сдвигается буква открытого текста. Изменение угловых положений дисков осуществлялось равномерным их вращением. Ясно, что шифратор реализует шифр гаммирования. Советский Союз производил шифрмашины обоих названных типов.

Таким образом, перед второй мировой войной все ведущие страны имели на вооружении электромеханические шифрсистемы, обладающие высокой скоростью обработки информации и высокой стойкостью. Считалось, что применяемые системы недешифруемы и наступил конец криптографии. Впоследствии в ходе войны это мнение было опровергнуто и все участники военных действий имели криптографические успехи, а шифровальные службы были непосредственным участником военных действий. Поучительная история дешифрования «Энигмы» описана у Д. Кана и других авторов.

Ограничимся упоминанием теоретического открытия, оказавшего существенное влияние на разви-

тие криптографии. Речь идет о работе американского инженера К. Шеннона «Теория связи в секретных системах», выполненной в 1945 году (опубликованной в 1949 году) и работе советского ученого-радиотехника В. А. Котельникова «Основные положения автоматической шифровки», датированной 19 июня 1941 года. В данных работах были сформулированы и доказаны математическими средствами необходимые и достаточные условия недешифруемости системы шифра. Они заключаются в том, что получение противником шифртекста не изменяет вероятностей используемых ключей. При этом было установлено, что единственным таким шифром является так называемая лента одноразового использования, когда открытый текст шифруется с помощью случайного ключа такой же длины. Это обстоятельство делает абсолютно стойкий шифр очень дорогим в эксплуатации.

Упомянем также об участии математиков в этот период в криптографической работе. В Англии во время войны к криптографической работе был привлечен А. Тьюринг, известный работами по формализации концепции вычислимости и разрешимости, автор «машины Тьюринга». В США С. Куллбак — крупный специалист по математической статистике, в Советском Союзе крупные математики А. А. Марков и А. О. Гельфонд. А. А. Марков известен работами по теории алгоритмов, автор теории «нормальных алгоритмов», которые сейчас называются алгоритмами Маркова. А. О. Гельфонд — крупный специалист по теории чисел, известный решением проблемы Гильберта № 7 о трансцендентности степеней алгебраических чисел.

## 8 О криптографии нового времени

Начиная с 50-х годов криптография становится «электронной». Это означает, что широкое применение средств электронной техники для построения систем шифров и их исследования. Возможности применения электронной памяти позволили осуществлять обработку открытых текстов целыми отрезками (блоками) и это вызвало применение так называемых блочных шифров. С 70-х годов сфера применения криптографии начинает расширяться, криптография становиться гражданской отраслью. Это означает, что криптографические средства начинают применяться для защиты коммерческой информации. Для этих целей в США в 1978 году был принят стандарт шифрования данных DES, который является блочным шифром с длиной блока 64 бит. Этот процесс получил развитие и в настоящее время все развитые страны имеют свои стандарты шифрования. Разработан криптографический алгоритм IDEA, который рассматривается в качестве кандидата для международного стандарта шифрования.

В 70-х годах американские ученые Диффи и Хеллман предложили использовать так называемые системы с открытыми ключами, в которых нет канала для распространения ключей, но есть возможность двустороннего обмена информацией между отправителем и получателем. Фиксированная процедура такого обмена позволяет выработать общий секретный ключ. В этот период были предложены несколько систем с открытыми ключами. Среди них — система RSA, названная так по первым буквам ее авторов — Райвест, Шамир, Адлеман, в которой открытые сообщения кодируются натуральными числами, а операция шифрования заключается в возведении в степень числа, представляющего открытый текст, и в приведении полученного числа по некоторому модулю. Дешифрование данной системы представляет собой известную математическую задачу «дискретное логарифмирование», для которой к настоящему моменту не найдено эффективных алгоритмов.

Другая система шифра — система Меркля — Хеллмана — основана на известной математической проблеме «о рюкзаке», заключающейся в представлении натурального числа в виде суммы чисел из множества заданных. Данная проблема относится к классу NP-полных проблем, что соответствует ее труднорешаемости.

Данные идеи оказались плодотворными. Во-первых, они расширили область средств , применяемых для обоснования шифров. Во-вторых, способствовали притоку математиков к решению криптографических проблем. В-третьих, привели к возникновению новых направлений криптографии. Например, процедура обмена информацией при выработке общего ключа привела к понятию криптографического протокола. В-четвертых, они привели к появлению новых направлений в дискретной математике. Например, возникло понятие однонаправленной функции, для которой имеется простой алгоритм вычисления значения функции, но сложно вычисляется значение аргумента по значению функции. Для криптографических применений это понятие трансформировано в понятие односторонней функции с секретом. Хотя в настоящее время существование односторонних функций не доказано, имеется ряд кандидатов для этого, которые используются для построения систем шифров.

В заключение два слова о будущем криптографии. Ее роль будет возрастать в связи с расши-

рением ее областей приложения (цифровая подпись, аутентификация и подтверждение подлинности и целостности электронных документов, безопасность электронного бизнеса, защита информации, передаваемой через Интернет и др.). Знакомство с криптографией потребуется каждому пользователю электронных средств обмена информацией, поэтому криптография в будущем станет «третьей грамотностью» наравне со «второй грамотностью» — владением компьютером и информационными технологиями.

## Литература

[1] Соболева Т. А. Тайнопись в истории России. М.: 1994.

[2] Kahn D. Codebreakers.. N. Y.: 1967.

[3] Жельников В. Криптография от папируса до компьютера. М.: 1996.

[4] Brassard G. Modern Cryptology. Springer-Verlag, 1988.

[5] Саломаа А. Криптография с открытым ключом. М.: 1996.

[6] Schneier B. Applied Cryptography. John Wiley & Sons, 1996.

[7] Диффи У., Хеллмэн М. Защищенность и имитостойкость: Введение в криптографию. ТИИЭР, 1979, **67**, № 3.

[8] Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. М.: 2001.

[9] Чмора А. Л. Современная прикладная криптография. М.: 2001.

[10] Математическая энциклопедия. Т. 1–5, М.: 1977–1985.

# Развитие комбинаторно-вероятностных направлений в математике и криптография

В. Н. Сачков

## 1 Введение

Во второй половине прошлого столетия интенсивное развитие отечественной криптографии, становление ее как современной науки, широко использующей математические методы, послужило основой для проведения ряда исследований комбинаторно-вероятностного характера, результаты которых нашли отражение в большом количестве статей в математических журналах и целом ряде монографий. Источником этих результатов в ряде случаев было изучение разнообразных комбинаторных конфигураций, имеющих прикладное значение в криптографии. В целях изучения применялись не только известные классические методы, но и разрабатывались новые подходы, составляющие определенный вклад в развитие комбинаторного анализа и дискретной теории вероятностей.

Формулы для определения количества комбинаторных конфигураций нередко имеют весьма сложный вид и затрудняют возможность оценки влияния параметров, определяющих конфигурацию, на рост их числа.

В связи с этим большую роль в исследованиях играют асимптотические методы. Теоретико-вероятностный подход к решению задач перечисления комбинаторных конфигураций позволяет использовать в этих целях развитый аппарат теории вероятностей, а в процессе применения асимптотических методов опираться на разработанный арсенал предельных теорем.

В процессе более чем полувекового развития комбинаторно-вероятностные направления сложились в один из разделов дискретной математики, получивший название вероятностной комбинаторики. Данная статья не ставит своей целью дать сколько-нибудь полный обзор этого раздела, который содержит большое количество разнообразных результатов. Значительная часть этих результатов содержится в публикациях журнала «Теория вероятностей и ее применения», «Математический сборник», «Дискретная математика» и «Трудах по дискретной математике», издаваемых Российской Академией Наук и Академией криптографии Российской Федерации, а также других отечественных и зарубежных математических журналах.

В данной статье рассматриваются десять комбинаторно-вероятностных направлений исследований, результаты которых с полными доказательствами содержатся в статьях и монографиях, названия которых приведены в списке литературы в конце статьи. Эти результаты в большинстве случаев связаны с изучением комбинаторных конфигураций, представляющих интерес для криптографии и принадлежат выпускникам Московского государственного университета, юбилею которого посвящается данная работа.

## 2 Общая комбинаторная схема

Общая комбинаторная схема представляет собой общий метод построения производящих функций для перечисления классов эквивалентности отображений конечных множеств при различных ограничениях на первичные и вторичные спецификации этих отображений. Первичная и вторичная спецификации отображения определяются частотами встречаемости образов отображения. Классы эквивалентности определены относительно групп подстановок $G$ и $H$, действующих на множестве прообразов и образов, соответственно. В общей комбинаторной схеме рассматриваются четыре частных случая в зависимости от того, являются ли группы $G$ и $H$ единичными или симметрическими. Эти частные случаи соответствуют ряду частных комбинаторных схем перечисления, в которых комбинаторные

конфигурации могут быть определены как отображения с данными первичными или вторичными спецификациями (размещения частиц в ячейки, разбиения множеств, разбиения чисел, сочетание и размещение и т. д.). Производящие функции для перечисления конфигураций строятся с использованием так называемых нумераторов, соответствующих частным случаям общей комбинаторной схемы.

Отличие общей комбинаторной схемы от метода построения производящих функций для перечисления комбинаторных конфигураций в общей теории перечисления Пойа — ДеБрейна состоит в том, что в ней не требуется сложного вычисления индексов групп подстановок. Систематическое изложение общей комбинаторной схемы дано в книгах Сачкова В. Н. [2], [4].

## 3 Классическая задача размещения

Такое название утвердилось за частной комбинаторной схемой, связанной со случайным размещением различных частиц в различимые ячейки. Впервые достаточно полное изложение результатов по изучению этой схемы дано в монографии Колчина В. Ф., Севастьянова Б. А., Чистякова В. П. [1], где основное содержание составляют разнообразные предельные теоремы для вероятностных распределений случайных величин, характеризующих размещение при неограниченном росте числа ячеек и числа частиц. Рассмотрены распределения таких случайных величин как число пустых ячеек, число ячеек, содержащих данное число частиц, число частиц при последовательном размещении до достижения фиксированного заполнения. Исследована задача размещения со случайным числом частиц и размещение частиц комплектами.

Определена обобщенная схема размещения, с помощью которой изучаются распределения случайных величин, связанных с циклами случайных подстановок. Предельные теоремы используются для расчетов статистических критериев, в частности, критерия «пустых ящиков» и его обобщений. Отметим, что классическая задача размещения описывается одним из частных случаев общей комбинаторной схемы. Ряд вероятностных задач, относящихся к этому частному случаю, рассмотрен в книге Сачкова В. Н. [3].

## 4 Случайные подстановки и отображения

Одной из первых работ по этому направлению исследований является статья В. Л. Гончарова [12], в которой предложен общий способ построения производящих функций для перечисления подстановок с заданной цикловой структурой. На основе этих результатов в книге Сачкова В. Н. [2] предложены способы построения производящих функций для перечисления $\Lambda$-подстановок и $A$-подстановок, для которых частоты встречаемости длин циклов и длины циклов определяются произвольными фиксированными последовательностями $\Lambda$ и $A$ соответственно.

Результаты статьи [12] об асимптотической нормальности числа циклов в случайной подстановке при неограниченном увеличении ее степени и предельном пуассоновском распределении циклов заданной длины, а также об асимптотическом распределении циклов максимальной длины, получили дальнейшее развитие в ряде работ, в том числе в книгах Сачкова В. Н. и Колчина В. Ф. [3], [5], [8]. Ряд новых результатов для случайных подстановок, включая локальную теорему для числа циклов, распределение членов вариационного ряда, составленного из длин циклов и др., получены с использованием обобщенной схемы размещения, рассматриваемой в монографиях Колчина В.Ф. [5], [8] и сводящей ряд задач вероятностной комбинаторики к определению вероятностного распределения независимых одинаково распределенных случайных величин с заданной суммой. С использованием этой схемы аналогичные результаты доказаны и для числа компонент случайного отображения и вариационного ряда, составленного из величин его компонентов [5], [8].

Специфическими свойствами обладают рассмотренные в книге Сачкова В. Н. [3] случайные отображения $n$-множества, графы которых имеют максимальную высоту $h$. Если $\xi_i$ — число вершин такого графа высоты $i$, $1 \leqslant i \leqslant h$, то случайный вектор $(\xi_0, \xi_1, \ldots, \xi_{h-1})$ при $n \to \infty$ для нормировок, зависящих от решения некоторого уравнения, имеет в пределе собственное нормальное распределение с матрицей вторых моментов, выраженной через единственный при достаточно больших $n$ корень того же уравнения.

Предложен общий подход к построению производящих функций отображений с произвольными заданными ограничениями на длины контуров и высоту графов отображений. Получены предельные

теоремы о распределении числа циклических элементов и компонент графов случайных отображений данного класса.

## 5 Случайные графы

Начало данному направлению комбинаторно-вероятностных исследований было положено статьей Эрдёша и Реньи [9]. Значительное развитие теория случайных графов получила в книге Боллобаша [13]. В отечественной математической литературе это направление представлено работами Степанова В. Е. [10]. Достаточно полное изложение результатов по случайным графам содержится в книге Колчина В. Ф. [8]. На основе использования уже упомянутой обобщенной схемы размещения в книге рассматриваются вопросы связности случайных графов, вероятностные распределения размеров деревьев и максимального размера дерева в случайном лесу, а также характеристик случайных графов с одноцикловыми компонентами. Дальнейшее развитие в книге получили результаты, касающиеся эволюции случайных графов, включая неравновероятный случай.

## 6 Случайные разбиения множеств

К числу первых результатов в этой области следует отнести теорему Л. Харпера [14] об асимптотической нормальности числа блоков в случайном разбиении $m$-множества при $m \to \infty$. Другое доказательство этой теоремы опубликовано в книге Сачкова В. Н. [4]. Следующим шагом в изучении случайных разбиений было доказательство многомерной предельной теоремы для чисел блоков заданной величины в случайном разбиении и, в частности, асимптотической нормальности распределения числа блоков данной величины. Далее были найдены предельные распределения для максимального и минимального по величине блоков в случайном разбиении $m$-множества при $m \to \infty$. В частности, показано, что предельное дважды экспоненциальное распределение величины максимального блока сосредоточено около среднего значения порядка $e \ln m$ и вид его зависит от последовательности значений, которую пробегает $m$ при безграничном увеличении. Эти результаты опубликованы в книге Сачкова В. Н. [3]. В дальнейшем по случайным разбиениям появляется ряд статей, в которых упомянутые результаты получили дальнейшее развитие. Обзор содержания этих статей содержится в статье [11]. Метод построения производящих функций для перечисления разбиений, для которых величины блоков и частоты их встречаемости определяются заданными последовательностями, изложен в книге [3]. В этой же книге рассматривались случайные разбиения, для которых определяется дополнительный случайный процесс нанесения меток на блоки. Найдены предельные распределения для случайных величин, представляющих собой число помеченных блоков и число элементов в помеченных блоках.

В статье [7, т. 4, Сачков В. Н.] введены новые понятия разбиений с поглощениями и противоречивых разбиений множеств. Разбиение множества $X$ содержит поглощение по отношению к разбиению множества $U$, $U \subseteq X$, если существует блок разбиения $X$, включающий некоторый блок разбиения $U$. Разбиения множеств $X$ и $U$ непротиворечивы, если они имеют хотя бы один общий блок. В противном случае разбиения $X$ и $U$ противоречивы. Для $T_m^{(s)}(U_1, \ldots, U_r)$ — числа разбиений $m$ — множества, содержащих $s$ поглощений по отношению к разбиению множества $U = U_1 \cup \ldots \cup U_r$, и $T_{mn}^{(s)}(U_1, \ldots, U_r)$ — числа таких разбиений с $n$ блоками получены формулы, выражающие эти величины через числа Белла и числа Стирлинга второго рода, соответственно. В частности, при $s = 0$ имеют место формулы

$$T_m^{(0)}(U_1, \ldots, U_r) = \frac{1}{e} \sum_{j=0}^{\infty} \frac{j^{m+r-|U|}}{j!} \prod_{i=1}^{r} \left( j^{|U_i|-1} - 1 \right),$$

$$T_{mn}^{(0)}(U_1, \ldots, U_r) = \frac{1}{n!} \sum_{j=0}^{n} (-1)^j \binom{n}{j} (n-j)^m \prod_{i=1}^{r} \left( 1 - \frac{1}{(n-j)^{|U_i|-1}} \right).$$

Если $\widetilde{T}_m^{(s)}(U_1, \ldots, U_r)$ — число разбиений $m$-множества с $s$ блоками, непротиворечивых с разбиением $U = U_1 \cup \ldots \cup U_r$, то эта величина выражается также через числа Белла и, в частности, при $s = 0$

$$\widetilde{T}_m^{(0)}(U_1, \ldots, U_r) = \frac{1}{e} \sum_{j=0}^{\infty} \frac{1}{j!} \prod_{i=1}^{r} \left( j^{|U_i|} - 1 \right).$$

Если $\eta_m$ и $\xi_m$ — случайные величины, равные числу поглощений и числу совпадений блоков случайного разбиения $m$-множества по отношению к разбиению $U = U_1 \cup \ldots \cup U_r$, то производящие функции этих случайных величин имеют, соответственно, вид

$$P_m(x) = \frac{1}{eT_m} \sum_{j=0}^{\infty} \frac{1}{j!} \prod_{i=1}^{r} \left( j^{|U_i|} + j(x-1) \right),$$

$$\widetilde{P}_m(x) = \frac{1}{eT_m} \sum_{j=0}^{\infty} \frac{1}{j!} \prod_{i=1}^{r} \left( j^{|U_i|} + x - 1 \right),$$

где $T_m$ — число Белла.

Получен ряд предельных теорем при $m \to \infty$. Две предельные теоремы полностью описывают асимптотическое поведение вероятностных распределений случайных величин $\eta_m$ и $\xi_m$.

**Теорема 1.** *Если $\delta_2$ — число блоков из двух элементов в разбиении $U = U_1 \cup \ldots \cup U_r$ и $R$ — единственный при $m \to \infty$ действительный корень уравнения $R \ln R = m$, то при $m \to \infty$*

1) *если $\delta_2 / R \to 0$, то $\eta_m$ имеет асимптотически вырожденное распределение;*

2) *если $\delta_2 / R \to \lambda > 0$, то $\eta_m$ имеет в пределе распределение Пуассона с параметром $\lambda$;*

3) *если $\delta_2 / R \to \infty$, то случайная величина $(\eta_m - \delta_2/R)(\delta_2/R)^{-1/2}$ асимптотически нормальна с параметрами $(0, 1)$.*

**Теорема 2.** *Если $\delta_1$ — число блоков из одного элемента в разбиении $U = U_1 \cup \ldots \cup U_r$, то для $\xi_m$ при $m \to \infty$ имеют место такие же предельные распределения, что и для $\eta_m$, если в условиях теоремы 1 заменить $\delta_2$ на $\delta_1$.*

Формулы для числа разбиений без поглощений применяются для определения мощности некоторых классов булевых функций. Для числа бесповторных конъюнктивных нормальных форм, существенно зависящих от всех $n$ переменных, имеет место формула

$$D_n = \frac{1}{e} \sum_{j=0}^{\infty} \frac{(j^2-1)^n}{j!},$$

из которой при $n \to \infty$ следует асимптотика

$$D_n = \frac{1}{\sqrt{2n/r}} r^{2n-r} e^r (1 + o(1)), \quad r \ln r = n.$$

Понятие противоречивых разбиений используется для перечисления булевых функций с полиномиальной сложностью решения соответствующих систем функциональных уравнений. Так, в статье Горшкова С. П. [15] для числа $m_1(k)$ булевых функций, принадлежащих пересечению классов мультиаффинных и слабоположительных функций и зависящих от $k$ переменных, выведена формула, выражающая это число через количество разбиений множества без единичных блоков. Из этой формулы с использованием результатов для противоречивых разбиений, получено следующее выражение для $m_1(k)$ [11], [7, т. 4, Сачков В. Н.]:

$$m_1(k) = 1 + \frac{1}{e} \sum_{j=1}^{\infty} \frac{(j+2)^k}{j!},$$

из которого при $k \to \infty$ следует асимптотика

$$m_1(k) = \sqrt{\frac{r}{k}} r^{k+2} e^{r-1} (1 + o(1)),$$

где $r$ — действительный корень уравнения $r \ln r = k$.

# 7 Случайные покрытия множеств

Наибольший интерес в изучении покрытий конечных множеств представляют собой так называемые минимальные покрытия, которые перестают быть покрытиями при удалении любого из покрывающих подмножеств, называемого блоком покрытия. В статье Хирна и Вагнера [18] для числа минимальных $k$-блочных покрытий $n$-множества $L_n(k)$ получена формула, выражающая это число через числа Стирлинга второго рода. В книге Сачкова В. Н. [4] даны точные и асимптотические формулы для чисел $L_n(k)$ при $n, k \to \infty$.

В статье Сачкова В. Н. [17] и книге Сачкова В. Н. и Тараканова В. Е. [6] доказана следующая предельная теорема.

**Теорема 3.** *Если $\xi_n$ — число блоков в случайном минимальном покрытии $n$-множества, то*

1) *если $n$ четно, то для любого $j = 0, 1, \ldots$*

$$\lim_{n\to\infty} \mathsf{P}\left(\xi_n = \frac{n}{2} - j\right) = \lim_{n\to\infty} \mathsf{P}\left(\xi_n = \frac{n}{2} + j\right) = \frac{2^{j^2}}{1 + 2C_0};$$

2) *если $n$ нечетно, то для любого $j = 0, 1, \ldots$*

$$\lim_{n\to\infty} \mathsf{P}\left(\xi_n = \frac{n-1}{2} - j\right) = \lim_{n\to\infty} \mathsf{P}\left(\xi_n = \frac{n+1}{2} + j\right) = \frac{2^{-j(j+1)}}{2C_1},$$

*где*

$$C_0 = \sum_{j=1}^{\infty} \frac{1}{2^{j^2}}, \quad C_1 = \sum_{j=0}^{\infty} \frac{1}{2^{j(j+1)}}.$$

При $n \to \infty$ среднее значение $\mathsf{M}\xi_n = (n/2)(1 + o(1))$ и дисперсия $\mathsf{D}\xi_n$ ограничена.

Из теоремы следуют асимптотические формулы для числа минимальных покрытий $n$-множества при $n \to \infty$ для четных и нечетных $n$, соответственно:

$$L_n = \frac{2^{(n/2+1)^2}}{\sqrt{2\pi n}}(1 + 2C_0 + o(1)),$$
$$L_n = \frac{2^{(n/2+1)^2 - 1/4}}{\sqrt{2\pi n}}(2C_1 + o(1)).$$

Для минимального покрытия существует по крайней мере один однократно покрытый элемент $n$-множества. Если для любых $t$ блоков $k$-блочного покрытия существует элемент $n$-множества, принадлежащий этим $t$ блокам и не принадлежащий остальным $k - t$ блокам, то покрытие называется $t$-минимальным. Несовместная система функциональных булевых уравнений

$$f_i(z_1, \ldots, z_n) = a_i, \quad i = 1, 2, \ldots, k$$

называется $t$-квазисовместной, если для любых $t$ уравнений существует вектор $(z_1^0, \ldots, z_n^0)$, который не является решением этих $t$ уравнений и является решением остальных $k - t$ уравнений.

**Теорема 4.** *Если $Y_i = \{(z_1, \ldots, z_n) : f_i(z_1, \ldots, z_n) = a_i\}$, $X_i \cup Y_i = X$, $X_i \cap Y_i = \varnothing$, $i = 1, 2, \ldots, k$, то система*

$$f_i(z_1, \ldots, z_n) = a_i, \quad i = 1, 2, \ldots, k$$

*является $t$-квазисовместной тогда и только тогда, когда $X_1, X_2, \ldots, X_k$ являются блоками $t$-минимального покрытия множества $X$ [6], [16].*

Для случайной последовательности подмножеств $X_1, X_2, \ldots$, выбранных из множества $X$, определяется понятие индекса покрытия как минимального числа $\chi_n$ такого, что $X_1 \cup X_2 \cup \ldots \cup X_{\chi_n} = X$. Если на булеане $2^X$ $n$-множества $X$ задано равномерное вероятностное распределение, то функция распределения $\chi_n$ имеет вид

$$\mathsf{P}(\chi_n \leqslant x) = \left(1 - \frac{1}{2^{[x]}}\right)^n, \quad x \geqslant 0,$$

$[x]$ — целая часть от $x$. Для среднего значения $\mathsf{M}\chi_n$ при $n \to \infty$ имеет место асимптотика

$$\mathsf{M}\chi_n = \log_2 n + C_3 - C_4 + o(1),$$

где

$$C_3 = \sum_{j=1}^{\infty} e^{-2j}, \quad C_4 = \sum_{j=0}^{\infty} \left(1 - e^{-2^{-j}}\right),$$

и справедлива предельная теорема [16].

**Теорема 5.** *При $n \to \infty$ для любых $y \geqslant 0$, и всех $y < 0$ таких, что $|y| = o(\log_2 \sqrt{n})$, имеем*

$$\mathsf{P}(\chi_n \leqslant [\log_2 n] + y) = e^{-2^{-[y]+\delta_n}}(1 + o(1)),$$

*где $\delta_n = \{\log_2 n\}$ — дробная часть от $\log 2n$.*

В работе [7, т. 5, Сачков В. Н.] рассматриваются неравновероятные случайные покрытия и соответствующие системы булевых уравнений. Случайное подмножество $n$-множества $X$ определяется вектором-индикатором, который является реализацией $n$ испытаний в схеме Бернулли с вероятностью успеха $P_j^{(i)}$, где $i$ — номер подмножества, $j$ — номер координаты вектора, $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant n$. Получены предельные теоремы для числа непокрытых элементов $X$, совпадающего с числом решений системы функциональных булевых уравнений. Для $P_j^{(i)} = p$ найдены предельные распределения для индекса покрытия. Показано, что, если $\mathsf{M}\chi_n(p)$ — среднее значение индекса покрытия, то при $n \to \infty$ имеет место соотношение

$$\mathsf{M}\chi_n(p) - \log_{1/p} n \to C_5 - C_6,$$

где

$$C_5 = \sum_{j=0}^{\infty} \left(1 - e^{-p^j}\right), \quad C_6 = \sum_{j=1}^{\infty} e^{-p^{-j}}.$$

Дисперсия $\mathsf{D}\chi_n(p)$ при $n \to \infty$ имеет ограниченный предел.

## 8 Случайные многочлены над конечными полями

Случайные унитарные многочлены над полем GF(2) изучались впервые Степановым В. Е. в 1983 году в связи со сложностью логарифмирования в поле $\mathrm{GF}(2^n)$. В 1986 г. Сачковым В. Н. для случайных многочленов над полем $\mathrm{GF}(q)$ получены предельные теоремы для числа неприводимых множителей в каноническом разложении и числа неприводимых множителей данной степени, а также разработан метод построения производящих функций для перечисления многочленов с различными ограничениями на структуру канонического разложения.

В статье [7, т. 3, Ивченко Г. И., Медведев Ю. И.] введены понятия локальной и интегральной структур случайного многочлена над полем $\mathrm{GF}(q)$, связанных с разложением многочлена на неприводимые множители. Рассмотрены производящие функции, перечисляющие многочлены с заданными значениями структур. Получены предельные теоремы для членов вариационного ряда из степеней неприводимых сомножителей в разложении случайного многочлена над полем $\mathrm{GF}(q)$ и получен ряд других результатов.

## 9 Вероятностные преобразователи и цепи Маркова

Вероятностный преобразователь определяется как семейство зависящих от времени конечных автоматов без выхода $\langle X, Y, Y_0, \{f_t\}\rangle$, $t = 1, 2, \ldots$, где $X$ — входной алфавит, $Y$ и $Y_0$ — множества внутренних и начальных состояний, $\{f_t\}$ — последовательность функций перехода $f_t \colon X \times Y \to Y$, $t = 1, 2, \ldots$. Функционирование определяется равенством

$$y^{(t)} = f_t\left(x^{(t-1)}, y^{(t-1)}\right),$$

где $x^{(t)}$ и $y^{(t)}$ — символ входного алфавита и состояние автомата в момент времени $t$ соответственно.

Основные результаты по изучению вероятностных преобразователей изложены в статье [7, т. 1, Сачков В. Н.].

Вероятностный преобразователь при задании на входе случайной последовательности вырабатывает случайную последовательность состояний. Если последовательность на входе является реализацией независимых испытаний, то последовательность состояний образует простую, вообще говоря неоднородную цепь Маркова с матрицами переходных вероятностей вида

$$P_t = \sum_{k=1}^{m} \alpha_k^{(t)} \Theta_k^{(t)}, \quad t = 1, 2, \ldots,$$

$$\sum_{k=1}^{m} \alpha_k^{(t)} = 1,$$

где $\Theta_k^{(t)}$ — элементарная матрица, соответствующая преобразованию $n$-множества $Y$. Если преобразования являются подстановками степени $n$, которым отвечают подстановочные матрицы $\Pi_k^{(t)}$, $1 \leqslant k \leqslant m$, то вероятностный преобразователь называется подстановочным и дважды стохастические матрицы переходных вероятностей имеют вид

$$P_t = \sum_{k=1}^{m} \alpha_k^{(t)} \Pi_k^{(t)}, \quad t = 1, 2, \ldots.$$

При условии $\Pi_k^{(t)} = \Pi_k$, $1 \leqslant k \leqslant m$, $t = 1, 2, \ldots$ соответствующая цепь Маркова однородна и ее эргодические свойства определяются характеристиками мультиграфа $\Gamma(s_1, s_2, \ldots, s_m)$, полученного суперпозицией подстановочных графов $\Gamma(s_1), \Gamma(s_2), \ldots, \Gamma(s_m)$, где $s_k$ — подстановка, соответствующая подстановочной матрице $\Pi_k$, $1 \leqslant k \leqslant m$. Для случайного независимого и равновероятного выбора подстановок $s_1, s_2, \ldots, s_m$ степени $n$ вероятности неразложимости цепи Маркова при $n \to \infty$ имеют следующее асимптотическое представление:

$$P_n^{(m)} = 1 - \frac{1}{n^{m-1}} + o\left(\frac{1}{n^{2(m-1)}}\right), \quad m \geqslant 2,$$

$$P_n^{(1)} = \frac{1}{n}.$$

Для вероятности ацикличности имеет место оценка

$$\widetilde{P}_n^{(m)} \geqslant 1 - \left(\sqrt{\frac{e}{2n}} \log_2 n\right)^m, \quad m \geqslant 1.$$

Из этих оценок следует, что для вероятности эргодичности цепи Маркова $P(n, m)$ при $m \geqslant 2$ и $n \to \infty$ справедливо соотношение

$$P(n, m) \to 1.$$

Наряду с этими результатами в указанной выше статье [7, т. 1] в неоднородном случае даны необходимые и достаточные условия вполне неразложимости матриц переходных вероятностей. При некоторых дополнительных условиях свойство вполне неразложимости матриц переходных вероятностей обеспечивает эргодичность рассматриваемой неоднородной цепи Маркова. Вероятность вполне неразложимости матрицы при случайном равновероятном выборе подстановок $s_1, s_2, \ldots, s_m$ при $n \to \infty$ удовлетворяет соотношению

$$Q_n^{(m)} \to 1, \quad m \geqslant 3.$$

Для вероятностного преобразователя, отвечающего произвольной системе преобразований $n$-множества $\sigma_1, \sigma_2, \ldots, \sigma_m$, условия эргодичности цепи Маркова определены для так называемой правильной системы преобразований, для которой при любом $i$, $1 \leqslant i \leqslant m$ и для любой концевой вершины $x$ графа $\Gamma(\sigma_i)$ существует такое $j$, $1 \leqslant j \leqslant m$, что $x$ является циклической вершиной $\Gamma(\sigma_j)$. Если $s_1, s_2, \ldots, s_m$ — подстановки, являющиеся сужениями преобразований $\sigma_1, \sigma_2, \ldots, \sigma_m$ на множества циклических точек, то для правильной системы преобразований достаточные условия эргодичности однородной цепи Маркова состоят в том, чтобы мультиграф $\Gamma(s_1, s_2, \ldots, s_m)$ был связным и длины циклов хотя бы одной из подстановок $s_1, s_2, \ldots, s_m$ были взаимно просты. Для $m = 2$ при случайном выборе $\sigma_1$ и $\sigma_2$, образующих правильную систему преобразований, определены условия, при которых вероятность эргодичности соответствующей цепи Маркова для $n \to \infty$ стремится к единице [7, т. 1].

## 10 Группы подстановок и полугруппы преобразований со случайными образующими

В статье [7, т. 3, Сачков В. Н.] показано, что для случайных независимых и равновероятных подстановок $s_1, s_2, \ldots, s_m$ степени $n$ вероятность $P_n^{(m)}$ транзитивности группы $G = \langle s_1, s_2, \ldots, s_m \rangle$ и вероятность $P(n,m)$ совпадения ее с симметрической или знакопеременной группами подстановок степени $n$ при $n \to \infty$ и $m \geqslant 2$ асимптотически равны величине

$$1 - \frac{1}{n^{m-1}} + O\left(\frac{1}{n^{2(m-1)}}\right).$$

При $m = 2$ этот результат совпадает с соответствующими результатами работ [19] и [20].

Если $P_n^{(m)}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ — вероятность транзитивности группы $G = \langle s_1, s_2, \ldots, s_m \rangle$, где $s_1, s_2, \ldots, s_m$ случайно независимо и равновероятно выбираются из циклового класса $[1^{\alpha_1} 2^{\alpha_2} \ldots n^{\alpha_n}]$, то при выполнении условий для $n \to \infty$

$$\frac{\alpha_1 + \sqrt{\alpha_2}}{n^{1-1/m}} \to 0, \quad \frac{2^{\sum_{i=1}^{[n/2]} \alpha_i}}{n^{3(1-1/m)}} \to 0,$$

имеет место соотношение [7, т. 3]

$$P_n^{(m)}(\alpha_1, \alpha_2, \ldots, \alpha_n) \to 1.$$

Если $s_1, s_2, \ldots, s_m$ принадлежат цикловому классу с $n/l$ циклами длины $l$, то вероятность транзитивности $G = \langle s_1, s_2, \ldots, s_m \rangle$ при $n \to \infty$ стремится к единице тогда и только тогда, когда не выполнено хотя бы одно из равенств $m = 2$, $l = 2$. Если оба этих равенства выполнены, то предельное распределение числа орбит группы $G = \langle s_1, s_2 \rangle$ при $n \to \infty$ является нормальным с параметрами нормировки $\left((1/2)\ln n, \sqrt{(1/2)\ln n}\right)$ [7, т. 3].

Если преобразования $n$-множества $\sigma_1, \sigma_2, \ldots, \sigma_m$ выбираются случайно, независимо и равновероятно, то вероятность $Q(n,m)$ того, что полугруппа, порожденная $\sigma_1, \sigma_2, \ldots, \sigma_m$, совпадает с симметрической полугруппой преобразований $n$-множества при $n \to \infty$ удовлетворяет соотношениям

$$Q(n,m) \to \begin{cases} 0, & \delta_{nm} \to 0, \\ 1 - (1+\alpha)e^{-\alpha}, & \delta_{nm} \to \alpha > 0, \\ 1, & \delta_{nm} \to \infty, \end{cases}$$

где $\delta_{nm} = mn!/n^n$ [7, т. 3].

## 11 Оператор редуцирования

Оператор редуцирования — это новое математическое понятие, возникшее в криптографии. Ряд результатов по изучению этого понятия изложен в статье [7, т. 2, Сачков В. Н.]. Оператор редуцирования $R(M)$ определяется как отображение

$$R(M)\colon S_n \to S_{n-k},$$

где $M$ — фиксированное $k$-подмножество $n$-множества $X$, $S_n$ и $S_{n-k}$ — совокупности всех подстановок, действующих на $X$ и $X \setminus M$ соответственно. Действие $R(M)$ на подстановку $s \in S_n$, имеющее вид $R(M)(s) = s' \in S_{n-k}$, состоит в разложении подстановки $s$ в произведение независимых циклов, удаление из них всех элементов множества $M$ и построении $s'$ как произведения прореженных таким образом циклов.

Если $\xi_n$ — число циклов в случайной равновероятной подстановке $s \in S_n$ и $\overline{\xi}_{n-k}$ — число циклов в редуцированной подстановке $s' = R(M)(s)$, то производящая функция условного распределения имеет вид

$$\sum_{\mu=\nu}^{n} \mathsf{P}\left(\xi_n = \mu \,\middle|\, \overline{\xi}_{n-k} = \nu\right) x^\mu = x^\nu \frac{\Gamma(n+x)\Gamma(n-k+1)}{\Gamma(n+1)\Gamma(n-k+x)},$$

где $\Gamma$ — гамма-функция. С использованием этой производящей функции для вероятности $P(n,k)$ сохранения четности случайной подстановки при редуцировании получается формула

$$P(n,k)=\begin{cases}(1/2)(1+(n-k)(n-k-1)/n(n-1)), & k \text{ — четное;}\\ (1/2)(1-(n-k)(n-k-1)/n(n-1)), & k \text{ — нечетное.}\end{cases}$$

Доказана следующая теорема [7, т. 2].

**Теорема 6.** *При $n\to\infty$ условное распределение имеет следующие предельные распределения:*

1) *если $n/(n-k)\to\infty$, то предельное распределение — нормальное с параметрами нормировки $\left(\nu+\ln(n/(n-k)),\sqrt{\ln(n/(n-k))}\right)$;*

2) *если $n/(n-k)\to\alpha>0$, то предельное распределение после центрирования величиной $\nu$ является пуассоновским с параметром $\lambda=\ln\alpha$.*

Если $\nu_n^{(1)}$ и $\overline{\nu}_{n-k}^{(1)}$ — числа единичных циклов в случайных подстановках $s$ и $R(M)(s)$ соответственно, где $s\in S_n$ и $R(M)(s)\in S_{n-k}$, то условное распределение $\mathsf{P}\left(\nu_n^{(1)}=\mu\;\middle|\;\overline{\nu}_{n-k}^{(1)}=\nu\right)$ выражается следующим образом:

$$\begin{aligned}&\binom{n}{k}\mathsf{P}\left(\nu_n^{(1)}=\mu\;\middle|\;\overline{\nu}_{n-k}^{(1)}=\nu\right)\\ &\quad=\sum_{t=\max[0,(\mu+\nu-k)/2]}^{\min(\mu,\nu)}\frac{(\nu)_t}{t!(\mu-t)!}\sum_{r=0}^{k-\mu-\nu+2t}\frac{(-1)^r}{r!}\binom{n-\mu-\nu+t-r}{k-\mu-\nu+2t-r},\\ &\mu=0,1,\ldots,n.\end{aligned}$$

Имеет место следующая предельная теорема [7, т. 2].

**Теорема 7.** *При $n\to\infty$, $k/n\to\gamma$ предельные распределения для условного распределения $\mathsf{P}\left(\nu_n^{(1)}=\mu\;\middle|\;\overline{\nu}_{n-k}^{(1)}=\nu\right)$, $\nu=0,1,\ldots,n$, $\mu=0,1,\ldots$, имеют следующий вид:*

1) *при $\gamma=0$*

$$\mathsf{P}\left(\nu_n^{(1)}=\mu\;\middle|\;\overline{\nu}_{n-k}^{(1)}=\nu\right)\to\begin{cases}1, & \mu=\nu\\ 0, & \mu\neq\nu\end{cases};$$

2) *при $\gamma=1$*

$$\mathsf{P}\left(\nu_n^{(1)}=\mu\;\middle|\;\overline{\nu}_{n-k}^{(1)}=\nu\right)\to\frac{1}{\mu!}e^{-1};$$

3) *при $0<\gamma<1$*

$$\mathsf{P}\left(\nu_n^{(1)}=\mu\;\middle|\;\overline{\nu}_{n-k}^{(1)}=\nu\right)\to e^{-\gamma}\sum_{t=0}^{\min(\mu,\nu)}\binom{\nu}{t}(1-\gamma)^t\frac{\gamma^{\mu+\nu-2t}}{(\mu-\nu)!}.$$

**Следствие.** *При $0<\gamma<1$ предельное распределение пункта 3 теоремы 7 совпадает с распределением суммы двух независимых случайных величин, одна из которых имеет распределение Пуассона с параметром $\gamma$, а другая — биномиальное распределение с числом испытаний $\nu$ и вероятностью успеха $1-\gamma$.*

Справедливость следствия вытекает из вида производящей функции предельного распределения пункта 3 теоремы 7.

$$f(x;\nu)=e^{\gamma(x-1)}(\gamma+(1-\gamma)x)^\nu.$$

Если $2^X$ — булеан множества $X$, на котором действуют подстановки симметрической группы $S_n$, то для $M_1,M_2\in 2^X$ определена операция умножения операторов редуцирования $R(M_1)$ и $R(M_2)$ с помощью равенства

$$R(M_1)R(M_2)=R(M_1\cup M_2).$$

Совокупность операторов редуцирования, определяемых на $2^X$, по отношению к этой операции образует коммутативную полугруппу идемпотентов [7, т. 2].

## Литература


[1] Колчин В. Ф., Севастьянов Б. А., Чистяков В. П. Случайные размещения. М.: Наука, 1976.

[2] Сачков В. Н. Комбинаторные методы дискретной математики. М.: Наука, 1977.

[3] Сачков В. Н. Вероятностные методы в комбинаторном анализе. М.: Наука, 1978.

[4] Сачков В. Н. Введение в комбинаторные методы дискретной математики. М.: Наука, 1982.

[5] Колчин В. Ф. Случайные отображения. М.: Наука, 1984.

[6] Сачков В. Н., Тараканов В. Е. Комбинаторика неотрицательных матриц. М.: ТВП, 2000.

[7] Труды по дискретной математике. РАН и Академия криптографии РФ. Т. 1 — 1997, т. 2 — 1998, т. 3 — 2000, т. 4 — 2001, т. 5 — 2002.

[8] Колчин В. Ф. Случайные графы. М.: Наука, 2000.

[9] Erdős P., Renyi. On the evolution of random graphs. Publ. Math. Inst. Hungar. Acad. Sci, A, 1960, **5**, 17–61.

[10] Степанов В. Е. Фазовый переход в случайных графах. Теория вероятности и ее применения, 1970 **15**, № 2.

[11] Сачков В. Н. Случайные разбиения множеств. Математические вопросы кибернетики, 1999, вып. 8.

[12] Гончаров В. Л. Из области комбинаторики. Известия АН СССР, сер. матем., 1944, **8**, № 1, 3–48.

[13] Bollobas B. Random graphs. London, Acad. Press, 1985.

[14] Harper L. Stirling behavior is asymptotically normal. Ann. Math. Stat., 1961, **38**, № 2.

[15] Горшков С. П. О пересечениях классов мультиаффинных, биюнктивных, слабо положительных и слабо отрицательных булевых функций. Обозр. прикл. и промышл. матем, 1997, **4**, вып. 2.

[16] Сачков В. Н. Случайные покрытия и системы функциональных уравнений. Интеллектуальные системы, МГУ и Академия технологических наук, 1997, **2**, вып. 1–4.

[17] Сачков В. Н. Случайные минимальные покрытия множеств. Дискретная математика, 1992, **4**, вып. 3.

[18] Hearne T., Wagner C. Minimal covers finite sets. Discr. Math., 1973, № 5.

[19] Dixon J. D. The probability of generating the symmetric group. Math. Z., 1969, **110**.

[20] Babai L. The probability of generating the symmetric group. J. Comb. Theory, 1989, **A52**.

# Криптография и теория кодирования

В. М. Сидельников

## Часть I
# О криптографии

## 1 Введение

Современная криптография является наукой и одновременно искусством защиты информации. Наиболее известные математической общественности результаты современной криптографии относятся к теории чисел и теории сложности. Менее известно, что теория кодирования так же или даже более необходима для решения широкого круга криптографических задач.

Настоящий доклад призван рассказать о достижениях криптографии, которые получены с помощью теории кодирования, и указать на их значимость.

Теория кодирования в первую очередь связана с традиционной криптографией, а именно с ее главным разделом, в котором изучается так называемое симметрическое шифрование.

*Симметрическое шифрование* — это современное название процедуры шифрования и расшифрования, которые реализуются на обоих концах линии связи с помощью одинаковых или почти одинаковых шифровальных устройств (шифраторов). Между прочим, еще 25 лет назад других шифрований, одно из которых сейчас называется асимметрическим, не было известно, — все системы шифрования были симметрическими. Симметрическое шифрование является наиболее распространенным в современном мире, хотя усилия известных математиков в последние годы по ряду причин почти полностью были направлены на исследования проблем, связанных с асимметрическим шифрованием и открытым распределением ключей.

Особым видом симметрического шифрования является, так называемый, шифр Вернама, который представляет из себя наложение на открытую информацию «белой» гаммы. Это один из немногих видов шифрования, для которого можно строго доказать (см. [1]) его абсолютную нераскрываемость. Шифры, подобные шифру, Вернама обычно изучают в рамках теории информации, которая и возникла в трудах К. Шеннона под сильным влиянием его занятий криптографией. Подобные шифры и связанные с ними теоретико-информационные проблемы мы в настоящей работе рассматривать не будем. В работе под симметрическим шифрованием понимается автоматное шифрование с относительно небольшим ключом.

При симметрическом шифровании нападающая сторона (противник) не может прочитать зашифрованное сообщение из-за того, что он не знает алгоритма шифрования, который в значительной мере определяется секретным ключом.

*Асимметрическое шифрование* принципиально отличается от симметрического тем, что его алгоритм шифрования, который представляет собой отображение некоторого множества в себя, общеизвестен. Стойкость этого шифрования основывается на том, что противник (нелегитимный пользователь) не в состоянии доступными ему средствами вычислить обратное отображение. Вместе с тем вычисление обратного отображения для легитимного пользователя вычислительно доступно из-за того, что он знает некоторый секрет, который был использован при построении прямого отображения.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта № 02-01-00687).

Асимметрическое шифрование принципиально отличается от симметрического еще также тем, что для него не нужен абсолютно надежный канал для рассылки секретных ключей. Это свойство в некоторых случаях дает асимметрическим системам шифрования значительные практические преимущества перед традиционным симметрическим. Вместе с тем необходимо отметить, что, во-первых, сложность вычисления значений «одностороннего отображения» и его обратного, т.е. сложность асимметрического зашифрования и расшифрования, обычно значительно выше, чем сложность этих процедур при традиционных симметрических автоматных методах шифрования, и, во-вторых, — в настоящее время неизвестны практически реализуемые системы асимметрического шифрования, для которых достаточно убедительно доказана невозможность их раскалывания квалифицированным незаконным пользователем.

Следует сказать, что всегда (это справедливо и в данном случае) высокую стойкость криптографической системы криптографу удается обосновать лишь в рамках рассматриваемых им же методов анализа этой системы.

Стойкость всех асимметрических систем шифрования, подвергнувшихся серьезному криптографическому анализу, всегда существенно ниже, чем мощность пространства ключей, и имеет явную тенденцию к постоянному снижению.

Настоящая работа включает в себя несколько этюдов по отдельным разделам криптографии, которые так или иначе связаны с теорией кодирования. Автор на полноту охвата предмета не претендует.

Особенно существенным и интересным автору представляется последний раздел работы (часть II), где конкретно и подробно рассматривается один метод определения ключей асимметрической системы шифрования. Как может увидеть читатель, для того чтобы «расколоть» даже относительно несложную систему необходимо использовать нетривиальные и глубокие математические результаты. По мнению автора, стойкость криптографической системы существенно зависит от квалификации и способностей того, кто анализирует эту систему.

## 2 Теоретико-кодовые асимметрические системы шифрования

В настоящее время известно только 3–4 типа асимметрических систем с предположительно высокой стойкостью шифрования. Одним из них являются системы открытого шифрования МакЭлиса и Нидеррайтера, в основе которых лежат коды, корректирующие ошибки. Их стойкость основана на том, что декодирование кодов «общего положения» является NP-трудной задачей [20], в то время как сложность декодирования некоторых алгебраических кодов является относительно простой вычислительной задачей. Поэтому основная идея, которая используется при построении этих систем, состоит в «маскировке» алгебраических кодов под коды общего положения. Стойкость этих систем в основном зависит от того, насколько хорошо выполнена такая маскировка.

Теоретико-кодовые системы отличаются от других систем тем, что у них, с одной стороны, скорость зашифрования и расшифрования заметно выше, а с другой стороны — объем их открытого ключа значительно больше, чем у остальных систем открытого шифрования. Первое является значительным преимуществом, а второе — недостатком.

Теория кодирования доставляет несколько примеров стойких систем открытого шифрования. Остановимся на одном из них.

Пусть $\mathcal{C}$ — линейный код с параметрами $(n, k, d)$ над конечным полем $\mathbf{F}_q$, который имеет простое декодирование, и $M$ — его порождающая $k \times n$-матрица. Пусть $H$ — невырожденная $k \times k$-матрица и $\Gamma$ — перестановочная $n \times n$-матрица.

Открытой информацией, подлежащей шифрованию, в теоретико-кодовой асимметрической системе шифрования является $k$-мерный вектор $\omega \in \mathbf{F}_q^k$, а шифрованной информацией — $n$-мерный вектор $\text{ш} = \omega H \cdot M \cdot \Gamma + \boldsymbol{e}$, где $\boldsymbol{e}$ — случайный вектор веса $\mathrm{wt}(\boldsymbol{e}) \leqslant [\frac{d-1}{2}]$. Секретный ключ образуют матрицы $H$ и $\Gamma$, а общедоступным ключом является матрица $M' = H \cdot M \cdot \Gamma$. Случайный элемент $\boldsymbol{e}$ генерирует отправитель. Матрицы $H$ и $\Gamma$ «маскируют» порождающую матрицу $M$ с простым алгоритмом декодирования.

Получив ш, легитимный абонент $X$, который знает секретный ключ, вычисляет следующие элементы: $\text{ш}' = \text{ш}\Gamma^{-1}$, декодирует ш′, т.е. представляет его в виде $\text{ш}' = \boldsymbol{a} + \boldsymbol{e}'$, $\boldsymbol{a} \in \mathcal{C}$, $\mathrm{wt}(\boldsymbol{e}') \leqslant [\frac{d-1}{2}]$, где $\boldsymbol{a} = \omega H \cdot M$, и, наконец, с помощью последнего соотношения находит $\omega = \boldsymbol{a} H^{-1}$.

Проделать последнюю цепочку вычислений злоумышленнику трудно из-за того, что он не знает $\Gamma$. Поэтому ему трудно декодировать код $\mathcal{C}'$ с порождающей матрицей $M'$, который для него является

кодом «общего положения».

Известно, что сложность $N$ декодирования таких кодов общего положения имеет вид $N = 2^{c\min(k,n-k)}$ [22, 23]. Поэтому даже при относительно небольших $k$ и $n-k$ вычислительная сложность декодирования для таких кодов является неприемлемо большой.

Если в качестве $\mathcal{C}$ взять *Боуза — Чоудхури — Хоквингема код* [18] или *Рида — Маллера код* [12], то при подходящем $k$ и $n$ мы получим предположительно стойкую систему асимметрического шифрования. Если же в качестве $\mathcal{C}$ взять *Рида — Соломона код*, то получим заведомо слабую систему [11].

# 3 О стойкости симметрических систем шифрования

Возвратимся снова к симметрическим системам шифрования. По-видимому, наиболее значительным полем применения теоретико-кодовых конструкций, но в то же время наименее известным математической общественности, является анализ стойкости и синтез шифраторов. Традиционно *стойкость шифратора* определяется как число операций, необходимых для определения его ключа при некоторых предположениях. В первом приближении предполагается, что нападающая сторона, называемая также противником или злоумышленником, знает устройство шифратора, но не его ключ. Противник знает и некоторое число знаков, которые выработал шифратор на данном ключе.

Многие проблемы теоретической криптографии, относящиеся к анализу стойкости симметрических систем шифрования, изучаются в рамках давно сложившихся направлений математики: теории вероятностей и статистики, теории чисел, алгебры, теории кодирования, комбинаторики, теории сложности вычислений. В качестве примера укажем на методы построения рекуррентных последовательностей с определенными свойствами, методы выявления статистических закономерностей в массивах дискретной информации, поиск эффективных способов разложения на множители больших целых чисел, свойства булевых функций и преобразований, методы дискретной оптимизации и многие другие.

Особенно большое значение для криптографии имеют результаты, связанные с построением эффективных алгоритмов решения тех или иных конкретных задач. Например, решение системы линейных уравнений, умножение матриц, вычисление значений некоторых булевых функций и преобразований, а также и многие другие, являются массовыми задачами для многих методов определения ключа. Поэтому знание эффективных оценок сложности их решения (как верхних, так и нижних) позволяют делать относительно обоснованные выводы о стойкости систем шифрования.

Ввиду того, что задача определения ключа может быть представлена как задача решения некоторой системы нелинейных уравнений в конечном поле, для криптографии представляют значительный интерес методы решения систем того или иного вида и оценки их сложности. С примерами криптографических исследований можно познакомиться по многочисленным работам, связанным с изучением свойств преобразования DES, которые опубликованы в последние 20 лет в Procedings of Crypto, Procedings of Eurocrypt, Journal of Cryptology и в [6, 4].

Если говорить обобщенно, как правило при анализе и синтезе необходимо решить многие задачи, которые похожи или совпадают с традиционными задачами теории кодирования. При этом не следует умалять роль и многих других математических дисциплин, задачи которых также возникают при анализе криптосхем. Вместе с тем задачи теории кодирования играет здесь наиболее заметную роль. Это связано с тем, что теория кодирования и криптография, без сомнения, имеют родственные генетические основы: первая борется с атаками природы (ошибками), а вторая — с атаками злоумышленников. Методология защиты от этих атак во многом совпадают. Недаром основоположник научной криптографии К.Шеннон одновременно является и основоположником научных основ как криптографии, так и теории кодирования.

# 4 Аппроксимация булевыми функциями

Одним из примеров криптографической задачи, в решении которой значительную роль играют идеи и методы теории кодирования, является задача приближения одной сложной и не до конца известной булевой функции другой простой, которая принадлежит некоторому узкому классу булевых функций.

Более подробно: пусть нам известна двоичная последовательность

$$\boldsymbol{\gamma} = (f(\boldsymbol{a}_1), f(\boldsymbol{a}_2), \ldots, f(\boldsymbol{a}_N)), \boldsymbol{a}_j \in \mathbf{F}_2^m, \tag{1}$$

где $f$ — неизвестная булева функция, связанная некоторым образом с неизвестным ключом шифратора. Координаты последовательности $\boldsymbol{\gamma}$ определяются известными нам «входами» $\boldsymbol{a}_j$. Мы хотим приблизить в метрике Хемминга последовательность $\boldsymbol{\gamma}$ последовательностью

$$\boldsymbol{\sigma}_h = (h(\boldsymbol{a}_1), h(\boldsymbol{a}_2), \ldots, h(\boldsymbol{a}_N)), \tag{2}$$

где $h$, например, является аффинной функцией. Ближайшая функция $h$, как правило, дает некоторую информацию об «устройстве» функции $f$. Эта информация может быть полезна при определении ключа шифратора.

На самом деле в этой задаче заложено две подзадачи. Во-первых, надо выбрать схему шифратора так, чтобы последовательность $\boldsymbol{\gamma}$ «плохо» приближалась последовательностями $\boldsymbol{\sigma}_h$, определяемыми функциями $h$, которые принадлежат узкому классу $L$. Во-вторых, надо иметь эффективные алгоритмы, которые позволяют находить ближайшую к $\boldsymbol{\gamma}$ последовательность $\boldsymbol{\sigma}_h$ и, следовательно, функцию $h$.

Последний алгоритм естественно рассматривать как алгоритм декодирования искаженной последовательности $\boldsymbol{\gamma}$ кода $\mathcal{K}$ длины $N$, который образован всевозможными последовательностями $\boldsymbol{\sigma}_h$, $h \in L$. Подробно подобная задача рассматривалась в работе [13].

В теории кодирования известно не так много кодов, которые имеют эффективные алгоритмы декодирования. Одним из таких кодов является код Рида — Маллера первого порядка. Для него и некоторых его модификаций известно [21] , [25] несколько различных алгоритмов быстрого декодирования. Все они так или иначе используют «быстрый» алгоритм умножения вектора на матрицу Адамара — Уолша. Последний алгоритм весьма широко используется в современной криптографии.

## 5 Криптографические протоколы

Переходим теперь к обсуждению некоторых криптографических протоколов. Упомянем из них только те, в которых по существу используются теоретико-кодовые конструкции.

В симметрических системах шифрования все пользователи должны быть тем или иным способом снабжены ключами. Обычно это осуществляется с помощью дополнительных секретных каналов связи, которые в свою очередь подвержены атакам противника. Безопасное хранение и использование таких секретных ключей является также весьма нетривиальной проблемой. Задачи безопасной пересылки и сохранения ключей в секрете решаются как с помощью физических методов, так и в последнее время с помощью методов теории кодов, корректирующих ошибки. В частности, рассматривались теоретико-кодовые методы «разделения секретов» и методы, защищающие секретные ключи от компрометации при их пересылке и хранении. Некоторые из этих весьма нетривиальных и практически полезных методов защиты ключей были разработаны в России.

Одной из важнейших задач криптографии является разработка методов, защищающих информацию, например, финансовую или командную, от неконтролируемого ее изменения при передаче ее по общедоступным каналам связи, при хранении и при некоторых других видах ее использования. В этому же кругу задач относятся и механизмы доказательства принадлежности. При этом скрытие информации не всегда является необходимым.

К криптографическим протоколам, решающих подобные задачи, относится *цифровая подпись и имитозащита информации*. Цифровая подпись является общеизвестным криптографическим протоколом, в котором широко используются теоретико-числовые конструкции. Вместе с тем известны подходы по созданию цифровой подписи на базе кодов, корректирующих ошибки.

С другой стороны, методы имитозащиты информации полностью базируются на очень изящных конструкциях, которые родственны или совпадают с конструкциями, которые разработаны в теории кодирования. Так, одна из основных таких конструкций называется кодами, обнаруживающими обман.

Пусть необходимо передать элемент $a$ из конечного множества A. В качестве $a$ часто выступает значение хеш-функции. Будем предполагать, что на обоих концах канала связи имеется секретный элемент $b$ (ключ) из множества $B$. Пусть функция $\varphi(x, y) : A \times B \xrightarrow{\varphi} C$ инъективна при каждом

фиксированном $y$ и обладает тем свойством, что для каждого $a$ и $c$ множество $S(a,c), S(a,c) \subset B$, решений уравнения $\varphi(a,y) = c$ имеет достаточно много элементов.

В рассматриваемой системе имитозащиты по общедоступному каналу связи вместо элемента $a$ из A передается элемент $c = \varphi(a,b)$. Законный пользователь знает ключ $b$, поэтому он, получив элемент $c$, решает уравнение $c = \varphi(x,b)$ и определяет элемент $a$.

Представим, что элемент $a$ известен незаконному пользователю (злоумышленнику), который предполагает заменить его на другой элемент $a'$ (навязать фиксированный элемент $a'$). Для этого злоумышленник вместо $c$ должен послать $c'$ такое, что уравнение $c' = \varphi(x,b)$ имело решение $x = a'$; только в этом случае законный пользователь не заметит подмены и произойдет неконтролируемое изменение информации. Стратегия поведения злоумышленника в этом случае может состоять только в переборе элементов множества $\varphi(a', S(a,c))$ с надеждой напасть на подходящий элемент $c'$. Если это множество имеет достаточно много элементов, то эта стратегия становится неэффективной.

Рассмотренная выше идея может быть реализована, например, с помощью множеств $A = F_q$, $B = \{b = (b_1, b_2) | b_i \in F_q, b_1 \neq 0\}$, $C = F_q$ и аффинной функции $\varphi(a,b)$ вида $c = a \cdot b_1 + b_2$, где $F_q$ — конечное поле с $q$ элементами. Отметим, что при каждом $b$ из $B$ функция $\varphi(x,b)$ является перестановкой элементов поля $F_q$, а функции $\{\varphi(x,b); b \in B\}$ — дважды транзитивной группой перестановок на $F_q$. Несколько более сложная конструкция позволяет построить систему имитозащиты, которая практически исключает возможность навязывания не только фиксированного элемента $a'$, но и какого-либо $a'$, отличного от $a$. Отметим, что в рассмотренном примере одновременно с имитозащитой осуществляется и шифрование сообщения $a$.

# Часть II
# Как раскалывается одна асимметрическая система шифрования

## 6 Введение

Основной целью данного раздела работы является рассказ со всеми подробностями о том, как можно расколоть за полиномиальное время систему открытого шифрования Нидеррайтера или МакЛиса, построенную на основе кодов Рида — Соломона. Основные результаты этой статьи впервые изложены в работе Шестакова С. О. и автора [11]. Как полагает автор, статья будет полезной молодым исследователям.

Не надо думать, что все системы открытого шифрования, основанные на кодах, корректирующих ошибки, являются не стойкими. Данная работа является единственным известным примером кодовой системы открытого шифрования, которая раскалывается за полиномиальное время. Даже эту относительно простую систему расколоть, как будет видно ниже, весьма нетривиально. Для этого используются многие замечательные алгебраические конструкции: группы, матрицы, конечные поля и т.п. Как представляет себе автор, доказательство нестойкости даже отдельной системы шифрования, которая только деталями отличается от подобных стойких систем, имеет существенное как педагогическое, так и научное значение — не всё предлагаемое в открытой криптографии является качественным. Автор попытался сделать изложение замкнутым, но, по-видимому, полностью осуществить это ему не удалось.

## 7 Коды Рида — Соломона

### 7.1 Основные понятия теории кодирования.

В настоящем разделе будут даны только начальные сведения о теории кодирования, необходимые для определения систем открытого шифрования, предложенных Маклисом [10] и Нидеррайтером [14]. Для простоты, мы рассматриваем только частные случаи кодов, которые имеют наибольшее значение для криптографии. Значительно более полное изложение теории кодирования имеется в книгах [17] и [35].

Мы рассматриваем конечное поле $\mathbf{F}_q$, $q = p^l$, где $p$ — простое число и $l$ — положительное целое, содержащее $q$ элементов. Множество $\mathbf{F}_q^n = \{\boldsymbol{x} = (x_1, \ldots, x_n) | x_j \in \mathbf{F}_q\}$, мы обычным образом рассматриваем как линейное пространство размерности $n$.

На пространстве $\mathbf{F}_q^n$ задана метрика Хемминга, которая определяется следующим образом. Расстояние $d(\boldsymbol{x}, \boldsymbol{y})$ между двумя векторами $\boldsymbol{x}$ и $\boldsymbol{y}$ из $\mathbf{F}_q^n$ равно числу координат, в которых эти векторы различаются. Например, расстояние между векторами $(0,1,2)$ и $(2,1,0)$ из $\mathbf{F}_3^3$ (трехмерное пространство над полем $\mathbf{F}_3 = \{0,1,2\}$ из трех элементов) равно 2, так как эти векторы различаются только в первой и последней координате. Метрическое пространстве $\mathbf{F}_q^n$ с метрикой Хемминга будем называть пространством Хемминга. На пространстве Хемминга рассматривают еще одну функцию $\mathrm{wt}(\boldsymbol{x})$ — вес вектора $\boldsymbol{x}$, равный числу его ненулевых координат. Функции $d(\boldsymbol{x}, \boldsymbol{y})$ и $\mathrm{wt}(\boldsymbol{x})$ связаны соотношениями $d(\boldsymbol{x}, \boldsymbol{y}) = \mathrm{wt}(\boldsymbol{x} - \boldsymbol{y})$, $d(0, \boldsymbol{x}) = \mathrm{wt}(\boldsymbol{x})$.

Кодом называется произвольное подмножество $\mathcal{K}$ пространства $\mathbf{F}_q^n$. Кодовое расстояние $d(\mathcal{K})$ кода $\mathcal{K}$ определяется как минимальное расстояние между двумя различными элементами $\mathcal{K}$, т.е. $d(\mathcal{K}) = \min_{\boldsymbol{x},\boldsymbol{y} \in \mathcal{K}; \boldsymbol{x} \neq \boldsymbol{y}} d(\boldsymbol{x}, \boldsymbol{y})$. Всюду далее мы в качестве кодов $\mathcal{K}$ будем рассматривать только линейные подпространства $L$ пространства $\mathbf{F}_q^n$. Размерность $L$ всегда будем обозначать буквой $k$. Такие коды называются $q$-значными линейными кодами. Их параметры коротко записываются в виде $[n, k, d]_q$, где $n$ — длина кода $\mathcal{K}$, $k$ — его размерность и $d = d(\mathcal{K})$ — его кодовое расстояние. Число $r = n - k$ обычно называют избыточностью кода.

Следует заметить, что кодовое расстояние линейного кода может представлено и несколько иным, во многих случаях более удобным способом. А именно, $d(\mathcal{K})$ = минимальному весу ненулевого элемента кода $\mathcal{K}$.

Определенные выше коды используются для коррекции ошибок при передачи информации в канале связи. Схема такого использования состоит в следующем.

Под одиночной ошибкой типа замещения мы понимаем замену одного из символов в векторе $\boldsymbol{x} \in \mathbf{F}_q^n$ на другой символ. Если в векторе $\boldsymbol{x}$ произошло $t$ ошибок, то $t$ координат изменило свое значение. То, что пространство $\mathbf{F}_q^n$ является метрическим, позволяет утверждать, что $t$-кратная ошибка превращает кодовый вектор $\boldsymbol{x}$ в вектор $\boldsymbol{x}'$, отстоящий от $\boldsymbol{x}$ на расстояние $t$, т.е. $d(\boldsymbol{x}, \boldsymbol{x}') = t$. Таким образом, если в канале связи происходит не более, чем $t$ ошибок, то искаженный кодовый вектор $\boldsymbol{x}'$ находится в шаре (в метрике Хемминга) радиуса $t$ с центром в точке $\boldsymbol{x} \in \mathcal{K}$.

## 7.2 Геометрическая интерпретация кода.

Если все шары радиуса $t$ с центрами в кодовых точках кода $\mathcal{K}$ не пересекаются, то из очевидных геометрических соображений следует, что код может исправить любые $t$ или меньше ошибок, которые поразили кодовый вектор $\boldsymbol{x}$ в канале связи. Для этого необходимо использовать процедуру декодирования, которая находит тот центр шара $\boldsymbol{x}$ (кодовый вектор), к которому принадлежит искаженный вектор $\boldsymbol{x}'$. Из сказанного выше вытекает, что если код имеет кодовое расстояние $d(\mathcal{K}) \geqslant 2t + 1$, то он может корректировать все ошибки кратности $\leqslant t$.

Вектору $\vec{a} = (a_1, \ldots, a_k)$, $a_j \in \mathbf{F}_q$, который переносит информацию, поставим в соответствие кодовый вектор $\boldsymbol{x}(\vec{a}) \in \mathcal{K}$. Для передачи информационного вектора $\vec{a}$ по каналу связи с шумами в канал вместо $\vec{a}$ посылают кодовый вектор $\boldsymbol{x}(\vec{a})$. На выходе канала после декодирования определяется вектор $\boldsymbol{x}(\vec{a})$, а затем и информационный вектор $\vec{a}$.

Рассмотренную геометрическую модель коррекции ошибок можно построить из-за того, что $\mathbf{F}_q^n$ является метрическим пространством, метрика которого в согласована с видом искажений, которые возникают в канале связи. Можно сказать, что с геометрической точки зрения теория кодов, исправляющих ошибки, представляет собой науку, которая занимается упаковками шаров в метрических пространствах, в частности, в пространстве Хемминга, а также задачами декодирования кодов того или иного вида. Таким образом, такое весьма абстрактное математическое понятие, как метрическое пространство, оказывается весьма полезным для содержательных и наглядных представлений кодов $\mathcal{K}$, корректирующих ошибки, и в конечном итоге для их построения и использования.

Одной из основных задач теории кодирования является задача построения кода длины $n$ с кодовым расстоянием $d$ с возможно большим числом элементов, т.е. в случае линейного кода с возможно большой размерностью $k$. За многие годы развития теории кодирования создано большое число разнообразных кодов. Мы остановимся только на относительно узком классе: классических и давно известных кодах Рида — Соломона и кодах Боуза — Чоудхури — Хоквингема (БЧХ-код). Код Рида — Соломона является частным случаем БЧХ-кода.

## 7.3 Проверочная и порождающая матрицы линейного кода и их свойства.

Будем пользоваться без объяснений стандартными понятиями теории конечных полей и линейной алгебры.

Подпространство $\mathcal{K}$ (линейный код над конечным полем $\mathbf{F}_q$) пространства $\mathbf{F}_q^n$ может быть определено (задано) двумя способами: как своим базисом, так и базисом пространства $\mathcal{K}^\perp$, двойственного к $\mathcal{K}$ (определение ниже). Первый способ определения кодов является более естественным, но зато второй во многих случаях более удобен для их построения и исследования их свойств. Он преимущественно используется в теории кодирования. Мы также часто будем пользоваться вторым способом задания линейного кода. Подробно объясним, что это такое.

Скалярное произведение $\langle \boldsymbol{x}, \boldsymbol{y} \rangle$ векторов $\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{y} = (y_1, \ldots, y_n) \in \mathbf{F}_q^n$ в поле $\mathbf{F}_q$ определяется соотношением

$$\langle \boldsymbol{x}, \boldsymbol{y} \rangle = \sum_{j=1}^{n} x_j y_j, \tag{3}$$

где сложение и умножение в последней сумме выполняется в поле $\mathbf{F}_q$.

Код $\mathcal{K}^\perp$ над $\mathbf{F}_q$ состоит из всех векторов $\boldsymbol{b} \in \mathbf{F}_q^n$, таких, что $\langle \boldsymbol{b}, \boldsymbol{a} \rangle = 0$ для всех $\boldsymbol{a} \in \mathcal{K}$. По другому, если $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_k$ — базис кода $\mathcal{K}$, то базисом кода $\mathcal{K}^\perp$ являются векторы $\boldsymbol{b}_1, \ldots, \boldsymbol{b}_{n-k}$, для которых $\langle \boldsymbol{b}_j, \boldsymbol{a}_s \rangle = 0$ для всех $s = 1, \ldots, k$. Отметим, что сумма размерностей кодов $\mathcal{K}$ и $\mathcal{K}^\perp$ равна $n$.

Матрица $B$, строками которой являются базисные векторы $\boldsymbol{b}_s$ кода $\mathcal{K}^\perp$ (их число $n-k$) называется проверочной матрицей кода $\mathcal{K}$, а матрица $A$, строками которой являются базисные векторы кода $\mathcal{K}$, называется порождающей матрицей кода $\mathcal{K}$. Таким образом, коду $\mathcal{K}$ принадлежат все векторы $\boldsymbol{a}$, для которых выполнено

$$B\boldsymbol{a}^T = 0, \quad \boldsymbol{a} \in \mathbf{F}_q^n, \tag{4}$$

где значок $^T$ обозначает «транспонирование» соответствующего объекта, или все векторы $\boldsymbol{a}$, которые имеют вид

$$\boldsymbol{a} = \vec{a}A, \quad \vec{a} \in \mathbf{F}_q^k, \ \boldsymbol{a} \in \mathbf{F}_q^n. \tag{5}$$

Заметим, что в формуле (4) $\boldsymbol{a}^T$ — столбец высоты $n$. Матрицы $B$ и $A$ по определению взаимно ортогональны: $A \cdot B^T = 0$, $B \cdot A^T = 0$.

**Утверждение 1.** *Код $\mathcal{K}$ имеет кодовое расстояние $d$, если выполнены два условия*

i. *Любой комплект из $d-1$ столбцов матрицы $B$ является линейно-независимым.*

ii. *Найдется комплект из $d$ столбцов матрицы $B$, который является линейно-зависимым.*

С помощью утверждения 1 все или почти все методы построения кодов $\mathcal{K}$ с кодовым расстоянием $d$ сводятся к построению проверочной матрицы $B$, у которой любой комплект из $d-1$ ее столбцов является линейно-независимым.

Наиболее известными матрицами $B$, для которых выполнено утверждение 1, являются матрицы

$$B = B_{\mathfrak{A}} = \begin{pmatrix} \alpha_1^0 & \alpha_2^0 & \cdots & \alpha_n^0 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_1^{d-2} & \alpha_2^{d-2} & \cdots & \alpha_n^{d-2} \end{pmatrix}, \ d > 2, \tag{6}$$

где $n \leqslant q-1$ и $\mathfrak{A} = \{\alpha_1, \alpha_1, \ldots, \alpha_n\}$ — различные ненулевые элементы поля $\mathbf{F}_q$. Столбцы любого комплекта из $d-1$ столбцов матрицы $B$ является линейно-независимыми. Это следует из того, что определитель

$$\begin{vmatrix} \beta_1^0 & \beta_2^0 & \cdots & \beta_{d-1}^0 \\ \beta_1 & \beta_2 & \cdots & \beta_{d-1} \\ \beta_1^2 & \beta_2^2 & \cdots & \beta_{d-1}^2 \\ \vdots & \vdots & \cdots & \vdots \\ \beta_1^{d-2} & \beta_2^{d-2} & \cdots & \beta_{d-1}^{d-2} \end{vmatrix}, \ \beta_j \in \{\alpha_1, \alpha_2, \ldots, \alpha_n\}, \tag{7}$$

с попарно различными $\beta_j$ является отличным от 0 определителем Вандермонда.

Множество $\mathfrak{A}$ часто расширяют, а именно, добавляют к нему элементы $0 \in \mathbf{F}_q$ и особый элемент $\infty$. Мы далее будем полагать, что матрица $B$ в (6) определена именно для такого расширенного множества $\mathfrak{A}$. О подробностях такого определения удобно рассказать ниже в разделе 7.4.

Нумерацию столбцов матрицы $B$ будем производить с помощью элементов множества $\mathfrak{A}$. Так, столбец с номером $\alpha$ является $j$-ым столбцом, если $\alpha = \alpha_j$. Совершенно аналогично поступаем с координатами вектора $\boldsymbol{x} = (x_{\alpha_1}, x_{\alpha_2}, \ldots, x_{\alpha_n}) \in \mathbf{F}_q^n$, их также индексируем элементами множества $\mathfrak{A}$, которые записаны в определенном порядке.

## 7.4 Коды Рида — Соломона.

Мы рассмотрим три вида кодов Рида — Соломона длин $n = q-1$, $q$, $q+1$. Все они имеют в качестве проверочной матрицу вида (6), но различные множества $\mathfrak{A}$.

Тип 1. $n = q-1$. В этом случае множество $\mathcal{A}$ состоит из всех ненулевых элементов поля $\mathbf{F}_q$.

Тип 2. $n = q$. В этом случае множество $\mathcal{A}$ состоит из всех элементов поля $\mathbf{F}_q$. Следует сказать, что столбец $(\alpha_j^0, \alpha_j, \ldots, \alpha_j^{d-2})^T$, у которого $\alpha_j = 0$ имеет вид $(1, 0, \ldots, 0)^T$.

Тип 3. $n = q+1$, $d > 3$. В этом случае множество $\mathcal{A}$ состоит из всех элементов поля $\mathbf{F}_q$ и еще одного элемента $\infty$ (бесконечности). Предполагается, что элемент $\infty$ обладает естественными свойствами этого понятия. Например, $a\infty = \infty$, $a \neq 0$, $\frac{a}{\infty} = 0$ и т.п. Столбец $(\alpha_j^0, \alpha_j, \ldots, \alpha_j^{d-2})^T$, у которого $\alpha_j = \infty$ по определению имеет вид $(0, 0, \ldots, 1)^T$. Более обще, мы считаем, что значение многочлена $f(x) = \sum_{s=0}^{d-2} f_s x^s$ степени не выше $d-2$ в точке $\infty$ является коэффициент $f_{d-2}$. В частности, $f(\infty) = 0$, если степень $f(x)$ меньше $d-2$. В этом случае мы говорим, что $f(x)$ имеет корень $\infty$. Можно сказать, что мы рассматриваем проективное пространство $\mathbf{F}_q \cup \{\infty\}$ и многочлены на нем.

Коды Рида — Соломона всех типов будем обозначать одним символом $RS_q(n, d)$. Все они имеют параметры $[n, n-d+1, d]_q$ и являются, так называемым, $q$-значными МДР-кодами (см. [17]), а именно кодами, которые имеют максимально возможную размерность $n - d + 1$ при заданных $n$ и $d$.

Одна из модификаций кода типа 3 (длины $n = q+1$) будет далее использована как основа для построения «системы открытого шифрования», которую мы будем подробно изучать. В частности, мы рассмотрим группу автоморфизмов (определение — ниже) этого кода. Эта группа имеет наиболее сложное строение по сравнению с группами автоморфизмов кодов типов 1 и 2. Поэтому мы сначала достаточно подробно изучим группу автоморфизмов кодов типа 2, а затем в основном без доказательства приведем нужные свойства группы автоморфизмов кода типа 3.

Надо сказать, что коды типа 3, в некотором смысле, являются наиболее интересными среди определенных ранее трех типов кодов Рида — Соломона. В частности, они имеют наиболее мощную группу автоморфизмов и наибольшую длину и размерность при заданном кодовом расстоянии $d$. Коды типа 1 используются для построения циклических кодов Боуза — Чоудхури — Хоквингема. Коды $RS_q(n, d)$ всех типов могут быть заданы (определены) и несколькими другими способами.

## 7.5 Код Боуза — Чоудхури — Хоквингема.

Предположим, что поле $\mathbf{F}_r, r = p^{l'}$ , где число $l'$ делит $l$ $(l'|l)$, является подполем поля $\mathbf{F}_q$, $q = p^l$. В этом случае мы будем рассматривать $r$-значный подкод кода $RS_q(n, d)$, $n = q-1$, который состоит из всех векторов $RS_q(n, d)$, координаты которых принадлежат полю $\mathbf{F}_r$. Этот код называют кодом Боуза — Чоудхури — Хоквингема (обозначение: $BCH_r(n, d)$). Он имеет параметры $[q-1, d', k']_r$, где $d' \geqslant d$, $k' \geqslant q - 1 - (d - 1 - [\frac{d-1}{r}])\frac{l}{l'}$. По поводу этих оценок и замечательных свойств кода $BCH_r(n, d)$ см. книгу [17].

Следует обратить внимание на то, что размерности кода $RS_q(n, d)$ и кода $BCH_r(n, d)$ вычисляются над разными полями: размерность первого — над $\mathbf{F}_q$, а размерность второго — над его подполем $\mathbf{F}_r$.

## 7.6 Группа автоморфизмов кода $RS_q(n, d)$, $n = q$.

Если переставить координаты кодового вектора $\boldsymbol{a}$ кода $\mathcal{K}$, то полученный вектор $\boldsymbol{a}'$ может как принадлежать, так и не принадлежать коду $\mathcal{K}$. Если перестановка координат $\sigma$ такова, что $\sigma(\boldsymbol{a}) = \boldsymbol{a}' \in \mathcal{K}$ для всех $\boldsymbol{a} \in \mathcal{K}$, то она называется автоморфизмом кода $\mathcal{K}$. Очевидно, что если $\sigma'$ — другой автоморфизм, то произведение $\sigma \cdot \sigma'$ также является автоморфизмом. Поэтому все автоморфизмы кода $\mathcal{K}$ образуют

группу $\Sigma_{\mathcal{K}}$, которая называется группой автоморфизмов кода $\mathcal{K}$. Заметим, что на множестве перестановок координат векторов пространства $\mathbf{F}_q^n$ можно естественным образом определить операцию $\cdot$, по отношению к которой все они образуют группу $S_n$ порядка $n!$, называемую симметрической группой.

Перестановку $\sigma$ удобно представлять себе в виде перестановочной матрицы $\Gamma_\sigma = \Gamma = \|\gamma_{i,j}\|$, которая реализует эту перестановку в виде матричного умножения. А именно, элемент матрицы $\gamma_{i,j}$ равен 1 тогда и только тогда, когда координата с номером $i$ переходит посредством действия $\sigma$ в координату с номером $j$. Во всех остальных случаях $\gamma_{i,j} = 0$. Таким образом, матрица $\Gamma$ представляет из себя матрицу, у которой в любой строке и в любом столбце имеется ровно одна 1. Перестановочная матрица $\Gamma$ реализует перестановку $\sigma$ координат вектора $\boldsymbol{a}$ в виде матричного умножения следующим образом $\sigma(\boldsymbol{a}) = \boldsymbol{a}\Gamma$. Матричная группа автоморфизмов $G = G_{\mathcal{K}}$ образована всеми матрицами $\Gamma_\sigma$, у которых $\sigma \in \Sigma_{\mathcal{K}}$.

Если $\Gamma \in G_{\mathcal{K}}$, а матрица $B$ является проверочной матрицей кода $\mathcal{K}$, то $B \cdot \Gamma$, очевидно, также является проверочной матрицей этого кода $\mathcal{K}$. Поэтому она может быть представлена в виде $B \cdot \Gamma = h \cdot B$, где невырожденная матрица $h$ размера $n-k \times n-k$ является матрицей перехода от одного базиса пространства строк матрицы $B$ к другому $B'$. Последнее высказывание на языке матриц записывается как раз в виде $B' = h \cdot B$.

Интересно отметить, что указанное отображение $\Gamma \to h$ реализует гомоморфизм матричной группы $G_{\mathcal{K}}$ автоморфизмов кода $\mathcal{K}$ (матрицы размера $n \times n$) в матричную группу, образованную матрицами $h$ размера $n-k \times n-k$. Ядро $J(\mathcal{K})$ этого гомоморфизма образуют элементы $\Gamma$, которые оставляют на месте все векторы кода $\mathcal{K}$. Поэтому матрицы $h$, на которые отображается группа $G_{\mathcal{K}}$ посредством соответствия $B \cdot \Gamma = h \cdot B$, изоморфна факторгруппе $G_{\mathcal{K}}/J(\mathcal{K})$. Так как далее мы ограничимся рассмотрением только кодов, у которых ядро $J(\mathcal{K})$ тривиально (состоит из одного элемента), то мы всегда будем полагать, группа, образованная матрицами $h$, изоморфна группе $G_{\mathcal{K}}$. К таким кодам относятся коды $RS_q(n,d)$ и коды $BCH_q(n,d)$. Доказательство этого утверждения в более общей форме см. ниже (Лемма 2).

Рассмотрим ансамбль (множество) $\mathcal{B}_{\mathcal{K}}$ кодов, определяемых проверочными матрицами из множества $\mathfrak{B} = \{B \cdot \Gamma | \Gamma \in S_n\}$, где $B$ — одна, не важно какая, матрица вида (6). Число $\text{Ч}_q(n,d)$ различных (как множеств) кодов $\mathcal{K} = RS_q(n,d)$ в ансамбле $\mathcal{B}_{\mathcal{K}}$ (по другому, кодов с проверочной матрицей вида (6)), как нетрудно видеть, равно

$$\text{Ч}_q(n,d) = \frac{n!}{|G_{\mathcal{K}}|}, \tag{8}$$

где $\mathcal{K} = RS_q(n,d)$ — один из фиксированных кодов Рида — Соломона с проверочной матрицей (6).

Как мы видим, число различных кодов Рида — Соломона полностью определяется порядком его группы автоморфизмов. К настоящему времени группа автоморфизмов $G_{\mathcal{K}}$ кода $\mathcal{K} = RS_q(n,d)$ не вычислена. Можно только утверждать, в $G_{RS_q(n,d)}$ входят подстановочные матрицы, которые реализуют подстановку $x \to ax, a \in \mathbf{F}_q \setminus \{0\} = \mathbf{F}_q^*$, элементов поля $\mathbf{F}_q$ в себя. Эти матрицы образуют группу, которая изоморфна, так называемой, мультипликативной группе поля $\mathbf{F}_q$. Эта группа является циклической, поэтому и коды Рида — Соломона также как и коды Боуза — Чоудхури — Хоквингема при $n = q-1$ с помощью соответствующей нумерации множества $\mathfrak{A}$ могут быть сделаны циклическими. На этом здесь останавливаться не будем (см. [17]).

## 7.7 Число проверочных матриц кода $RS_q(n,d)$

Если $h$ — невырожденная матрица размера $d-1 \times d-1$, то, как нетрудно видеть, проверочные матрицы $B$ и $hB$ определяют один и тот же код $RS_q(n,d)$. *Матрицы $B$ и $hB$ различны, если $h \neq E$ (единичная матрица).* Отсюда следует, что число различных проверочных матриц, которые определяют один и тот же код $RS_q(n,d)$, равно $N_{q,d-1}$, где $N_{q,s}$ — число невырожденных квадратных матриц $h$ размера $s \times s$.

**Лемма 1.** *Число $N_{q,s}$ равно*

$$N_{q,s} = (q^s - 1)(q^s - q) \cdots (q^s - q^{s-1}). \tag{9}$$

## 7.8 Обобщенные коды $RS_q(n,d)$, $n = q+1$, Рида — Соломона.

Нам удобно рассмотреть несколько более широкий по сравнению с $RS_q(n,d)$ класс кодов, который мы будем называть обобщенные коды Рида — Соломона и обозначать их тем же символом $RS_q(n,d)$.

Пусть $\mathbf{F}'_q = \mathbf{F}_q \cup \infty$ — поле, к которому добавлен элемент $\infty$. Рассмотрим матрицу

$$C = \begin{pmatrix} z_1\alpha_1^0 & z_2\alpha_2^0 & \cdots & z_n\alpha_n^0 \\ z_1\alpha_1 & z_2\alpha_2 & \cdots & z_n\alpha_n \\ z_1\alpha_1^2 & z_2\alpha_2^2 & \cdots & z_n\alpha_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ z_1\alpha_1^{d-2} & z_2\alpha_2^{d-2} & \cdots & z_n\alpha_n^{d-2} \end{pmatrix}, \quad d > 3,\ n = q = 1, \tag{10}$$

где $\alpha_j \in \mathbf{F}'_q$, $\alpha_j \neq \alpha_i$ при $j \neq i$ и при $\alpha_j = \infty$ соответствующий столбец матрицы $C$ имеет вид $(0, \ldots, 0, z_j)^T$.

Так же, как для обычного кода Рида — Соломона, обобщенный код длины $n = q+1$ имеет кодовое расстояние равное $d$ и размерность $n - d + 1$.

Матрица $C$, очевидно, может быть представлена в виде $C = B \cdot D$, где $D = \mathrm{diag}(z_1, z_2, \ldots, z_n)$, $z_j \in \mathbf{F}_q \setminus \{0\}$, — диагональная матрица и $B$ — проверочная матрица кода Рида — Соломона типа 3. Преобразованная матрица $C$ будет выступать далее как проверочная матрица системы открытого шифрования. В этой связи значительный интерес представляет строение группы обобщенных автоморфизмов кода Рида — Соломона с проверочной матрицей $B$, к изучению которой мы переходим.

Обобщенный код $BCH_r(n, d)$ определяется аналогично тому, как это было сделано в разделе 7.5: $BCH_r(n, d) = RS_q(n, d) \cap \mathbf{F}_r^n$, т.е. коду $BCH_r(n, d)$ принадлежат все векторы кода $RS_q(n, d)$, координаты которых принадлежат подполю $\mathbf{F}_r$ поля $\mathbf{F}_q$. Обобщенные коды $BCH_r(n, d)$ включают в себя и, так называемые, кода Гоппы (см. [17]).

Код можно задать и с помощью своей проверочной матрицы над полем $\mathbf{F}_r$ размера $n-k \times n$, где $k$ — размерность (над $\mathbf{F}_r$) кода $BCH_r(n, d)$. Эта матрица также может иметь вид (10). Определить размерность $k$ даже в частных случаях обобщенных кодов $BCH_r(n, d)$, в отличие от размерности любого кода $RS_q(n, d)$, очень нетривиально. В общем случае сделать это не представляется возможным.

## 7.9 Группа обобщенных автоморфизмов кода $RS_q(n, d)$, $n = q + 1$, Рида — Соломона

. Если в качестве обычных автоморфизмов кода $\mathcal{K}$ выступали перестановочные матрицы $\Gamma$, то в качестве обобщенных автоморфизмов выступают матрицы вида $\Lambda = \Gamma \cdot D$, где $D$ — невырожденная диагональная матрица, которые носят название мономиальных. Другими словами, $\Lambda$ — перестановочная матрица, у которой ненулевыми элементами являются ненулевые элементы поля $\mathbf{F}_q$.

Мономиальные матрицы сохраняют расстояние Хемминга. А именно, $d(\boldsymbol{a}, \boldsymbol{b}) = d(\boldsymbol{a}\Lambda, \boldsymbol{b}\Lambda)$. Как будет видно ниже, это свойство позволяет использовать эти матрицы в системе открытого шифрования. Нашей основной целью является получение нетривиальных нижних верхних оценок порядка группы обобщенных автоморфизмов кода $RS_q(n, d)$ и затем оценок для числа различных кодов $RS_q(n, d)$.

Теперь переформулируем для обобщенных автоморфизмов некоторые из определений раздела 7.6.

Если мономиальная матрица $\Lambda$ такова, что $\boldsymbol{a}\Lambda = \boldsymbol{a}' \in \mathcal{K}$ для всех $\boldsymbol{a} \in \mathcal{K}$, то она называется обобщенным автоморфизмом кода $\mathcal{K}$. Очевидно, что если $\Lambda'$ — другой автоморфизм, то произведение $\Lambda \cdot \Lambda'$ также является автоморфизмом. Поэтому все обобщенные автоморфизмы кода $\mathcal{K}$ образуют группу $\Xi_{\mathcal{K}}$, которая называется группой обобщенных автоморфизмов кода $\mathcal{K}$. Элементами группы $\Xi_{\mathcal{K}}$ являются, так называемые, мономиальные матрицы размера $n \times n$. Также как в разделе 7.6 можно рассмотреть представление $H_{\mathcal{K}}$ группы обобщенных автоморфизмов $\Xi_{\mathcal{K}}$ в виде невырожденных матриц над $\mathbf{F}_q$ размера $n - k \times n - k$. А именно, элементу $\Lambda$ из $\Xi_{\mathcal{K}}$ сопоставим матрицу $h = h_\Lambda$, которая определяется соотношением

$$h_\Lambda \cdot B = B \cdot \Lambda. \tag{11}$$

Произведению $\Lambda \cdot \Lambda'$ двух элементов из $\Xi_{\mathcal{K}}$ соответствует произведение $g(\Lambda \cdot \Lambda') = h_{\Lambda'} \cdot h_\Lambda$ двух элементов из $H_{\mathcal{K}}$. Заметим, что порядок следования сомножителей в $H_{\mathcal{K}}$ обратный по сравнению с $\Xi_{\mathcal{K}}$. Поэтому рассматриваемое отображение является гомоморфизмом $g : \Lambda \to h_\Lambda$ группы $\Xi_{\mathcal{K}}$ в группу матриц размера $n - k \times n - k$ над полем $\mathbf{F}_q$.

**Лемма 2.** *Для кода $\mathcal{K} = RS_q(n, d)$ гомоморфизм $g$ является изоморфизмом, т.е. $|\Xi_{\mathcal{K}}| = |H_{\mathcal{K}}|$.*

**Теорема 1.** *Порядок группы $\Xi_{\mathcal{K}}$ автоморфизмов кода Рида — Соломона $\mathcal{K} = RS_q(n, d)$ не превосходит $N_{q,d-1}$, где $N_{q,s}$ — число невырожденных квадратных матриц $h$ размера $s \times s$ над полем $\mathbf{F}_q$.*

Хотя оценка для числа $\Xi_{\mathcal{K}}$ во многих случаях, по-видимому, весьма грубая, ничего лучшего не известно.

Рассмотрим ансамбль (множество) $\mathcal{A}_{\mathcal{K}}$, $\mathcal{K} = RS_q(n,d)$, кодов, определяемых проверочными матрицами из множества $\mathfrak{B} = \{B\Lambda | \Lambda \in U_{q,n}\}$, где $B$ — одна, не важно какая, матрица вида (6), а $U_{q,n}$ — множество всех мономиальных матриц над полем $\mathbf{F}_q$. Заметим, что ансамбль $\mathcal{A}_{\mathcal{K}}$ совпадает с множеством кодов, проверочные матрицы которых имеют вид (10). Кроме того, нетрудно установить, что $|U_{q,n}| = n!(q-1)^n$. Нас будет интересовать число различных кодов в ансамбле $\mathcal{A}_{\mathcal{K}}$.

По тем же соображениям, что приведены в разделе 7.6, для числа $A_q(n,d)$ различных обобщенных кодов Рида — Соломона $\mathcal{K} = RS_q(n,d)$ в ансамбле $\mathcal{A}_{\mathcal{K}}$ имеет место равенство

$$A_q(n,d) = \frac{n!(q-1)^n}{|\Xi_{\mathcal{K}}|}. \tag{12}$$

К сожалению, группа $\Xi_{\mathcal{K}}$ обобщенных автоморфизмов кода Рида — Соломона не известна. Поэтому мы не можем воспользоваться равенством (12) для вычисления числа $A_q(n,d)$.

Из теоремы 1 и соотношений (9) и (12) следует

**Следствие 1.** *Для числа $A_q(n,d)$ различных обобщенных Рида — Соломона $\mathcal{K} = RS_q(n,d)$ в ансамбле $\mathcal{A}_{\mathcal{K}}$ имеет место оценка*

$$A_q(n,d) \geqslant \frac{n!(q-1)^n}{N_{q,k}} = \frac{n!(q-1)^n}{(q^{d-1}-1)(q^{d-1}-q)\cdots(q^{d-1}-q^{d-2})}, \tag{13}$$

*где $k = n-d+1$ — размерность кода $\mathcal{K} = RS_q(n,d)$ и $N_{q,k}$ — число различных невырожденных матриц размера $k \times k$.*

Далее мы докажем, что группа $\Xi_{\mathcal{K}}$ содержит подгруппу, изоморфную группе дробно-линейных преобразований. Строение последней группы мы изучим в следующем разделе.

## 7.10 Группа дробно-линейных преобразований.

Элементами группы дробно-линейных преобразований $\Phi_q$ множества $\mathbf{F}'_q = \mathbf{F}_q \cup \{\infty\}$ в себя являются дробно-линейные функции $\varphi(x) = \frac{ax+b}{cx+e}$, отличные от постоянной, т.е. функции, у которых определитель матрицы $\begin{pmatrix} a & b \\ c & e \end{pmatrix}$ отличен от нуля. Очевидно, каждое дробно-линейных преобразование $\varphi(x)$ взаимно однозначно отображает множество $\mathbf{F}'_q$ в себя.

Множество $\Phi_q$ действительно является некоммутативной группой. «Умножением» $\otimes$ в ней служит суперпозиция функций, т.е. $\varphi \otimes \varphi' = \varphi(\varphi'(x))$. Группа $\Phi_q = PGL(2,q)$ имеет порядок $(q+1)q(q-1)$. Очень интересным свойством группы $\Phi_q$ является ее трижды транзитивность. Это означает, что для любых двух пар троек $(a_1,a_2,a_3)$ и $(b_1,b_2,b_3)$, $a_i, b_i \in \mathbf{F}'_q$, с попарно различными координатами в группе $\Phi_q$ найдется элемент $\varphi$ (всегда один), для которого выполнено $\varphi(a_i) = b_i$, $i = 1,2,3$.

**Теорема 2.** *Группа $\Xi_{\mathcal{K}}$ обобщенных автоморфизмов кода $\mathcal{K} = RS_q(n,d)$, $n = q+1$, Рида — Соломона с проверочной матрицей $B$ (см. (6)) содержит подгруппу, которая изоморфна группе дробно-линейных преобразований множества $\mathbf{F}'_q$.*

Этот результат будет использован при анализе стойкости системы открытого шифрования, построенной с помощью кода Рида — Соломона.

Группа $\Xi_{\mathcal{K}}$ обобщенных автоморфизмов кода Рида — Соломона также является трижды транзитивной в следующем смысле. Для любой пары упорядоченных троек из попарно различных элементов $(\beta_1,\beta_2,\beta_3)$ и $(\gamma_1,\gamma_2,\gamma_3)$, где $\{\beta_1,\beta_2,\beta_3\}$, $\{\gamma_1,\gamma_2,\gamma_3\} \in \mathfrak{A} = \{\alpha_1,\alpha_2,\ldots,\alpha_n\} = \mathbf{F}'_q$ существует такая мономиальная матрица $\Lambda_\varphi \in \Xi_{\mathcal{K}}$, которая переводит координаты $x_{\beta_1}, x_{\beta_2}, x_{\beta_3}$ вектора $\boldsymbol{x} = (x_{\alpha_1}, x_{\alpha_2}, \ldots, x_{\alpha_n})$ в координаты $x_{\gamma_1}, x_{\gamma_2}, x_{\gamma_3}$ вектора $\boldsymbol{x}\Lambda_\varphi$ с умножением их на соответствующие постоянные, определяемые диагональной матрицей $D_\varphi = \operatorname{diag}(d_{\alpha_1}, d_{\alpha_2}, \ldots, d_{\alpha_n})$. Например, с помощью подходящей матрицы $\Lambda_\varphi$ можно передвинуть на первые три места любые три координаты вектора $\boldsymbol{x}$. В частности, если $\{\beta_1 = 1, \beta_2 = 0, \beta_3 = \infty\}$ и $\gamma_1 = \alpha_1, \gamma_2 = \alpha_2, \gamma_3 = \alpha_3$, то $\boldsymbol{x}\Lambda_\varphi = (d_{\alpha_1}x_1, d_{\alpha_2}x_0, d_{\alpha_3}x_\infty, d_{\alpha_4}x_{\varphi(\alpha_4)}, \ldots, d_{\alpha_n}x_{\varphi(\alpha_n)})$ для некоторой подходящей функции $\varphi(x)$.

# 8 Декодирование

Мы приведем ряд утверждений о декодировании кодов, которые будут играть центральную роль при обосновании стойкости рассматриваемых систем открытого шифрования.

Неформально говоря, под термином «декодирование» понимается алгоритм, который позволяет по искаженному ошибками кодовому вектору $\boldsymbol{a}'$ восстановить исходный кодовый вектор $\boldsymbol{a}$. Таким образом, декодирование сводится к решению уравнения

$$\boldsymbol{a}' = \boldsymbol{a} + \boldsymbol{e},\ \boldsymbol{a} \in \mathcal{K},\ \ \mathrm{wt}(\boldsymbol{e}) \leqslant t, \tag{14}$$

где неизвестными являются кодовый вектор $\boldsymbol{a}$ и вектор ошибки $\boldsymbol{e}$.

Имеется несколько различных типов декодирования.

i. *Корреляционное декодирование кода $\mathcal{K}$.* Это алгоритм, который по предъявленному вектору $\boldsymbol{x} \in \mathbf{F}_q^n$ находит один или несколько кодовых векторов $\boldsymbol{a} \in \mathcal{K}$, ближайших (в метрике Хемминга) к $\boldsymbol{x}$.

ii. *Декодирование кода $\mathcal{K}$ в пределах его кодового расстояния.* Это алгоритм, который по вектору $\boldsymbol{x}$, который отстоит от одного из кодовых векторов $\mathcal{K}$ на расстояние $\leqslant \frac{d(\mathcal{K})-1}{2}$, вычисляет этот ближайший кодовый вектор. Этот вектор обязательно является единственным. Векторы $\boldsymbol{x}$, которые отстоят от всех кодовых точек на расстояние большее, чем половина кодового расстояния, могут быть декодированы как угодно, в частности, алгоритм может вообще отказаться от их декодирования.

iii. *Декодирование кода $\mathcal{K}$ за пределами его кодового расстояния.* (Алгоритм промежуточного положения между i. и ii.) Это алгоритм, который по вектору $\boldsymbol{x}$, находящемуся не очень далеко ($d(\boldsymbol{x}, \boldsymbol{a}) \leqslant t'$) от некоторого кодового вектора $\boldsymbol{a}$ кода $\mathcal{K}$, вычисляет один или несколько кодовых векторов $\boldsymbol{a}'$, находящихся на расстоянии $\leqslant t'$ от $\boldsymbol{x}$, где $t' > \frac{d(\mathcal{K})-1}{2}$ — некоторая постоянная (параметр алгоритма).

Наиболее сильным и трудным для реализации является алгоритм i. В настоящее время не известно ни одного нетривиального класса кодов, которые имеют алгоритм декодирования этого типа с простой реализацией. Другими словами, этот алгоритм может быть реализован только с помощью перебора. А именно, можно сравнивать $\boldsymbol{x}$ со всеми векторами кода и выделять среди них ближайшие кодовые векторы, или осуществлять просмотр векторов из окрестности $\boldsymbol{x}$, пытаясь найти в ней кодовый вектор. Какой из этих упомянутых алгоритмов перебора выгодней с вычислительной точки зрения зависит от соотношений между параметрами кода.

Сложность реализации корреляционного декодирования нетривиальных кодов возрастает как экспоненциальная функция от их длины. На практике ни один из таких кодов на современных вычислительных средствах не может быть декодирован, начиная с длины $\approx 100$.

Наиболее легким для реализации является алгоритм декодирования типа ii. Для большинства так называемых алгебраических кодов известны алгоритмы декодирования в пределах их кодового расстояния, сложность которых возрастает как полином небольшой степени от длины кода. К таким кодам относятся и, рассмотренные нами, обобщенные коды Рида — Соломона $RS_q(n, d)$. Их декодирование в пределах кодового расстояния может быть осуществлено не более, чем за $O(n^3)$ операций в поле $\mathbf{F}_q$ [17], [15].

Не надо думать, что для каждого кода существует простой алгоритм декодирования в пределах его кодового расстояния. По современным представлениям такие алгоритмы могут существовать только для кодов, которые снабжены определенной алгебраической или комбинаторной структурой. Вместе с тем у большинства кодов, не очень точно выражаясь, отсутствует в проверочной матрице какая-либо структура, — это коды «общего положения». Примером первого типа кодов является код Рида — Соломона или код Рида — Маллера (совершенно разные коды), а примером второго — код, у которого проверочная матрица выбрана случайно среди всех матриц определенной размерности.

Декодирование в пределах кодового расстояния (типа ii.) некоторых типов кодов общего положения является NP-полной задачей, т.е. предположительно не может быть осуществлено за полиномиальное время от их длины. Более того, общепринято, что

> **Тезис А:** *декодирование последовательности кодов, которые не обладают полезной для декодирования алгебраической или комбинаторной структурой, не может быть осуществлено за полиномиальное время от их длины.*

Это достаточно расплывчатое, но очень правдоподобное утверждение строго не доказано и в настоящее время возможность его доказательства весьма проблематична. Вместе с тем на этом утвер-

ждении «держится» обоснование стойкости открытого шифрования на базе кодов, корректирующих ошибки. Мы далее, специально не указывая на это, будем постоянно его придерживаться.

Обычно при построении кода, корректирующего ошибки, стараются наделять его определенной структурой, которая обеспечивает, с одной стороны, заданное значение его кодового расстояния, и, с другой, позволяет осуществлять его декодирование с малой вычислительной сложностью.

Приведем одно почти очевидное утверждение о сложности декодирования любого кода с помощью алгоритма типа ii.

**Утверждение 2.** *Любой линейный код $\mathcal{K}$ с параметрами $[n,k,d]_r$, $d \leqslant n/2$, имеет алгоритм декодирования в пределах его кодового расстояния, сложность которого не выше* $O(\min(nr^k, n\sum_{j=0}^{t}\binom{n}{j}))$, *где* $t = [\frac{d-1}{2}]$.

Отметим, что $r^k$ — число элементов в коде $\mathcal{K}$ и $O(nr^k)$ — число операций, требуемых для перебора всех элементов кода и сравнения каждого из них с искаженным кодовым вектором $\boldsymbol{a}'$. Далее, $\sum_{j=0}^{t}\binom{n}{j}(r-1)^j$ — число элементов в шаре радиуса $t$ с центром в точке $\boldsymbol{x}$ и $O(n\sum_{j=0}^{t}\binom{n}{j})$ — число операций, требуемых для перебора всех элементов шара с целью нахождения среди них кодового вектора.

# 9 Система открытого шифрования на основе кода, корректирующего ошибки

## 9.1 Система открытого шифрования Маклиса.

Идею построения системы открытого шифрования проще всего пояснить на примере кода Боуза — Чоудхури — Хоквингема $BCH_r(n,d)$ размерности $k$.

Пусть $A$ — фиксированная порождающая матрица обобщенного кода $BCH_r(n,d)$ над $\mathbf{F}_r$, т.е. матрица ранга $k$ и размера $k \times n$, для которой $A \cdot C^T = 0$, где $C$ — матрица, определенная соотношением (10). Между прочим, в качестве $A$ можно взять матрицу, которая имеет тот же вид, что и $C$. Этот факт мы использовать не будем.

Ансамбль $\mathcal{A}_r(n,d)$ порождающих матриц обобщенного кода $BCH_r(n,d)$ определим как множество всех матриц вида $h \cdot A \cdot \Gamma \cdot D$, где $h$ пробегает множество всех невырожденных $k \times k$-матриц над $\mathbf{F}_r$, $D$ — множество всех диагональных матриц с ненулевыми на диагонали элементами, а $\Gamma$ — множество всех перестановочных матриц размера $n \times n$. Соответственно, ансамбль кодов $\mathcal{K}_r(n,d)$ определяется как множество всех кодов с порождающими матрицами из ансамбля $\mathcal{A}_r(n,d)$. Матрицы $h$, $\Gamma$, $D$ «маскируют» матрицу $A$.

Передача секретного сообщения абонента $\mathcal{Y}$, предназначенного абоненту $\mathcal{X}$, предваряется следующими действиями. Абонент $\mathcal{X}$ случайно, равновероятно в соответствующем множестве и независимо от других абонентов выбирает матрицы $h = h_{\mathcal{X}}$, $D = D_{\mathcal{X}}$, $\Gamma = \Gamma_{\mathcal{X}}$ и вычисляет матрицу $A' = A'_{\mathcal{X}} = h_{\mathcal{X}} \cdot A \cdot \Gamma_{\mathcal{X}} \cdot D_{\mathcal{X}}$ из ансамбля $\mathcal{A}_r(n,d)$. Матрица $A'_{\mathcal{X}}$ является открытым (общедоступным для всех абонентов) ключом (public key), а матрицы $h_{\mathcal{X}}, \Gamma_{\mathcal{X}}, D_{\mathcal{X}}$ — секретным ключом (private key) абонента $\mathcal{X}$.

Шифрованная информация $\mathbf{b}$ (криптограмма), которую абонент $\mathcal{Y}$ передает по общедоступному каналу абоненту $\mathcal{X}$, в системе Маклиса [10] представляет собой вектор длины $n$ и вида $\boldsymbol{b} = \vec{a}A'_{\mathcal{X}} + \boldsymbol{e}$, где $\vec{a}$ — $r$-значный вектор длины $k$, несущий конфиденциальную информацию абонента $\mathcal{Y}$, а $\boldsymbol{e}$ — секретный вектор ошибок веса, не превосходящего $t$, и длины $n$, который случайно и равновероятно выбирается абонентом $\mathcal{Y}$ среди всех векторов веса не выше t.

Таким образом, для того чтобы расколоть открытую информацию, необходимо представить вектор $\boldsymbol{b}$ в виде

$$\boldsymbol{b} = \boldsymbol{a} + \boldsymbol{e}, \tag{15}$$

где вектор $\boldsymbol{a} = \vec{a}A'_{\mathcal{X}}$ принадлежит коду $K = K_{\mathcal{X}}$ с порождающей матрицей $A'_{\mathcal{X}}$, а вектор $\boldsymbol{e}$ имеет вес $\leqslant t$.

Другими словами, злоумышленнику необходимо декодировать код $K$ с известной порождающей матрицей $A'_{\mathcal{X}}$. Матрица $A'_{\mathcal{X}}$ замаскирована матрицами $h$, $D$ и $\Gamma$ и поэтому она, вообще говоря, представляется нападающей стороне как матрица общего положения. По тезису А в этом случае сложность

декодирования не является полиномиальной от длины $n$ кода $K$. Следовательно, при достаточно больших $n$ процедура декодирования недоступна для злоумышленника из-за ее большой вычислительной сложности. Вместе с тем декодирование кода $K$ той же длины $n$ для легитимного абонента $\mathcal{X}$, знающего секретный ключ, является вычислительно достижимым.

Действительно, абонент $\mathcal{X}$, получив вектор $\boldsymbol{b}$, восстанавливает кодовый вектор $\vec{a}A'_{\mathcal{X}}$ следующим образом. Сначала он строит вектор $\boldsymbol{b}' = \boldsymbol{b}D^{-1} \cdot \Gamma^{-1}$, который , очевидно, является вектором кода $BCH_r(n,d)$ с порождающей матрицей $A$, искаженный не более, чем в $t$ разрядах. Как раз здесь используется тот факт, что мономиальная матрица $D^{-1} \cdot \Gamma^{-1}$ сохраняет вес вектора $\boldsymbol{e}$ (см. раздел 7.9). Затем с помощью какого-либо общеизвестного полиномиального алгоритма декодирования кода $BCH_r(n,d)$ находится вектор $\vec{a}'$, который удовлетворяет условию $\boldsymbol{b}' = \vec{a}'A + \mathbf{e}'$, где $w(\boldsymbol{e}') \leqslant t$. Затем вычисляется вектор $\vec{a}$ в виде $\vec{a} = \vec{a}'h^{-1}$.

Мы будем предполагать, что $t \leqslant (d-1)/2$. Вместе с тем можно полагать, что $t > d-1)/2$, но $t$ меньше некоторой границы. При этом надо использовать алгоритм декодирования работы [15], который работают при определенном ограничении на величину $t$ «почти всегда» правильно. Как будет видно ниже, чем больше алгоритм декодирования исправляет ошибок, тем выше будет стойкость системы шифрования. Вместе с тем при возрастании числа исправляемых ошибок, как правило, возрастает и сложность его реализации. В идеале, лучше всего использовать корреляционный алгоритм, но его сложность является слишком высокой и он не доступен для реализации. Обычно в системе Маклиса используют алгоритмы типа ii или iii.

## 9.2 Система открытого шифрования Нидеррайтера.

В системе Нидеррайтера [14] рассматривается ансамбль $\mathcal{B}_r(n,d)$ проверочных матриц кода $BCH_r(n,d)$, который определяется как множество всех матриц вида $B' = h \cdot C \cdot D \cdot \Gamma$, где $C$ — фиксированная проверочная матрица вида (10), $h$ пробегает множество всех невырожденных $n-k \times n-k$-матриц над $\mathbf{F}_r$, $D$ — множество всех диагональных матриц с ненулевыми на диагонали элементами, а $\Gamma$ — множество всех перестановочных матриц размера $n \times n$.

Подобно системе Маклиса открытым ключом абонента $\mathcal{X}$ в системе Нидеррайтера является матрица $B'$, а секретным — матрицы $h$, $D$, $\Gamma$.

Шифрованная информация $\boldsymbol{c}$ абонента $\mathcal{Y}$ и предназначенная абоненту $\mathcal{X}$ в системе Нидеррайтера представляет собой $r$-значный длины $n-k$ и вида

$$\boldsymbol{c} = \boldsymbol{e}{B'}^T, \tag{16}$$

где $B' = B'_{\mathcal{X}}$ проверочная матрица, которая случайно выбрана абонентом $\mathcal{X}$ из ансамбля $\mathcal{B}_r(n,d)$ и $k$ — размерность кода с этой проверочной матрицей. Вектор $\boldsymbol{e}$ является вектором длины $n$ и веса, не превосходящего $t$, который несет конфиденциальную информацию абонента $\mathcal{Y}$.

Заметим, что конфиденциальная информация является одним из решений уравнения

$$\boldsymbol{c} = \mathbf{x}{B'}^T. \tag{17}$$

Найти какое-либо решение этого уравнения — простая задача, так как это линейное уравнение с $n-k$ уравнениями и $n$ неизвестными. Найти среди всех решений (их число $2^k$) решение с минимальным весом — это уже сложная задача, которая эквивалентна задаче декодирования кода с проверочной матрицей $B'$.

Также как в системе Маклиса в системе Нидеррайтера матрица $B'$ представляется нападающей стороне матрицей общего положения.

В теории кодирования вектор $\boldsymbol{c}$ из (16) называют синдромом вектора $\boldsymbol{e}$. Отметим, что матрицы $B'$ и $A'$ связаны соотношением $B' \cdot {A'}^T = 0$, где $A'$ — одна из матриц ансамбля $\mathcal{A}_r(n,d)$. Строки матрицы $B'$ являются базисом подпространства размерности $n-k$, ортогонального к пространству строк матрицы $A'$.

Абонент $\mathcal{X}$, получив сообщение $\boldsymbol{c}$, находит какой-либо вектор $\boldsymbol{b}$, который является решением уравнения $\mathbf{x}{B'}^T = \boldsymbol{c}$. Очевидно, вектор $\boldsymbol{b}$ является вектором вида $\boldsymbol{b} = \vec{a}A' + \boldsymbol{e}$ при некотором неизвестном $\vec{a} \in \mathbf{F}_r^k$. Затем абонент $\mathcal{X}$ также, как в системе Маклиса, декодирует вектор $\boldsymbol{b}\Gamma^{-1} \cdot D^{-1} = \boldsymbol{b}' = \vec{a}'A + \boldsymbol{e}'$, но вместо кодового вектора $\vec{a}'A$ находит вектор $\boldsymbol{e}' = \boldsymbol{b}' - \vec{a}'A$, а затем и вектор $\boldsymbol{e} = \boldsymbol{e}'\Gamma \cdot D$. Отметим, что в отличие от системы Маклиса, в системе при расшифровании (восстановлении вектора $\boldsymbol{e}$) никак не участвует матрица $h$. Она нужна только для маскировки матрицы $B'$.

Как и выше, предполагаем, что используемый алгоритм декодирования кода $BCH_r(n,d)$ всегда правильно восстанавливает вектор ошибок $\mathbf{e}$.

## 9.3 Сравнение систем открытого шифрования Маклиса и Нидеррайтера.

Системы Маклиса и Нидеррайтера обладают одинаковой стойкостью к нападению, ибо криптографическая атака на одну из систем может быть легко трансформирована в атаку на другую. Поясним это подробно.

Мы полагаем, что обе взаимно ортогональные матрицы $A'$ (открытый ключ системы Маклиса) и $B'$ (открытый ключ системы Нидеррайтера) известны нападающей стороне, так как одна из другой может быть получена как решение линейной системы уравнений $A' \cdot B'^T = 0$, т.е. с помощью не более, чем $O(n^3)$ операций.

При известном синдроме $\boldsymbol{c} = \boldsymbol{e}B'^T$ нетрудно вычислить вектор $\boldsymbol{b} = \vec{a}A' + \boldsymbol{e}$ с некоторым вектором $\vec{a} \in \mathbf{F}_r^k$ такой, что $\boldsymbol{c} = \boldsymbol{b}B'^T$. Для этого надо найти какое-либо решение $\boldsymbol{b}$ уравнения (17). Вектор $\boldsymbol{b}$ мы будем рассматривать как криптограмму в системе Маклиса. Если для системы Маклиса найдена криптографическая атака со сложностью $Q$, т.е. известен алгоритм вычисления вектора $\vec{a}$ (конфиденциальная информация в системе Маклиса), то вектор $\boldsymbol{e}$ (конфиденциальная информация в системе Нидеррайтера), очевидно, представляется в виде $\boldsymbol{e} = \boldsymbol{b} - \vec{a}A'$, т.е. сложность определения $\boldsymbol{e}$, по существу, совпадает со сложностью определения $\vec{a}$.

Наоборот, если для системы Нидеррайтера известна криптографическая атака со сложностью $Q$, то используя в качестве криптограммы этой системы вектор $\boldsymbol{c} = \boldsymbol{b}B'^T = (\vec{a}A' + \boldsymbol{e})B'^T = \boldsymbol{e}B'^T$, где $\boldsymbol{b}$ — криптограмма системы Маклиса, вычислим вектор ошибок $\boldsymbol{e}$, а затем и вектор $\vec{a}$, который является единственным решением линейного уравнения $\vec{y}A' = \boldsymbol{b} - \boldsymbol{e}$.

Соображения, использованные в предыдущих двух абзацах, любезно сообщены автору в устной беседе Г.А. Кабатянским.

## 9.4 Некоторые свойства систем открытого шифрования Маклиса и Нидеррайтера.

Две эти системы различаются скоростью передачи. Если код $\mathcal{K}$ является низкоскоростным, т.е. $k/n$ — малое число, то скорость передачи у системы Нидеррайтера всегда выше по сравнению с системой Маклиса. Поэтому далее будем рассматривать только ее. Вместе с тем будем предполагать, не оговаривая этого особо, что криптограммой системы Нидеррайтера является $n$-мерный вектор $\boldsymbol{b} = \vec{a}A' + \boldsymbol{e}$, который является каким-либо решением системы (17), где $\boldsymbol{c} = \boldsymbol{b}B'^T = \boldsymbol{e}B'^T$ и $\boldsymbol{e}$ — вектор веса не выше $t$ (информационный вектор абонента $\mathcal{Y}$). Это связано с тем, что алгоритм декодирования кода $RS_q(n,d)$, рассмотренный в [16], и некоторые известные криптографические атаки оперируют с искаженным кодовым вектором $\boldsymbol{b}$, а не с его синдромом $\boldsymbol{c}$.

Шифрование сообщения $\boldsymbol{e}$ состоит в вычислению его синдрома и поэтому его сложность равна $O((n-k)n)$ операций. Сложность расшифрования (сложность восстановления вектора $\boldsymbol{e}$) определяется, в основном, трудоемкостью алгоритма декодирования кода $RS_q(n,d)$ и при использовании алгоритма декодирования работы [16] не превосходит $O(n^3)$ операций. Для декодирования в пределах кодового расстояния известны и более быстрые алгоритмы.

Как известно [18], кодовые системы открытого шифрования имеют большую скорость шифрования по сравнению с другими подобными системами, например, с системой RSA. Вместе с тем они обладают, по меньшей мере, двумя недостатками.

Во-первых, скорость передачи у кодовой системы всегда меньше 1 (обычно меньше 1/2), в то время как в системе RSA (см. [19] и многие другие работы) она равна 1.

Во-вторых, открытый ключ (в рассматриваемой кодовой системе — матрица $B'$) имеет объем примерно в $n-k$ раз больший, чем у упомянутой системы RSA. Если $k$ — относительно маленькое число, то выгодней в качестве открытого ключа системы рассматривать матрицу $A'$, которая связана с $B'$ соотношением $B' \cdot A' = 0$.

Кроме того, работ по оценке стойкости кодовых систем известно значительно меньше, чем для системы RSA.

В системе открытого шифрования Нидеррайтера в качестве открытой информации выступают векторы $\boldsymbol{e}$ веса $t$ и менее. Для ее реализации необходимо иметь алгоритм, который отображает

множество всех $r$-ных векторов длины $s$ в множество $W_t$ векторов длины $n$ и веса не выше $t$, где $s \leqslant \tau(t, N) = [\lg_r \sum_{i=0}^{t} \binom{N}{i}(r-1)^i]$ (логарифм числа возможных сообщений в системе Нидеррайтера).

Система Нидеррайтера полностью определяется как проверочной матрицей $B'$, так и ортогональной к ней порождающей матрицей $A'$, и наоборот. Поэтому открытым ключом этой системы естественно считать матрицу, которая содержит меньшее число строк, хотя криптограмма $\boldsymbol{c} = \boldsymbol{e}B'$ всегда реально строится с помощью матрицы $B'$.

Переход от системы Маклиса к системе Нидеррайтера полезен не только с точки зрения повышения скорости передачи, но и, что, возможно, более важно, позволяет с помощью несложной модернизации существенно усилить ее стойкость к криптографическим атакам. По поводу этого вопроса см. работу [12].

## 10 Как раскалывается система открытого шифрования Нидеррайтера, построенная с помощью обобщенного кода Рида — Соломона? Общие подходы.

В этом разделе мы рассматриваем систему Нидеррайтера, построенную с помощью $q$-значного кода из ансамбля $\mathcal{B}_q(n, d)$ (см. начало раздела 9.2). Как было установлено в разделе 9.3, соответствующая система Маклиса (система, в которой порождающие матрицы выбираются из ансамбля $\mathcal{A}_q(n, n-d+1)$ имеет примерно ту же стойкость к нападению, что и рассматриваемая система открытого шифрования.

Имеется два вида атак на систему открытого шифрования.

i. «Чтение» открытого сообщения абонента $\mathcal{Y}$ без использования секретного ключа абонента $\mathcal{X}$ (бесключевое чтение). В данном случае секретным ключом являются матрицы $h, \Gamma, D$.

ii. Вычисление секретного ключа абонента $\mathcal{X}$ с последующим вычислением открытых сообщений абонента $\mathcal{Y}$, направляемых им абоненту $\mathcal{X}$.

Рассмотрим сначала атаку i. Для ее реализации необходимо решить уравнение (17). С точки зрения нападающей стороны матрица $B'$ является матрицей общего положения. Поэтому для нахождения решения $\boldsymbol{e}$ уравнения (17) веса $\mathrm{wt}(\boldsymbol{e}) \leqslant t$ в соответствие с тезисом А необходимо проделать экспоненциальное от его длины $n$ число операций. Можно полагать, что при большем $n \approx 100$ это невозможно на современном уровне развития вычислительной техники.

Другой подход, реализующий атаку i., состоит в следующем. Можно «угадать» обобщенный код Рида — Соломона, определяемый проверочной матрицей $B'$, и произвести декодирование (решить уравнение (17)) в этом коде. По следствию 1 число таких кодов $A_q(n, d)$ не меньше $\frac{n!(q-1)^n}{(q^{d-1}-1)(q^{d-1}-q)\cdots(q^{d-1}-q^{d-2})}$. Это число при $n \approx 100$, $d \leqslant n/2$ и $q \geqslant 2$ больше, чем $10^{77}$. Поэтому это событие очень маловероятно и его можно не рассматривать.

Таким образом, по современным представлением с учетом тезиса А бесключевое чтение (атака i) в рассматриваемой системе невозможно при достаточно большом $n$.

Рассмотрим теперь атаку ii. Задачей в этом случае является определение матрицы $h, \Gamma, D$, исходя из известной матрице $B'$. Как будет показано ниже, и это основной результат работы, эта задача может быть решена за $O(s^4 + sn)$ операций в поле $\mathbf{F}_q$.

## 11 Алгоритм определения секретного ключа системы открытого шифрования, использующего обобщенный код Рида — Соломона

Любая матрица ансамбля $\mathcal{B}_q(n, d)$ имеет вид

$$B' = \begin{pmatrix} z_1 f_0(\omega_1) & z_2 f_0(\omega_2) & \cdots & z_n f_0(\omega_n) \\ z_1 f_1(\omega_1) & z_2 f_1(\omega_2) & \cdots & z_n f_1(\omega_n) \\ z_1 f_2(\omega_1) & z_2 f_2(\omega_2) & \cdots & z_n f_2(\omega_n) \\ \vdots & \vdots & \cdots & \vdots \\ z_1 f_{d-2}(\omega_1) & z_2 f_{d-2}(\omega_2) & \cdots & z_n f_{d-2}(\omega_n) \end{pmatrix}, \tag{18}$$

где $f_i(x)$ многочлен степени не выше $d-2$, который определяются матрицей $h=\{h_{i,j}\}$ следующим образом $f_i(x)=\sum_{j=0}^{d-2} h_{i,j}$. Многочлены $f_i(x)$ являются линейно-независимыми.

Итак, перед нами стоит задача: по заданной матрице $B'$ найти невырожденную матрицу $h$, элементы $\omega_1,\omega_2,\ldots,\omega_n \in \mathbf{F}'_q=\mathbf{F}_q\cup\{\infty\}$ и элементы $z_1,z_2,\ldots,z_n\in\mathbf{F}_q\setminus\{0\}$ такие, что $B'=h\cdot B\cdot\Gamma\cdot D$, $D=\operatorname{diag}(z_1,z_2,\ldots,z_n)$.

Задачу будем решать в два этапа: сначала найдем элементы $\omega_1,\omega_2,\ldots,\omega_n$, а затем элементы $z_1,z_2,\ldots,z_n$ и матрицу $h$.

## 11.1 Как определить первые три элемента $\omega_j$?

Перед тем как искать элементы $\omega_1,\omega_2,\ldots,\omega_n$ сделаем несколько замечаний.

Пусть $h$, $\Lambda$ — некоторое решение уравнения (18), т.е. $B'=h\cdot B\cdot\Lambda$, $\Lambda=\Gamma\cdot D$, и $\Lambda_\varphi=\Gamma_\varphi\cdot D_\varphi$, $D_\varphi=\operatorname{diag}(z'_1,z'_2,\ldots,z'_n)$, — некоторый обобщенный автоморфизм кода $\mathcal{K}$ с порождающей матрицей $B$ (см. 10), соответствующий дробно-линейной функции $\varphi(x)$ (см. раздел 7.10). Тогда решением уравнения (18) является также пара $h'$, $\Lambda'$, где $h'=h\cdot h''^{-1}$, $\Lambda'=\Lambda_\varphi\cdot\Lambda$, где матрица $h''$ определяется соотношением $h''\cdot B=B\cdot\Lambda_\varphi$.

Группа обобщенных автоморфизмов $\Xi_{\mathcal{K}}$ кода $\mathcal{K}=RS_q(n,d)$ Рида — Соломона типа 3 (см. раздел 7.4) действует на координатах векторов $\boldsymbol{x}=(x_{\alpha_1},x_{\alpha_2},\ldots,x_{\alpha_n})$. Она образована всеми мономиальными матрицами $\Lambda_\varphi$ (теорема 2) и является трижды транзитивной. Смысл этого понятия объяснен в разделе 7.10. Поэтому найдется дробно-линейная функция $\varphi(x)$ такая, что

$$h'\cdot B\cdot\Lambda_\varphi\cdot\Lambda=\begin{pmatrix} z''_1f'_0(1) & z''_2f'_0(0) & z''_3f'_0(\infty) & \cdots & z''_nf'_0(\beta_n)\\ z''_1f'_1(1) & z''_2f'_1(0) & z''_3f'_1(\infty) & \cdots & z''_nf'_1(\beta_n)\\ z''_1f'_2(1) & z''_2f'_2(0) & z''_3f'_2(\infty) & \cdots & z''_nf'_2(\beta_n)\\ \vdots & \vdots & \vdots & \cdots & \vdots\\ z''_1f'_{d-2}(1) & z''_2f'_{d-2}(0) & z''_3f'_{d-2}(\infty) & \cdots & z''_nf'_{d-2}(\beta_n)\end{pmatrix}, \tag{19}$$

Т.е. найдется такая матрица $\Lambda_\varphi\cdot\Lambda$, что $(x_{\omega_1},x_{\omega_2},\ldots,x_{\omega_n})\Lambda_\varphi\cdot\Lambda=(d_1x_1,d_2x_0,d_3x_\infty,\beta_4,\ldots,\beta_n)$, где $d_\omega$ — элементы диагональной матрицы $D'$, определяемой соотношением $\Lambda_\varphi\cdot\Lambda=\Lambda'=\Gamma'\cdot D'$ (см. раздел 7.10).

Для этого, как нетрудно видеть, нужно подобрать такую функцию $\varphi(x)$, что $\varphi(\omega_1)=\beta_1$, $\varphi(\omega_2)=\beta_2$, $\varphi(\omega_3)=\beta_3$, где элементы $\beta_i$ определяются тем условием, что матрица $\Lambda$ переводит координату $x_{\beta_1}$ в координату $x_1$, координату $x_{\beta_2}$ в $x_0$ и координату $x_{\beta_3}$ в $x_\infty$.

Таким образом, всегда можно полагать, что в (18) $\omega_1=1$, $\omega_2=0$, $\omega_3=\infty$.

## 11.2 Определение элементов $\omega_j$, $j>3$.

Найдем такие постоянные $c_s^{(1)}$, $s=0,\ldots,d-2$, не все равные нулю, для которых выполнено

$$\sum_{s=0}^{d-2} c_s^{(1)}z_jf_s(\omega_j)=0,\ j=1,d,d+1,\ldots,2d-4. \tag{20}$$

Для этого необходимо решить однородную систему линейных уравнений от $d-1$ неизвестных с известной матрицей коэффициентов $(z_jf_s(\omega_j))$ — части матрицы $B'$. Эта система всегда имеет решение, так как уравнений меньше, чем число неизвестных.

Следует отметить, что все элементы $c_s^{(1)}$ отличны от нуля, так как в противном случае в матрице $B'$ нашлись бы $d-1$ линейно-зависимых столбцов, что по ее построению не может иметь место.

Положим

$$F^{(1)}(x)=\sum_{s=0}^{d-2}c_s^{(1)}f_s(x),\quad \gamma_i^{(1)}=\sum_{s=0}^{d-2}c_s^{(1)}z_if_s(\omega_i)=z_iF^{(1)}(\omega_i). \tag{21}$$

Очень существенно то, что элементы $\gamma_i^{(1)}$ могут быть вычислены, исходя только из известных элементов $z_if_s(\omega_i)$ матрицы $B'$.

Поскольку элементы $z_i$ отличны от нуля, то из (21) следует, что элементы $\omega_j$, $j=1,d,d+1,\ldots,2d-4$ являются корнями многочлена $F^{(1)}(x)$. Заметим, что ни один из элементов $\omega_1,\omega_d,\omega_{d+1},\ldots,\omega_{2d-4}$ не равен $\infty$, так как $\omega_3=\infty$.

Степень многочлена $F^{(1)}(x)$ не превосходит $d-2$, так как степени $f_j(x)$, из которых он составлен, также не превосходят $d-2$. Кроме того, многочлен $F^{(1)}(x)$ не равен тождественно 0, ибо многочлены $f_s(x)$ линейно-независимы, а коэффициенты $c_s^{(1)}$ все отличны от нуля. Отсюда вытекает, что $F^{(1)}(x) = a^{(1)}(x-1)(x-\omega_d)\cdots(x-\omega_{2d-4})$, $a^{(1)} \neq 0$.

Отметим, что $F^{(1)}(\omega) \neq 0$, если $\omega \neq \omega_j$, $j = 1, d, d+1, \ldots, 2d-4$, $\omega \neq \infty$ и $F^{(1)}(\infty) = a^{(1)}$.

Теперь проделаем ту же процедуру для элементов $\omega_j$, $j = 2, d, d+1, \ldots, 2d-4$.. А именно, найдем такие постоянные $c_s^{(2)}$, $s = 0, \ldots, d-2$, не все равные нулю, для которых выполнено

$$\sum_{s=0}^{d-2} c_s^{(2)} f_s(\omega_j) = 0,\ j = 2, d, d+1, \ldots, 2d-4. \tag{22}$$

Положим

$$F^{(2)}(x) = \sum_{s=0}^{d-2} c_s^{(2)} f_s(x),\ \gamma_i^{(2)} = \sum_{s=0}^{d-2} c_s^{(2)} z_i f_s(\omega_i) = z_i F^{(2)}(\omega_i). \tag{23}$$

По тем же соображениям, что и выше, имеем $F^{(2)}(x) = a^{(2)}x(x-\omega_d)\cdots(x-\omega_{2d-4})$, $a^{(1)} \neq 0$.

Рассмотрим отношение $\theta(x) = \frac{F^{(1)}(x)}{F^{(2)}(x)} = \frac{a^{(1)}(x-1)}{a^{(2)}x}$ многочленов $F^{(1)}(x)$ и $F^{(2)}(x)$. Как уже было замечено, $F^{(i)}(\omega) \neq 0$, $i = 1, 2$, если $\omega \neq \omega_j$, $j = 1, 2, d, d+1, \ldots, 2d-4$, $\omega \neq \infty$. Таким образом, мы можем вычислить значение функции $\theta(x)$ во всех точках $\omega_j$ за исключением $j = d, d+1, \ldots, 2d-4$ с точностью до постоянного множителя $\frac{a^{(1)}}{a^{(2)}}$.

Множитель $\frac{a^{(1)}}{a^{(2)}}$ можно вычислить, если положить $x = \infty$ (значению $\omega_3$) в $\theta(x)$. В этом случае $z_3 F^{(i)}(\infty) = \sum_{s=0}^{d-2} c_s^{(i)} z_3 f_s(\infty)$, $i = 1, 2$. Таким образом, значение $\theta(\infty)$ может быть вычислено непосредственно, исходя из матрицы $B'$, ибо $z_3 f_s(\infty)$ — элементы третьего столбца $B'$. Для полноты изложения заметим, что $F^{(i)}(\infty) \neq 0$, ибо по построению среди всех $d-2$ корней многочлена $F^{(i)}(x)$, степени не выше $d-2$, нет корня $\infty$. Отсюда вытекает, что

$$\theta(x) = \frac{F^{(1)}(\infty)}{F^{(2)}(\infty)} \left(\frac{x-1}{x}\right) \tag{24}$$

Как уже отмечалось, значения многочленов $F^{(i)}(x)$ и, следовательно, значение $e_\omega = \theta(\omega)$ дробно-линейной функции $\theta(x)$ можно вычислить в любой точке $\omega \in \mathbf{F}_q'$ за исключением $\omega \neq \omega_j$, $j = 1, 2, d, d+1, \ldots, 2d-4$, $\omega \neq \infty$. Отсюда вытекает, что

$$\omega_j = \theta^{-1}(e_{\omega_j}),\ \ j \neq 1, 2, 3, d, d+1, \ldots, 2d-4 \tag{25}$$

Заметим, впрочем, что элементы $\omega_i$, $i = 1, 2, 3$, уже известны.

Функция $\theta^{-1}(x)$, как нетрудно вычислить, равна $\theta^{-1}(x) = \frac{F^{(1)}(\infty)}{F^{(1)}(\infty) - xF^{(2)}(\infty)}$. Таким образом, мы можем определить значения $\omega_j$ для всех $j$, исключая $j = d, d+1, \ldots, 2d-4$.

Недостающие $\omega_j$ можно определить, если выбрать другие элементы, определяющие многочлены $F^{(i)}(x)$. Скажем, в качестве такого набора для определения $F^{(1)}(x)$ можно взять элементы $1, \omega_{2d-3}, \omega_{2d-2}, \ldots, \omega_{3d-6}$ и с их помощью вычислить недостающие $\omega_j$, $j = d, d+1, \ldots, 2d-4$.

В этой секции с помощью многочленов $F^{(i)}(x)$ произведена самая основная и трудная работа: найдена первая часть ключа — элементы $\omega_j$ для всех $j$. Вся остальная работа по определению оставшейся части ключа, как это и обычно бывает, является более легкой и может быть произведена различными способами, один из которых излагается ниже. Кроме того, заметим, что мы использовали нетривиальные свойства подгруппы группы автоморфизмов кода Рида — Соломона, а именно ее трижды транзитивность. Если бы подгруппа была только дважды транзитивной, то мы, например не смогли бы вычислить множитель $\frac{a^{(1)}}{a^{(2)}}$ и, следовательно, вычислить все $\omega_j$.

Трудозатраты этой части алгоритма, как нетрудно подсчитать, не больше $O(d^3 + dn)$.

## 11.3 Определение элементов $z_j$ и матрицы $h$.

Заметим, что если каждый элемент матрицы $\Lambda$ умножить на $a \in \mathbf{F}_q \setminus \{0\}$, а каждый элемент $h$ на $a^{-1}$, то произведение $B' = h \cdot B \cdot \Lambda$ останется неизменным. Поэтому можно считать, что $z_1 = 1$.

Найдем такие элементы $c_1, c_2, \ldots, c_d$, что

$$\sum_{s=1}^{d} c_s z_s f_j(\omega_s) = 0, \quad j = 0, \ldots, d-2. \tag{26}$$

Отметим, что все элементы $c_1, c_2, \ldots, c_d$ отличны от нуля, поскольку в противном случае код с проверочной матрицей $B'$ имел бы кодовое расстояние меньшее $d$ (см. раздел 7.3, утверждение 1).

Соотношение (26) в матричной форме имеет вид

$$B''_d \cdot \mathrm{diag}(z_1, z_2, \ldots, z_d)(c_1, c_2, \ldots, c_d)^T = 0, \tag{27}$$

где $B''_d = (f_i(\omega_j))$, $i = 0, 1, \ldots, d-2$, $j = 1, 2, \ldots, d$ — матрица размера $d-1 \times d$. Заметим, что матрица $B''_d \cdot \mathrm{diag}(z_1, z_2, \ldots, z_d)$ является матрицей, совпадающей с первыми $d$ столбцами матрицы $B'$. Как нетрудно видеть $B''_d = h \cdot B_d$, где

$$B_d = \begin{pmatrix} \omega_1^0 & \omega_2^0 & \cdots & \omega_d^0 \\ \omega_1 & \omega_2 & \cdots & \omega_d \\ \omega_1^2 & \omega_2^2 & \cdots & \omega_d^2 \\ \vdots & \vdots & \cdots & \vdots \\ \omega_1^{d-2} & \omega_2^{d-2} & \cdots & \omega_d^{d-2} \end{pmatrix} \tag{28}$$

Откуда и из (27) вытекает, что

$$h \cdot B_d \cdot \cdot \mathrm{diag}(z_1, z_2, \ldots, z_d)(c_1, c_2, \ldots, c_d)^T = 0, \tag{29}$$

или

$$B_d \cdot \mathrm{diag}(c_1, c_2, \ldots, c_d) \cdot (z_1, z_2, \ldots, z_d)^T = 0. \tag{30}$$

Соотношение (30) мы будем рассматривать как линейную систему уравнений относительно неизвестных $z_2, z_3, \ldots, z_d$ с учетом того, что ненулевые элементы $c_1, c_2, \ldots, c_d$ и элементы $\omega_1, \omega_2, \ldots, \omega_d$ уже известны, а $z_1 = 1$. Эта система имеет единственное решение, поскольку ее матрица ее коэффициентов

$$\begin{pmatrix} \omega_2^0 & \omega_3^0 & \cdots & \omega_d^0 \\ \omega_2 & \omega_3 & \cdots & \omega_d \\ \omega_2^2 & \omega_3^2 & \cdots & \omega_d^2 \\ \vdots & \vdots & \cdots & \vdots \\ \omega_2^{d-2} & \omega_3^{d-2} & \cdots & \omega_d^{d-2} \end{pmatrix} \cdot \mathrm{diag}(c_2, c_3, \ldots, c_d) \tag{31}$$

является, очевидно, невырожденной. Решая эту систему, найдем элементы $z_1, z_2, \ldots, z_d$.

Найдем теперь элементы матрицы $h = (h_{i,j})$, $i, j = 0, \ldots, d-2$. Имеем

$$z_j \sum_{s=0}^{d-2} h_{i,s} \omega_j^s = z_j f_i(\omega_j). \tag{32}$$

Зафиксировав какое-либо $i$, $0 \leqslant i \leqslant d-2$, и изменяя $j$ от 1 до $d-1$, получим систему линейных уравнений с неизвестными $h_{i,0}, h_{i,1}, \ldots, h_{i,d-2}$. Определитель этой системы является определителем Вандермонда, поэтому ее решение $h_{i,0}, h_{i,1}, \ldots, h_{i,d-2}$ находится однозначно. Решив эту систему для каждого $i$, мы найдем матрицу $h$.

Таким образом, мы сумели определить матрицу $h$, элементы $\omega_1, \omega_2, \ldots, \omega_d$ и элементы $z_1, z_2, \ldots, z_d$. Для того чтобы определить оставшиеся элементы $z_{d+1}, z_{d+2}, \ldots, z_n$, проще всего поступить следующим образом.

Умножим матрицу $B'$ слева на матрицу $h^{-1}$. В результате получим матрицу

$$h^{-1} \cdot B' = \begin{pmatrix} z_1\omega_1^0 & z_2\omega_2^0 & \cdots & z_n\omega_n^0 \\ z_1\omega_1 & z_2\omega_2 & \cdots & z_n\omega_n \\ z_1\omega_1^2 & z_2\omega_2^2 & \cdots & z_n\omega_n^2 \\ \vdots & \vdots & \cdots & \vdots \\ z_1\omega_1^{d-2} & z_2\omega_2^{d-2} & \cdots & z_n\omega_n^{d-2} \end{pmatrix}. \tag{33}$$

Вид последней матрицы делает задачу определения элементов $z_{d+1}, z_{d+2}, \ldots, z_n$ тривиальной.

Число операций, требуемых для реализации этой части алгоритма по определению оставшейся части ключа (матрицы $h$ и всех элементов $z_j$), не выше $O(d^4+dn)$. Таким образом, общее число операций по реализации всего алгоритма не более, чем $O(d^4+dn)$. Следовательно, сложность этого алгоритма является полиномиальной от длины $n$ используемого кода. Соответствующая система открытого шифрования как Маклиса, так и Нидеррайтера, построенная на коде Рида — Соломона, не является стойкой. Это основной результат работы.

### 11.4 Заключительные замечания

Естественно встает вопрос о модернизации рассмотренной системы шифрования для того, чтобы увеличить ее стойкость. Наиболее естественный путем является выбор для ее построения другого кода — не Рида — Соломона. Напомним, что для использования в системе шифрования подходит только тот код, который имеет легкое декодирование. Таких кодов известно не очень много.

Возможно, подходящим вариантом может послужить обобщенный код Боуза — Чоудхури — Хоквингема длины $n = q + 1$ (см. конец раздела 7.8) над полем $\mathbf{F}_r$, где число $r$ существенно меньше числа $q$. Нечетко выражаясь, в этом случае построить многочлены $F^{(i)}(x)$ не удается из-за того, матрица $h$, определенная над $\mathbf{F}_r$, «размазывает» $z_j$ между различными коэффициентами многочленов $f_j(x)$. Имеются и некоторые другие сложности. Вместе с тем у автора имеются основания считать, что система шифрования, построенная на основе обобщенного кода Боуза — Чоудхури — Хоквингема, может быть расколота за полиномиальное время.

Другим направлением является использование в системе шифрования двоичных кодов Рида — Маллера. В работе [12] рассмотрена такая система и ее модификации. Проведен подробный анализ ее криптографических свойств. В частности, оценена ее стойкость, которая оказалась высокой.

Третьем направлением являются алгебро-геометрические коды. Эти коды образуют значительно более мощные ансамбли по сравнению с ансамблями, построенными с помощью кода Рида — Соломона. Происходит это из-за того, что мы можем варьировать не только матрицы $h$ и $\Lambda$, как в случае использования кода Рида — Соломона, но и вид алгебраической кривой, с помощью которой построен этот код. Это является очень мощным методом маскировки свойств открытого ключа — проверочной матрицы $B'$.

Четвертым совсем не исследованным направлением является использование каскадных кодов или сверточных кодов. По мнению автора на этом направлении могут быть найдены хорошие системы открытого шифрования.

## Литература

[1] Шеннон К., Теория связи в секретных системах, в кн.: Шеннон К. Э., Работы по теории информации и кибернетике, М.: ИЛ, 1963.

[2] Защита информации. ТИИЭР Т.78, N5, 1988

[3] Menezes A.J., van Oorshot P.S., Vanstone, Handbook of applied cryptography. CRC Press. 1997.

[4] А. Чмора, Современная прикладная криптография, Гелиос АРБ, 2001

[5] Neal Koblitz, Algebraic Aspects of Cryptography, Springer, 1997

[6] H.Beker, F. Piper, Cipher System, Northwood Books, 1982.

[7] Cryptology and computational number theory, Proc. of Symp. in Appl. Math., **v. 42**, 1990.

[8] M. Luby, Pseudorandmness and cryptographic applications, N.Y., Princeton Univ. Press, 1996.

[9] Сидельников В. М., Черепнев М. А., Ященко В. В., Системы открытого распределения ключей на основе некоммутативных полугрупп, Доклады РАН, 1993, **т. 332**, № 5.

[10] R.J. McEliece,A Public-Key Cryptosystem Based on Algebraic Coding Theory", *pp.*114 – 116 in DGN Progres Report 42 – 44, Jet Propulsi on Lab.,Pasadena, CA, January– February,1978.

[11] Сидельников В. М., Шестаков С. О., О системе шифрования, построенной на основе обобщенных кодов Рида — Соломона, Дискретная математика, 1992, **т. 4**, № 3, 57-63.

[12] Сидельников В.М., Открытое шифрование на основе двоичных кодов Рида — Маллера, Дискретная математика, т.6, вып. 3 ,стр. 3-20 ,1994.

[13] Сидельников В.М., Быстрые алгоритмы построения набора маркировок массивов дискретной информации, Труды по дискретной математике, т. 1, стр. 251-263, Из-во ТВП, 1997.

[14] H. Niederreiter. Knapsack-Type Cryptosystems and Algebraic Coding Theory. Probl. Control and Inform. Theory, 1986, V. 15, $pp.19-34$.

[15] Сидельников В.М. Декодирование кода Рида — Соломона при числе ошибок, большем $\frac{d-1}{2}$, и нули многочленов нескольких переменных, Пробл. перед. инф. т.30, вып. 3 ,стр. 51-69 ,1994.

[16] Сидельников В.М., Першаков А.С. Декодирование кодов Рида — Маллера при большом числе ошибок. Пробл. перед. инф. т.28, N3 ,стр. 80-94 ,1992.

[17] МакВильямс Ф.Д., Слоэн Н.Дж. Теория кодов, исправляющих ошибки. М., Связь, 1979.

[18] Riek J.R. Observations on the Application of Error-Correcting Codes to Public Key Encryption. Inter. Carnahan Conf. on Security Technology. 1990, $pp.15-18$.

[19] Cryptology and Computational Number Theory. Proc. of Sym. in App. Math. Vol 42, 1989.

[20] E.R.Berlekamp, R.J. McEliece, H.C.A.van Tilborg,On the Inherent Intractability of Certain Coding Problem IEEE Trans. vol.IT$-24, pp384-386, 1978$.

[21] Зайцев Г.В., Зиновьев В.А., Семаков Н.В. Быстрое корреляционное декодирование блочных кодов. Сб. Кодирование и передача дискретных сообщений в системах связи М. Наука, 1976, стр.$74-85$.

[22] Евсеев Г.С. О сложности декодирования линейных кодов Пробл. перед. инф. т.19, N 1, 1983.

[23] Крук Е.А. Границы для сложности декодирования линейных кодов Пробл. перед. инф. т.25, N 3,стр. $103-107, 1989$.

[24] Бассалыго Л.А.,Зяблов В.В., Пинскер М.С. Проблемы сложности в теории корректирующих кодов Пробл. перед. инф. т.13, стр. $5-13, 1977$.

[25] Корякин Ю.Д. Быстрое корреляционное декодирование кодов Рида — Маллера. Пробл. перед. инф. т. 23, вып 2, 1987, стр. $40-49$.

[26] L.B.Levitin, C.P.Hartman, A New Approach to the General Minimum Distance Decoding Problem: The zero-neighbors Algorithm IEEE Trans. vol.IT-31, N3, $pp378-384, 1985$.

[27] G.C. Ntafos, G.L. Hakimi, On The Complexity of Gome Coding Problems IEEE Trans. vol.IT$-27, pp794-796, 1981$.

[28] Coffey J.T.,Goodman R.M. The Complexity of Informatin Get Decoding. IEEE Trans. on Information Theory, vol. IT-36, N5, $pp1031-1037, 1990$.

[29] C.M.Adams, H.Meijer, Security-Related Coments Regarding McEliac's Public-Key Cryptosystem in Advancts in Cryptology — CRYPTO'87 (Ed. C. Pomerance), pp 224-228, Lecture Notes in Computer Sci.No.293, Heidenberg and New York: Spinger-Verlag, 1988.

[30] P.J.Lee and E.F.Brickell, An Observation on the Security of the McEliace Public-Key Cryptosystem in Advancts in Cryptology — EUROCRYPT'88 (Ed. C. Gunther), pp 224-228, Lecture Notes in Computer Sci.No.230 ,Heidenberg and New York: Spinger-Verlag, 1988.

[31] J.G.Leon, A Probalistic Algorithm for Computing Weights of Large Error-Correcting Codes. IEEE Trans.,vol.IT-34, N 5 , pp.1354-1359, 1988.

[32] Кнут Д. Искусство программирования для ЭВМ. т.3. Сортировка и поиск. М. Мир. 1979.

[33] Ленг С., Алгебра, М. Мир, 1968.

[34] Глухов М.М., Елизаров В.П, Нечаев А.А., Алгебра, часть 2, стр. 344-345, М. 1991.

[35] Петерсон У., Уэлдон Э., Коды, корректирующие ошибки, М. Мир, 1976.

# О доказательстве простоты чисел (следуя работе M. Agrawal, N. Kayal, N. Saxena)

Ю. В. Нестеренко

## 1 Введение

Настоящая статья посвящена вопросу: *как определить, является заданное число простым или составным.* С практической точки зрения эта задача в настоящее время имеет вполне удовлетворительное решение.

Если нечетное число $N$ при некотором целом $a$, $1 < a < N$, удовлетворяет условию $a^{N-1} \not\equiv 1 \pmod N$, оно, конечно, не является простым. Это противоречило бы малой теореме Ферма. К сожалению, выполнимость условия

$$a^{N-1} \equiv 1 \pmod N \qquad \text{для любого } a \in \mathbb{Z},\ (a, N) = 1, \tag{1}$$

еще не гарантирует простоту числа $N$. Составные числа, удовлетворяющие условию (1) называются *числами Кармайкла.* Таким, например, является $561 = 3 \cdot 11 \cdot 17$. Можно доказать (Кармайкл, 1912), что любое из чисел Кармайкла имеет вид $N = p_1 \cdots p_r$, $r \geqslant 3$, где все простые $p_i$ различны, причем $N - 1$ делится на каждую разность $p_i - 1$. Лишь в 1994 г. было доказано, что множество таких чисел бесконечно, см. [5].

Существующие в настоящее время алгоритмы проверки чисел на простоту используют различные модификации малой теоремы Ферма. Наиболее быстрый детерминированный алгоритм предложен в 1980 г. (Адлеман, Померанс, Рамели [6]) и усовершенствован в работах [10]), [7]. Основу этого алгоритма составляет проверка условий, аналогичных малой теореме Ферма, в полях алгебраических чисел $\mathbb{Q}(\zeta_p)$, где $\zeta_p = \exp(2\pi i/p)$ — корень из 1 степени $p$.

Опишем эти условия несколько подробнее. Напомним, что функция $\chi\colon \mathbb{Z} \to \mathbb{C}$ называется характером по модулю $m \in \mathbb{Z}$, $m > 1$, если она периодична с периодом $m$, мультипликативна и принимает отличные от нуля значения только для значений аргумента взаимно простых с $m$. Например, если $q$ — простое число, $g$ — первообразный корень по модулю $q$ и $\xi$ — произвольный корень из 1 степени $q - 1$, то функция

$$\chi(x) = \begin{cases} 0, & \text{если } q \mid x; \\ \xi^u, & \text{если } q \nmid x \text{ и } x \equiv g^u \pmod q \end{cases}$$

есть характер по модулю $q$. В дальнейшем будем считать, что $\xi = \zeta_p$, где $p > 2$ — простое число, $p \mid (q - 1)$. Фиксируем некоторые целые числа $a, b$, не делящиеся на $p$, с условиями

$$p \nmid a + b, \quad a^p + b^p \not\equiv (a + b)^p \pmod{p^2},$$

и определим

$$J = \sum_{x=0}^{q-1} \chi(x)^a \chi(1 - x)^b.$$

Эта сумма принадлежит кольцу $\mathbb{Z}[\zeta_p]$ и называется суммой Якоби. Для каждого $c \in \mathbb{Z}$, $p \nmid c$, обозначим $\sigma_c$ автоморфизм поля $\mathbb{Q}(\zeta_p)$, для которого $\sigma_c(\zeta_p) = \zeta_p^c$. Используя введенные обозначения, можно утверждать, что для каждого нечетного простого числа $N$, отличного от $p$ и $q$, в кольце $\mathbb{Z}[\zeta_p]$ справедливо сравнение

$$\prod_{c=1}^{p-1} \sigma_c^{-1}(J)^{[Nc/p]} \equiv \eta \pmod N, \tag{2}$$

где $\eta$ – некоторый корень из 1 степени $p$.

Если целое число $N$ удовлетворяет сравнениям (2) при некоторых парах простых $p, q$, $p \mid q-1$, то информация о корнях из единицы $\eta$, накопленная в результате таких испытаний, позволяет очертить не очень большое множество, где только и могут находиться возможные делители $N$. Непосредственный перебор этого множества позволяет проверить, что делители отсутствуют, и, значит, доказывает простоту $N$.

Оценка сложности этого алгоритма представляет собой трудную задачу аналитической теории чисел. Доказывается лишь существование множества пар чисел $p$ и $q$, использование которых в алгоритме, приводит к оценке его сложности $O((\ln N)^{c \ln\ln\ln N})$. В предположении справедливости расширенной гипотезы Римана это множество может быть указано эффективно.

Существует эффективный на практике, но недетерминированный алгоритм проверки на простоту произвольных чисел, использующий вычисления на эллиптических кривых над кольцами вычетов $\mathbb{Z}/N\mathbb{Z}$. Он был предложен в работе Гольдвассер и Килиана [9], и усовершенствован в неопубликованной работе Аткина. При некоторых правдоподобных предположениях о распределении простых чисел этот алгоритм для любого простого числа $N$ доказывает его простоту в среднем за $O((\log N)^c)$ арифметических операций, где $c$ — некоторая положительная постоянная. В основе этого алгоритма лежит следующее утверждение, в некотором смысле также подобное малой теореме Ферма.

**Теорема 1.** *Пусть $N$ — целое число, взаимно простое с 6 и $E$ — эллиптическая кривая над кольцом $A = \mathbb{Z}/N\mathbb{Z}$, а $m$ и $s$ — натуральные числа, причем $m$ делится на $s$. Предположим, что существует такая точка $P \in E(A)$, что*

1) $m \cdot P = O$;

2) *для каждого простого делителя $q$ числа $s$ выполнено $(m/q) \cdot P = (x_q, y_q, z_q)$, где $(z_q, N) = 1$.*

*Тогда для каждого простого делителя $p$ числа $N$ выполняется сравнение*

$$\#E(\mathbb{Z}/p\mathbb{Z}) \equiv 0 \pmod{s},$$

*причем, если $s > (n^{1/4}+1)^2$, то $N$ — простое число.*

Важной составной частью этого метода доказательства простоты является алгоритм вычисления количества точек эллиптической кривой над конечным полем.

Указанные алгоритмы позволяют на практике доказывать простоту чисел, записываемых 100–200 десятичными знаками.

Стоящий в оценке сложности детерминированного алгоритма проверки на простоту третий логарифм $\ln\ln\ln N$ есть очень медленно растущая функция, в пределах практического использования не доставляющая хлопот. Тем не менее в течение длительного времени стояла открытой теоретическая проблема: *доказать, что задача проверки на простоту имеет полиномиальную сложность.* Эту проблему решили летом текущего 2002 года индийские математики Агравал, Кайал и Саксена [4]. Они нашли полиномиальный алгоритм, требующий $O(\ln^{12} N)$ арифметических операций. Следующий ниже алгоритм, именно ему посвящена настоящая статья, представляет собой несколько модифицированную версию алгоритма из [4].

Условимся о некоторых обозначениях. Символом $\log n$ в дальнейшем обозначается логарифм по основанию 2, $\nu_p(n)$ — кратность с которой простое число $p$ входит в разложение целого $n$ и $\#G$ — количество элементов в множестве $G$.

### Алгоритм

Дано целое нечетное число $N \geqslant 23$. Требуется определить, является $N$ простым или составным.

1. Если $N = a^b$, $b > 1$, т. е. $N$ есть степень целого числа, то $N$ *составное.*
2. Если $N$ имеет простой делитель $\leqslant \log^2 N$ то $N$ — *составное.*
3. Положить $r$ равным наименьшему нечетному числу с условием $r > \log^2 N$.
4. Если $(r, N) \neq 1$, то $N$ — *составное.*

5. Если $r$ — простое и $q$ — наибольший простой делитель $r-1$, проверить выполнимость условий

$$q \geqslant 2\sqrt{r}\log N, \quad N^{\frac{r-1}{q}} \not\equiv 1 \pmod{r}. \tag{3}$$

Если хотя бы одно из этих условий нарушено, перейти в п. 7.

6. Если для всех $j \in \mathbb{Z}$, $1 \leqslant j \leqslant \sqrt{r}\log N$ в кольце $A[x]$, где $A = \mathbb{Z}/N\mathbb{Z}$, выполнены сравнения

$$(x-j)^N \equiv x^N - j \pmod{x^r-1}, \tag{4}$$

то $N$ — *простое*, а в противном случае $N$ — *составное*.

7. Если $r < \sqrt{N}$, положить $r := r+2$ и перейти в п. 4. В противном случае $N$ — *простое*.

Предполагается, что как только алгоритм выдает некоторый ответ, *простое* или *составное*, он завершает свою работу и останавливается.

## 2 Обоснование корректности алгоритма.

В процессе работы алгоритма число $r$ не уменьшается. Поэтому алгоритм может пройти через пункт 7 не более $\sqrt{N}/2$ раз, и, следовательно, через пункты 4, 5 не более $1+\sqrt{N}/2$ раз. Это значит, что алгоритм всегда завершает свою работу.

Кроме того, в процессе работы алгоритма всегда выполняется

$$\log^2 N < r \leqslant 2 + \max(\log^2 N, \sqrt{N}). \tag{5}$$

Заметим, что правая часть последнего неравенства меньше $N$ при $N \geqslant 23$. Отсюда, в частности следует, что если алгоритм останавливается в одном из пунктов 1, 2, 4, то он при этом дает правильный ответ.

Если алгоритм останавливается в п. 7, то $r > \sqrt{N}$ и число $N$ не имеет простых делителей меньших $r$, т. е. меньших $\sqrt{N}$. Это возможно только в случае, если число $N$ — простое. Так что и в этом случае ответ алгоритма правилен.

Допустим теперь, что алгоритм остановился в пункте 6. Это значит, что простые числа $r, q$ удовлетворяют условиям (3).

Если существует число $j$, для которого нарушается условие (4), то число $N$ не может быть простым. Действительно, согласно малой теореме Ферма в этом случае в кольце $A[x]$ должно выполняться равенство

$$(x-j)^N = x^N - j^N = x^N - j.$$

Это значит, что при простом $N$ сравнение (4) должно выполняться не только по модулю $x^r-1$, но и по модулю любого многочлена. Итак, в этом случае ответ алгоритма правилен.

Предположим теперь, что условия (4) выполнены при любом $j, 1 \leqslant j \leqslant \sqrt{r}\log N$. Для доказательства правильности ответа в этом случае нам понадобится следующее утверждение.

**Теорема 2.** *Пусть $N, s$ — натуральные, $r, q$ — простые числа с условиями*

$$r \nmid N, \quad q \mid r-1, \quad N^{\frac{r-1}{q}} \not\equiv 1 \pmod{r}, \quad \binom{s+q-1}{s} > N^{2\sqrt{r}}. \tag{6}$$

*Если в кольце $A[x]$, где $A = \mathbb{Z}/N\mathbb{Z}$, выполнены сравнения*

$$(x-j)^N \equiv x^N - j \pmod{x^r-1}, \quad 1 \leqslant j \leqslant s, \tag{7}$$

*и $N$ не имеет собственных простых делителей $\leqslant s$, то $N$ есть степень простого числа.*

Проверим, что в последнем из случаев проверки корректности алгоритма выполняются условия теоремы 2 с $s = [\sqrt{r}\log N]$.

Из (3) следует, что

$$2s \leqslant 2\sqrt{r}\log N \leqslant q.$$

Кроме того, в силу (5) и $N \geqslant 23$ имеем

$$s \geqslant \sqrt{r}\log N - 1 \geqslant \log^2 N - 1 \geqslant 15.$$

Поэтому

$$\binom{s+q-1}{s} \geqslant \binom{3s-1}{s} = \frac{(3s-1)!}{s!(2s-1)!} \geqslant 4^{s+1}.$$

Легко проверить, что последнее неравенство выполняется при $s \geqslant 10$. Таким образом,

$$\binom{s+q-1}{s} \geqslant 4^{\sqrt{r}\log N} = N^{2\sqrt{r}}.$$

Все условия (6) выполнены.

Из (5) и определения $s$ находим

$$s \leqslant \sqrt{r}\log N < r.$$

В силу того, что $N$ не имеет простых делителей, меньших $r$, заключаем, что и последнее условие теоремы 2 выполнено. Согласно этой теореме $N$ есть степень простого числа. Поскольку алгоритм не остановился в пункте 1, можно утверждать, что $N$ — простое. Значит и в этом, последнем, случае алгоритм дает правильный ответ.

Перейдем теперь к доказательству теоремы 2.

*Доказательство.* Предположим, что $N$ — составное число. Тогда

$$N = p_1 \cdots p_k,$$

где $k \geqslant 2$ и $p_j$ — простые числа. Для каждого целого $b$ символ $\operatorname{ord}_r(b)$ будет обозначать в дальнейшем наименьшее натуральное $t$ с условием $b^t \equiv 1 \pmod r$.

Так как

$$\operatorname{ord}_r(N) \mid \text{НОК}(\operatorname{ord}_r(p_1), \ldots, \operatorname{ord}_r(p_k)), \tag{8}$$

и согласно (3)

$$\operatorname{ord}_r(N) \mid r-1, \quad \text{но} \quad \operatorname{ord}_r(N) \nmid \frac{r-1}{q},$$

то $\nu_q(\operatorname{ord}_r(N)) = \nu_q(r-1) \geqslant 1$. Это значит, что $q \mid \operatorname{ord}_r(N)$, и, согласно (8), для некоторого простого числа $p$, делящего $N$, имеем

$$q \mid \operatorname{ord}_r(p).$$

Следующий результат хорошо известен, см., например, [2, гл. 7, § 2, теорема 2], где он формулируется в терминах разложения простого числа в произведение идеалов кругового поля.

**Лемма 3.** *Пусть $h(x)$ — неприводимый делитель многочлена $x^r - 1$ в кольце $\mathbf{F}_p[x]$, где $\mathbf{F}_p$ — конечное поле из $p$ элементов. Тогда* $\deg h(x) = \operatorname{ord}_r(p)$.

*Доказательство.* Обозначим для краткости $d = \operatorname{ord}_r(p)$ и $t = \deg h(x)$. Так как $\mathbf{F}_p[x]/(h(x))$ есть поле степени $k$ над $\mathbf{F}_p$ и мультипликативная группа $(\mathbf{F}_{p^k})^*$ ненулевых элементов этого поля циклична, то $x^{p^k-1} \equiv 1 \pmod{h(x)}$. В то же время выполняется сравнение $x^r \equiv 1 \pmod{h(x)}$, причем $r$ — простое число. Это возможно лишь в случае $p^k \equiv 1 \pmod r$, т. е. при $d \mid k$.

Так как $r \mid p^d - 1$, то $x^r - 1 \mid x^{p^d} - x$. Следовательно,

$$x^{p^d} \equiv x \pmod{x^r - 1}.$$

Пусть $g(x) \in \mathbf{F}_p[x]$ и $g(x) \pmod{h(x)}$ — образующая группы $(\mathbf{F}_{p^k})^*$. Тогда $g(x)^p = g(x^p) \in \mathbf{F}_p[x]$ и, следовательно,

$$g(x)^{p^d} = g(x^{p^d}) \equiv g(x) \pmod{x^r - 1}.$$

Так как $g(x) \pmod{h(x)}$ есть образующая группы $(\mathbf{F}_{p^k})^*$, то $p^k - 1 \mid p^d - 1$. Но это возможно лишь при $k \leqslant d$. Соотношения, доказанные для $d$ и $k$ означают равенство $d = k$. □

В дальнейшем степень многочлена $h(x)$ будет обозначаться буквой $d$.

Пусть $\alpha$ — корень многочлена $h(x)$ в поле $F = \mathbf{F}_{p^d}$. Рассмотрим подгруппу $G \subset F^*$, порожденную разностями $\alpha - j$, $1 \leqslant j \leqslant s$. Докажем, что все элементы

$$\prod_{j=1}^{s}(\alpha - j)^{k_j}, \quad k_j \geqslant 0, \quad k_1 + \cdots + k_s < d, \tag{9}$$

различны. Действительно, предположим, что для двух различных наборов неотрицательных показателей $(k_1, \ldots, k_s)$, $(\ell_1, \ldots, \ell_s)$, с условиями $k_1 + \cdots + k_s < d$, $\ell_1 + \cdots + \ell_s < d$ в поле $F$ выполняется равенство

$$\prod_{j=1}^{s}(\alpha - j)^{k_j} = \prod_{j=1}^{s}(\alpha - j)^{\ell_j}.$$

Обозначим

$$u(x) = \prod_{j=1}^{s}(x - j)^{k_j} - \prod_{j=1}^{s}(x - j)^{\ell_j} \in \mathbf{F}_p.$$

Так как $u(\alpha) = 0$, то $h(x) \mid u(x)$. Поскольку $\deg u(x) < d = \deg h(x)$, то $u(x) \equiv 0$ или

$$\prod_{j=1}^{s}(x - j)^{k_j} = \prod_{j=1}^{s}(x - j)^{\ell_j} \in \mathbf{F}_p[x].$$

Так как $N$ не имеет простых делителей $\leqslant s$, то $p > s$, и все элементы $j = 1, \ldots, s \in \mathbf{F}_p$ различны. Из единственности разложения многочленов на неприводимые множители в кольце $\mathbf{F}_p[x]$ следует, что $k_j = \ell_j$, $j = 1, \ldots, s$. Получившееся противоречие доказывает, что все элементы (9) различны. Их количество есть $\binom{s+d-1}{s}$. Таким образом

$$\#G \geqslant \binom{s + d - 1}{s}.$$

Поскольку $G \subset F^*$ и $F^*$ циклична, то $G$ также циклична. Пусть

$$\overline{g} = \prod_{j=1}^{s}(\alpha - j)^{k_j}$$

— образующая $G$. Тогда

$$\operatorname{ord}\overline{g} = \#G \geqslant \binom{s + d - 1}{s}.$$

Обозначим $g(x) = \prod_{j=1}^{s}(x - j)^{k_j}$. Поскольку $p \mid N$, то в кольце $\mathbf{F}_p[x]$ согласно условию теоремы выполняются сравнения

$$(x - j)^N \equiv x^N - j \pmod{x^r - 1}, \quad j = 1, \ldots, s. \tag{10}$$

Кроме того в этом же кольце справедливы равенства

$$(x - j)^p = x^p - j, \quad j = 1, \ldots, s. \tag{11}$$

Из (10), (11) следует, что

$$g(x)^N \equiv g(x^N) \pmod{x^r - 1}, \quad g(x)^p \equiv g(x^p) \pmod{x^r - 1}. \tag{12}$$

Обозначим

$$I = \{m \in \mathbb{Z}, m \geqslant 1 : g(x)^m \equiv g(x^m) \pmod{x^r - 1}\}.$$

Тогда $N, p \in I$.

**Лемма 4.** *Если $m_1, m_2 \in I$, то $m_1 m_2 \in I$.*

*Доказательство.* Так как $m_1, m_2 \in I$, то

$$g(x)^{m_1} \equiv g(x^{m_1}) \pmod{x^r - 1}, \quad g(x)^{m_2} \equiv g(x^{m_2}) \pmod{x^r - 1}. \tag{13}$$

Так как $x^r - 1 \mid x^{m_1 r} - 1$, то из второго сравнения (13) находим

$$g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{x^r - 1}$$

и

$$g(x)^{m_1 m_2} = (g(x)^{m_1})^{m_2} \equiv g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{x^r - 1}.$$

Лемма доказана. □

Так как $N, p \in I$, то по лемме 4 $N^i p^j \in I$, $i \geqslant 0$, $j \geqslant 0$. Обозначим

$$E = \{N^i p^j \mid 0 \leqslant i \leqslant [\sqrt{r}], 0 \leqslant j \leqslant [\sqrt{r}]\}.$$

Предположим, что все элементы множества $E$ различны. Тогда

$$\#E = (1 + [\sqrt{r}])(1 + [\sqrt{r}]) > \sqrt{r}\sqrt{r} = r.$$

Значит, существуют

$$m_1 = N^{i_1} p^{j_1}, \quad m_2 = N^{i_2} p^{j_2} \in E, \quad (i_1, j_1) \neq (i_2, j_2)), \quad m_2 \equiv m_1 \pmod{r}.$$

Не уменьшая общности можно считать, что $m_2 > m_1$. Тогда

$$x^{m_2 - m_1} \equiv 1 \pmod{x^r - 1}.$$

Имеем

$$g(x)^{m_2} \equiv g(x^{m_2}) = g(x^{m_1} \cdot x^{m_2 - m_1}) \equiv g(x^{m_1}) \equiv g(x)^{m_1} \pmod{x^r - 1}.$$

Подставляя в это сравнение $\alpha$ вместо $x$ и пользуясь тем, что $\alpha^r = 1$, находим $\overline{g}^{m_2} = \overline{g}^{m_1}$ и $\overline{g}^{m_2 - m_1} = 1$. Следовательно, $\operatorname{ord} \overline{g} \mid m_2 - m_1$ и

$$m_2 - m_1 \geqslant \operatorname{ord} \overline{g} \geqslant \binom{s + d - 1}{s} > N^{2\sqrt{r}}.$$

С другой стороны

$$0 < m_2 - m_1 < m_2 = N^{i_2} p^{j_2} \leqslant N^{\sqrt{r}} N^{\sqrt{r}} \leqslant N^{2\sqrt{r}}.$$

Получившиеся неравенства противоречат друг другу. Значит, в множестве $E$ имеются одинаковые элементы $m_1 = m_2$ или $N^{i_1} p^{j_1} = N^{i_2} p^{j_2}$. Так как $(i_1, j_1) \neq (i_2, j_2)$ то $i_1 \neq i_2$ и, в силу единственности разложения целых чисел на простые множители, заключаем, что $N = p^k$, $k \geqslant 2$. Это завершает доказательство теоремы. □

# 3 Оценка сложности алгоритма

Указанный выше алгоритм имеет полиномиальную сложность. Доказательство этого утверждения опирается на очень трудный и глубокий результат аналитической теории чисел, доказанный в 1985 г. Фуври, см. [8].

**Теорема 3.** *Существует такая постоянная $c > 0$, что любой достаточно длинный отрезок $[1, X]$ содержит не менее, чем $cX/\log X$ простых чисел $p$ с условием, что $p - 1$ имеет простой делитель $q$ превосходящий $X^{2/3}$, т. е. при всех $X \geqslant X_0$ выполняется неравенство:*

$$\#\{p \leqslant X : \exists \text{ простое } q \mid p - 1, q \geqslant X^{2/3}\} \geqslant c \cdot \frac{X}{\log X}. \tag{14}$$

Эта теорема позволяет доказать, что для всех достаточно больших $N$ простое число $r$, удовлетворяющее условиям (3) из пункта 5 алгоритма, имеет величину $O(\log^6 N)$, что обеспечивает полиномиальную оценку сложности алгоритма.

Теорема Фуври, имеющая большую предисторию, была получена в результате существенного развития методов решета в теории чисел. После общеизвестного решета Эратосфена, в теории чисел были разработаны методы оценки количества простых чисел с различными свойствами, называемые решето Бруна (1920), решето Сельберга (1947), так называемое «большое решето» Линника (1941) и другие. Историю вопроса см. [8].

Оценивая сложность алгоритма, мы, очевидно, можем считать $N$ большим натуральным числом.

**Лемма 5.** *Существуют такие положительные постоянные $c_1, c_2$, что для любого достаточно большого числа $N$ отрезок $[c_1 \log^6 N, c_2 \log^6 N]$ содержит такое простое число $r$, что наибольший простой делитель $q$ числа $r-1$ удовлетворяет условиям*

$$q > 2\sqrt{r}\log N, \quad N^{\frac{r-1}{q}} \not\equiv 1 \pmod{r}.$$

*Доказательство.* Положим $X = c_2 \log^6 N$, где $c_2$ — некоторая положительная постоянная, которая будет выбрана в дальнейшем. Назовем простое число $p$ *специальным*, если $p \leqslant X$ и наибольший простой делитель $q \mid p-1$ удовлетворяет неравенству $q \geqslant X^{2/3}$. Согласно теореме Чебышева количество $\pi(x)$ простых чисел на отрезке $[1, x]$ может быть оценено сверху величиной $5\frac{x}{\log x}$. Пользуясь теоремой 3, находим

$$\begin{aligned}&\#\{\text{Специальных чисел}\} - \pi(c_1 \log^6 N)\\ &\quad \geqslant c\frac{c_2 \log^6 N}{7 \log\log N} - 5\frac{c_1 \log^6 N}{6 \log\log N} \geqslant c_3 \frac{\log^6 N}{\log\log N},\end{aligned}$$

где $c_3 = cc_2/7 - 5c_1/6$. Выберем $c_1 = 64$ и $c_2$ столь большим, чтобы было $c_3 > 0$. Тогда количество специальных чисел на отрезке $[c_1 \log^N, c_2 \log^6 N]$ будет больше $c_3 \log^6 N / \log\log N$.

Пусть

$$\Pi = \prod_{k=1}^{[X^{1/3}]+1} (N^k - 1).$$

Тогда

$$\log \Pi \leqslant \log N \cdot \sum_{k=1}^{[X^{1/3}]+1} k \leqslant X^{2/3} \log N.$$

Это неравенство означает, что

$$\#\{\text{простые делители } \Pi\} \leqslant X^{2/3} \log N < c_2^{2/3} \log^5 N < c_3 \frac{\log^6 N}{\log\log N}.$$

Следовательно, существует специальное простое число $r$ с условиями

$$r \leqslant c_2 \log^6 N, \quad r \nmid N^k - 1 \quad \text{для любого } k \leqslant [X^{1/3}] + 1.$$

Пусть $q$ — наибольший простой делитель $r-1$. Так как $r$ специальное, то

$$q \geqslant X^{2/3} = c_2^{2/3} \log^4 N \geqslant 2\sqrt{r}\log N.$$

Последнее неравенство обеспечивается за счет выбора $c_1$. Действительно, имеем $c_2 \geqslant c_1 = 64$, так что

$$2\sqrt{r}\log N \leqslant 2\sqrt{c_2}\log^4 N \leqslant c_2^{2/3}\log^4 N.$$

Поскольку

$$\frac{r-1}{q} \leqslant \frac{c_2 \log^6 N}{c_2^{2/3} \log^4 N} = c_2^{1/3} \log^2 N < [X^{1/3}] + 1,$$

то $r \nmid N^{\frac{r-1}{q}} - 1$. □

Из доказанной леммы следует, что простое число $r$ в процессе работы алгоритма будет оцениваться величиной $O(\log^6 N)$. Это значит, что цикл в пунктах 4, 5, 7 алгоритма будет повторяться $O(\log^6 N)$ раз, пока не найдет нужное значение $r$. Наиболее трудоемкая часть алгоритма связана с вычислениями в п. 6 степеней многочленов. Учитывая, что с помощью быстрого преобразования Фурье умножение двух многочленов степени $r-1$ можно выполнить за $O(r \log r)$ арифметических операций в кольце $A$, см. [1], а для одного возведения в степень требуется $O(\log N)$ таких умножений, находим оценку для наиболее трудоемкой части алгоритма $O(\sqrt{r} \log N \cdot \log N \cdot r) = O(\log^{11} N)$ — арифметических операций в кольце $A$ (здесь не учтены множители порядка $\log\log N$). В битовых операциях сложность оказывается равной $O(\log^{12} N)$.

Заметим, что любой результат аналогичный теореме 2 с константой $\delta > 0,5$ вместо $2/3$ дает полиномиальную оценку сложности алгоритма. Соответствующий показатель степени у $\log N$ равняется $\frac{6\delta}{2\delta-1}$. Например, доказанная в 1973 г. Хоули оценка с $\delta = 0,6250 + \varepsilon$ привела бы к оценке сложности $O(\log^{15+\varepsilon} N)$. Следует отметить, что оценка $O(\ln^{12} N)$ сложности алгоритма скорее всего весьма завышена.

Алгоритм при своей реализации требует достаточно большой памяти. Неравенства

$$\frac{r}{2} > \frac{r-1}{2} \geqslant q \geqslant 2\sqrt{r}\log N$$

показывают, что простое число $r$, для которого выполняются условия (3) должно быть достаточно большим $r > 16\log^2 N$. Учитывая, что многочлены, возникающие при вычислении $(x-j)^N \pmod{x^r-1}$ в кольце $A[x]$ должны иметь степень $r-1$, т. е. записываться $r$ коэффициентами, каждый из которых есть вычет по модулю $N$, получаем, что память, необходимая для записи одного многочлена, не меньше, чем $16\log^3 N$. Для $N \sim 10^{100}$ это составляет примерно $6 \cdot 10^8$. Таким образом, реальный практический интерес алгоритм будет иметь лишь после существенного снижения границ в пунктах 5 и 6.

## Литература


[1] Ахо А., Хопкрофт Дж., Ульман Дж. Построение и анализ вычислительных алгоритмов. М.: Мир, 1979.

[2] Боревич З. И., Шафаревич И. Р. Теория чисел. М.: Наука, 1972.

[3] Гаусс К. Ф. Арифметические исследования. М.: Изд-во Академии Наук СССР, 1959.

[4] Agrawal M., Kayal N., Saxena N, PRIMES is in P. 2002, available from `http://www.cse.iitk.ac.in/news/primality.pdf`.

[5] Alford W. R., Granville A., Pomerance C. There are infinitely many Carmichael numbers. Ann. Math., 1994, **140**, 703–722.

[6] Adleman L. M., Pomerance C., Rumely R. S. On distinguishing prime numbers from composite numbers. Ann. of Math., 1983, **117**, № 2, 173–206.

[7] Cohen H., Lenstra H. W. (jr.) Primality testing and Jacobi sums. Math. of Comput., 1984, **42**, № 165, 297–330.

[8] Fouvry E. Théorème de Brun–Titchmarsh; application au théorème de Fermat. Invent. Math., 1985, **79**, 383–407.

[9] Goldwasser S., Kilian J. Almost all primes can be quickly certified. Proc. 18th Annual ACM Symp. on Theory of Computing, New York, 1986, 316–329.

[10] Lenstra H. W. (jr.) Primality testing algorithms (after Adleman, Rumely and Williams). Lecture Notes in Math., 1981, **901**, 243–257.

# Математическая криптография. Несколько этюдов

Н. П. Варновский

## 1 Введение

В заголовке настоящей статьи использован термин «математическая криптография». Поскольку в области защиты информации до сих пор нет общепринятой терминологии, мы начнем с объяснения нашей трактовки основных терминов. Подчеркнем, что эту трактовку следует расценивать как наши предложения по терминологии.

Криптография — инженерно-техническая дисциплина, которая занимается математическими методами защиты информации. Эта область деятельности существует уже не первое тысячелетие.

В XX веке возникло новое направление — применение математических методов к исследованию задач, возникающих в процессе разработки и (или) анализа криптографических схем. Все эти задачи следовало бы называть математическими задачами криптографии. Отметим, что все они образуют спорадическую совокупность задач из различных отраслей математики.

Ближе к концу XX века, точнее в 80-е годы, образовалась еще одна дисциплина, которую мы предлагаем называть математической или теоретической криптографией (заметим, что первые работы по математической криптографии появились значительно раньше, например, классические работы К. Шеннона). Математическая криптография — отрасль дискретной математики, или математической кибернетики, которая исследует математические модели криптографических схем.

Условно эти три области деятельности, связанные с математическими методами защиты информации, можно изобразить в виде диаграммы на рис. 1.


Рис. 1:

Подчеркнем, что мы никоим образом не претендуем на то, что топология этого рисунка каким-либо образом отражает соотношение между этими тремя дисциплинами, хотя взаимовлияние, безусловно, очевидно.

Математическая криптография — научная дисциплина, включающая в себя значительное разнообразие задач, подходов и методов. В отдельной статье, конечно же, невозможно не только изложить основы этой теории, но и даже дать сколь-нибудь целостное представление о ее предмете и методах. Поэтому в данной работе мы вообще не ставили задачи добиваться систематичности изложения. Вместо этого вниманию читателя предлагается набор этюдов из различных областей математической криптографии.

При выборе тем мы преследовали две основные цели. Во-первых, продемонстрировать многообразие проблем, исследуемых в математической криптографии. Во-вторых, рассказать о таких задачах, которые не относятся к категории «общих мест», редко встречаются в книгах по криптографии, а в литературе на русском языке, по-видимому, вообще никогда не рассматривались.

## 2 Входные данные для вычислительно трудных задач

Современная криптография с открытым ключом практически целиком опирается на гипотезы о вычислительной трудности двух хорошо известных теоретико-числовых задач — факторизации целых чисел и дискретного логарифмирования. Такое положение дел не может быть признано удовлетворительным, поскольку открытие новых, более эффективных алгоритмов для этих задач или создание квантового компьютера может оставить от всей криптографии с открытым ключом одни лишь теоретические результаты.

Поиски замены задачам факторизации и дискретного логарифмирования — одно из направлений исследований в математической криптографии. Следует подчеркнуть, что проблема эта весьма сложная, поскольку требуется найти задачу, удовлетворяющую сразу нескольким достаточно жестким требованиям, из которых основными являются следующие два. Во-первых, задача-кандидат должна быть вычислительно трудной в среднем. Во-вторых, должен существовать эффективный способ генерации случайных входных данных для этой задачи с известным решением. Именно этой последней проблеме и посвящен настоящий раздел.

Начнем со следующего замечания. Очевидно, что задачи, возникающие в криптографии, не выводят за пределы класса NP, так что в поисках задач-кандидатов достаточно ограничиться этим классом.

Далее, предположим, что нам нужно подобрать подходящую задачу для протокола интерактивного доказательства с нулевым разглашением. Классическая теорема Гольдрайха и др. [12] гласит: если существуют односторонние функции, то доказательство с нулевым разглашением существует для всякого языка из класса NP. Это означает, что в данном случае задачу-кандидат целесообразно искать среди NP-полных задач.

Всякая задача $T$ из класса NP описывается множеством строк $I = \{i, i \in \{0,1\}^*\}$, называемых входными данными, и предикатом $P(\cdot,\cdot)$, вычислимым за полиномиальное время. Одно из определений класса NP сформулировано на языке существования для входных данных $i \in I$ строки $w \in \{0,1\}^*$ полиномиальной от $|i|$ длины такой, что $P(i,w) = 1$. Когда класс NP рассматривается как класс языков, строка $w$ называется догадкой, сертификатом (witness). Отметим, что недавно был предложен новый и очень удачный термин: NP-доказательство (NP-proof). Но мы рассматриваем не языки, а задачи и поэтому будем говорить о строке $w = w(i)$ как о решении задачи $T$ для входных данных $i$.

В протоколе интерактивного доказательства общим входом участников (проверяющего и доказывающего) является строка $i \in I$ (открытый ключ) и доказывающий должен продемонстрировать (проверяющему), что он знает решение $w$ (секретный ключ). Для этого доказывающий должен знать решение $w = w(i)$. В теоретической постановке проблемы не возникает: доказывающий обладает неограниченными вычислительными ресурсами и всегда может найти решение.

Для практического применения необходимы эффективные рандомизированные алгоритмы, генерирующие входные данные $i \in I$ с известными решениями $w$ (подобно тому как модули RSA генерируются с известными простыми сомножителями). Для многих NP-полных задач такие алгоритмы предложить несложно. Например, целый класс NP-полных задач на графах состоит в поиске в заданном графе подграфа, обладающего некоторыми фиксированными свойствами. Очевидный подход состоит в следующем: строим граф, состоящий из одного только подграфа-решения, а затем маскируем решение, добавляя в граф случайные ребра. Вопрос, однако, в том, будет ли рассматриваемая задача вычислительно сложной и для полученного таким образом распределения вероятностей на множестве графов? Исследования этой проблемы [4, 16] показали, что ситуация здесь нетривиальная.

Для дальнейшего изложения нам потребуются следующие обозначения.

Пусть $G = (V, E)$ — граф с $n$ вершинами. Пусть $p \in (0,1)$. Через $\mathcal{G}_{n,p}$ обозначается распределение Эрдёша–Реньи с параметрами $(n,p)$, т. е. распределение на множестве $n$-вершинных графов, которое возникает, если каждое ребро присутствует с вероятностью $p$ независимо от других ребер.

Хорошо известно, что задача распознавания наличия в заданном графе гамильтонова цикла является NP-полной. Если же рассматривать задачу поиска гамильтонова цикла с помощью рандомизированных алгоритмов, то ее сложность зависит от распределения вероятностей на множестве графов. Так, например, известно, что случайный граф из $\mathcal{G}_{n,p}$, где $p = d/n$, $d > \ln n/2$, почти наверное содержит гамильтонов цикл и последний может быть найден за полиномиальное время [3]. Таким образом, для графов достаточно высокой плотности задача поиска гамильтонова цикла не является вычислительно трудной.

С другой стороны, для графов низкой плотности, скажем из распределения $\mathcal{G}_{n,p}$, где $p = d/n$,

$d = const$, полиномиальные алгоритмы, решающие задачу о гамильтоновом цикле, не известны. Поэтому кажется естественным следующий метод построения «трудных» графов с известными гамильтоновыми циклами.

- Строится гамильтонов цикл $H$ на $n$ вершинах.
- $H$ маскируется путем добавления в граф каждого из возможных ребер независимо с вероятностью $d/n$, $d = const$.

Основной результат работы [4] показывает, что этот метод не работает. Предложен алгоритм, который за время $O(dn^3)$, где $d > d_0$, $d_0 = const$, почти наверное находит в построенном таким образом графе некоторый гамильтонов цикл (не обязательно совпадающий с $H$).

В работе [4] отмечается, что остается еще неисследованным случай графов очень низкой плотности, когда, например, к гамильтонову циклу добавляется случайное совершенное паросочетание.

Пример противоположного свойства продемонстрирован в работе [16].

Кликой размера $k$ в графе $G = (V, E)$ называется полный подграф на $k$ вершинах. Задача определения по заданным $G$ и $k$, имеется ли в графе $G$ клика размера $k$, называется задачей о клике. Она также относится к категории NP-полных задач. Задача поиска клик в заданном графе $G$ может быть поставлена в двух вариантах: найти максимальную клику, либо найти клику заданного размера.

Известно, что в случайном графе из $\mathcal{G}_{n,p}$, где $p = 1/2$, максимальная клика почти наверное имеет размер $2\log_2 n - O(\log\log n)$ [7]. Кроме того, с помощью рандомизированных жадных алгоритмов можно легко находить клики размера до $\log_2 n$ за полиномиальное в среднем время. В то же время все попытки продвинуться дальше за эту логарифмическую границу к успеху не привели. В результате возникла следующая гипотеза.

**Гипотеза.** Для всякой константы $\varepsilon > 0$ не существует полиномиального алгоритма, который с достаточно большой вероятностью находит клики размера $(1+\varepsilon)\log_2 n$ в случайном графе из $\mathcal{G}_{n,p}$, $p = 1/2$.

«Достаточно большая вероятность» здесь имеет стандартный для математической криптографии смысл: достаточно, чтобы эта вероятность была ограничена снизу величиной $1/n^c$ для некоторой константы $c$.

Для случайных графов из $\mathcal{G}_{n,p}$, где $p = const \neq 1/2$, ситуация аналогична и сформулированная выше гипотеза обобщается, очевидным образом, на случай произвольного такого $p$.

Неформально, основной результат работы [16] таков. Рассмотрим простейший алгоритм, который выбирает случайный граф $G$ и случайным образом встраивает в него клику размера $k \leqslant (1+\varepsilon)\log n$. Тогда задача поиска в полученном графе клик размера $\geqslant (1+\varepsilon)\log n$ остается, по существу, столь же сложной как и для исходного графа $G$.

Формально, пусть $G$ — случайный граф из $\mathcal{G}_{n,p}$. Выберем в графе $G$ случайным образом $k$ вершин и построим на этих $k$ вершинах клику, т. е. добавим в граф $G$ ребра так, чтобы подграф, индуцированный данными $k$ вершинами, был полным. Через $\tilde{\mathcal{G}}_{n,p,k}$ обозначим создаваемое таким образом распределение вероятностей на множестве графов.

**Теорема 1.** *Пусть $\delta, \varepsilon$ — константы такие, что $0 < \delta < 2$ и $0 < \varepsilon < \delta/4$. Пусть число $p$ таково, что для всех достаточно больших $n$, $n^{-(2-\delta)} < p < 1 - n^{-\varepsilon}$, и пусть $1 \leqslant k \leqslant (2-\delta)\log_{1/p} n$.*

*Предположим, что существует детерминированный полиномиальный алгоритм $A$, который находит клики размера $k$ в случайных графах из $\tilde{\mathcal{G}}_{n,p,k}$ с вероятностью $1/q(n)$ для некоторого полинома $q(n)$. Тогда существует полином $Q(n) = O(q^3(n)n^{-2\varepsilon})$ такой, что алгоритм $A$ находит клики размера $k$ в случайных графах из $\mathcal{G}_{n,p}$ с вероятностью $1/Q(n)$.*

В работе [16] отмечается, что данная теорема может быть обобщена на случай рандомизированных алгоритмов, а также на случай, когда в случайный граф $G$ из $\mathcal{G}_{n,p}$ встраиваются не одна, а $m$ клик размера $k$, $m = const$.

# 3 Инкрементальная криптография

Предположим, что отправитель сообщения применил к этому сообщению некоторое криптографическое преобразование. Например, вычислил его криптограмму или электронную подпись. И только

после этого, но еще до отправки сообщения по каналу связи, обнаружил в его тексте опечатку. Исправление опечатки, конечно, не представляет собой никакой проблемы. Но как быть с криптограммой или электронной подписью сообщения? Обычные криптографические схемы допускают только следующее решение: после исправления сообщения полностью повторить все вычисления. Существуют ли более эффективные способы?

Этот вопрос впервые был поднят Белларом и др. в 1994 г. [5]. В этой работе появилось понятие инкрементальной криптографии. Более обстоятельное изложение идей и результаты дальнейших исследований содержатся в работе [6] тех же авторов.

В самом общем виде концепция инкрементальной криптографии такова. Предположим, что у нас имеется некоторая криптографическая функция, которая всякому сообщению $m$ сопоставляет значение $A(m)$. Пусть значение $A(m)$ уже вычислено и нам необходимо значение $A(m')$ для нового сообщения $m'$, которое получено из $m$ внесением небольших изменений. Описание таких изменений мы будем обозначать через $\sigma(m, m')$. Требуется инкрементальный алгоритм $Inc$ такой, что $Inc(A(m), m, \sigma(m, m')) = A(m')$ и при этом количество операций, выполняемых алгоритмом $Inc$ существенно меньше, чем потребовалось бы для вычисления значения $A(m')$ «с нуля».

Если $A(m)$ — случайная величина (как, например, в случае, когда $A(m)$ является криптограммой сообщения $m$, вычисленной криптосистемой вероятностного шифрования, или электронной подписью сообщения $m$), вместо указанного выше равенства алгоритм $Inc$ должен обеспечивать, чтобы его выход был корректным значением данной криптографической функции для сообщения $m$.

Подчеркнем, что $Inc$ — это криптографический алгоритм, новый элемент криптографической схемы. Поэтому, если, скажем, $A$ — функция шифрования криптосистемы, то алгоритму $Inc$ должен быть известен ее ключ шифрования.

С практической точки зрения потребность в инкрементальных алгоритмах очевидна. Например, во многих приложениях требуется генерировать электронные подписи для большого количества документов, получаемых путем заполнения определенных полей некоторой стандартной формы.

В некоторых случаях существуют тривиальные инкрементальные алгоритмы. Если у нас есть подпись $s$ для сообщения $m$ и описание $\sigma(m, m')$ изменений, переводящих $m$ в новое сообщение $m'$, то подпись для пары $(s, \sigma)$ будет удовлетворять всем требованиям, предъявляемым к подписи для сообщения $m'$. Однако, для большинства приложений такой подход неприемлем, хотя бы уже потому, что увеличивается объем вычислений, необходимых для проверки подписей.

Основное требование к инкрементальным алгоритмам — эффективность, поэтому целью инкрементальной криптографии является разработка таких алгоритмов $Inc$, время выполнения которых на входе $(A(m), m, \sigma(m, m'))$ является функцией (достаточно медленно растущей) от «расстояния» между сообщениями $m$ и $m'$, а не от их длины. Это требование может показаться невыполнимым. Оно и в самом деле таково, если под алгоритмом понимается машина Тьюринга, поскольку только на перемещения по ленте, чтобы добраться до нужных битов сообщения $m$ требуется, вообще говоря, время порядка $O(|m|)$. Но эти трудности легко преодолеваются, если в качестве модели вычислений использовать машину с произвольным доступом к памяти. В такой машине можно обращаться к содержимому памяти по адресам, как это делается в обычных компьютерах.

При первом знакомстве может сложиться впечатление, что вся проблематика инкрементальной криптографии исчерпывается вопросами эффективности. Ведь алгоритм $Inc$ создается для криптографической схемы, которая изначально предполагается стойкой, а выход этого алгоритма (криптограмма, электронная подпись и т. п.) должен удовлетворять спецификациям схемы. Но на самом деле в инкрементальной криптографии возникают новые проблемы со стойкостью, которые не имеют аналогов в случае обычных криптографических схем. Обсуждение сущности этих проблем — та тема, ради которой написан данный раздел.

Рассмотрим случай, когда $A$ — функция шифрования $E$ какой-либо криптосистемы вероятностного шифрования. Инкрементальный алгоритм $Inc$ получает на вход $E(m)$, $m$ и $\sigma(m, m')$ и выдает $E(m')$.

Предположим, что исходная криптосистема (обозначим ее через $E$) является стойкой. Каким образом можно было бы доказать стойкость инкрементальной криптосистемы $E + Inc$? Стойкость криптосистемы можно определить только после того, как сформулированы конкретные предположения о противнике. Будем считать, что криптосистема $E$ является стойкой против атаки с выбором открытого текста. Тогда естественно предположить, что противник, атакующий криптосистему $E + Inc$, имеет доступ к обоим алгоритмам $E$ и $Inc$, т. е. может проводить комбинированную атаку, состоящую из атаки с выбором открытого текста на алгоритм $E$, и инкрементальных запросов к алгоритму

$Inc$. Будем считать, что противник использует самый слабый вариант такой комбинированной атаки, а именно, выбирает сообщение $m_1$ и получает его криптограмму $E(m_1)$, а затем, используя инкрементальные запросы, получает криптограммы

$$Inc(E(m_1), m_1, \sigma(m_1, m_2)), \ldots, Inc(E(m_{t-1}), m_{t-1}, \sigma(m_{t-1}, m_t))$$

последовательных модификаций $m_2, \ldots, m_t$ этого сообщения. Очевидно, что ту же самую атаку можно смоделировать и без доступа к алгоритму $Inc$: атака с выбором открытого текста на криптосистему $E$ позволяет получить криптограммы $E(m_1), \ldots, E(m_t)$.

Но для доказательства импликации вида: если криптосистема $E$ стойкая, то и криптосистема $E + Inc$ стойкая, недостаточно показать, что всякая атака на последнюю моделируется атакой на криптосистему $E$. Необходимо, чтобы противник в результате этих двух атак получал одинаковую информацию. Следовательно, имеются две возможности:

- Разрабатывать инкрементальные криптосистемы таким образом, чтобы для всех сообщений $m$, $m'$ и для любого инкрементального запроса $\sigma(m, m')$ распределения вероятностей $E(m')$ и $Inc(E(m), m, \sigma(m, m'))$ были неотличимы. Такое требование представляется весьма ограничительным.

- Рассматривать анализ стойкости инкрементальной криптосистемы $E + Inc$ как отдельную криптографическую задачу.

Приведем еще такой пример. Пусть $A$ — алгоритм $S$ генерации электронной подписи. Предположим, что в инкрементальной схеме подписи $S + Inc$ противник имеет доступ к алгоритму $Inc$ и выдает ему запрос $(s, m, \sigma(m, m'))$, где $s$ *не является* корректной подписью для сообщения $m$. Представляется, что информацию, полученную в результате выполнения такого запроса, не даст никакая атака на исходную схему подписи $S$. Поэтому необходим анализ стойкости инкрементальных схем подписи $S + Inc$ против атак указанного типа. Заметим, что казалось бы очевидная контрмера, состоящая в проверке корректности подписи $s$ для сообщения $m$ и в отказе от выполнения запроса, если подпись некорректна, не реализуема. У алгоритма $Inc$ просто нет времени на такую проверку.

Обсуждавшиеся выше проблемы Беллар и др. [6] относят к категории проблем стойкости (security). Для инкрементальных криптографических схем возникает еще и совершенно новая категория проблем конфиденциальности (privacy). Если стойкость относится к противнику, который специально предпринимает определенные усилия по взлому криптографической схемы, то конфиденциальность схемы означает, что в процессе ее функционирования отсутствует нежелательная утечка информации к законным участникам. Вернемся к тому же примеру инкрементальной схемы электронной подписи. Предположим, что подпись $s$ для сообщения $m$ получена из подписи для другого сообщения $m'$ с помощью инкрементального алгоритма $Inc$. Не дает ли этот факт, в совокупности с парой $(s, m)$, законному получателю какую-либо информацию о сообщении $m'$. Для многих приложений возможность такой утечки информации по крайней мере нежелательна. Идеальным вариантом здесь является совершенная (perfect) конфиденциальность: получатель не может отличить подписи, созданные инкрементальным алгоритмом $Inc$ от подписей, сгенерированных алгоритмом $S$.

Рассмотренные нами примеры со всей очевидностью показывают, что инкрементальная криптография является новым направлением исследований не только, и даже не столько, в теории алгоритмов, сколько в математической криптографии.

Приведем простейший пример инкрементального алгоритма [6], вычисляющего коды аутентификации сообщений (MAC'и).

Предположим, что сообщение $m$ состоит из $l$ блоков $m_1, \ldots, m_l$ длины $d$ каждый. В начало и в конец сообщения дописываются специальные блоки $m_0$ и $m_{l+1}$ соответственно. Через rand обозначается алгоритм, который на входе $v$ выбирает случайную $k$-битовую строку и дописывает ее в конец строки $v$. Пусть $f_1$ и $f_2$ — функции, выбранные из семейства псевдослучайных функций. Эти функции отображают входные строки длины $2(d + k)$ и $n$ соответственно в выходные строки длины $n$. Код аутентификации сообщения $m$ вычисляется по следующему алгоритму.

- Для каждого $i = 0, \ldots, l + 1$ вычисляется $r_i = \text{rand}(m_i)$.

- Вычисляется хэш-значение $h = \oplus_{i=0}^{l} f_1(r_i, r_{i+1})$.

- MAC вычисляется по формуле $T = f_2(h)$.

Рассматриваются два типа инкрементальных запросов — добавление и удаление блока. В качестве примера приведем алгоритм выполнения запроса на добавление блока. Такой запрос задается парой $(i, \tilde{m})$ и означает добавление блока $\tilde{m}$ между блоками $m_i$ и $m_{i+1}$. Алгоритм состоит из следующих шагов.

- Вычисляется $\tilde{r}$ =rand($\tilde{m}$).
- Вычисляется хэш-значение $\tilde{h} = h \oplus f_1(r_i, r_{i+1}) \oplus f_1(r_i, \tilde{r}) \oplus f_1(\tilde{r}, r_{i+1})$.
- Новый MAC вычисляется по формуле $\tilde{T} = f_2(\tilde{h})$.

Стойкость полученной схемы аутентификации сообщений анализируется в предположении, что противник может в ходе атаки на схему выдать $M_c$ запросов на генерацию MAC'ов для новых сообщений и $M_i$ инкрементальных запросов, каждый из которых задает удаление или добавление блока. Пусть $M = M_c + M_i$ и пусть $L$ — максимальная длина сообщения, возникающего в процессе атаки. Будем говорить, что противник подделывает MAC, если он создает корректный MAC для какого-либо нового сообщения, т. е. не входящего в число тех $M$ сообщений, MAC'и для которых были получены в результате атаки.

**Теорема 2.** *Предположим, что существует алгоритм, который за время $t$ на основе описанной выше атаки подделывает MAC с вероятностью $p$. Тогда существует алгоритм, который работает за время $O(t+(LM_c+M_i)(k+d+n))$, выдает $O(M_cL+M_i)$ запросов к оракулу и отличает семейство псевдослучайных функций (из которого выбраны $f_1$ и $f_2$) от случайной функции с вероятностью $p/2 - O(M^2 2^{-n}) - O((M_cL + M_i)^2 2^{-k})$.*

# 4 Односторонность конечных функций

Заголовок данного раздела может показаться парадоксальным. Определение односторонней функции требует, чтобы задача ее инвертирования была вычислительно трудной. Последнее требование может быть сформулировано только на языке теории сложности вычислений. Следовательно, односторонняя функция должна иметь бесконечную область определения. Но всякая такая функция представляет собой последовательность конечных функций, исследование свойств которых позволяет подойти к изучению односторонних функций как бы «с другого конца».

Пусть $B^n$ — $n$-мерный булев куб, $f : B^n \to B^n$ — перестановка. Через $C(f)$ обозначается сложность минимальной схемы в базисе из всех двуместных булевых функций, вычисляющей функцию $f$.

Прежде всего, возникает вопрос, существуют ли перестановки $f$ такие, что $f^{-1}$ вычисляется сложнее, чем $f$. Бойак [8] (цитируем по работе [13]) построил первые примеры перестановок, для которых $C(f) \neq C(f^{-1})$.

Хильтген [14, 15] построил бесконечные семейства $\{f_n\}$ линейных и нелинейных перестановок таких, что $\lim_{n\to\infty} C(f_n^{-1})/C(f_n) = 2$. Такие семейства называются слабо (feebly) односторонними. В данном случае — слабо односторонними порядка 2. Вообще, для данной перестановки $f$ естественно называть отношение $C(f^{-1})/C(f)$ мерой односторонности или просто односторонностью $f$.

Разумеется, односторонность порядка 2 является слишком слабой с любой точки зрения. Однако, новое направление исследований открыто и основная проблема здесь ставится следующим образом: определить, насколько порядок односторонности может быть повышен. Хильтген определил также порядок практической односторонности как

$$\lim_{n\to\infty} \log_2 C(f^{-1}) / \log_2 C(f).$$

Переведенное на этот язык общепринятое определение односторонней перестановки означает требование практической односторонности бесконечного порядка. По мнению же Хильтгена, практическая односторонность порядка 4 уже представляет интерес с прикладной точки зрения.

Перестановка $f : B^n \to B^n$ называется линейной, если каждая из $n$ ее булевых функций-компонент линейна. Линейная перестановка однозначно определяется булевой матрицей размера $n \times n$. Допуская некоторую вольность, будем обозначать эту матрицу той же буквой $f$.

Бойак [8] доказал, что если ограничиться схемами без памяти, то для всякой линейной перестановки $f$, $C(f^{-1}) = C(f)$. Напомним, что схемой без памяти называется схема, ширина которой не превосходит количества входов.

Если рассматривать схемы без ограничения на ширину, то, как уже отмечалось выше, появляются нетривиальные примеры. Приведем один из них, несмотря на некоторую его громоздкость.

$$f = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Хильтген [15] доказал, что $C(f) = 12$, а $C(f^{-1}) = 15$.

В работе [13] рассматриваются так называемые $t$-линейные перестановки, т. е. перестановки с треугольной матрицей $f$ (очевидно, что достаточно рассматривать верхние треугольные матрицы). Отметим сразу же, что на данный момент не известно ни одного примера $t$-линейной перестановки $f$ такой, что $C(f) \neq C(f^{-1})$. Однако, работа [13] интересна, прежде всего, исследованием качественных аспектов: если нетривиальная односторонность $t$-линейных перестановок все же существует, то откуда она берется и как структурные свойства перестановки на нее влияют. Это — один из побудительных мотивов обращения к односторонности конечных функций. Никаких результатов о внутренней структуре функций, односторонних в общепринятом смысле, не известно.

Матрица $f$, определяющая $t$-линейную перестановку при четном $n$ имеет вид $f = \begin{pmatrix} \theta & \lambda \\ 0 & \tau \end{pmatrix}$, где $\theta$ и $\tau$ — $t$-линейные перестановки, т. е. верхние треугольные матрицы, $\lambda$ — квадратная булева матрица, 0 — нулевая матрица. Очевидно, что обратная матрица $f^{-1}$ имеет вид $f^{-1} = \begin{pmatrix} \theta^{-1} & \theta^{-1}\lambda\tau^{-1} \\ 0 & \tau^{-1} \end{pmatrix}$.

В дальнейшем будем рассматривать случай $n = 2^\mu$.

**Лемма 6.** *Пусть $f$ — $t$-линейная перестановка, имеющая указанный выше вид и пусть $C(f) > 2^{\mu-2}$. Тогда если $C(\lambda) \geqslant \max\{C(\theta^{-1}), C(\tau^{-1})\}$, то $C(f^{-1})/C(f) < 5$.*

Эта лемма показывает, насколько хрупкой субстанцией является односторонность. Если у $t$-линейной перестановки $f$ была односторонность достаточно высокого порядка (много больше 5), то ее очень легко разрушить, просто заменив преобразование $\lambda$ на другое подходящее преобразование $\lambda'$ достаточно большой сложности. Более точно, достаточно взять любое такое $\lambda'$, удовлетворяющее неравенству $C(\lambda') \geqslant \{C(\theta^{-1}), C(\tau^{-1})\}$.

Дальнейший анализ показал также откуда односторонность может вообще возникнуть. Для этого необходимо, чтобы $\theta$ и $\tau$ имели почти одинаковую сложность и почти одинаковую односторонность. Кроме того, требуется, чтобы совместная реализация перестановок $\theta$ и $\tau$ на непересекающихся множествах входных переменных имела сложность $C(\theta \times \tau)$, существенно меньшую, чем $2\max\{C(\theta), C(\tau)\}$, а сложность $C(\theta^{-1} \times \tau^{-1})$ при этом была бы близка к $2\max\{C(\theta^{-1}), C(\tau^{-1})\}$.

Вопрос о существовании функций $f$ таких, что $C(f \times f) < 2C(f)$, исследовался Паулем [19] и Улигом [20]. В частности, Пауль доказал следующую теорему.

**Теорема 3.** *Для всякого $\varepsilon > 0$ существуют значения $n$ такие, что существуют $t$-линейные перестановки $f : B^n \to B^n$, удовлетворяющие неравенству*

$$C(f \times f) < (1 + \varepsilon)2^{\omega-2}C(f),$$

*где $\omega$ — минимальная экспонента такая, что умножение двух $N \times N$ матриц может быть выполнено схемой размера $N^{\omega+o(1)}$.*

В заключение отметим, что линейные перестановки, по понятным причинам, не могут иметь высокий порядок односторонности. Предметом дальнейших исследований может стать порядок односторонности перестановок, булевы функции-компоненты которых являются криптографическими, например, бент-функциями.

## 5 Неподатливая криптография

Одной из важнейших задач математической криптографии является исследование различных формализаций понятия стойкости криптографической схемы того или иного типа. Основное внимание уделяется классификации атак, но и угрозы безопасности криптографических схем также не забыты. рассмотрим в качестве примера криптосистемы с открытым ключом. Угроза полного извлечения противником открытого текста из криптограммы является очень сильной, а стойкость против нее, соответственно, слишком слабой. В литературе по математической криптографии такая стойкость практически никогда не рассматривается.

Можно потребовать, чтобы противник не мог извлечь из криптограммы ни одного бита открытого текста. Такая стойкость может оказаться достаточной для некоторых приложений. Гольдвассер и Микали [11] ввели понятие семантической стойкости. Неформально, криптосистема называется семантически стойкой, если полиномиально ограниченный противник не может извлечь из криптограммы никакой (полезной для себя, с учетом ограниченности вычислительных ресурсов) информации. Можно сказать, что такая стойкость является теоретико-сложностным или полиномиальным аналогом шенноновской совершенной секретности. Семантическую стойкость не следует рассматривать как некий абстрактный недостижимый идеал. Существуют криптосистемы с открытым ключом, для которых такая стойкость доказана в предположении вычислительной трудности теоретико-числовых задач. Первый пример такого рода содержится в той же работе Гольдвассер и Микали [11].

Казалось бы, для криптосистем с открытым ключом семантическая стойкость является максимальным требованием, которое невозможно, да и незачем, усиливать. Однако, Долев и др. [10] не согласны с такой точкой зрения и в качестве аргумента приводят следующий сценарий. Объявлен конкурс на строительство некоторого объекта по уже утвержденному проекту. Для приема заявок с предложениями цены организация, проводящая конкурс, опубликовала ключ шифрования криптосистемы с открытым ключом. Предположим, что строительная компания $A$ подала заявку, разумеется в зашифрованном виде, на 1 миллион. Могут ли ее конкуренты из компании $B$, перехватившие криптограмму, извлечь из этого какую-либо пользу? Если криптосистема семантически стойкая, то за разумное время невозможно получить из криптограммы какую-либо информацию о предложении цены компании $A$. Но для конкурентов это и не обязательно. Достаточно модифицировать криптограмму таким образом, чтобы получилась заявка с выгодной для компании $B$ ценой. Если существует эффективный способ модификации криптограммы так, что с вероятностью, существенно большей $1/2$, цена окажется меньше миллиона, то криптосистема называется податливой. В противном случае — неподатливой, нековкой (non-malleable).

Требование неподатливости может быть сформулировано и для других типов криптографических схем. В той же работе Долева и др. [10] описан еще и такой сценарий. Исследователь $A$ доказал, что P≠NP и хочет убедить в этом профессора $B$. По понятным причинам, для этого необходим протокол интерактивного доказательства с нулевым разглашением. Но обеспечивает ли такой протокол защиту авторских прав исследователя $A$ в полном объеме? Предположим, что профессор $B$ хочет присвоить открытие себе и «доказывает» утверждение P≠NP профессору $C$, просто пересылая запросы от $C$ к $A$, а ответы — от $A$ к $C$. Заметим, что в работах по протоколам интерактивной аутентификации подобные действия $B$ называются атакой посредника (man-in-the-middle) или мафиозной угрозой.

Математически строгое определение неподатливой криптосистемы с открытым ключом основывается на формализации следующего требования: для всякого отношения $R(\cdot,\cdot)$ противник может по данному шифртексту $E(\alpha)$ сгенерировать другой шифртекст $E(\beta)$ такой, что $R(\alpha,\beta)$, лишь «с тем же успехом», что и в случае, когда шифртекст $E(\alpha)$ ему вообще недоступен. Из литературы известны два способа задать меру успешности действий противника. В первоначальном определении Долева и др. [10] «эталоном», с которым сравниваются результаты, полученные противником, является моделирующая машина, которая пытается сгенерировать $E(\beta)$, не зная $E(\alpha)$. В альтернативном определении Беллара и др. [2] сравниваются вероятности, с которым противник создает шифртекст $E(\beta)$ такой, что $R(\alpha,\beta)$, в двух случаях: в регулярном, когда он получает на вход $E(\alpha)$, и в «эталонном», когда

ему дается шифртекст $E(\tilde{\alpha})$ для случайного $\tilde{\alpha}$.

Всюду ниже $A$ обозначает полиномиальный вероятностный алгоритм противника, выполняемый в две стадии, обозначаемые $A_1$ и $A_2$.

Определение стойкости криптосистемы с открытым ключом зависит от атаки противника. Для простоты изложения мы предполагаем, что противник проводит атаку с выбором открытого текста (напомним, что в случае криптосистемы с открытым ключом такая атака всегда возможна).

Первое из определений [10] предполагает следующую модель.

- На первой стадии противник, а именно алгоритм $A_1$, получает на вход открытый ключ криптосистемы и выдает пару $(M_k, \sigma)$, где $M_k$ — описание распределения вероятностей на множестве открытых текстов, $\sigma$ — битовая строка, $k$ — параметр безопасности (например, длина открытого ключа). Предполагается, что существует полиномиальный рандомизированный алгоритм, генерирующий на входе $1^k$ открытые тексты в соответствии с распределением $M_k$.

- На второй стадии алгоритм $A_2$ получает криптограмму $y$ сообщения $x$, выбранного из распределения $M_k$, и выдает вектор криптограмм $Y$.

- Пусть $R(\cdot,\cdot,\cdot,\cdot)$ — произвольное, но фиксированное отношение, вычислимое за полиномиальное время и пусть $X$ — вектор открытых текстов, соответствующий вектору криптограмм $Y$. Через $P_A$ обозначается вероятность того, что в итоге алгоритм $A$ выдаст вектор $Y$ такой, что $y \notin Y$ и $R(x, X, M_k, \sigma)$.

- Моделирующая машина $S$ — это полиномиальный вероятностный алгоритм, который получает на вход открытый ключ криптосистемы и выдает пару $(\sigma, Y)$, где $\sigma$ — битовая строка, а $Y$ — вектор криптограмм. Как и выше, через $X$ обозначается соответствующий вектор открытых текстов. Через $P_S$ обозначается вероятность, что $y \notin Y$ и $R(x, X, M_k, \sigma)$. Здесь опять $x$ — открытый текст, выбранный из распределения $M_k$.

**Определение 1.** [10] Криптосистема с открытым ключом называется неподатливой, если для любого отношения $R$, вычислимого за полиномиальное время и для любого полиномиального алгоритма противника $A$ существует моделирующая машина $S$ такая, что для всякого полинома $P$ и всех достаточно больших $k$, $|P_A - P_S| < 1/P(k)$.

Модель для второго из определений [2] такова.

- На первой стадии алгоритм $A_1$, получив на вход открытый ключ криптосистемы, выдает только распределение вероятностей $M_k$.

- На второй стадии алгоритм $A_2$ получает некоторую криптограмму $y$ и выдает пару $(R, Y)$. Здесь $R$ — описание некоторого двуместного отношения, вычислимого за полиномиальное время, а $Y$ — вектор криптограмм. Как и выше, соответствующий вектор открытых текстов обозначается через $X$.

- Через $P_1$ обозначается вероятность, что $y \notin Y$ и $R(x, X)$, где сообщение $x$ выбрано из распределения $M_k$, а $y$ — его криптограмма.

- Пусть $x, \tilde{x}$ выбраны независимо из распределения $M_k$ и $y$ — криптограмма сообщения $\tilde{x}$. Через $P_2$ обозначается вероятность, что $y \notin Y$ и $R(x, X)$.

**Определение 2.** [2] Криптосистема с открытым ключом называется неподатливой, если для любого полиномиального алгоритма $A$, любого полинома $P$ и всех достаточно больших $k$, $|P_1 - P_2| < 1/P(k)$.

Даже беглого взгляда на эти два определения достаточно, чтобы заметить существенные различия. Тем не менее, Беллар и Сахаи [9] доказали их эквивалентность.

**Теорема 4.** *Определения 1 и 2 эквивалентны в том смысле, что если криптосистема с открытым ключом является неподатливой в смысле одного из них, то она является таковой и в смысле другого.*

Метод доказательства этой теоремы даже интереснее самого результата. Эквивалентность двух определений неподатливой криптосистемы установлена путем доказательства эквивалентности каждого из них третьему.

В этом новом определении противник может осуществить атаку с выбором шифртекста на криптосистему. Он может выбрать вектор шифртекстов $c_1, \ldots, c_n$ и получить соответствующие открытые тексты $m_1, \ldots, m_n$. Единственное ограничение состоит в том, что выбор очередного шифртекста $c_i$ не может зависеть от предыдущих результатов $m_1, \ldots, m_{i-1}$. Такие атаки называются параллельными. Их удобно моделировать следующим образом: противник передает оракулу в качестве запроса сразу весь вектор шифртекстов $_1, \ldots, c_n$, а в качестве ответа получает весь вектор открытых текстов $m_1, \ldots, m_n$.

Для определения [9] используется следующая модель.

- Противником является полиномиальный вероятностный алгоритм $A = (A_1, A_2, A_3)$, выполняемый в три стадии.
- На первой стадии алгоритм $A_1$ получает на вход открытый ключ криптосистемы и выдает пару сообщений $(x_0, x_1)$.
- Далее выбирается случайный бит $b$ и пусть $y$ — криптограмма сообщения $x_b$. На второй стадии алгоритм $A_2$ на входе $y$ выдает вектор криптограмм $c_1, \ldots, c_n$. Пусть $m_1, \ldots, m_n$ — соответствующие открытые тексты.
- На третьей стадии алгоритм $A_3$ на входе $m_1, \ldots, m_n$ выдает бит $\delta$. Пусть $P_A$ обозначает вероятность, что $\delta = b$ и $y \notin c_1, \ldots, c_n$.

**Определение 3.** [9] Криптосистема с открытым ключом называется неподатливой, если для любого полиномиального алгоритма $A$, любого полинома $P$ и всех достаточно больших $k$, $|P_A - 1/2| < 1/P(k)$.

Эквивалентность определения 3 каждому из определений 1 и 2 — неординарный результат, требующий осмысления. Ведь неподатливость — это, по существу, требование целостности информации: активный противник не может модифицировать криптограмму так, чтобы открытый текст изменился выгодным для него образом. Что же касается определения 3. то оно сформулировано на обычном для криптосистем языке атак и угроз и фактически является определением стойкости криптосистемы, т. е. требованием конфиденциальности информации. Этот удивительный пример эквивалентности требований целостности и конфиденциальности стоит тех усилий, которые необходимо затратить, чтобы ознакомиться с содержимым настоящего раздела.

В заключение сделаем еще два замечания.

Во-первых, обеспечение целостности информации — одна из задач криптографии и исследуется достаточно давно. В частности, требование, аналогичное неподатливости, для криптосистем с секретным ключом обеспечивается средствами имитозащиты. В случае криптосистем с открытым ключом ситуация иная. Целостность шифруемой информации в принципе можно обеспечить с помощью схемы электронной подписи. Но не для всех приложений такое решение приемлемо. Это в особенности верно в тех случаях, когда криптосистемы используются в качестве примитива для построения сложных прикладных криптографических протоколов.

Во-вторых, необходимо подчеркнуть, что существуют примеры конструкций криптосистем с открытым ключом, которые являётся неподатливыми при достаточно правдоподобных предположениях [10], таких же, какие используются, например, для доказательства семантической стойкости. Открытой остается проблема построения достаточно эффективных неподатливых криптосистем.

## 6 Вычислительная сложность в среднем

Как уже отмечалось в разделе 2, для математических задач, на которых (по крайней мере, потенциально) могут основываться конструкции криптографических схем, вычислительная трудность «в худшем случае» недостаточна. Требуются задачи, трудные в среднем. Проблема поиска таких задач – одна из важнейших в математической криптографии. И тот факт, что прогресс в поисках ее решения на данный момент следует признать весьма незначительным, — свидетельство сложности этой

проблемы. Ясно, например, что хорошо развитая теория NP-полноты здесь не помогает. Не составляет никакого труда строить примеры NP-полных задач, разрешимых в среднем за полиномиальное время.

К этой проблеме можно подходить с чисто практических позиций — рассматривать задачи, которые достаточно интенсивно исследовались, но тем не менее для их решения так и не найдено полиномиальных в среднем алгоритмов.

Но если мы желаем иметь более обоснованную гипотезу о сложности в среднем, то необходимо искать другой подход. Для сложности в среднем есть аналоги как класса NP, так и понятия NP-полноты [17]. Поэтому естественной выглядит идея выбрать подходящую задачу и доказать ее полноту в таком классе. Но к настоящему моменту на данном пути не было достигнуто сколь-нибудь значительных успехов. Основная трудность в том, что при рассмотрении меры сложности «в среднем» существенным элементом определения задачи $T$ является семейство распределений вероятностей на множествах строк $\{0,1\}^n$ (носители этих распределений являются множествами входных строк длины $n$ задачи $T$). Чтобы продемонстрировать сводимость задачи $T_1$ к задаче $T_2$, необходимо построить вероятностный алгоритм, который работает за полиномиальное время и преобразует семейство распределений вероятностей задачи $T_1$ в аналогичное семейство задачи $T_2$. Ситуация осложняется еще и требованием эффективной конструируемости распределения вероятностей задачи $T_1$, т. е. должен существовать полиномиальный рандомизированный алгоритм, который генерирует входные данные задачи $T_1$ в соответствии с этим распределением (см. раздел 2).

Альтернативно, можно попытаться доказать сводимость другого рода: если задача $T_2$ трудна в худшем случае, то задача $T_1$ трудна в среднем. Разумеется, задача $T_2$ должна быть выбрана таким образом, чтобы гипотеза о ее вычислительной сложности выглядела достаточно обоснованной. Априори неясно, чем этот подход перспективнее предыдущего. Но пока именно он привел к наибольшим успехам. Для ряда задач доказана сводимость к их же рандомизированным вариантам. Другими словами, если эти задачи трудны в худшем случае, то они трудны и в среднем. В их число входят задача дискретного логарифмирования и задача распознавания квадратичных вычетов по модулю чисел Блюма (число вида $pq$ называется числом Блюма, если $p$ и $q$ — простые и $p \equiv q \equiv 3 \mod 4$).

Еще один очень интересный результат такого рода доказан Айтаи в его известной работе [1]. Вначале, следуя автору, мы изложим этот результат неформально.

Построен класс $\Lambda$ решеток в $Z^m$ со следующими свойствами.

- Существует эффективный вероятностный алгоритм, генерирующий случайные элементы класса $\Lambda$ вместе с принадлежащими им короткими векторами.

- Если существует полиномиальный вероятностный алгоритм, который в случайной решетке из $\Lambda$ находит короткий вектор с достаточно большой вероятностью (скажем, $1/2$), то существует полиномиальный вероятностный алгоритм, который для *всякой* решетки в $Z^n$, где $m = O(n \log n)$, решает с вероятностью, экспоненциально близкой к 1, *каждую* из следующих трех задач.

  (P1) Найти длину кратчайшего вектора решетки с точность до полиномиального (от $n$) множителя.

  (P2) Найти кратчайший ненулевой вектор в решетке, при условии, что такой вектор $v$ единственный в том смысле, что всякий другой вектор решетки, имеющий длину не более $n^c\|v\|$, параллелен $v$. Здесь $c$ — некоторая достаточно большая абсолютная константа.

  (P3) Найти в решетке базис $b_1, \ldots, b_n$ минимальной, с точность до полиномиального множителя, длины. Длина базиса определяется как $\max_i \|b_i\|$.

Таким образом, если хотя бы одна из трех задач P1–P3 трудна в худшем случае, то задача поиска коротких векторов в решетках из класса $\Lambda$ является вычислительно сложной в среднем.

Предположение о трудности задач P1–P3 выглядит весьма убедительно. Рассмотрим, например, задачу P1. Для нее не известна даже принадлежность классу NP. Ведь даже если нам и удастся угадать значение длины кратчайшего ненулевого вектора в решетке, то остается неясным, каким способом (а он должен быть вычислительно эффективным) можно было бы проверить такую догадку.

Зададимся теперь таким вопросом: для какой из задач, использовавшихся в конструкциях криптографических схем, гипотеза о трудности в среднем выглядит на сегодняшний день наиболее обоснованной? Ответ на этот вопрос большинству криптографов покажется по меньшей мере неожиданным.

Это — задача РЮКЗАК. Дело в том, что у цитированного выше результата Айтаи имеются два следствия:

- Если хотя бы одна из задач Р1–Р3 трудна в худшем случае, то существуют односторонние функции;
- При том же предположении существует трудный в среднем вариант задачи РЮКЗАК.

Более подробно эти следствия мы обсудим ниже. Пока же лишь отметим, что причины определенного скепсиса криптографов в отношении задачи РЮКЗАК имеют чисто психологическую природу. Хорошо известны многочисленные неудачные попытки построить на основе этой задачи криптосистему с открытым ключом. Но тот факт, что все эти криптосистемы оказались нестойкими, свидетельствует лишь о слабости предлагавшихся конструкций и никак не связан с вычислительной сложностью самой задачи РЮКЗАК.

Гипотеза о трудности в среднем теоретико-числовых задач выглядит менее обоснованной по сравнению с задачей РЮКЗАК хотя бы уже по следующей причине. Указанная выше сводимость для теоретико-числовых задач доказана только при фиксированном значении параметра (простой модуль в задаче дискретного логарифмирования, число Блюма в задаче о квадратичных вычетах). Например, если задача дискретного логарифмирования по данному простому модулю трудна в худшем случае, то она трудна и в среднем при том же фиксированном модуле. Возможно, существуют значения параметров, для которых эти теоретико-числовые задачи решаются эффективно. Во всяком случае, на данный момент не предложено никаких эффективных методов генерации значений параметров, для которых теоретико-числовые задачи являются гарантированно сложными. Такого рода гарантией могло бы быть, например, доказательство следующей импликации: если для данной задачи нет полиномиальных алгоритмов, то эта задача трудна для всех (достаточно больших) значений параметра, сгенерированных данным алгоритмом.

Переходим к более строгому изложению результатов Айтаи [1].

**Решетки.** Пусть $a_1, \ldots, a_n$ — линейно независимые векторы в $R^n$. Множество

$$\{\sum_{i=1}^{n} k_i a_i | k_1, \ldots, k_n \in Z\}$$

называется решеткой в $R^n$ и обозначается через $L(a_1, \ldots, a_n)$. Множество $a_1, \ldots, a_n$ называется базисом решетки. Под длиной вектора $a \in R^n$ понимается его эвклидова норма $\|a\|$ в $R^n$. Длина кратчайшего вектора в решетке $L$ обозначается через $sh(L)$, а длина кратчайшего базиса этой решетки — через $bl(L)$. Напомним, что длина базиса $a_1, \ldots, a_n$ определяется как $\max_i \|a_i\|$. Кратчайший вектор $u$ решетки $L$ называется $\alpha$-уникальным, если всякий другой вектор $v$ решетки $L$ такой, что $\|v\| < \alpha\|u\|$, параллелен $u$.

Задача поиска коротких векторов в решетках была поставлена Дирихле еще в 1842 г. Прогресс в ее решении, достигнутый с тех пор, нельзя назвать значительным. Самый известный результат — алгоритм Ленстры, Ленстры и Ловаса (алгоритм приведения базиса решетки, или $L^3$-алгоритм). Это — детерминированный полиномиальный алгоритм [18], который в каждой решетке $L \subseteq R^n$ находит вектор длины не более $2^{\frac{n-1}{2}} sh(L)$. В дальнейшем Шнорр показал, что множитель $2^{\frac{n-1}{2}}$ в этой оценке может быть заменен множителем $(1+\varepsilon)^n$ для любого фиксированного $\varepsilon > 0$. Этот результат Айтаи цитирует в работе [1] без ссылки на источник.

**Класс $\Lambda$.** Пусть $c_1$ и $c_2$ — две абсолютные константы и пусть для данного $n$, $m = [c_1 n \log n]$, $q = [n^{c_2}]$. Квадратные скобки обозначают целую часть числа.

Пусть $\lambda = (u_1, \ldots, u_m)$, где $u_i \in Z^n$. Решетку $\Lambda(\lambda, q)$ образуют все $m$-ки целых чисел $h_1, \ldots, h_m$ такие, что $\sum_{i=1}^{m} h_i u_i \equiv 0(\mod q)$. Здесь сравнимость двух векторов понимается покоординатно. Всякая решетка в классе $\Lambda$ имеет вид $\Lambda(\lambda, q)$ для некоторого $\lambda$ и фиксированного $q$ (при фиксированном $n$).

Далее, для того, чтобы говорить о сложности в среднем, необходимо задать некоторое распределение вероятностей на решетках вида $\Lambda(\lambda, q)$. Простейший способ состоит в случайном выборе $m$-ки $\lambda$. Для наших целей он не подходит, поскольку нам нужно сгенерировать случайную решетку $\Lambda(\lambda, q)$ вместе с принадлежащим ей коротким вектором. Поэтому применяется следующая модификация.

Векторы $v_1, \ldots, v_{m-1}$ выбираются независимо и случайно, относительно равномерного распределения, из множества всех векторов вида $(x_1, \ldots, x_n) \in Z^n$ с ограничением $0 \leqslant x_i < q$. Кроме того,

независимо генерируются $m-1$ случайных битов $\delta_1, \ldots, \delta_{m-1}$. Вектор $v_m$ определяется из следующего сравнения: $v_m \equiv -\sum_{i=1}^{m-1} \delta_i v_i (\mod q)$ при дополнительном ограничении, что каждая координата вектора $v_m$ принадлежит интервалу $[0, q-1]$. Сгенерированная таким образом $m$-ка $(v_1, \ldots, v_m)$ является случайной величиной, которую, чтобы не перегружать обозначения, будем обозначать той же буквой $\lambda$. Подчеркнем, что на самом деле таким образом построено семейство случайных величин $\lambda = \lambda(n, c_1, c_2)$, параметризованное значением $n$ и константами $c_1$ и $c_2$. Отметим также следующий факт. Для всякой данной $m$-ки $\lambda$ вектор $(\delta_1, \ldots, \delta_{m-1}, 1)$ принадлежит решетке $\Lambda(\lambda, q)$ и имеет длину не больше $n$, т. е. является тем коротким вектором, который требовалось построить.

**Алгоритмы.** Для решения задачи о коротком векторе в решетках из класса $\Lambda$ необходим полиномиальный вероятностный алгоритм $A$, который получает на вход значения параметров $n$, $m$ и $q$, а также значение случайной величины $\lambda$. На этом входе алгоритм $A$ должен выдать ненулевой вектор из решетки $\Lambda(\lambda, q)$ длины не больше $n$. Будем считать, что алгоритм $A$ решает задачу, если он выдает такой вектор с вероятностью по крайней мере $1/2$. Как и обычно в вероятностных вычислениях, константу $1/2$ можно заменить величиной порядка $n^{-c}$ для произвольной константы $c$. Результат останется в силе, более того, не изменятся и значения констант (чтобы подчеркнуть этот факт, они названы абсолютными). Вероятность успеха алгоритма $A$ определяется его собственными случайными величинами и распределением вероятностей на входных словах, создаваемым случайной величиной $\lambda$.

Задачи Р1–Р3 решаются с помощью вероятностного алгоритма $B$. Он получает на вход $n$-ку линейно независимых векторов $a_1, \ldots, a_n \in \mathbb{Z}^n$. Заметим, что на величину целочисленных координат этих векторов нет никаких ограничений. Поэтому длина входа алгоритма $B$ определяется как суммарная длина всех этих $n^2$ координат в двоичной записи. Мы будем обозначать эту длину через $\sigma$. Хотя алгоритм $B$ вероятностный, мы оцениваем его эффективность по худшему случаю. Поэтому вероятность успеха этого алгоритма определяется исключительно его собственными случайными величинами. В определении же сложности в худшем случае стоит квантор всеобщности по входным данным.

**Теорема 5.** *Существуют абсолютные константы $c_1$, $c_2$, $c_3$ такие, что справедливо следующее утверждение. Если существует полиномиальный вероятностный алгоритм $A$, который с вероятностью по крайней мере 1/2 выдает ненулевой вектор в $\Lambda(\lambda, q)$ длины не более $n$, то существует вероятностный алгоритм $B$, который на всяком входе $(a_1, \ldots, a_n)$ за полиномиальное от $\sigma$ время выдает значения $z$, $u$, $(d_1, \ldots, d_n)$ такие, что с вероятностью по крайней мере $1 - 2^{-\sigma}$ выполняются следующие условия.*

- *Если $v$ — кратчайший ненулевой вектор в решетке $L(a_1, \ldots, a_n)$, то $z \leqslant \|v\| \leqslant n^{c_3} z$.*
- *Если $v$ — $n^{c_3}$-уникальный ненулевой кратчайший вектор в решетке $L(a_1, \ldots, a_n)$, то либо $u = v$, либо $u = -v$.*
- *$d_1, \ldots, d_n$ — базис решетки $L(a_1, \ldots, a_n)$, удовлетворяющий условию*

$$\max_i \|d_i\| \leqslant n^{c_3} bl(L)$$

.

Теперь рассмотрим два следствия из этой теоремы.

**Односторонняя функция.** Для данного $n$ определяется функция $f = f^{(n)}$. Семейство всех таких конечных функций будет односторонней функцией. Область определения функции $f$ состоит из всех наборов вида $(v_1, \ldots, v_{m-1}, \delta_1, \ldots, \delta_{m-1})$, где все $v_i$ являются $n$-мерными векторами вида $(x_1, \ldots, x_n) \in \mathbb{Z}^n$ с ограничением $0 \leqslant x_i < q$, а все $\delta_i$ принимают значения 0 или 1. Пусть вектор $v_m$ определен так же, как в определении класса $\Lambda$. Тогда $f(v_1, \ldots, v_{m-1}, \delta_1, \ldots, \delta_{m-1}) = (v_1, \ldots, v_{m-1}, v_m)$. Из теоремы следует, что если хотя бы одна из задач Р1–Р3 трудна в худшем случае, то $f$ — односторонняя функция.

**Задача РЮКЗАК.** Пусть $q_1, \ldots, q_n$ — различные простые числа в диапазоне от $q$ до $2q$ и пусть $r$ — их произведение. Пусть далее $a_1, \ldots, a_m, b$ — независимые случайные целые числа, распределенные равномерно в диапазоне от 1 до $r-1$. Задача РЮКЗАК ставится как задача поиска таких значений $x_i = 0, 1$, что $\sum_{i=1}^{m} x_i a_i = b (\mod r)$. Из доказательства теоремы следует, что если хотя бы одна из задач Р1–Р3 трудна в худшем случае, то данная задача РЮКЗАК трудна в среднем.

## Литература


[1] M. Ajtai. *Generating hard instances of lattice problems.* 28th STOC, 1996, 99–108

[2] M. Bellare, A. Desai, D. Pointcheval, P. Rogaway. *Relations among notions of security for public-key encryption schemes.* Crypto'98, 1998, 26–45

[3] B. Bollobás, T. Fenner, A. Frieze. *An algorithm for finding Hamilton paths and cycles in random graphs.* Combinatorica, **7**, 1987, 327–341

[4] A. Broder, A. Frieze, E. Shamir. *Finding hidden Hamiltonian cycles.* 23rd STOC, 1991, 182–189

[5] M. Bellare, O. Goldreich, S. Goldwasser. *Incremental cryptography: the case of hashing and signing.* Crypto'94, 1994, 216–233

[6] M. Bellare, O. Goldreich, S. Goldwasser. *Incremental cryptography and application to virus protection.* 27th STOC, 1995, 45–56

[7] B. Bollobás. *Random graphs.* Academic Press, 1985

[8] S. Boyack. *The robustness of combinatorial measures of Boolean matrix complexity.* Ph. D. thesis, Massachusetts Inst. of Technology, 1985

[9] M. Bellare, A. Sahai. *Non-malleable encryption: equivalence between two notions, and an indistinguishability-based caracterization.* Crypto'99, 1999, 519–536

[10] D. Dolev, C. Dwork, M. Naor. *Non-malleable cryptography.* 23rd STOC, 1991, 542–552

[11] S. Goldwasser, S. Micali. *Probabilistic encryption.* J. Comput. System Sci., **28**, 1984, 270–299

[12] O. Goldreich, S. Micali, A. Wigderson. *Proofs that yield nothing but their validity and a methodology of cryptographic protocol design.* 27th FOCS, 1986, 174–187

[13] A. Hiltgen. *Towards a better understanding of one-wayness: facing linear permutations.* EUROCRYPT', 319–333

[14] A. Hiltgen. *Constructions of feebly one-way families of permutations.* Auscrypt'92, 1993, 422–434

[15] A. Hiltgen. *Cryptographically relevant contribution to combinational complexity theory.* ETH series in information processing, **3**, 1994

[16] A. Juels, M. Peinado. *Hiding cliques for cryptographic security.* Designs, Codes and Cryptography, **20**, 2000, 269–280

[17] L. Levin. *Average case complete problems.* SIAM J. Computing, **15**, 1986, 285–286

[18] A. Lenstra, H. Lenstra, L. Lovász. *Factoring polynomials with rational coefficients.* Math. Ann. **261**, 1982, 515–534

[19] W. Paul. *Realizing Boolean functions on disjoint sets of variables.* Theoret. Comput. Sci., **2**, 1976, 383–396

[20] D. Uhlig. *On the synthesis of self-correcting schemes from functional elements with small number of reliable elements.* Matemat. Zametki, **16**, N6, 1974, 937–944 (Оригинал на русском языке: Мат. заметки, том 15, 1974, 558–562)


---

STOC = Proceedings of the Annual. ACM Symposium on Theory of Computing. New York: ACM Press.

FOCS = Proceedings of the Annual Symposium on the Foundations of Computer Science. Los Alamitos, CA: IEEE Computer Society Press.

# Линейные рекуррентные последовательности и их приложения

А. С. Кузьмин, В. Л. Куракин, А. В. Михалев, А. А. Нечаев

Хорошо известны понятия линейных [17, 19, 43, 44, 48, 83, 84] и полилинейных [53, 62, 78, 79] рекуррентных последовательностей над полями. Такие последовательности обладают целым рядом хороших свойств, позволяющих использовать их как инструмент для построения датчиков псевдослучайных чисел и кодов, исправляющих ошибки. В данной работе в обзорной форме рассматриваются обобщения этих результатов для полилинейных рекуррентных последовательностей над кольцами и модулями, а также некоторые приложения.

## 1 Полилинейные рекуррентные последовательности над модулями

Используемые далее сведения о кольцах и модулях можно найти, например, в монографиях [2, 5, 11, 47]. Термин кольцо означает кольцо с единицей, термин модуль используется для левого модуля, если явно не указано, что модуль правый. В этом параграфе вводятся основные понятия, связанные с $k$-линейными рекуррентными последовательностями над модулями [16, 62, 65].

Пусть $M$ — модуль над кольцом $R$. Произвольное отображение $u\colon \mathbb{N}_0 \to M$, где $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$, называется последовательностью над $M$. Последовательность $u = (u(0), u(1), \ldots)$ называется *линейной рекуррентной последовательностью* (сокращенно ЛРП или 1-ЛРП), если существуют число $m \geqslant 1$ и элементы $c_0, \ldots, c_{m-1} \in R$ такие, что

$$u(i+m) = c_{m-1}u(i+m-1) + \ldots + c_1 u(i+1) + c_0 u(i), \qquad i \geqslant 0.$$

Многочлен $F(x) = x^m - c_{m-1}x^{m-1} - \ldots - c_1 x - c_0 \in R[x]$ называется *характеристическим многочленом* ЛРП $u$, вектор $u(\overline{0, m-1}) = (u(0), \ldots, u(m-1)) \in M^m$ — ее *начальным вектором*. Характеристический многочлен наименьшей степени называется *минимальным многочленом* ЛРП $u$, его степень называется *рангом* ЛРП $u$ и обозначается $\operatorname{rank} u$. Ранг нулевой последовательности полагается равным 0.

Если $k \geqslant 1$, то произвольное отображение $u\colon \mathbb{N}_0^k \to M$ называется *$k$-последовательностью* (часто просто последовательностью) над $M$. Последовательность $u$ называется *полилинейной* или *$k$-линейной рекуррентной последовательностью* (далее $k$-ЛРП или ЛРП) над модулем $M$, если существуют унитарные многочлены $F_1(x), \ldots, F_k(x) \in R[x]$ такие, что для любого $s \in \overline{1,k}$ и для любых фиксированных $i_1, \ldots, i_{s-1}, i_{s+1}, \ldots, i_k \in \mathbb{N}_0$ 1-последовательность $v(i) = u(i_1, \ldots, i_{s-1}, i, i_{s+1}, \ldots, i_k)$, $i \in \mathbb{N}_0$, есть 1-ЛРП над $M$ с характеристическим многочленом $F_s(x)$. Многочлены $F_1(x_1)$, ..., $F_k(x_k)$ из кольца $R[\boldsymbol{x}] = R[x_1, \ldots, x_k]$ многочленов от $k$ переменных называются *элементарными характеристическими многочленами $k$-ЛРП $u$*. Множество всех $k$-последовательностей над $M$ обозначается через $M^{\langle k\rangle}$, множество всех $k$-ЛРП над $M$ — через $\mathcal{L}_R M^{\langle k\rangle}$. Множество всех $k$-ЛРП над $M$ с элементарными характеристическими многочленами $F_1(x_1)$, ..., $F_k(x_k)$ будем обозначать $L_M(F_1, \ldots, F_k)$. Множество $M^{\langle k\rangle}$ является абелевой группой относительно естественного (покоординатного) сложения последовательностей.

Для вектора $\boldsymbol{s} = (s_1, \ldots, s_k) \in \mathbb{N}_0^k$ обозначим $\boldsymbol{x}^{\boldsymbol{s}} = x_1^{s_1} \ldots x_k^{s_k}$. Если $u \in M^{\langle k\rangle}$, то последовательность $v = \boldsymbol{x}^{\boldsymbol{s}} u \in M^{\langle k\rangle}$ со знаками $v(\boldsymbol{i}) = u(\boldsymbol{i} + \boldsymbol{s})$, $\boldsymbol{i} \in \mathbb{N}_0^k$, называется *сдвигом* последовательности $u$ на вектор $\boldsymbol{s}$ (или на $s$ шагов влево при $k = 1$). Произведение произвольного многочлена $F(\boldsymbol{x}) = \sum_{\boldsymbol{s} \in \mathbb{N}_0^k} c_{\boldsymbol{s}} \boldsymbol{x}^{\boldsymbol{s}} \in R[\boldsymbol{x}]$ на последовательность $u$ определяется по линейности:

$$v = F(\boldsymbol{x})u = \sum_{\boldsymbol{s} \in \mathbb{N}_0^k} c_{\boldsymbol{s}} \boldsymbol{x}^{\boldsymbol{s}} u, \quad \text{т. е.} \quad v(\boldsymbol{i}) = \sum_{\boldsymbol{s} \in \mathbb{N}_0^k} c_{\boldsymbol{s}} u(\boldsymbol{i} + \boldsymbol{s}), \quad \boldsymbol{i} \in \mathbb{N}_0^k. \tag{1}$$

Относительно этой операции абелева группа $(M^{\langle k\rangle}, +)$ превращается в левый $R[\boldsymbol{x}]$-модуль [62]. Будем говорить, что $F(\boldsymbol{x})$ аннулирует $u$, если $F(\boldsymbol{x})u = 0$. Левый идеал

$$\mathrm{An}(u) = \{F(\boldsymbol{x}) \in R[\boldsymbol{x}] : F(\boldsymbol{x})u = 0\}$$

кольца $R[\boldsymbol{x}]$ называется *аннулятором* последовательности $u$.

Левый (правый, двусторонний) идеал $I$ кольца $R[\boldsymbol{x}]$ назовем *унитарным*, если он содержит многочлены $F_1(x_1)$, ..., $F_k(x_k)$ такие, что $F_s(x_s)$ — унитарный многочлен от одной переменной, $s \in \overline{1,k}$. Такие многочлены будем называть *элементарными характеристическими многочленами идеала* $I$. Согласно приведенным определениям, последовательность $u \in M^{\langle k\rangle}$ есть $k$-ЛРП тогда и только тогда, когда левый идеал $\mathrm{An}(u)$ унитарен, при этом $u \in L_M(F_1, \ldots, F_k)$ тогда и только тогда, когда $F_1(x_1)$, ..., $F_k(x_k) \in \mathrm{An}(u)$.

Для произвольного подмножества $T \subseteq R[\boldsymbol{x}]$ обозначим

$$L_M(T) = \{u \in M^{\langle k\rangle} : Tu = 0\}.$$

Тогда $L_M(T)$ является абелевой группой и $L_M(T) = L_M(R[\boldsymbol{x}]T)$, где $R[\boldsymbol{x}]T$ — левый идеал кольца $R[\boldsymbol{x}]$, порожденный множеством $T$. Если левый идеал $R[\boldsymbol{x}]T$ унитарен, то множество $T$ называется *унитарным слева*. В этом случае $L_M(T) \subseteq \mathcal{L}_R M^{\langle k\rangle}$, и абелева группа $L_M(T)$ называется *ЛРП-семейством* (или $k$-ЛРП-семейством). Всякое ЛРП-семейство содержится в ЛРП-семействе вида $L_M(F_1, \ldots, F_k)$. Если левый идеал $R[\boldsymbol{x}]T$ является также правым идеалом (в частности, если кольцо $R$ коммутативно), то $L_M(T)$ — левый $R[\boldsymbol{x}]$-подмодуль в $M^{\langle k\rangle}$.

Подмодуль

$$R[\boldsymbol{x}]u = \{F(\boldsymbol{x})u : F(\boldsymbol{x}) \in R[\boldsymbol{x}]\}$$

$R[\boldsymbol{x}]$-модуля $M^{\langle k\rangle}$ (т. е. циклический подмодуль, порожденный элементом $u$) называется *модулем сдвигов* $k$-последовательности $u$, а $R[\boldsymbol{x}]$-модуль $R[\boldsymbol{x}]/\mathrm{An}(u)$ — ее *модулем операторов*. Если $\mathrm{An}(u)$ — двусторонний идеал в $R[\boldsymbol{x}]$, в частности, если $R$ коммутативно, то $R[\boldsymbol{x}]/\mathrm{An}(u)$ — кольцо, называемое *кольцом операторов* $k$-последовательности $u$.

Если $M_R$ — правый модуль над кольцом $R$, то аналогично даются определения $k$-ЛРП над правым модулем $M_R$, произведения $uF(\boldsymbol{x})$ последовательности $u \in M^{\langle k\rangle}$ на многочлен $F(\boldsymbol{x})$ и другие определения. Множество $k$-ЛРП над правым модулем $M_R$ будем обозначать $\mathcal{L}M_R^{\langle k\rangle}$.

Если ${}_AM_B$ — бимодуль над кольцами $A$ и $B$, то *левой $A$-$k$-ЛРП* (соответственно *правой $B$-$k$-ЛРП*) *над бимодулем* ${}_AM_B$ будем называть произвольную $k$-ЛРП над модулем ${}_AM$ (соответственно над правым модулем $M_B$). Наряду с этим можно ввести понятие (*двусторонней*) *$k$-ЛРП над бимодулем* ${}_AM_B$. Например, в случае $k = 1$ мы говорим, что $u \in M^{\langle 1\rangle}$ есть *1-ЛРП над бимодулем* ${}_AM_B$, если существуют параметры $m$, $t \in \mathbb{N}$, числа $i_1$, ..., $i_t \in \overline{0, m-1}$ (не обязательно различные) и наборы коэффициентов $a_1$, ..., $a_t \in A$, $b_1$, ..., $b_t \in B$ такие, что

$$u(i+m) = a_1u(i+i_1)b_1 + \ldots + a_tu(i+i_t)b_t, \qquad i \geqslant 0. \tag{2}$$

Множество всех $k$-ЛРП над бимодулем ${}_AM_B$ обозначим $\mathcal{L}_AM_B^{\langle k\rangle}$.

Кольцо $R$ можно рассматривать как левый и как правый $R$-модуль, а также как бимодуль над собой. *Левой* (соответственно *правой*) *$k$-ЛРП над кольцом $R$* назовем произвольную $k$-ЛРП над модулем ${}_RR$ (соответственно над модулем $R_R$). *Двухсторонней $k$-ЛРП над кольцом $R$* назовем $k$-ЛРП над бимодулем ${}_RR_R$. Если кольцо $R$ коммутативно, то понятия левой, правой и двухсторонней $k$-ЛРП совпадают.

На множестве $\mathbb{N}_0^k$ зададим отношения частичного (покоординатного) порядка $\leqslant$, полагая для $\boldsymbol{i} = (i_1, \ldots, i_k)$, $\boldsymbol{j} = (j_1, \ldots, j_k) \in \mathbb{N}_0^k$

$$\boldsymbol{i} \leqslant \boldsymbol{j} \qquad \Leftrightarrow \qquad i_1 \leqslant j_1, \ \ldots, \ i_k \leqslant j_k.$$

Для векторов из $\mathbb{N}_0^k$ будем использовать обозначения

$$\mathbf{1} = (1, \ldots, 1), \quad \mathbf{0} = (0, \ldots, 0), \quad \mathbf{1}_s = (0, \ldots, 0, 1, 0, \ldots, 0),$$

где единица в векторе $\mathbf{1}_s$ находится на $s$-ом месте, $1 \leqslant s \leqslant k$.

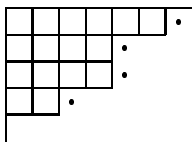

Рис. 1: Диаграмма Ферре

Конечное множество $\mathcal{F} \subset \mathbb{N}_0^k$ назовем *диаграммой Ферре* (см. рис. 1), если

$$\forall \boldsymbol{i}, \boldsymbol{j} \in \mathbb{N}_0^k \qquad (\boldsymbol{i} \in \mathcal{F},\ \boldsymbol{j} \leqslant \boldsymbol{i}) \quad \Rightarrow \quad (\boldsymbol{j} \in \mathcal{F}).$$

Пусть $\boldsymbol{i} + \mathcal{F} = \{\boldsymbol{i} + \boldsymbol{j} : \boldsymbol{j} \in \mathcal{F}\}$. Множество $\Delta_s \mathcal{F} = (\mathbf{1}_s + \mathcal{F}) \setminus \mathcal{F}$ назовем (внешней) *границей диаграммы Ферре* $\mathcal{F}$ *в направлении* $s$, а множество $\Delta\mathcal{F} = \Delta_1\mathcal{F} \cup \ldots \cup \Delta_k\mathcal{F}$ — (внешней) *границей* диаграммы Ферре $\mathcal{F}$ (см. рис. 1, на котором изображена диаграмма Ферре в $\mathbb{N}_0^2$ и точками отмечена ее граница в одном из направлений). Вектор $\boldsymbol{j} \in \mathcal{F}$ называется (внутренним) *углом* диаграммы Ферре $\mathcal{F}$, если $\boldsymbol{j} + \mathbf{1}_s \notin \mathcal{F}$ для любого $s \in \overline{1,k}$.

Важным частным случаем диаграммы Ферре является *параллелепипед* $\Pi(\boldsymbol{m})$ размеров $m_1 \times \ldots \times m_k$ в $\mathbb{N}_0^k$, где $m_1, \ldots, m_k \in \mathbb{N}$:

$$\Pi = \Pi(\boldsymbol{m}) = \Pi(m_1, \ldots, m_k) = \overline{0, m_1 - 1} \times \ldots \times \overline{0, m_k - 1}.$$

Если $k = 1$, то $\Pi(m)$ есть просто отрезок натурального ряда: $\Pi(m) = \overline{0, m-1}$, и такими отрезками исчерпываются все диаграммы Ферре.

Будем считать, что на множестве $\mathbb{N}_0^k$ задан некоторый полный (например, лексикографический) порядок $\preceq$. Пусть $\Omega = \{\boldsymbol{i}_1, \ldots, \boldsymbol{i}_m\} \subset \mathbb{N}_0^k$ — конечное множество, элементы которого занумерованы так, что $\boldsymbol{i}_1 \preceq \ldots \preceq \boldsymbol{i}_m$. Вектор

$$u[\Omega] = (u(\boldsymbol{i}_1), \ldots, u(\boldsymbol{i}_m)) \in M^m$$

будем называть *диаграммой* (или *вектором*) *значений* $k$-последовательности $u$ на множестве $\Omega$. Если $u$ — $k$-ЛРП с элементарными характеристическими многочленами $F_1(x_1)$, ..., $F_k(x_k)$ степеней $m_1$, ..., $m_k$ соответственно, то параллелепипед $\Pi = \Pi(\boldsymbol{m})$ назовем *начальным параллелепипедом* $k$-ЛРП $u$, а $u[\Pi]$ — *диаграммой начальных значений* (или *начальным вектором*) $k$-ЛРП $u$. Так же, как и элементарные характеристические многочлены, начальный параллелепипед $k$-ЛРП $u$ определяется не однозначно.

Пусть $M^\Omega$ — множество всех отображений $\delta\colon \Omega \to M$. Вектор $\delta[\Omega] = (\delta(\boldsymbol{i}_1), \ldots, \delta(\boldsymbol{i}_m)) \in M^m$ назовем *диаграммой* (или *вектором*) *значений* отображения $\delta$ на множестве $\Omega$. В дальнейшем мы будем отождествлять отображение $\delta \in M^\Omega$ с его вектором значений $\delta[\Omega] \in M^m$ и считать, что $M^\Omega = M^m$.

Кольцо $R$ называется *локальным* (см. [11, 47]), если оно содержит единственный максимальный идеал $J$, совпадающий в этом случае с радикалом Джекобсона кольца $R$. В локальном кольце множество $R^*$ обратимых элементов совпадает с $R \setminus J$. В дальнейшем всегда используются только коммутативные локальные кольца. В этом случае факторкольцо $\bar{R} = R/J$ является полем, называемым *полем вычетов* локального кольца $R$. Через $\bar{a}$, $\bar{F}(x)$ и $\bar{u}$ будем обозначать естественные образы элемента $a \in R$, многочлена $F(x) \in R[x]$ и $k$-последовательности $u \in R^{\langle k \rangle}$ над полем вычетов $\bar{R}$. Унитарный многочлен $F(x) \in R[x]$ называется *многочленом Галуа*, если его образ $\bar{F}(x)$ является неприводимым над полем $\bar{R}$ многочленом.

Любое артиново (в частности, конечное) коммутативное кольцо с единицей представляется в виде прямой суммы локальных колец [2]. Вследствие этого большинство задач для линейных рекуррент над коммутативными артиновыми кольцами стандартным образом сводятся к случаю локального кольца. Этим объясняется важность локальных колец и тот факт, что часто рассматриваются ЛРП именно над локальными кольцами.

*Кольцом Галуа* называется конечное коммутативное локальное кольцо $R$, максимальный идеал которого равен $pR$ для некоторого простого числа $p$ (см. [9, 35, 69]). Кольцо Галуа с точностью до изоморфизма определяется своей характеристикой $p^n$ и числом элементов $q^n$, где $q = p^r$, и обозначается $GR(q^n, p^n)$. Частные случаи колец Галуа: примарные кольца вычетов $\mathbb{Z}_{p^n} = GR(p^n, p^n)$ и конечные поля $GF(q) = GR(q, p)$. Если $F(x)$ — многочлен Галуа степени $m$ над кольцом Галуа $R = GR(q^n, p^n)$, то

кольцо $S = R[x]/F(x) = R[\theta]$, где $\theta = [x]_F \in S$, является кольцом Галуа $S = GR(q^{mn}, p^n)$, называемым расширением Галуа степени $m$ кольца Галуа $R$.

## 2 Периодичность и мультипликаторы

В этом параграфе $R$ — конечное коммутативное кольцо с единицей $e$, ${}_RM$ — конечный точный $R$-модуль, $u : \mathbb{N}_0^k \to M$ — $k$-ЛРП над $M$ с аннулятором $I = \mathrm{An}(u)$. Кольцо операторов $S = R[\boldsymbol{x}]/I$ конечно, что является критерием унитарности идеала $I$. Кольцо операторов *несингулярной* $k$-ЛРП $u$, т.е. такой, что $I \cap R = 0$, имеет вид $S = R[\theta_1, \ldots, \theta_k]$, где $\theta_s = x_s + I$, $s \in \overline{1,k}$, — *элементарные операторы* $k$-ЛРП $u$. Элементы кольца $S$ имеют вид $A(\boldsymbol{\theta}) = A(\theta_1, \ldots, \theta_k)$, где $A(\boldsymbol{x}) \in R[\boldsymbol{x}]$, и их действие на $u$ определяется равенством $A(\boldsymbol{\theta})u = A(\boldsymbol{x})u$. Напомним следующие понятия [62, 16].

*Реверсивная $k$-ЛРП $u$*: $k$-ЛРП $u$ с аннулятором $I$, содержащим многочлены $x_1^{t_1} - e$, ..., $x_k^{t_k} - e$ для некоторых $t_1, \ldots, t_k \in \mathbb{N}$. Критерий реверсивности $u$ — обратимость элементарных операторов: $\theta_1, \ldots, \theta_k \in S^*$.

Далее предполагается, что $u$ есть несингулярная реверсивная $k$-ЛРП над $M$.

*Цикловая группа $u$*: подгруппа $\mathcal{T}(u) = \mathcal{T}(I) = < \theta_1, \ldots, \theta_k >$ группы $S^*$.

*Цикл $u$* — совокупность $k$-ЛРП $\mathcal{T}(I)u$.

*Период $u$*: $T(u) = |\mathcal{T}(I)u| = |\mathcal{T}(I)|$.

*Вектор-период $u$*: вектор $\boldsymbol{\tau} \in \mathbb{N}_0^k \setminus \mathbf{0}$ такой, что $\boldsymbol{x}^{\boldsymbol{\tau}} u = u$, т.е. $\boldsymbol{x}^{\boldsymbol{\tau}} - e \in I$.

*Группа вектор-периодов $u$*: $\mathfrak{P}(u) = \mathfrak{P}(I)$ — подгруппа группы $(\mathbb{Z}^k, +)$, порожденная всеми вектор-периодами $k$-ЛРП $u$. Имеют место следующие соотношения:

$$\mathcal{T}(I) \cong \mathbb{Z}^k/\mathfrak{P}(I), \quad T(u) = |\mathbb{Z}^k : \mathfrak{P}(u)|.$$

Если $u$ есть несингулярная реверсивная 1-ЛРП над кольцом $R$ с периодом $T(u) = t$, то ее кольцо операторов есть $S = R[\theta] = R[x]/I$, где $\theta = x + I$ — обратимый элемент $S$, $\mathrm{ord}\,\theta = t$. Цикловая группа $u$ есть $\mathcal{T}(I) = < \theta >$, и цикл $u$ имеет вид $\mathcal{T}(I)u = \{u, \theta u, \ldots, \theta^{t-1}u\}$. Для наглядности цикл $u$ часто представляют начальным отрезком длины $t$ последовательности $u$:

$$u[\overline{0, t-1}] = (u(0), u(1), \ldots, u(t-1)). \tag{3}$$

Мы будем называть 3 *диаграммой цикла* ЛРП $u$. При этом

$$u = (u[\overline{0, t-1}], u[\overline{0, t-1}], \ldots).$$

Известно, что диаграмму цикла 3 ЛРП $u$ зачастую можно разбить на более мелкие блоки, отличающиеся друг от друга умножением на константы. Последние составляют циклическую подгруппу $\mathrm{Mult}(u) = < \theta > \cap R^* = < a >$ группы $< \theta >$. Группа $\mathrm{Mult}(u)$ называется *группой мультипликаторов* 1-ЛРП $u$. Если $\mathrm{ord}\, a = d$, то $d|t$ и $t = \pi d$. При этом отрезок 3 имеет вид

$$u[\overline{0, t-1}] = (u[\overline{0, \pi-1}], au[\overline{0, \pi-1}], \ldots, a^{d-1}u[\overline{0, \pi-1}]). \tag{4}$$

Параметр $\pi$ иногда называют *предпериодом* или *редуцированным периодом* ЛРП $u$. Будем использовать обозначение $\pi = T_{red}(u)$. Тогда

$$T(u) = |\,\mathrm{Mult}(u)| \cdot T_{red}(u). \tag{5}$$

Пусть $u \in M^{\langle k \rangle}$ есть несингулярная реверсивная $k$-ЛРП такая, что

$$M = \mathrm{Supp}(u), \tag{6}$$

где $\mathrm{Supp}(u)$ — *носитель* ЛРП $u$, т.е. $R$-модуль, порожденный всеми знаками $u(\boldsymbol{i})$, $\boldsymbol{i} \in \mathbb{N}_0^k$. Пусть $E({}_RM)$ — кольцо эндоморфизмов $R$-модуля $M$. Определим действие эндоморфизма $\varphi \in E({}_RM)$ на $k$-последовательности $v \in M^{\langle k \rangle}$ следующим образом:

$$\varphi(v) = \lambda \in M^{\langle k \rangle}, \quad \forall \boldsymbol{i} \in \mathbb{N}_0^k \quad \lambda(\boldsymbol{i}) = \varphi(v(\boldsymbol{i})).$$

Нетрудно видеть, что в таком случае для любого многочлена $A(\boldsymbol{x}) \in R[\boldsymbol{x}]$ справедливо равенство

$$A(\boldsymbol{x})\varphi(v) = \varphi(A(\boldsymbol{x})v) \tag{7}$$

и поэтому, в частности, $\mathrm{An}(v) \subseteq \mathrm{An}(\varphi(v))$.

Скажем, что эндоморфизм $\varphi$ есть *мультипликатор* $k$-ЛРП $u$, если существует $\boldsymbol{\tau} \in \mathbb{N}_0^k$ со свойством

$$\boldsymbol{x}^{\boldsymbol{\tau}} u = \varphi(u). \tag{8}$$

Множество всех мультипликаторов $k$-последовательности $u$ обозначим $\mathrm{Mult}(u) = \mathcal{M}(u)$. Воспользовавшись свойствами кольца операторов $S$, равенство 8 можно переписать также в виде

$$\boldsymbol{\theta}^{\boldsymbol{\tau}} u = \varphi(u). \tag{9}$$

Таким образом, мультипликатору $\varphi$ поставлен в соответствие элемент $\breve{\varphi} = \boldsymbol{\theta}^{\boldsymbol{\tau}}$ из цикловой группы $\mathcal{T}(u) = \langle \theta_1, \ldots, \theta_k \rangle$ $k$-ЛРП $u$. Мы будем называть $\breve{\varphi}$ также *мультипликатором* или *операторным мультипликатором* $k$-ЛРП $u$. Совокупность всех операторных мультипликаторов $u$ обозначается через $\breve{\mathcal{M}}(u)$. Таким образом,

$$\breve{\mathcal{M}}(u) = \{g \in \mathcal{T}(u) : \exists \varphi \in E({}_R M) : gu = \varphi(u)\}.$$

Мы имеем естественную сюръекцию

$$\omega : \mathrm{Mult}(u) \to \breve{\mathcal{M}}(u), \quad \omega(\varphi) = \breve{\varphi}. \tag{10}$$

**Предложение 1.** *Если $u$ есть несингулярная реверсивная $k$-ЛРП со свойством 6, то* $\mathrm{Mult}(u)$ — *абелева подгруппа группы* $\mathrm{Aut}({}_R M)$ *автоморфизмов модуля* ${}_R M$, *и отображение $\omega$ есть изоморфизм групп. Группа* $\mathrm{Mult}(u)$ *порождается $k$ элементами.*

Факторгруппу $\mathcal{T}_{red}(u) = \mathcal{T}(u)/\breve{\mathcal{M}}(u)$ назовем *редуцированной цикловой группой $k$-ЛРП $u$*, а ее мощность $T_{red}(u) = |\mathcal{T}_{red}(u)|$ — *редуцированным периодом* или *факторпериодом $u$*. Непосредственно из определений имеем по аналогии с 5

$$T(u) = |\,\mathrm{Mult}(u)| \cdot T_{red}(u).$$

Факторпериод можно описать также иначе.

Назовем вектор $\boldsymbol{\tau} \in \mathbb{N}_0^k \setminus \mathbf{0}$ *редуцированным вектор-периодом* $k$-ЛРП $u$, если он удовлетворяет условию 8 для некоторого $\varphi \in E({}_R M)$, т.е. если

$$\boldsymbol{\theta}^{\boldsymbol{\tau}} \in \breve{\mathcal{M}}(u). \tag{11}$$

Подгруппу $\mathfrak{P}_{red}(u)$ группы $(\mathbb{Z}^k, +)$, порожденную всеми такими $\boldsymbol{\tau}$, назовем *группой редуцированных вектор-периодов $u$*. Очевидно,

$$\mathfrak{P}(u) \leqslant \mathfrak{P}_{red}(u) \leqslant \mathbb{Z}^k. \tag{12}$$

Группа $\mathfrak{P}_{red}(u)$ обладает свойствами, сходными со свойствами группы $\mathfrak{P}(u)$. Пусть

$$\mathfrak{P}^+_{red}(u) = \mathfrak{P}_{red}(u) \cap (\mathbb{N}_0^k \setminus \mathbf{0}).$$

**Предложение 2.** *Группа $\mathfrak{P}_{red}(u)$ есть свободная абелева группа ранга $k$. Любой вектор $\boldsymbol{\tau} \in \mathfrak{P}^+_{red}(u)$ есть редуцированный вектор-период $u$.*

**Предложение 3.** *Имеют место соотношения*

$$\mathfrak{P}_{red}(u)/\mathfrak{P}(u) \cong \breve{\mathcal{M}}(u), \quad \mathbb{Z}^k/\mathfrak{P}_{red}(u) \cong \mathcal{T}_{red}(u),$$

$$T_{red}(u) = |\mathbb{Z}^k : \mathfrak{P}_{red}(u)|, \quad T(u) = T_{red}(u) \cdot |\,\mathrm{Mult}(u)|.$$

Заметим, что каждое из включений 12 может обращаться в равенство.

**Пример 1.** *Пусть $M = R$, $a_1, \ldots, a_k \in R^*$, причем $R^* = \langle a_1, \ldots, a_k \rangle$. Зададим $k$-ЛРП $u \in R^{\langle k \rangle}$ следующим образом: $u(\boldsymbol{i}) = a_1^{i_1} \ldots a_k^{i_k}$, $\boldsymbol{i} \in \mathbb{N}_0^k$. Тогда $u$ — реверсивная несингулярная $k$-ЛРП со свойством 6. Гомотетии $\hat{a}_s : R \to R$, $\hat{a}_s(r) = a_s r$, $s \in \overline{1,k}$, являются мультипликаторами $u$ и $x_s u = \hat{a}_s(u)$, $s \in \overline{1,k}$. Следовательно,*

$$\mathfrak{P}_{red}(u) = \langle (1,0,\ldots,0), (0,1,0,\ldots,0), \ldots, (0,\ldots,0,1) \rangle = \mathbb{Z}^k.$$

*При этом $\mathfrak{P}(u) \neq \mathbb{Z}^k$, если хотя бы один из элементов $a_s$ отличен от $e$.*

**Пример 2.** *Пусть* $M = R = GF(q)$, $F = GF(q^m)$ — *расширение* $R$ *и* $\xi_1, \ldots, \xi_k \in F^*$ — *такая система элементов, что*

$$F = R(\xi_1, \ldots, \xi_k), \quad \langle \xi_1, \ldots, \xi_k \rangle \cap R^* = e.$$

*Зададим* $k$*-ЛРП* $u \in R^{\langle k \rangle}$ *с помощью функции след* $\mathrm{tr}_R^F : F \to R$ *по правилу*

$$u(\boldsymbol{i}) = \mathrm{tr}_R^F(\xi_1^{i_1} \ldots \xi_k^{i_k}) = \mathrm{tr}_R^F(\boldsymbol{\xi}^{\boldsymbol{i}}), \quad \boldsymbol{i} \in \mathbb{N}_0^k.$$

*Тогда* $u$ *удовлетворяет всем условиям Предложения 1. Эндоморфизмы модуля* $M = R$ *суть гомотетии* $\hat{a} : R \to R$, $a \in R$. *Ни один из них, кроме* $\hat{e}$, *не является мультипликатором* $u$, *так как если* $\boldsymbol{x}^{\boldsymbol{\tau}} u = au$, *где* $a \in R^*$, *то* $\mathrm{tr}_R^F(\boldsymbol{\xi}^{\boldsymbol{i}+\boldsymbol{\tau}}) = \mathrm{tr}_R^F(a\boldsymbol{\xi}^{\boldsymbol{i}})$ *для всех* $\boldsymbol{i} \in \mathbb{N}_0^k$, *и потому* $\boldsymbol{\xi}^{\boldsymbol{\tau}} = a \in R^*$, *что возможно лишь если* $a = e$ *и* $\boldsymbol{\tau} \in \mathfrak{P}(u)$. *Следовательно,* $\mathfrak{P}_{red}(u) = \mathfrak{P}(u)$.

Далее, для краткости, будем использовать обозначения $\mathcal{M} = \mathrm{Mult}(u)$, $\breve{\mathcal{M}} = \breve{\mathcal{M}}(u)$. Введем на цикле $\mathcal{T}(u)u$ $k$-ЛРП $u$ отношение *редуцированной эквивалентности* $\underset{red}{\sim}$ условием

$$\forall u_1, u_2 \in \mathcal{T}(u)u \qquad u_1 \underset{red}{\sim} u_2 \quad \Leftrightarrow \quad \exists \breve{\varphi} \in \breve{\mathcal{M}} : u_2 = \breve{\varphi} u_1.$$

Это отношение разбивает цикл $\mathcal{T}(u)u$ на классы мощности $|\mathrm{Mult}(u)|$ вида $\breve{\mathcal{M}}u_1$, $u_1 \in \mathcal{T}(u)u$. Фактормножество $\mathcal{T}(u)u/\underset{red}{\sim}$ назовем *редуцированным циклом* $k$-ЛРП $u$. Имеет место равенство

$$\mathcal{T}(u)u/\underset{red}{\sim} = \mathcal{T}_{red}(u)u. \tag{13}$$

Здесь произведение элемента $\boldsymbol{\theta}^{\boldsymbol{\sigma}}\breve{\mathcal{M}} \in \mathcal{T}_{red}(u) = \mathcal{T}(u)/\breve{\mathcal{M}}$ на последовательность $u$ есть класс

$$(\boldsymbol{\theta}^{\boldsymbol{\sigma}}\breve{\mathcal{M}})u = \breve{\mathcal{M}}(\boldsymbol{\theta}^{\boldsymbol{\sigma}}u) = \{\breve{\varphi}\boldsymbol{\theta}^{\boldsymbol{\sigma}}u : \breve{\varphi} \in \breve{\mathcal{M}}\} \in \mathcal{T}(u)u/\underset{red}{\sim}.$$

Укажем способ перечисления различных элементов редуцированного цикла $\mathcal{T}_{red}(u)u$ и описания с его помощью всего цикла $\mathcal{T}(u)u$ $k$-ЛРП $u$. Это описание — естественное обобщение равенства 4, указанного выше для 1-ЛРП над $R$.

**Лемма 7.** *Существуют параметры* $t_1, \ldots, t_k \in \mathbb{N}$, $s_1, \ldots, s_k \in \mathbb{N}$ *такие, что*

$$s_i | t_i, \quad i \in \overline{1,k}, \tag{14}$$

$$\mathcal{T}(u) = \{\boldsymbol{\theta}^{\boldsymbol{\tau}} : \boldsymbol{\tau} \in \Pi(t_1, \ldots, t_k)\}, \tag{15}$$

$$\mathcal{T}_{red}(u) = \{\boldsymbol{\theta}^{\boldsymbol{\sigma}}\breve{\mathcal{M}} : \boldsymbol{\sigma} \in \Pi(s_1, \ldots, s_k)\}. \tag{16}$$

□ Воспользуемся равенством $\mathcal{T}(u) = \langle \theta_1, \ldots, \theta_k \rangle$ и выберем $t_1, \ldots, t_k$ из соотношений

$$t_1 = |\langle \theta_1 \rangle|, \quad t_i = |\langle \theta_1, \ldots, \theta_i \rangle : \langle \theta_1, \ldots, \theta_{i-1} \rangle|, \quad i \in \overline{2,k}. \tag{17}$$

Тогда, очевидно, элементы $\boldsymbol{\theta}^{\boldsymbol{\tau}} : \boldsymbol{\tau} \in \Pi(\boldsymbol{t})$ попарно различны, и 15 следует из равенства $|\mathcal{T}(u)| = t_1 \ldots t_k$.

Заметим, что $\mathcal{T}_{red}(u) = \langle \theta_1\breve{\mathcal{M}}, \ldots, \theta_k\breve{\mathcal{M}} \rangle$, и выберем $s_1, \ldots, s_k$ из соотношений

$$s_1 = |\langle \theta_1\breve{\mathcal{M}} \rangle|, \quad s_i = |\langle \theta_1\breve{\mathcal{M}}, \ldots, \theta_i\breve{\mathcal{M}} \rangle : \langle \theta_1\breve{\mathcal{M}}, \ldots, \theta_{i-1}\breve{\mathcal{M}} \rangle|, \quad i \in \overline{2,k}. \tag{18}$$

Тогда, очевидно, верно 16. Условия 14 вытекают из того, что по определению $t_i$ есть порядок элемента $\theta_i$ по модулю подгруппы $\langle \theta_1, \ldots, \theta_{i-1} \rangle$, а $s_i$ — порядок того же элемента по модулю большей подгруппы $\langle \theta_1, \ldots, \theta_{i-1} \rangle\breve{\mathcal{M}}$. □

Зафиксируем параметры леммы 7 и перенумеруем (пока произвольно) элементы введенных параллелепипедов

$$\Pi = \Pi(t_1, \ldots, t_k) = \{\boldsymbol{i}_1, \ldots, \boldsymbol{i}_T\}, \quad \Pi_{red} = \Pi(s_1, \ldots, s_k) = \{\boldsymbol{j}_1, \ldots, \boldsymbol{j}_{T_{red}}\}. \tag{19}$$

Тогда цикл $\mathcal{T}(u)u$ $k$-ЛРП $u$ можно наглядно представить диаграммой значений $u$ на $\Pi$

$$u[\Pi] = (u(\boldsymbol{i}_1), \ldots, u(\boldsymbol{i}_T)). \tag{20}$$

Редуцированный цикл $\mathcal{T}_{red}(u)u$ можно представить диаграммой

$$u[\Pi_{red}] = (u(\boldsymbol{j}_1), \ldots, u(\boldsymbol{j}_{T_{red}})). \tag{21}$$

Мы будем называть эти диаграммы, соответственно, *диаграммой цикла* и *диаграммой редуцированного цикла* $k$-ЛРП $u$. Пусть $|\mathcal{M}| = d$ и $\mathcal{M} = \{\varphi_0 = \varepsilon, \varphi_1, \ldots, \varphi_{d-1}\}$. Тогда, очевидно, нумерации 19 элементов параллелепипедов $\Pi$ и $\Pi_{red}$ можно подобрать так, что диаграммы 20 и 21 связаны соотношениями

$$u[\Pi] = \big(u[\Pi_{red}], \varphi_1(u[\Pi_{red}]), \ldots, \varphi_{d-1}(u[\Pi_{red}])\big).$$

Последнее равенство можно записать также в виде

$$u[\Pi] = (\varphi_0, \varphi_1, \ldots, \varphi_{d-1}) \otimes u[\Pi_{red}], \tag{22}$$

где справа стоит тензорное произведение строк, определяемой очевидным образом.

Подбирая специальным образом систему образующих группы $\breve{\mathcal{M}}$, представление 22 диаграммы цикла $k$-ЛРП $u$ можно заменить еще более "структурированным" представлением.

Пусть параметры $s_i$ и $t_i$ удовлетворяют соотношениям 17, 18, и $d_i = t_i/s_i$, $i \in \overline{1,k}$. Введем обозначения $\mathcal{T}_0 = \langle e \rangle$, $\mathcal{T}_i = \langle \theta_1, \ldots, \theta_i \rangle$, $i \in \overline{1,k}$. Тогда

$$\theta_i^{s_i} \in \mathcal{T}_{i-1}\breve{\mathcal{M}}, \quad i \in \overline{1,k},$$

и существуют $\breve{\varphi}_i \in \breve{\mathcal{M}}$ такие, что

$$\theta_i^{s_i} \in \mathcal{T}_{i-1}\breve{\varphi}_i, \quad i \in \overline{1,k}. \tag{23}$$

**Предложение 4.** *Для* $i \in \overline{1,k}$ *справедливы равенства*

$$\mathcal{T}_i \cap \breve{\mathcal{M}} = \langle \breve{\varphi}_1, \ldots, \breve{\varphi}_i \rangle, \quad \breve{\mathcal{M}} = \langle \breve{\varphi}_1, \ldots, \breve{\varphi}_k \rangle, \tag{24}$$

$$\operatorname{ord} \breve{\varphi}_i \mod \langle \breve{\varphi}_1, \ldots, \breve{\varphi}_{i-1} \rangle = d_i,$$

$$\breve{\mathcal{M}} = \{\breve{\varphi}_1^{\delta_1}, \ldots, \breve{\varphi}_k^{\delta_k} : (\delta_1, \ldots, \delta_k) \in \Pi(d_1, \ldots, d_k)\}. \tag{25}$$

Нетрудно видеть, что при подходящей нумерации диаграмм $\Pi$ и $\Pi_{red}$ справедливо равенство

$$u[\Pi] = \big(\varphi_1^{\delta_1}, \ldots, \varphi_k^{\delta_k} u[\Pi_{red}]; (\delta_1, \ldots, \delta_k) \in \Pi(d_1, \ldots, d_k)\big).$$

Например, при $k = 2$ диаграммы $u[\Pi]$ и $u[\Pi_{red}]$ можно представить таблицами

$$u[\Pi] = \boxed{\begin{array}{ccc} u(0,0) & \ldots & u(t_1-1,0) \\ u(0,1) & \ldots & u(t_1-1,1) \\ \ldots & & \ldots \\ u(0,t_2-1) & \ldots & u(t_1-1,t_2-0) \end{array}}$$

$$u[\Pi_{red}] = \boxed{\begin{array}{ccc} u(0,0) & \ldots & u(s_1-1,0) \\ u(0,1) & \ldots & u(s_1-1,1) \\ \ldots & & \ldots \\ u(0,s_2-1) & \ldots & u(s_1-1,s_2-0) \end{array}}$$

При этом справедливо равенство

$$u[\Pi] = \boxed{\begin{array}{cccc} u[\Pi_{red}] & \varphi_1(u[\Pi_{red}]) & \ldots & \varphi_1^{d_1-1}(u[\Pi_{red}]) \\ \varphi_2(u[\Pi_{red}]) & \varphi_1\varphi_2(u[\Pi_{red}]) & \ldots & \varphi_1^{d_1-1}\varphi_2(u[\Pi_{red}]) \\ \ldots & \ldots & & \ldots \\ \varphi_2^{d_2-1}(u[\Pi_{red}]) & \varphi_1\varphi_2^{d_2-1}(u[\Pi_{red}]) & \ldots & \varphi_1^{d_1-1}\varphi_2^{d_2-1}(u[\Pi_{red}]) \end{array}}$$

Последнее можно естественным образом представить в виде тензорного произведения таблиц

$$u[\Pi] = \begin{bmatrix} \varphi_1^0\varphi_2^0 & \varphi_1\varphi_2^0 & \ldots & \varphi_1^{d_1-1}\varphi_2^0 \\ \varphi_1^0\varphi_2 & \varphi_1\varphi_2 & \ldots & \varphi_1^{d_1-1}\varphi_2 \\ \ldots & \ldots & & \ldots \\ \varphi_1^0\varphi_2^{d_2-1} & \varphi_1\varphi_2^{d_2-1} & \ldots & \varphi_1^{d_1-1}\varphi_2^{d_2-1} \end{bmatrix} \otimes u[\Pi_{red}].$$

В общем случае, когда $k \geqslant 2$, это произведение заменяется тензорным произведением $k$-мерных матриц:

$$u[\Pi] = \left[\varphi_1^{\delta_1}, \ldots, \varphi_k^{\delta_k} : \boldsymbol{\delta} \in \Pi(\boldsymbol{d})\right] \otimes u[\Pi_{red}].$$

Здесь элемент $u(\boldsymbol{\tau})$ матрицы $u[\Pi]$, $\boldsymbol{\tau} = (\tau_1, \ldots, \tau_k) \in \Pi(\boldsymbol{t})$, вычисляется следующим образом. Пусть $\tau_i = \delta_i s_i + r_i$, где $r_i \in \overline{0, s_i - 1}$, $\delta_i \in \overline{0, d_i - 1}$. Тогда $u(\boldsymbol{\tau}) = \varphi_1^{\delta_1}, \ldots, \varphi_k^{\delta_k}(u(r_1, \ldots, r_k))$.

Заметим, что если ${}_RM = {}_RQ$ — квазифробениусов $R$-модуль (в частности, если $M = R$ — QF-кольцо [38], например, кольцо главных идеалов), то $E(R) = \hat{R}$ — множество гомотетий $\hat{r} : Q \to Q$, $\hat{r}(\alpha) = r\alpha$, $r \in R$ (см. [38]). В этом случае для подходящих $a_1, \ldots, a_k \in R^*$ справедливы равенства

$$\breve{\mathcal{M}}(u) = \{a_1^{\delta_1}, \ldots, a_k^{\delta_k} : (\delta_1, \ldots, \delta_k) \in \Pi(d_1, \ldots, d_k)\} = \langle a_1, \ldots, a_k \rangle,$$

и мы имеем определение группы мультипликаторов в "обычном" смысле. В общем случае группу $\mathcal{T}(u) \cap R^*$ естественно назвать *группой $R$-мультипликаторов* и обозначить $\breve{\mathcal{M}}_R(u)$.

Реверсивную $k$-ЛРП $u$ над кольцом Галуа $R = GR(q^n, p^n)$ назовем *$k$-максимальной ЛРП*, если ее кольцо операторов $S = R[x]/\operatorname{An}(u)$ есть кольцо Галуа, $\bar{u} \neq 0$ и $T(u) = |S^*|$. Если при этом $S = GR(q^{mn}, p^n)$, то будем говорить, что $u$ есть $k$-max-ЛРП ранга $m$. Условие $T(u) = |S^*|$ равносильно условию $S = GR(q^{mn}, p^n)$, $S^* = \langle \theta_1, \ldots, \theta_k \rangle$, где $\theta_s = x_s + \operatorname{An}(u)$. Пусть мультипликативная группа $S^*$ кольца $S$ порождается $k_0$ элементами. Следующая теорема показывает, что при условии $k \geqslant k_0$ указанные рекурренты существуют.

**Теорема 1.** *Пусть $S = GR(q^{mn}, p^n)$ и элементы $a_1, \ldots, a_k \in S$ таковы, что $S^* = \langle a_1, \ldots, a_k \rangle$. Тогда $k$-последовательность $u \in R^{\langle k \rangle}$ вида*

$$u(\boldsymbol{i}) = \operatorname{Tr}_R^S(c\boldsymbol{a}^{\boldsymbol{i}}) = \operatorname{Tr}_R^S(ca_1^{i_1} \ldots a_k^{i_k})$$

*для любой константы $c \in S^*$ есть $k$-max-ЛРП ранга $m$ над $R$, имеющая период*

$$T(u) = (q^m - 1)q^{m(n-1)}.$$

**Пример 3.** *Пусть $u$ есть $k$-max-ЛРП ранга $m$ над кольцом $R = GR(q^n, p^n)$ из предыдущей теоремы. Тогда $u$ удовлетворяет всем ограничениям, сформулированным в начале данного параграфа, при этом $M = R$ и $E(M) = \hat{R}$ — кольцо гомотетий. Поэтому $\breve{\mathcal{M}}(u) = \breve{\mathcal{M}}_R(u)$. Более того, каждый элемент $a \in R^*$ является мультипликатором $u$, так как если $t_i = |\langle \xi_1, \ldots, \xi_i \rangle : \langle \xi_1, \ldots, \xi_{i-1} \rangle|$, $i \in \overline{1, k}$, то $a = \boldsymbol{\xi}^{\boldsymbol{\tau}}$ для подходящего $\boldsymbol{\tau} = (\tau_1, \ldots, \tau_k) \in \Pi(t_1, \ldots, t_k) = \Pi(\boldsymbol{t}) = \Pi$, и потому $au = \boldsymbol{x}^{\boldsymbol{\tau}}u$. Определим параметры*

$$s_i = \operatorname{ord} \xi_i \mod \langle \xi_1, \ldots, \xi_{i-1}, R^* \rangle$$

*Тогда $\xi_i^{s_i} \in \langle \xi_1, \ldots, \xi_{i-1} \rangle a_i$ для подходящего $a_i \in R^*$, и справедливы соотношения*

$$R^* = \langle a_1, \ldots, a_k \rangle, \quad \operatorname{ord} a_i \mod \langle a_1, \ldots, a_{i-1} \rangle = d_i, \quad i \in \overline{1, k}.$$

*Система элементов $\boldsymbol{\xi}^{\boldsymbol{\sigma}}$, $\boldsymbol{\sigma} \in \Pi(s_1, \ldots, s_k) = \Pi(\boldsymbol{s}) = \Pi_{red}$, есть полная система различных представителей смежных классов $S^*$ по $R^*$, и справедливы соотношения*

$$T(u) = |S^*| = (q^m - 1)q^{m(n-1)}, \quad |\operatorname{Mult}(u)| = |R^*| = (q-1)q^{n-1},$$

$$T_{red}(u) = \frac{q^m - 1}{q - 1} q^{(m-1)(n-1)}, \quad u[\Pi] = [\boldsymbol{a}^{\boldsymbol{\sigma}} : \boldsymbol{\sigma} \in \Pi(\boldsymbol{d})] \otimes u[\Pi_{red}].$$

# 3 Распределение элементов в линейных рекуррентах

Пусть $F(x)$ — многочлен Галуа степени $m$ над кольцом $R = GR(q^n, p^n)$. Период $T(F)$ такого многочлена $F(x)$ равен $(q^m - 1)p^\nu/d$, где $d$ — некоторый делитель числа $q^m - 1$, а $\nu \in \overline{0, n-1}$. Через $\alpha$ обозначим корень многочлена $F(x)$ в расширении $S = GR(q^{mn}, p^n)$ кольца $R$. Пусть $u$ — ЛРП над кольцом $R$ с характеристическим многочленом $F(x)$, а $T(u)$ — ее период. Пусть $r$ — натуральное

число, $s_1, s_2, \ldots, s_r \in \mathbb{N}_0^k$, $z_1, z_2, \ldots, z_r \in R$, $\boldsymbol{s} = (s_1, s_2, \ldots, s_r)$, $\boldsymbol{z} = (z_1, z_2, \ldots, z_r)$. Обозначим через $N_{\boldsymbol{z}}^{\boldsymbol{s}}(u)$ количество целых чисел $i \in \overline{0, T(u)-1}$ таких, что $u(i+s_j) = z_j$, $j \in \overline{1,r}$. Будем изучать отклонение частот $N_{\boldsymbol{z}}^{\boldsymbol{s}}(u)$ от величины $\omega_{\boldsymbol{z}}(u)$, которая определена следующими равенствами:

$$\omega_{\boldsymbol{z}}(u) = \begin{cases} \dfrac{q^{m-nr}-1}{q^m-1}T(u), & \text{если } \boldsymbol{z} = \boldsymbol{0}, \\ \dfrac{q^{m-nr}}{q^m-1}T(u), & \text{если } \boldsymbol{z} \neq \boldsymbol{0}. \end{cases}$$

При фиксированных значениях $q$, $n$, $r$ и достаточно больших значениях $T(u)$ величины $\omega_{\boldsymbol{z}}(u)/T(u)$ и $1/q^{nr}$, — естественное среднее количество появлений $r$-граммы, можно считать равными.

**Теорема 2.** *Пусть среди элементов $u(0), u(1), \ldots, u(m-1)$ есть хотя бы один обратимый элемент кольца $R$ и система элементов $\bar{\alpha}^{s_1}, \bar{\alpha}^{s_2}, \ldots, \bar{\alpha}^{s_r}$ линейно независима над полем $\bar{R}$. Тогда справедливо неравенство:*

$$|N_{\boldsymbol{z}}^{\boldsymbol{s}}(u) - \omega_{\boldsymbol{z}}(u)| < p^{\nu+n-1}q^{m/2}. \tag{26}$$

Неравенство 26 для случая $r = 1$ доказано А. С. Кузьминым, в общем случае — О. В. Камловским. С использованием аппарата тригонометрических сумм доказывается следующая нижняя оценка для модуля отклонения частот появления $r$-грамм на циклах ЛРП максимального периода от "идеального" значения.

**Теорема 3.** *Пусть $T(F) = (q^m-1)p^{n-1}$ и система элементов $\bar{\alpha}^{s_1}, \bar{\alpha}^{s_2}, \ldots, \bar{\alpha}^{s_r}$ линейно независима над полем $\bar{R}$. Тогда найдутся ЛРП максимального периода $u \in L_R(F)$ и $r$-грамма $\boldsymbol{z} \in R^r$ такие, что*

$$\left| N_{\boldsymbol{z}}^{\boldsymbol{s}}(u) - \frac{T(u)}{q^{nr}} \right| > C_{n,r}(q) q^{\frac{m}{2}}, \tag{27}$$

*где*

$$C_{n,r}(q) = \begin{cases} \left(\dfrac{(p-1)^2(n-1)}{p^3}\right)^{\frac{1}{2}}, & \text{если} \quad q^r = p, n > 1, \\ \left(\dfrac{(q^r-1)(p-1)p^{n-2}}{q^{(n+1)r}}\right)^{\frac{1}{2}}, & \text{если} \quad q^r > p, n > 1. \end{cases}$$

Неравенство 27 показывает, что в оценке 26 множитель $q^{m/2}$ не может быть заменен на показательную функцию (от переменной $m$) с меньшим основанием степени.

В случае, когда $R = GF(q)$ — конечное поле из $q$ элементов, оценку 26 можно уточнить с использованием тригонометрических сумм Гаусса.

**Теорема 4.** *Пусть в условиях теоремы 2 $R = GF(q)$. Тогда*

$$|N_{\boldsymbol{0}}^{\boldsymbol{s}}(u) - \omega_{\boldsymbol{0}}(u)| \leqslant \frac{q^r-1}{q^r}\left(\frac{T}{h} - \frac{1}{d}\right) q^{\frac{m}{2}},$$

*а при $\boldsymbol{z} \neq \boldsymbol{0}$*

$$|N_{\boldsymbol{z}}^{\boldsymbol{s}}(u) - \omega_{\boldsymbol{z}}(u)| \leqslant \left(\frac{2q^{r-1}-1}{q^{r-1}}\left(\frac{T}{h} - \frac{1}{d}\right) + \frac{h-T}{h}q^{\frac{1}{2}}\right) q^{\frac{m}{2}-1},$$

*где $T = T(u)$, $h = \text{НОК}[T, q-1]$, $d = (q^m-1)/T$.*

Если $u$ — ЛРП максимального периода ранга $m > 1$ над кольцом $R = \mathbb{Z}_{p^n}$, то число $\nu_{u,l}(a)$ появления элемента $a \in R$ на отрезке длины $l < T$ ЛРП $u$ удовлетворяет оценке

$$\left| \nu_{u,l}(a) - \frac{l}{p^n} \right| \leqslant p^{3n/4} T^{3/4} \ln T.$$

В работе [1] ранее было показано, что это неравенство справедливо почти для всех ЛРП максимального периода над $R$. Получены также нижние оценки отклонения величины $\nu_{u,l}(a)$.

Рассмотрим частоты появления нулей на отрезках ЛРП над конечными полями. Пусть $l$ — натуральное число, $N_{l,\boldsymbol{0}}^{\boldsymbol{s}}(u)$ — количество появлений $r$-граммы из одних нулей среди $r$-грамм $(u(i+s_1), u(i+s_2), \ldots, u(i+s_r))$, где $i \in \overline{0, l-1}$. С применением аппарата тригонометрических сумм доказывается

**Теорема 5.** *Пусть в условиях теоремы 2* $R = GF(q)$ *и* $l \leqslant T(u)/2(T(u), q-1)$. *Тогда*

$$\left| N_l^s(u) - \frac{l}{q^r} \right| \leqslant \frac{q^r - 1}{q^r(q-1)} \left( \frac{3q}{2} \left( q^m l - (q-1)l^2 \right) \right)^{\frac{1}{3}}. \tag{28}$$

Приведенные выше результаты этого параграфа получены О. В. Камловским. Указанные в них оценки улучшают и обобщают ряд ранее известных результатов о распределении элементов на отрезках ЛРП над конечными полями и примарными кольцами вычетов. Оценки теоремы 4 улучшают соответствующие оценки, полученные в работах [49, 77]. Неравенство 28 качественно улучшает оценку из [46]. При некоторых естественных ограничениях на длину $l$ отрезка ЛРП оценка 28 уточняет соответствующие результаты, полученные в работах [13, 14, 49, 77].

Рассмотрим теперь вопрос о получении точных значений количества встречаемости знаков на циклах линейных рекуррент над кольцами Галуа. Известно, что у ЛРП порядка $m$ над конечным полем $GF(q)$, имеющей максимально возможный период $q^m - 1$, элементы поля появляются на цикле с почти одинаковой частотой: каждый ненулевой элемент появляется $q^{m-1}$ раз, а нулевой элемент появляется $q^{m-1} - 1$ раз. Ниже рассматривается распределение элементов на циклах ЛРП над кольцами Галуа и QF-модулями характеристики 4.

Пусть $R = GR(q^2, 4)$, $q = 2^l$. Если $u$ — ЛРП над кольцом $R$ с характеристическим многочленом степени $m$ такая, что $\bar{u}$ — ЛРП максимального периода над полем $\bar{R}$, то последовательность $u$ имеет период $q^m - 1$ или $2(q^m - 1)$. В первом случае ЛРП $u$ называется *отмеченной*, во втором — ЛРП *максимального периода*. Обозначим через $N_u(c)$ число появлений элемента $c \in R$ на цикле ЛРП $u$. Пусть $\lambda = [m/2]$ — целая часть числа $m/2$ и $\delta(c = 0)$ — характеристическая функция события $c = 0$, т. е. 1, если $c = 0$, или 0, если $c \neq 0$.

**Теорема 6.** *Пусть* $u$ *— отмеченная ЛРП порядка* $m$ *над кольцом Галуа* $R = GR(q^2, 4)$. *Тогда*

$$N_u(c) = q^{m-2} \pm wq^{\lambda-1} - \delta(c = 0),$$

*где* $w \in \{1,\ q-1\}$, *если* $m = 2\lambda + 1$, *и* $w \in \{0,\ 1,\ q-1\}$, *если* $m = 2\lambda$. *Число различных типов распределения знаков на цикле ЛРП и не превосходит* $2q + 1$.

**Следствие 1.** *Справедлива оценка* $\left| N_u(c) - q^{m-2} \right| \leqslant \frac{q-1}{q} q^\lambda + 1$.

**Теорема 7.** *Пусть* $u$ *— ЛРП максимального периода порядка* $m$ *над кольцом Галуа* $R = GR(q^2, 4)$. *Тогда*

$$N_u(c) = 2q^{m-2} \pm wq^{\lambda-1} - 2\delta(c = 0),$$

*где* $w \in \{0,\ 2,\ q-2,\ q,\ 2(q-1)\}$, *если* $m = 2\lambda + 1$, *и* $w \in \{0,\ 1,\ 2,\ q-1,\ 2(q-1)\}$, *если* $m = 2\lambda$. *Число различных типов распределения знаков на цикле ЛРП и не превосходит* $2q + 1$.

**Следствие 2.** *Справедлива оценка* $\left| N_u(c) - 2q^{m-2} \right| \leqslant 2\frac{q-1}{q} q^\lambda + 2$.

**Теорема 8.** *Существуют многочлены* $F(x) \in R[x]$ *такие, что среди множества ЛРП максимального периода с характеристическим многочленом* $F(x)$ *половина последовательностей и имеет вполне равномерное распределение элементов на цикле:*

$$N_u(c) = 2q^{m-2}, \quad \text{если } c \neq 0, \qquad N_u(0) = 2q^{m-2} - 2.$$

В качестве следующего шага рассмотрим частотные характеристики циклов ЛРП над модулями. В [38] показано, что наиболее содержательная алгебраическая теория может быть построена для линейных рекуррент над QF-модулями. Этим объясняется выбор модуля, над которым берутся рекурренты. Поля и кольца Галуа являются квазифробениусовыми кольцами, т. е. QF-модулями над собой. Наименьшее не квазифробениусово кольцо состоит из 8 элементов и имеет вид $\mathbb{Z}_4[x]/(x^2, 2x)$. Мы рассмотрим не квазифробениусово кольцо более общего вида $A = R[x]/(x^2, 2x)$, где $R = GR(q^2, 4)$, $q = 2^l$, — кольцо Галуа характеристики 4. Кольцо $A$ состоит из $q^3$ элементов и является расширением $R[\pi]$ кольца Галуа $R$ элементом $\pi$ таким, что $\pi^2 = 2\pi = 0$. Как и над всяким конечным коммутативным кольцом, над кольцом $A$ существует единственный с точностью до изоморфизма квазифробениусов модуль Q. Этот модуль состоит из $q^3$ элементов и порождается элементами $\sigma$ и $\tau$ такими, что $4\sigma = 2\tau = \pi\sigma = 0$, $\pi\tau = 2\sigma$. Элементы $\sigma$ и $\tau$ можно интерпретировать как последовательности

$\sigma = (1,0,0,\ldots)$, $\tau = (0,2,0,0,\ldots)$ над $R$, а их умножение на элемент $\pi$ как сдвиг последовательности влево. Собственные подмодули $A$-модуля $Q$ состоят из $q^2$ или $q$ элементов.

Последовательность $u\colon \mathbb{N}_0 \to Q$ назовем *сюръективной*, если $u(\mathbb{N}_0) = Q$. Семейство $L_Q(F)$ состоит из $q^{3m}$ последовательностей, $m = \deg F$. Если ЛРП $u$ порядка $m$ имеет период $q^m - 1$ или $2(q^m - 1)$, то она называется соответственно *отмеченной* или ЛРП *максимального периода* над модулем $Q$. Обозначим через $N_u(c)$ число появлений элемента $c \in Q$ на цикле ЛРП $u$.

**Теорема 9.** *Пусть $u$ — отмеченная ЛРП порядка $m$ над QF-модулем $Q$. Если $u$ сюръективна, то*

$$N_u(c) = q^{m-3} \pm w_1 q^{\lambda-1} - \delta(c=0), \quad \text{где } w_1 \in \{0,\ 1,\ q-1\},$$

*и при $m = 2\lambda$, кроме этого, имеются последовательности, для которых*

$$N_u(c) = q^{m-3} \pm w_2 q^{\lambda-2} - \delta(c=0), \quad \text{где } w_2 \in \{1,\ q-1\}.$$

*Если $u$ не сюръективна, то множество ее значений $U = u(\mathbb{N}_0)$ образует подмодуль модуля $Q$. Если $|U| = q^2$, то для $c \in U$*

$$N_u(c) = q^{m-2} \pm w_3 q^{\lambda-1} - \delta(c=0), \quad \text{где } w_3 \in \{0,\ 1,\ q-1\}.$$

*Если же $|U| = q$, то для $c \in U$*

$$N_u(c) = q^{m-1} - \delta(c=0).$$

*Число различных типов распределения знаков на цикле ЛРП $u$ не превосходит $2q^3 + 3q + 2$.*

**Теорема 10.** *Пусть $u$ — ЛРП максимального периода порядка $m$ над QF-модулем $Q$. Если $u$ сюръективна, то*

$$N_u(c) = 2q^{m-3} \pm w_1 q^{\lambda-1} - 2\delta(c=0),$$

*где $w_1 \in \{0,\ 1,\ 2,\ q-2,\ q-1,\ q,\ 2(q-1)\}$, и при $m = 2\lambda$, кроме этого, имеются последовательности, для которых*

$$N_u(c) = 2q^{m-3} \pm w_2 q^{\lambda-2} - 2\delta(c=0), \quad \text{где } w_2 \in \{2,\ q-2,\ 2(q-1)\}.$$

*Если $u$ не сюръективна, то множество ее значений $U = u(\mathbb{N}_0)$ образует подмодуль модуля $Q$. Если $|U| = q^2$, $c \in U$, то*

$$\begin{aligned} &N_u(c) = q^{m-1} + q^{m-2} - 2\delta(c=0) \text{ или} \\ &q^{m-2} - 2\delta(c=0) \text{ или} \\ &2q^{m-2} \pm w_3 q^{\lambda-1} - 2\delta(c=0), \end{aligned}$$

*где $w_3 \in \{0,\ 1,\ 2,\ q-2,\ q-1,\ q,\ 2(q-1)\}$. Если же $|U| = q$, то для $c \in U$*

$$N_u(c) = q^{m-1} - 2\delta(c=0) \quad \text{или} \quad 2q^{m-1} - 2\delta(c=0).$$

*Число различных типов распределения знаков на цикле ЛРП $u$ не превосходит $4q^5 + 4q^3$.*

**Теорема 11.** *Для любого $m \geqslant 2$ существуют ЛРП максимального периода ранга $m$ над модулем $Q$, имеющие вполне равномерное распределение элементов на цикле:*

$$N_u(c) = 2q^{m-3}, \quad \text{если } c \neq 0, \qquad N_u(0) = 2q^{m-3} - 2.$$

Заметим, что отмеченных линейных рекуррент над кольцом Галуа $R$ или над QF-модулем $Q$ с вполне равномерным распределением элементов на цикле не существует.

Доказательства изложенных результатов (см. [23, 40]) основываются на представлении знаков линейных рекуррент над кольцом Галуа $R$ и над модулем $Q$ функцией след и на теории квадратичных форм над полем характеристики 2.

# 4 Линейная сложность

*Ранг*, т. е. степень минимального многочлена, псевдослучайной периодической последовательности над полем является одной из ее основных характеристик. Для 1-ЛРП над конечным кольцом, и тем более для $k$-ЛРП над модулем, имеется уже целый набор числовых параметров, характеризующих линейные зависимости между знаками $k$-ЛРП, возможность ее выработки $k$-линейным регистром сдвига, длину начального вектора и другие свойства последовательности. Будем говорить, что каждый из этих параметров характеризует *линейную сложность* $k$-ЛРП.

В отечественной литературе степень минимального многочлена 1-ЛРП принято называть ее рангом. В зарубежной литературе для этой цели применяется термин "линейная сложность" (linear complexity). Мы используем термин линейная сложность в более широком смысле, как набор числовых параметров (потенциально неограниченный), характеризующий свойства последовательности, сохраняя за термином ранг его прежний, принятый в отечественной литературе, смысл.

Пусть $u$ — $k$-ЛРП над модулем ${}_R M$, $R[\boldsymbol{x}]u$ — ее модуль сдвигов, рассматриваемый как $R$-модуль, $\Omega$ и $\mathcal{F}$ — конечное подмножество и диаграмма Ферре в $\mathbb{N}_0^k$, ${}_R(S)$ — левый $R$-модуль, порожденный множеством $S$. Обозначим

$$
\begin{aligned}
r_1 &= \min\{t \geqslant 0 :\ R[\boldsymbol{x}]u \text{ порождается } t \text{ элементами}\},\\
r_2 &= \min\{|\Omega| :\ R[\boldsymbol{x}]u = {}_R(\boldsymbol{x}^{\boldsymbol{i}}u,\ \boldsymbol{i} \in \Omega)\},\\
r_3 &= \min\{|\mathcal{F}| :\ R[\boldsymbol{x}]u = {}_R(\boldsymbol{x}^{\boldsymbol{i}}u,\ \boldsymbol{i} \in \mathcal{F})\},\\
r_4 &= \max\{t \geqslant 0 :\ R[\boldsymbol{x}]u \text{ содержит } t \text{ лин. независ. элементов}\},\\
r_5 &= \max\{|\Omega| :\ \boldsymbol{x}^{\boldsymbol{i}}u,\ \boldsymbol{i} \in \Omega, \text{ линейно независимы над } R\},\\
r_6 &= \max\{|\mathcal{F}| :\ \boldsymbol{x}^{\boldsymbol{i}}u,\ \boldsymbol{i} \in \mathcal{F}, \text{ линейно независимы над } R\},\\
r_7 &= \min\{t \geqslant 0 :\ \exists \text{ мономорфизм } R\text{-модулей } R[\boldsymbol{x}]u \to M^t\},\\
r_8 &= \min\{|\Omega| :\ R[\boldsymbol{x}]u \to M^{\Omega},\ v \to v[\Omega],\ \text{— мономорфизм}\},\\
r_9 &= \min\{|\mathcal{F}| :\ R[\boldsymbol{x}]u \to M^{\mathcal{F}},\ v \to v[\mathcal{F}],\ \text{— мономорфизм}\}.
\end{aligned}
$$

Для краткости мы пишем $r_i$ вместо $r_i(u)$. В определениях $r_4$–$r_6$ имеется в виду линейная независимость над кольцом $R$, отображения в определениях $r_7$–$r_9$ являются мономорфизмами $R$-модулей. Очевидно,

$$r_1 \leqslant r_2 \leqslant r_3, \qquad r_4 \geqslant r_5 \geqslant r_6, \qquad r_7 \leqslant r_8 \leqslant r_9.$$

Запись $r_i \leqslant r_j$ означает, что $r_i(u) \leqslant r_j(u)$ для всех $u$ из рассматриваемого класса $k$-ЛРП (в данном случае — для всех $k$-ЛРП над любым модулем ${}_R M$). Для произвольного $R$-модуля $N$ обозначим

$$
\begin{aligned}
r_1(N) &= \min\{t \geqslant 0 :\ N \text{ порождается } t \text{ элементами}\},\\
r_4(N) &= \max\{t \geqslant 0 :\ N \text{ содержит } t \text{ лин. независ. элементов}\}.
\end{aligned}
$$

Величины $r_1(N)$ и $r_4(N)$ называют *рангом модуля* $N$. Тогда $r_1(u) = r_1(R[\boldsymbol{x}]u)$ и $r_4(u) = r_4(R[\boldsymbol{x}]u)$, поэтому параметры $r_1$–$r_6$ характеризуют, с алгебраической и комбинаторной точек зрения, ранг модуля сдвигов $k$-ЛРП $u$. Параметр $r_8$ равен наименьшему числу $|\Omega|$ знаков, однозначно определяющих произвольную $k$-ЛРП $v \in R[\boldsymbol{x}]u$, параметр $r_9$ — наименьшему числу $|\mathcal{F}|$ "подряд идущих", (т. е. индексы которых образуют диаграмму Ферре) знаков, а параметр $r_7$ — наименьшему числу $t$ "обобщенных знаков", однозначно определяющих $k$-ЛРП $v \in R[\boldsymbol{x}]u$.

Множество $\Phi = \{H_{\boldsymbol{r}}(\boldsymbol{x}),\ \boldsymbol{r} \in \Delta\mathcal{F}\}$ многочленов из $R[\boldsymbol{x}]$ вида

$$H_{\boldsymbol{r}}(\boldsymbol{x}) = \boldsymbol{x}^{\boldsymbol{r}} - \sum_{\boldsymbol{i} \in \mathcal{F}} h_{\boldsymbol{r}\boldsymbol{i}} \boldsymbol{x}^{\boldsymbol{i}}$$

назовем *полной системой $\mathcal{F}$-унитарных многочленов*. Обозначим

$$r_{10} = \min\{|\mathcal{F}| :\ \exists \text{ полная система } \mathcal{F}\text{-унит. многочленов } \Phi \subset \mathrm{An}(u)\}.$$

Параметр $r_{10}(u)$ является непосредственным обобщением понятия ранга (степени минимального многочлена) 1-ЛРП на случай $k$-ЛРП: если $k = 1$, то $r_{10}(u) = \operatorname{rank} u$.

Пара $\langle \chi, \mathcal{F} \rangle$, где $\chi \subseteq R[\boldsymbol{x}]$, называется *$k$-линейным регистром сдвига* ($k$-ЛРС) на диаграмме Ферре $\mathcal{F}$, если отображение

$$\sigma\colon L_M(\chi) \to M^{\mathcal{F}}, \qquad v \to v[\mathcal{F}],$$

биективно. Это означает, что существует взаимно однозначное соответствие между последовательностями $v \in L_M(\chi)$ и их начальными векторами $v[\mathcal{F}]$. Если $u \in L_M(\chi)$, то говорят, что $u$ является выходной последовательностью или выходом $k$-ЛРС $\langle \chi, \mathcal{F} \rangle$. Обозначим

$$r_{11} = \min\{|\mathcal{F}| : \exists\ k\text{-ЛРС } \langle \chi, \mathcal{F} \rangle \text{ с выходом } u\}.$$

Пусть $E = \mathrm{End}(M^{\mathcal{F}})$ — кольцо эндоморфизмов $R$-модуля $M^{\mathcal{F}} = M^{|\mathcal{F}|}$. Действие эндоморфизма $\varphi\colon M^{\mathcal{F}} \to M^{\mathcal{F}}$ на элемент $\delta[\mathcal{F}] \in M^{\mathcal{F}}$ можно записать следующим образом:

$$\varphi(\delta[\mathcal{F}]) = \Big(\varphi_{\boldsymbol{i}}(\delta[\mathcal{F}]),\ \boldsymbol{i} \in \mathcal{F}\Big) \in M^{\mathcal{F}},$$

где $\varphi_{\boldsymbol{i}}\colon M^{\mathcal{F}} \to M$, $\boldsymbol{i} \in \mathcal{F}$, — компоненты эндоморфизма $\varphi$. Эндоморфизм $\varphi$ будем называть *скалярным*, если все его компоненты — скалярные гомоморфизмы, т. е.

$$\varphi_{\boldsymbol{i}}(\delta[\mathcal{F}]) = \sum_{\boldsymbol{j} \in \mathcal{F}} c_{\boldsymbol{ij}}\delta(\boldsymbol{j}), \quad \boldsymbol{i} \in \mathcal{F},$$

для некоторых $c_{\boldsymbol{ij}} \in R$. Множество всех скалярных эндоморфизмов обозначается $\widehat{E} = \widehat{\mathrm{End}}(M^{\mathcal{F}})$. Скалярные эндоморфизмы и построенные на их основе $k$-ЛРС проще реализуются на практике. Если $M = R$, то все эндоморфизмы $\varphi\colon R^{\mathcal{F}} \to R^{\mathcal{F}}$ скалярные, т. е. $\mathrm{End}(R^{\mathcal{F}}) = \widehat{\mathrm{End}}(R^{\mathcal{F}})$. Для $\varphi_1, \ldots, \varphi_k \in E$, $\boldsymbol{i} = (i_1, \ldots, i_k) \in \mathbb{N}_0^k$ обозначим $\boldsymbol{\varphi}^{\boldsymbol{i}} = \varphi_1^{i_1} \ldots \varphi_k^{i_k}$. Положим

$$\begin{aligned} r_{12} = \min\{|\mathcal{F}| : \exists \text{ попарно перестановочные } \varphi_1, \ldots, \varphi_k \in E \\ \text{такие, что } u[\boldsymbol{i} + \mathcal{F}] = \boldsymbol{\varphi}^{\boldsymbol{i}}(u[\mathcal{F}]),\ \boldsymbol{i} \in \mathbb{N}_0^k\}, \\ r_{13} = \min\{|\mathcal{F}| : \exists \text{ попарно перестановочные } \varphi_1, \ldots, \varphi_k \in \widehat{E} \\ \text{такие, что } u[\boldsymbol{i} + \mathcal{F}] = \boldsymbol{\varphi}^{\boldsymbol{i}}(u[\mathcal{F}]),\ \boldsymbol{i} \in \mathbb{N}_0^k\}. \end{aligned}$$

Попарно перестановочные эндоморфизмы $\varphi_1, \ldots, \varphi_k \in E$, удовлетворяющие условию

$$\begin{gathered} \forall\, \delta[\mathcal{F}] \in M^{\mathcal{F}} \quad \forall\, s \in \overline{1,k} \quad \forall\, \boldsymbol{j} \in \mathcal{F} \\ \lambda[\mathcal{F}] = \varphi_s(\delta[\mathcal{F}]), \quad \boldsymbol{j} + \mathbf{1}_s \in \mathcal{F} \quad \Rightarrow \quad \lambda(\boldsymbol{j}) = \delta(\boldsymbol{j} + \mathbf{1}_s), \end{gathered}$$

называются *$\mathcal{F}$-ЛРС системой*. Положим

$$\begin{aligned} r_{14} = \min\{|\mathcal{F}| : \exists\ \mathcal{F}\text{-ЛРС система } \varphi_1, \ldots, \varphi_k \in E \text{ такая}, \\ \text{что } u[\boldsymbol{i} + \mathcal{F}] = \boldsymbol{\varphi}^{\boldsymbol{i}}(u[\mathcal{F}]),\ \boldsymbol{i} \in \mathbb{N}_0^k\}, \\ r_{15} = \min\{|\mathcal{F}| : \exists\ \mathcal{F}\text{-ЛРС система } \varphi_1, \ldots, \varphi_k \in \widehat{E} \text{ такая}, \\ \text{что } u[\boldsymbol{i} + \mathcal{F}] = \boldsymbol{\varphi}^{\boldsymbol{i}}(u[\mathcal{F}]),\ \boldsymbol{i} \in \mathbb{N}_0^k\}. \end{aligned}$$

Очевидно,

$$r_{12} \leqslant r_{13}, \quad r_{14} \leqslant r_{15}, \quad r_{12} \leqslant r_{14}, \quad r_{13} \leqslant r_{15}.$$

Параметры $r_{11}$–$r_{15}$ характеризуют сложность выработки знаков $k$-ЛРП $u$ линейным регистром сдвига. Параметры $r_{10}$, $r_{12}$–$r_{15}$ определяют также количество подряд идущих знаков, достаточных для выработки $k$-ЛРП $u$.

Следующие два параметра, наряду с $r_1$–$r_6$, характеризуют ранг модуля сдвигов ЛРП $u$. Обозначим

$$\begin{aligned} r_{16} &= \min\{t \geqslant 0 :\ R[\boldsymbol{x}]u \text{ содержится в } t\text{-порожденном } R\text{-модуле}\}, \\ r_{17} &= \min\{r_1(L_M(I)) : u \in L_M(I),\ I - \text{унитар. правый идеал } R[\boldsymbol{x}]\}. \end{aligned}$$

Если кольцо $R$ конечно, то определим

$$r_{18} = r_{18}(u) = \log_{|R|} |R[\boldsymbol{x}]u|.$$

Этот параметр можно назвать "информационной" линейной сложностью. Такой же термин, но уже в другом смысле, отчасти применим к $r_7$–$r_9$, поскольку эти параметры показывают, по скольким знакам последовательность $v \in R[\boldsymbol{x}]u$ определяется однозначно.

Существуют и другие естественные параметры, характеризующие линейную сложность. Например, пусть $u$ — $k$-ЛРП над коммутативным кольцом $R$ и $\Pi$ — некоторый ее начальный параллелепипед, $|\Pi| = m$. Из векторов столбцов $(u[\boldsymbol{i}+\Pi],\ \boldsymbol{i} \in \Pi)$ составим матрицу $U$ размеров $m \times m$. Если $k = 1$, то $U$ — ганкелева матрица ЛРП $u$. Обозначим

$$r_{19}(u) = \operatorname{rank} U, \qquad r_{20}(u) = \operatorname{rk} U,$$

где $\operatorname{rank} U$ — *ранг матрицы* $U$, т. е. наибольший порядок ненулевых миноров, $\operatorname{rk} U$ — *аннуляторный ранг*, т. е. наибольшее $t \geqslant 0$ такое, что $\operatorname{An}_R(I_U(t)) = 0$, где $I_U(t)$ — идеал кольца $R$, порожденный всеми минорами порядка $t$ матрицы $U$ (см. [9, 68]). Ниже в § 5 вводится и исследуется биномиальная линейная сложность $r_{21}(u)$.

Примеры показывают, что большинство введенных параметров не равны друг другу. В общем случае удается доказать равенство лишь двух из них: $r_3 = r_{10}$.

**Предложение 5.** *Пусть* $u \in \mathcal{L}_R M^{\langle k\rangle}$. *Тогда*

$$r_3 = r_{10}, \quad r_9 \leqslant r_{12}, \quad r_{10} \leqslant r_{13}, \quad r_{11} \leqslant r_{15},$$

*а если* $R$ *конечно, то* $\quad r_4 \leqslant r_{18} \leqslant r_1, \quad r_{18} \leqslant r_7 \log_{|R|} |M|$.

При $k = 1$, $u \in \mathcal{L}_R M^{\langle 1\rangle}$ удается доказать, что

$$r_6 \leqslant r_{10}, \quad r_{11} \leqslant r_{10}.$$

В коммутативном случае набор соотношений между параметрами линейной сложности увеличивается.

**Предложение 6.** *Если* $R$ *коммутативно,* $u \in \mathcal{L}_R M^{\langle k\rangle}$, $\nu = r_1(M)$, *то*

$$r_2 \geqslant r_8, \quad r_3 \geqslant r_9, \quad r_9 \leqslant r_{11}, \quad r_{11} \geqslant r_{14}, \quad r_{13} \leqslant (r_{12}\nu)^k, \quad r_{16} \leqslant r_{11}\nu.$$

*Если кольцо* $R$ *коммутативно или артиново слева, то*

$$r_4 \leqslant r_1, \quad r_4 \leqslant r_7\nu.$$

*Если* $R$ — *коммутативное локальное кольцо с максимальным идеалом* $J$ *такое, что* $\operatorname{An}(J) \neq 0$ (*последнее условие выполнено, если* $R$ *конечно*), *и* $u \in \mathcal{L}_R R^{\langle k\rangle}$, *то*

$$r_4 = r_5 = r_6.$$

Если $k = 1$, $R$ коммутативно, $u \in \mathcal{L}_R M^{\langle 1\rangle}$, то как следствие $r_1 = r_2 = r_3 = r_{10} = r_{13} = r_{15}$. Если к тому же $M = R$, получаем

**Предложение 7.** *Если* $k = 1$, *кольцо* $R$ *коммутативно,* $M = R$, $u \in \mathcal{L}_R R^{\langle 1\rangle}$, *то*

$$\begin{aligned} &r_6 \leqslant r_5 \leqslant r_4 \leqslant r_{18} \leqslant r_7 \leqslant r_8 \leqslant r_9 \leqslant \\ &\quad \leqslant r_1 = r_2 = r_3 = r_{10} = r_{11} = r_{12} = r_{13} = r_{14} = r_{15} = \operatorname{rank} u, \\ &r_{16} \leqslant r_1, \quad r_{17} \leqslant r_1. \end{aligned}$$

*Если к тому же* $R$ *артиново* (*в частности, если* $R$ *конечно*), *то*

$$\begin{aligned} &r_4 = r_5 = r_6 \leqslant r_{18} \leqslant r_7 \leqslant r_8 \leqslant r_9 \leqslant \\ &\quad \leqslant r_1 = r_2 = r_3 = r_{10} = r_{11} = r_{12} = r_{13} = r_{14} = r_{15} = \operatorname{rank} u. \end{aligned} \tag{29}$$

Примеры показывают, что в приведенных утверждениях большинство неравенств могут быть строгими.

Введенные числовые параметры позволяют характеризовать некоторые общие свойства ЛРП. Например, получен следующей критерий единственности минимального многочлена 1-ЛРП над модулем в терминах совпадения двух параметров ее линейной сложности (в коммутативном случае эквивалентность пунктов (а)–(в) хорошо известна).

**Предложение 8.** *Пусть* $k = 1$, $u \in \mathcal{L}_R M^{\langle 1\rangle}$. *Тогда следующие утверждения равносильны*:

(а) *ЛРП* $u$ *имеет единственный минимальный многочлен*;

(б) $\mathrm{An}(u)$ — *главный левый идеал кольца* $R[x]$, *порождаемый унитарным многочленом*;

(в) *минимальный многочлен ЛРП* $u$ *является ненулевым многочленом наименьшей степени в* $\mathrm{An}(u)$;

(г) $r_6(u) = r_{10}(u)$.

Перечислим теперь соотношения между параметрами линейной сложности для $k$-ЛРП над полями. Ряд свойств сохраняются в некоммутативном случае — для $k$-ЛРП над телами.

**Предложение 9.** *Пусть* $R$ — *тело*, $u \in \mathcal{L}_R M^{\langle k\rangle}$, $\nu = \dim_R M$ ($\nu \in \mathbb{N} \cup \{\infty\}$), $m = \dim_R R[\boldsymbol{x}]u$. *Тогда* $m < \infty$ *и справедливы соотношения:*

(а) $m = r_1 = r_2 = r_3 = r_4 = r_5 = r_6 = r_{10} = r_{16} \leqslant r_{13}$.

(б) *Если* $\nu < \infty$, *то* $r_7 = ]m/\nu[$, *где* $]x[$ — *наименьшее целое число, большее или равное* $x$. *Если* $\nu = \infty$, *то* $r_7 = 0$ *при* $m = 0$ *и* $r_7 = 1$ *при* $m \geqslant 1$.

(в) *Если* $k = 1$, *то ЛРП* $u$ *имеет единственный минимальный многочлен и* $r_{11} = m$.

**Предложение 10.** *Пусть* $R$ — *поле*, $u \in \mathcal{L}_R M^{\langle k\rangle}$, $\nu = \dim_R M$, $m$ — *параметр, введенный в предложении* 9. *Тогда*

$$m \leqslant r_{17} \leqslant m\nu, \quad m \leqslant r_{11}\nu, \quad ]m/\nu[ = r_7 \leqslant r_8 \leqslant r_9 \leqslant m, \quad r_{18} = m,$$

*где при* $\nu = \infty$ *вместо* $]m/\nu[$ *нужно брать* 0, *если* $m = 0$, *и* 1, *если* $m \geqslant 1$. *Если* $k = 1$, *то*

$$r_{13} = r_{15} = m, \quad r_{17} = m\nu.$$

*Если* $M = R$, *то все введенные параметры линейной сложности совпадают.*

$$r_i = m, \quad i \in \overline{1, 18}.$$

В связи с последним результатом возникает задача описания класса колец, для которых, как и для ЛРП над полем, все введенные параметры линейной сложности совпадают: $r_1 = \ldots = r_{18}$.

Если $u$ — $k$-последовательность над кольцом $R$ и $Q$ — расширение кольца $R$, то $u$ можно рассматривать также как последовательность над $Q$. Параметры линейной сложности $k$-последовательности $u$ над кольцом $Q$ будем обозначать $r_i^Q = r_i^Q(u)$. Коммутативное кольцо $R$ называется *областью Безу*, если $R$ — коммутативная область целостности, в которой каждый идеал, порожденный двумя элементами, является главным, т.е. порождается одним элементом. В этом случае любой конечно порожденный идеал является главным.

**Теорема 12.** *Пусть* $R$ — *коммутативная область Безу с полем частных* $Q$, $u \in \mathcal{L}_R R^{\langle 1\rangle}$. *Тогда*

$$r_i = r_i^Q = \operatorname{rank} u, \qquad i \in \overline{1, 18}.$$

*Минимальный многочлен* 1*-ЛРП* $u$ *над кольцом* $R$ *определен однозначно и совпадает с минимальным многочленом* 1*-ЛРП* $u$ *над полем* $Q$.

Теорема 12 показывает, что коммутативные области Безу являются классом колец, для 1-ЛРП над которыми свойства линейной сложности оказываются наиболее близкими к свойствам линейной сложности 1-ЛРП над полем. Этот класс колец включает (как собственное подмножество) коммутативные области главных идеалов, в частности, кольцо целых чисел $\mathbb{Z}$.

# 5 Представления знаков полилинейных рекуррент

Одной из задач, связанных с $k$-ЛРП, является нахождение явных формул, позволяющих вычислять $i$-й знак ЛРП без рекуррентного вычисления предыдущих знаков. Такая формула иногда называется аналитическим представлением рекурренты. Ниже рассматривается два таких представления: биномиальное представление и представление функцией след.

*Биномиальной $k$-последовательностью* над кольцом $R$ с корнем $\boldsymbol{a} = (a_1, \ldots, a_k) \in R^k$ порядка $\boldsymbol{l} = (l_1, \ldots, l_k) \in \mathbb{N}_0^k$ назовем $k$-последовательность $\boldsymbol{a}^{[\boldsymbol{l}]} \in R^{\langle k \rangle}$ со знаками

$$\boldsymbol{a}^{[\boldsymbol{l}]}(\boldsymbol{i}) = \begin{cases} \binom{\boldsymbol{i}}{\boldsymbol{l}} \boldsymbol{a}^{\boldsymbol{i}-\boldsymbol{l}} = \binom{i_1}{l_1} \ldots \binom{i_k}{l_k} a_1^{i_1-l_1} \ldots a_k^{i_k-l_k}, & \text{если } \boldsymbol{i} \geqslant \boldsymbol{l}, \\ 0, & \text{в противном случае.} \end{cases}$$

Если $R \subseteq S$ — расширение кольца $R$ и $u \in M^{\langle k \rangle}$, то через $[1 \otimes u]$ обозначим последовательность над модулем $S \otimes M$ со знаками $[1 \otimes u](\boldsymbol{i}) = 1 \otimes u(\boldsymbol{i}) \in S \otimes M$, $\boldsymbol{i} \in \mathbb{N}_0^k$. Линейную сложность $k$-ЛРП $[1 \otimes u]$ над $S$-модулем $S \otimes M$ будем обозначать $r_i^S(1 \otimes u)$, $i = 1, 4, 10$. Будем говорить, что $k$-ЛРП $u$ над модулем ${}_RM$ *обладает биномиальным представлением*, если существует расширение $R \subseteq S$ кольца $R$ такое, что канонический гомоморфизм $R$-модулей $\alpha\colon M \to S \otimes M$, $x \to 1 \otimes x$, является мономорфизмом, и последовательность $[1 \otimes u]$ над $S$-модулем $S \otimes M$ представляется в виде линейной комбинации биномиальных последовательностей с корнями из $S^k$ и коэффициентами из $S \otimes M$:

$$[1 \otimes u] = \sum_{\boldsymbol{a} \in S^k} \sum_{\boldsymbol{j} \geqslant \boldsymbol{0}} \boldsymbol{a}^{[\boldsymbol{j}]} c_{\boldsymbol{aj}}, \qquad c_{\boldsymbol{aj}} \in S \otimes M, \tag{30}$$

где лишь конечное число элементов $c_{\boldsymbol{aj}}$ не равны нулю.

Локальное кольцо, максимальный идеал которого является ниль-идеалом, будем называть *вполне примарным*.

**Теорема 13.** (а) *Произвольная $k$-ЛРП над модулем ${}_RM$, где $R$ — вполне примарное кольцо, обладает биномиальным представлением.*

(б) *Произвольная $k$-ЛРП над модулем без кручения ${}_RM$, где $R$ — область целостности, обладает биномиальным представлением.*

Пусть $R$ — локальное кольцо с максимальным идеалом $J$ и полем вычетов $\bar{R} = R/J$. Подмножество $B \subseteq R$ будем называть *координатным множеством*, если отображение $B \to \bar{R}$, $b \to \bar{b}$, биективно. Следующее предложение уточняет результат теоремы 13(а)

**Предложение 11.** *Пусть $M$ — модуль над вполне примарным кольцом $R$, $u$ — $k$-ЛРП над $M$ с элементарными характеристическими многочленами $F_1(x_1)$, ..., $F_k(x_k)$, $S$ — расширение кольца $R$, являющееся вполне примарным кольцом таким, что поле вычетов $\bar{S}$ является полем разложения многочленов $\bar{F}_1(x)$, ..., $\bar{F}_k(x)$, $B$ — произвольное координатное множество кольца $S$. Тогда $k$-ЛРП $[1 \otimes u]$ над $S$-модулем $S \otimes M$ имеет биномиальное представление с корнями из $B^k$ и коэффициентами из $S \otimes M$, причем коэффициенты такого биномиального представления определены однозначно.*

Пусть $k$-ЛРП $[1 \otimes u]$ имеет биномиальное представление 30. Для каждого $\boldsymbol{a} \in S^k$ обозначим через $\mathcal{F}(\boldsymbol{a})$ наименьшую диаграмму Ферре, содержащую множество $\{\boldsymbol{j} \in \mathbb{N}_0^k : c_{\boldsymbol{aj}} \neq 0\}$. Будем называть $\mathcal{F}(\boldsymbol{a})$ *диаграммой Ферре корня* $\boldsymbol{a}$, а $|\mathcal{F}(\boldsymbol{a})|$ — *кратностью корня* $\boldsymbol{a}$ в биномиальном представлении 30. *Биномиальной линейной сложностью* $k$-ЛРП $u$ над расширением $S$ кольца $R$ и расширением $S \otimes M$ модуля $M$ назовем величину

$$r_{21}^S(1 \otimes u) = \min\Big\{\textstyle\sum_{\boldsymbol{a} \in S^k} |\mathcal{F}(\boldsymbol{a})|\Big\},$$

где минимум берется по всем биномиальным представлениям 30.

**Теорема 14.** *Для любой 1-ЛРП $u$ над модулем ${}_RM$ верна оценка $r_{10}(u) \leqslant r_{21}^R(u)$.*

Другие результаты об оценках параметров линейной сложности $k$-ЛРП по ее биномиальному представлению можно найти в [32]. В дополнение к теореме 12 сформулируем следующий результат.

**Теорема 15.** *Пусть $R$ — коммутативная область Безу с полем частных $Q$, $u \in R^{\langle 1 \rangle}$ — 1-ЛРП над кольцом $R$, $S$ — расширение поля $Q$, в котором характеристический многочлен ЛРП $u$ раскладывается на линейные множители. Тогда*

$$r_i(u) = r_i^Q(u) = r_i^S(u) = \operatorname{rank} u = r_{21}^S(u), \qquad i \in \overline{1, 18}.$$

Рассмотрим теперь представление 1-ЛРП функцией след. Пусть $A$ — алгебра над $R$, являющаяся конечно порожденным проективным $R$-модулем. Согласно [4, 11], для любой системы образующих $a_1, \ldots, a_m$ модуля ${}_RA$ существуют гомоморфизмы $\varphi_i \in \mathrm{Hom}_R(A, R)$, $1 \leqslant i \leqslant m$, такие, что $a = \sum_{i=1}^{m} \varphi_i(a)a_i$ для всех $a \in A$. Набор $(a_i, \varphi_i)$ называется координатной системой проективного модуля $A$. *Следом* из $A$ в $R$ называется гомоморфизм $R$-модулей

$$\mathrm{tr}_{A/R} \colon A \to R, \qquad \mathrm{tr}_{A/R}(a) = \sum_{i=1}^{m} \varphi_i(aa_i), \qquad a \in A.$$

Это определение не зависит от выбора координатной системы [4, 57]. Если $R$ — поле и $A$ — его конечное алгебраическое расширение, то $\mathrm{tr}_{A/R}$ совпадает с обычной функцией след из поля $A$ в подполе $R$.

Пусть $R$ — коммутативное локальное кольцо с максимальным идеалом $J = J(R)$ и полем вычетов $R/J = \bar{R}$, $F(x) \in R[x]$ — унитарный многочлен степени $m$ и $S = R[x]/F(x) = R[\theta]$ — расширение кольца $R$ корнем $\theta = [x]_F$ многочлена $F(x)$. Модуль ${}_RS$ является свободным модулем ранга $m$ с базисом $1, \theta, \ldots, \theta^{m-1}$, и произвольный элемент $a \in S$ однозначно записывается в виде $a = a_0 + a_1\theta + \ldots + a_{m-1}\theta^{m-1}$, где $a_i \in R$. Положим $\varphi_i(a) = a_i$, $0 \leqslant i \leqslant m-1$. Тогда $(\theta^i, \varphi_i)$ — координатная система модуля ${}_RS$. Многочлен $F(x)$ будем называть *сепарабельным*, если многочлен $\bar{F}(x)$ не имеет кратных корней в поле разложения, где $\bar{F}(x)$ — канонический образ многочлена $F(x)$ над полем вычетов $\bar{R}$.

**Теорема 16.** *Пусть $R$ — локальное кольцо, $F(x) \in R[x]$ — унитарный сепарабельный многочлен такой, что его образ $\bar{F}(x)$ неприводим над полем $\bar{R}$. Тогда для любой ЛРП $u \in L_R(F)$ существует единственная константа $c \in S$ такая, что*

$$u(i) = \mathrm{tr}_{S/R}(c\theta^i), \qquad i \geqslant 0. \tag{31}$$

В случае, когда $R$ — поле Галуа или кольцо Галуа, представление 31 совпадает с известными ранее представлениями [19, 34, 35]. Действие функции след, как и в [35], выразим в терминах автоморфизмов и $p$-адических разложений. Кольцо $R$ называется *гензелевым* [3], если для всякого унитарного многочлена $F(x) \in R[x]$ и для любого разложения $\bar{F}(x)$ в произведение $\bar{F}(x) = g(x)h(x)$ унитарных взаимно простых многочленов существуют унитарные многочлены $G(x)$, $H(x) \in R[x]$ такие, что $\bar{G}(x) = g(x)$, $\bar{H}(x) = h(x)$ и $F(x) = G(x)H(x)$. Для сепарабельного многочлена $F(x)$ над гензелевым кольцом $R$ можно построить его кольцо разложения [57, 59], последовательно расширяя $R$ корнями делителей многочлена $F(x)$, неприводимых по модулю радикала.

**Теорема 17.** *Пусть $R$ — гензелево кольцо, $F(x)$ — сепарабельный многочлен степени $m$ и $T$ — его кольцо разложения над $R$. Тогда*

$$\mathrm{tr}_{T/R}(a) = \sum_{\sigma \in G} \sigma(a), \quad a \in T,$$

*где $G = \mathrm{Aut}(T/R)$, $|G| = [\bar{T} : \bar{R}]$. Если к тому же $\bar{F}(x)$ неприводим над полем $\bar{R}$, то*

$$\mathrm{tr}_{S/R}(a) = \sum_{\tau \in H} \tau(a), \quad a \in S,$$

*где $H$ — множество всех гомоморфных вложений кольца $S$ в $T$ над $R$, $|H| = m$.*

Предположим теперь, что $\bar{R} = GF(q)$ — конечное поле характеристики $p$, $J(R)$ — нильпотентный идеал индекса нильпотентности $n$ и $\bar{F}(x)$ — неприводимый над полем $\bar{R}$ многочлен. Тогда множество $\Gamma(R) = \{b \in R : b^q = b\}$ состоит из $q$ элементов, попарно несравнимых по модулю $J(R)$. Назовем его *$p$-адическим координатным множеством* кольца $R$. Зафиксируем базисы $\{e_{i\alpha} + J(R)^{i+1} : \alpha \in A_i\}$ пространств $J(R)^i/J(R)^{i+1}$ над полем $\bar{R}$, $0 \leqslant i \leqslant n-1$. Тогда $\{e_{i\alpha} + J(S)^{i+1} : \alpha \in A_i\}$ есть базис пространства $J(S)^i/J(S)^{i+1}$ над полем $\bar{S}$, и каждый элемент $a \in S$ однозначно представляется в виде

$$a = \sum_{i=0}^{n-1} \sum_{\alpha \in A_i} a_{i\alpha} e_{i\alpha}, \qquad a_{i\alpha} \in \Gamma(S) = \{b \in S : b^{q^m} = b\},$$

где лишь конечное число элементов $a_{i\alpha}$ отлично от нуля.

**Теорема 18.** $\operatorname{tr}_{S/R}(a) = \sum_{s=0}^{m-1} \sum_{i=0}^{n-1} \sum_{\alpha \in A_i} a_{i\alpha}^{q^s} e_{i\alpha}, \quad a \in S.$

Для модуля $M$ над локальным кольцом $R$ рассмотрим $S$-модуль $N = S \otimes_R M$, и определим функцию *след* $\operatorname{tr}_{N/M}\colon N \to M$ соотношением

$$\operatorname{tr}_{N/M}(s \otimes m) = \operatorname{tr}_{S/R}(s)m, \quad s \in S, \quad m \in M.$$

Предположим, что многочлен $F(x)$ представляется в виде $F(x) = F_1(x)^{k_1} \dots F_t(x)^{k_t}$, где $\bar{F}_j(x)$, $1 \leqslant j \leqslant t$, — различные унитарные неприводимые над полем $\bar{R}$ сепарабельные многочлены. Обозначим $S_j = R[x]/F_j(x) = R[\theta_j]$, где $\theta_j = [x]_{F_j}$.

**Теорема 19.** *Для любой ЛРП $u \in L_M(F)$ существует единственный набор констант $c_{jr} \in N_j = S_j \otimes_R M$, $1 \leqslant j \leqslant t$, $0 \leqslant r < k_j$, такой, что*

$$u(i) = \sum_{j=1}^{t} \sum_{r=0}^{k_j-1} \binom{i}{r} \operatorname{tr}_{N_j/M}(\theta_j^{i-r} c_{jr}), \qquad i \geqslant 0. \tag{32}$$

*Любая последовательность вида 32 принадлежит $L_R(F)$.*

Для ЛРП над полями, кольцами Галуа и квазифробениусовыми модулями специального вида представление функцией след использовалось для нахождения распределения элементов в линейных рекуррентных последовательностях [63], оценок линейной сложности линейных рекуррент и их координатных последовательностей [39, 62], построения помехоустойчивых кодов [34, 35, 58, 76, 63].

# 6 Аннуляторные соотношения

При исследовании линейных рекуррент над модулями бывает необходимым, чтобы выполнялись некоторые наиболее общие свойства, справедливые для линейных рекуррент над полем. Как известно, ЛРП-семейства над полем удовлетворяют ряду аннуляторных соотношений, чаще всего формулируемых в виде свойств ЛРП-семейств, связанных с суммами и пересечениями. Оказывается, что аннуляторные соотношения выполняются для ЛРП-семейств над артиновым квазифробениусовым бимодулем ${}_AM_B$.

Понятие линейной рекуррентной последовательности является частным случаем понятия представляющей функции на полугруппе. Мы введем здесь это понятие, и результаты об аннуляторных соотношениях будем излагать для семейств представляющих функций.

Пусть $M$ — левый $R$-модуль, $(G, \cdot)$ — полугруппа, $RG$ — полугрупповое кольцо, $M^G$ — $R$-модуль всех функций $u\colon G \to M$. Определим произведение элемента $F = \sum_{g \in G} a_g g \in RG$, где $a_g \in R$, на функцию $u \in M^G$ правилом (сравн. с 1)

$$Fu = v \in M^G, \quad v(h) = \sum_{g \in G} a_g u(hg), \quad h \in G. \tag{33}$$

Функция $u \in M^G$ называется *представляющей* если циклический модуль $RGu = {}_R(gu : g \in G)$ конечно порожден над $R$. Множество представляющих функций обозначим $\mathcal{L}_R M^G$. Аналогичные определения можно сформулировать для правого $R$-модуля.

В случае, когда $G = (\mathbb{N}_0^k, +)$ — полугруппа векторов с целыми неотрицательными координатами или изоморфная ей полугруппа $G = (\{\boldsymbol{x}^{\boldsymbol{i}} : \boldsymbol{i} \in \mathbb{N}_0^k\}, \cdot)$ мономов, $M^G$ есть не что иное, как множество $M^{\langle k \rangle}$ всех $k$-последовательностей над $M$, а полугрупповая алгебра $RG$ совпадает с алгеброй многочленов $R[\boldsymbol{x}]$. При этом структура $RG$-модуля на $M^G$, определяемая правилом 33, совпадает со структурой $R[\boldsymbol{x}]$-модуля на $M^{\langle k \rangle}$, введенной в 1, а циклический модуль $RGu = R[\boldsymbol{x}]u$ есть модуль сдвигов последовательности $u$.

**Предложение 12.** *Любая $k$-ЛРП над модулем $M$ является представляющей функцией на полугруппе $G = (\mathbb{N}_0^k, +)$. Если кольцо $R$ нетерово слева, или коммутативно, или если $k = 1$, то верно обратное утверждение.*

Если ${}_AM_B$ — бимодуль над кольцами $A$ и $B$ с единицами, то $M^G$ является $(AG, BG)$-бимодулем. Левый идеал $I \subseteq AG$ назовем *конечно копорожденным*, если левый $A$-модуль $AG/I$ конечно порожден. Правый идеал $J \subseteq BG$ назовем *конечно копорожденным*, если правый $B$-модуль $BG/J$ конечно порожден. Левый $AG$-подмодуль $L \subseteq M^G$, конечно порожденный как левый $A$-модуль, назовем *левым $AG$-семейством*. Правый $BG$-подмодуль $R \subseteq M^G$, конечно порожденный как правый $B$-модуль, назовем *правым $BG$-семейством*. Если $G = \mathbb{N}_0^k$ и кольцо $A$ нетерово слева, то левый идеал $I \subseteq AG = A[\boldsymbol{x}]$ конечно копорожден тогда и только тогда, когда он унитарен.

Следуя [50], бимодуль ${}_AM_B$ будем называть *квазифробениусовым QF-бимодулем*, если модули ${}_AM$ и $M_B$ точны (т. е. аннуляторы $l_A(M)$ и $r_B(M)$ равны 0) и для любого максимального левого идеала $I$ кольца $A$ и любого максимального правого идеала $J$ кольца $B$ каждый из аннуляторов $r_M(I)$ и $l_M(J)$ либо равен 0, либо является неприводимым правым $B$-модулем, соответственно неприводимым левым $A$-модулем. Если ${}_AM_B$ есть QF-бимодуль, то следующие условия эквивалентны [50, теорема 6]: (1) кольцо $A$ артиново слева и левый $A$-модуль $M$ конечно порожден; (2) кольцо $B$ артиново справа и правый $B$-модуль $M$ конечно порожден; (3) кольцо $A$ артиново слева и кольцо $B$ артиново справа. В этом случае будем называть ${}_AM_B$ *артиновым QF-бимодулем*. Артиново слева кольцо $A$ является квазифробениусовым тогда и только тогда, когда ${}_AA_A$ есть артинов QF-бимодуль.

Обозначим через $r_{M^G}(I)$, $l_{AG}(R)$, $r_{BG}(L)$, $l_{M^G}(J)$ аннуляторы подмножеств $I \subseteq AG$, $R$, $L \subseteq M^G$, $J \subseteq BG$ в множествах $M^G$, $AG$, $BG$ и $M^G$ соответственно. В случае $k$-последовательностей эти обозначения можно заменить соответственно на $L_M(I)$, $\mathrm{An}(R)$, $\mathrm{An}(L)$ и $L_M(J)$, хотя последние обладают тем недостатком, что оказываются одинаковыми для левых и правых аннуляторов.

**Теорема 20.** *Пусть ${}_AM_B$ — бимодуль, кольцо $A$ артиново слева, кольцо $B$ артиново справа, $G$ — полугруппа с нейтральным элементом. Тогда следующие условия эквивалентны.*

(а) *${}_AM_B$ есть артинов QF-бимодуль.*

(б) *Каждый левый идеал $I \subseteq AG$ и каждое правое $BG$-семейство $R \subseteq M^G$ удовлетворяют аннуляторным соотношениям*

$$I = l_{AG}(r_{M^G}(I)), \qquad R = r_{M^G}(l_{AG}(R)).$$

*Каждый правый идеал $J \subseteq BG$ и каждое левое $AG$-семейство $L \subseteq M^G$ удовлетворяют аннуляторным соотношениям*

$$J = r_{BG}(l_{M^G}(J)), \qquad L = l_{M^G}(r_{BG}(L)).$$

*При этом левый идеал $l_{AG}(R)$ кольца $AG$ и правый идеал $r_{BG}(L)$ кольца $BG$ конечно копорождены.*

(в) *Отображения*

$$I \to r_{M^G}(I), \qquad R \to l_{AG}(R)$$

*являются биективными взаимно обратными соответствиями Галуа между множеством конечно копорожденных левых идеалов $I \subseteq AG$ и множеством правых $BG$-семейств $R \subseteq M^G$. Отображения*

$$J \to l_{M^G}(J), \qquad L \to r_{BG}(L)$$

*являются биективными взаимно обратными соответствиями Галуа между множеством конечно копорожденных правых идеалов $J \subseteq BG$ и множеством левых $AG$-семейств $L \subseteq M^G$.*

(г) *Модули ${}_AM$ и $M_B$ конечно порождены; если $S \subseteq M^G$ является одновременно левым $AG$- и правым $BG$-семейством, $I = l_{AG}(S)$, $J = r_{BG}(S)$, то $(AG/I, BG/J)$-бимодуль $S$ является артиновым QF-бимодулем.*

**Следствие 3.** *Пусть ${}_AM_B$ — артинов QF-бимодуль. Тогда отображения $I \to r_{M^G}(I)$, $S \to l_{AG}(S)$ и отображения $J \to l_{M^G}(J)$, $S \to r_{BG}(S)$ являются двумя парами взаимно обратных биективных соответствий Галуа между тремя множествами: множеством конечно копорожденных двусторонних идеалов $I \lhd AG$, множеством подбимодулей $S \subseteq M^G$, являющихся одновременно левыми $AG$- и правыми $BG$-семействами, и множеством конечно копорожденных двусторонних идеалов $J \lhd BG$.*

Пусть $I_1$, $I_2$ — левые идеалы кольца $AG$ и $R_1$, $R_2$ — правые $B$-подмодули модуля $M^G$. Тогда

$$r_{M^G}(I_1+I_2) = r_{M^G}(I_1) \cap r_{M^G}(I_2), \quad l_{AG}(R_1+R_2) = l_{AG}(R_1) \cap l_{AG}(R_2), \tag{34}$$

$$r_{M^G}(I_1 \cap I_2) \supseteq r_{M^G}(I_1)+r_{M^G}(I_2), \quad l_{AG}(R_1 \cap R_2) \supseteq l_{AG}(R_1)+l_{AG}(R_2). \tag{35}$$

Аналогично если $J_1$, $J_2$ — правые идеалы кольца $BG$ и $L_1$, $L_2$ — левые $A$-подмодули модуля $M^G$, то

$$l_{M^G}(J_1+J_2)=l_{M^G}(J_1)\cap l_{M^G}(J_2),\quad r_{BG}(L_1+L_2)=r_{BG}(L_1)\cap r_{BG}(L_2), \tag{36}$$

$$l_{M^G}(J_1\cap J_2)\supseteq l_{M^G}(J_1)+l_{M^G}(J_2),\quad r_{BG}(L_1\cap L_2)\supseteq r_{BG}(L_1)+r_{BG}(L_2). \tag{37}$$

В общем случае включения в 35 и 37 могут быть строгими.

**Следствие 4.** *Если ${}_AM_B$ — артинов QF-бимодуль, $I_1$, $I_2$ — конечно копорожденные левые идеалы кольца $AG$, $R_1$, $R_2$ — правые $BG$-семейства в $M^G$, $J_1$, $J_2$ — конечно копорожденные правые идеалы кольца $BG$, $L_1$, $L_2$ — левые $AG$-семейства в $M^G$, то включения в 35, 37 обращаются в равенства.*

В случае $G=\mathbb{N}_0^k$ соотношения 34–37, обращающиеся в равенства в условиях следствия 4, называют соотношениями для сумм и пересечений $k$-ЛРП-семейств и их аннуляторов.

**Следствие 5.** *Если ${}_AM_B$ — артинов QF-бимодуль, то множество $\mathcal{L}_AM^G$ представляющих функций над модулем ${}_AM$ совпадает с множеством $\mathcal{L}M_B^G$ представляющих функций над модулем $M_B$, и это множество является $(AG,BG)$-подбимодулем в $M^G$.*

В случае $G=(\mathbb{N}_0^k,+)$ получим, что множество левых $A$-$k$-ЛРП над артиновым QF-бимодулем ${}_AM_B$ совпадает с множеством правых $B$-$k$-ЛРП. В частности, левая $k$-ЛРП над квазифробениусовым кольцом является правой $k$-ЛРП. Из следствия 5 также вытекает, что сумма $u+v$ левых $A$-$k$-ЛРП $u,v\in\mathcal{L}_AM^{\langle k\rangle}$ и произведение $au$, $a\in A$, являются левыми $A$-$k$-ЛРП (эти утверждения содержательны именно в некоммутативном случае).

Теорема 20 имеет приложения в теории модулей: пункт (г) этой теоремы позволяет строить QF-бимодуль над произвольным конечным кольцом в виде бимодуля функций. Например, верно

**Следствие 6.** *Если ${}_AM_B$ — артинов QF-бимодуль, $G$ — конечная полугруппа с нейтральным элементом, то $(AG,BG)$-бимодуль $MG$ является артиновым QF-бимодулем. В частности, если $A$ — квазифробениусово кольцо, то и кольцо $AG$ квазифробениусово.*

Результаты § 4 и указанные выше результаты показывают, что классическая теория линейной сложности ЛРП над полем наиболее полно сохраняется для 1-ЛРП над коммутативными областями Безу, а теория ЛРП-семейств — для $k$-ЛРП над артиновыми QF-бимодулями. В связи с этим отметим, что коммутативная область Безу, являющаяся артиновым QF-бимодулем над собой — это в точности поле.

# 7 Координатные последовательности

Пусть $R=\mathbb{Z}_{p^n}$ — примарное кольцо вычетов, $B=\{b_0=0,b_1,\dots,b_{p-1}\}$ — его координатное множество, т. е. множество, элементы которого образуют полную систему вычетов по модулю $p$. Примерами координатных множеств являются *$p$-адическое* координатное множество $\Gamma(R)=\{\beta\in R:\ \beta^p=\beta\}$ и *$p$-ичное* координатное множество $B=\overline{0,p-1}$.

Каждый элемент $a\in R$ однозначно представляется в виде

$$a=a_0+pa_1+\ldots+p^{n-1}a_{n-1},\qquad a_s=\gamma_s^B(a)\in B,\qquad s\in\overline{0,n-1},$$

называемом *разложением элемента $a$ в координатном множестве $B$*. Относительно операций

$$a\oplus b=\gamma_0^B(a+b),\qquad a\otimes b=\gamma_0^B(ab),\qquad a,b\in B,$$

алгебра $(B,\oplus,\otimes)$ является полем, изоморфным $\bar{R}=GF(p)$. Если $u$ — последовательность над кольцом $R$, то последовательность $u_s=\gamma_s^B(u)$ над полем $B$ со знаками $u_s(i)=\gamma_s^B(u(i))$, $i\geqslant 0$, называется ее *$s$-ой координатной последовательностью* в координатном множестве $B$.

Всюду далее в этом параграфе $u$ — ЛРП максимального периода над кольцом $R=\mathbb{Z}_{p^n}$ с минимальным многочленом $F(x)\in R[x]$ степени $m$, $u_s=\gamma_s^B(u)$, $s\in\overline{0,n-1}$ — ее координатные последовательности в координатном множестве $B$ кольца $R$.

**Теорема 21.** *Ранги нулевой и первой координатных последовательностей вычисляются по следующим формулам.*

(а) $\operatorname{rank} u_0 = m$;

(б) $\operatorname{rank} u_1 = 2m + \binom{m}{2}, \quad p = 2;$

(в) $\operatorname{rank} u_1 = m + \sum\limits_{l \in L} \binom{m+l-1}{l} + \binom{m+p-1}{p}$, *где* $\varnothing \subseteq L \subseteq \overline{2, p-1}$, $p \geqslant 3$. *Множество* $L$ *эффективно определяется по координатному множеству* $B$ (*см.* [24]).

Для $N$, $A \in \mathbb{N}$ обозначим

$$b(N, 0) = N, \quad b(N, A) = 0 \text{ при } N < pA, \tag{38}$$

и в остальных случаях

$$b(N, A) = N - pA + \begin{cases} \tilde{A}, & \text{если } p \geqslant 3, \text{ где } \tilde{A} \in \overline{1, p-1},\ \tilde{A} \equiv A \pmod{p-1}, \\ 1, & \text{если } p = 2,\ A \text{ четно или } A = 1, \\ 2, & \text{если } p = 2,\ A \text{ нечетно, } A \geqslant 3. \end{cases} \tag{39}$$

Пусть $\left\{ {m \atop N} \right\}_p$ — число размещений $N$ одинаковых предметов в $m$ различных ящиках при условии, что в каждый ящик попадет не более $p-1$ предметов. Согласно [45, с. 215]

$$\left\{ {m \atop N} \right\}_p = \sum_{j=0}^{N/p} (-1)^j \binom{m}{j} \binom{m+N-pj-1}{m-1}, \qquad N \geqslant 1. \tag{40}$$

Справедливы неравенства

$$\binom{m}{N} \leqslant \left\{ {m \atop N} \right\}_p \leqslant \binom{m+N-1}{N},$$

поскольку в левой части находится число размещений $N$ одинаковых шаров по $m$ различным ящикам при условии, что в каждый ящик попадает не более одного шара, а в правой части — число размещений $N$ шаров по $m$ ящикам без ограничений на число шаров в ящиках. Заметим также, что

$$\left\{ {m \atop N} \right\}_p = \binom{m+N-1}{N} \qquad \text{при} \quad N \in \overline{0, p-1},$$
$$\left\{ {m \atop N} \right\}_2 = \binom{m}{N} \qquad \text{при} \quad p = 2, \quad N \geqslant 0.$$

Если $N$, $p$ фиксированы, $m \to \infty$, то

$$\left\{ {m \atop N} \right\}_p = \binom{m+N-1}{N} \left(1 + O(\tfrac{1}{m})\right) \sim \frac{m^N}{N!}. \tag{41}$$

**Теорема 22.** *Пусть* $\bar{u}_s = \bar{\gamma}_s^B(u)$, $s \in \overline{0, n-1}$, $b(A) = b(p^s, A)$. *Тогда*

$$\operatorname{rank} u_s \leqslant \sum_{A=0}^{p^{s-1}} (A+1) \cdot \sum_{N=b(A+1)+1}^{b(A)} \left\{ {m \atop N} \right\}_p. \tag{42}$$

*Если* $u_s = \gamma_s(u)$ *— координатные последовательности ЛРП и в* $p$*-адическом координатном множестве* $\Gamma(R)$, *то оценка остается справедливой, если суммирование в 42 проводить лишь по числам* $N \equiv 1 \pmod{p-1}$. *Если* $u_s = \gamma_s^B(u)$ *— координатные последовательности ЛРП и в* $p$*-ичном координатном множестве* $B = \overline{0, p-1}$ *и* $p \geqslant 5$, *то оценка остается справедливой, если суммирование в 42 проводить лишь по числам* $N$, *удовлетворяющим условию:* $N \equiv 1 \pmod{2}$ *или* $N \equiv 0 \pmod{p-1}$.

Приведем теперь нижние оценки рангов координатных последовательностей. Так как $F(x)$ — многочлен максимального периода, то для $t \in \overline{0, n-1}$ существует многочлен $\Phi^{(t+1)}(x)$ над кольцом $R$ такой, что

$$x^{\tau_t} - e \equiv p^{t+1} \Phi^{(t+1)}(x) \pmod{F(x)}, \qquad \deg \Phi^{(t+1)}(x) < m, \quad \bar{\Phi}^{(t+1)}(x) \neq 0. \tag{43}$$

При этом если $p = 2$, то

$$\begin{aligned} &\bar{\Phi}^2(x) \equiv \bar{\Phi}^{(1)}(x) + \bar{\Phi}^{(1)}(x)^2 \pmod{\bar{F}(x)}, \\ &\Phi^{(t+1)}(x) \equiv \Phi^{(t)}(x) \pmod{2^{t-1}}, \qquad t \geqslant 2, \end{aligned} \tag{44}$$

и если $p \geqslant 3$, то

$$\Phi^{(t+1)}(x) \equiv \Phi^{(t)}(x) \pmod{p^t}, \qquad t \geqslant 1. \tag{45}$$

Обозначим

$$\begin{aligned} &L_0 = \{0, p^{s-1}\}; \\ &L_t = \{A:\ 1 \leqslant A \leqslant p^{s-1} - 1,\ A \equiv t \pmod{p-1}\}, \quad t \in \overline{1, p-1} \quad (p \geqslant 3); \\ &L_1 = \{1\} \cup \{A:\ 2 \leqslant A \leqslant 2^{s-1} - 2,\ A \text{ четно},\ 2^s - 2A + 1 < m\} \quad (p = 2); \\ &L_2 = \{A:\ 3 \leqslant A \leqslant 2^{s-1} - 1,\ A \text{ нечетно},\ 2^s - 2A + 2 < m\} \quad (p = 2); \end{aligned} \tag{46}$$

$$\mathcal{R}_t = \sum_{A \in L_t} (A+1) \left\{ \begin{matrix} m \\ b(A) \end{matrix} \right\}_p, \qquad \text{где } b(A) = b(p^s, A).$$

**Теорема 23.** (а) *Для любого* $s \in \overline{1, n-1}$ *справедлива оценка* $\operatorname{rank} u_s \geqslant \mathcal{R}_0$.

(б) *Если многочлен* $F(x)$ *выбран так, что многочлены* $\bar{\Phi}^{(1)}(x)^{p^r}$, $r \in \overline{0, m-1}$, *линейно независимы над полем* $\bar{R}$ *по модулю многочлена* $\bar{F}(x)$, *то при* $s \geqslant 2$

$$\operatorname{rank} u_s \geqslant \mathcal{R}_0 + \mathcal{R}_1 + \frac{m}{m+p} \cdot \mathcal{R}_2.$$

(в) *Если ранг системы многочленов* $\operatorname{Res}(\bar{\Phi}^{(2)}(x)^r / \bar{F}(x))$, $r \in \overline{0, m-1}$, *равен* $h > p$, *то при* $s \geqslant 2$

$$\operatorname{rank} u_s \geqslant \mathcal{R}_0 + \frac{h-p}{h} \cdot \mathcal{R}_1.$$

(г) *Если* $\deg \bar{\Phi}^{(2)}(x) = 0$ (*т.е.* $h = 1$), *то при* $s \geqslant 2$

$$\operatorname{rank} u_s \geqslant \mathcal{R}_0 + \mathcal{R}_1 + \ldots + \mathcal{R}_{p-1}.$$

**Следствие 7.** *Если* $p$, $s$ *фиксированы*, $m \to \infty$, *то*

$$\operatorname{rank} u_s = \binom{m}{p^s} \left(1 + O(\tfrac{1}{m})\right).$$

Заметим, что, в обозначениях теоремы 23, многочлен $F(x)$ всегда можно подобрать так, чтобы многочлен $\bar{\Phi}^{(1)}(x)$ (который полностью определяется многочленом $F(x)$, — см. 43) был бы произвольным наперед заданным многочленом (удовлетворяющим условиям 43), в частности, так, чтобы выполнялись условия теоремы 23.

Теоремы 22, 23 позволяют иногда весьма точно оценить ранги координатных последовательностей $u_s$ ЛРП $u$. Приведем несколько примеров. Пусть $p = 2$ и выполнены условия теоремы 23(b). Тогда

$$\begin{aligned} &\text{если } m = 3, \text{ то } 15 \leqslant \operatorname{rank} u_3 \leqslant 31,\ 195 \leqslant \operatorname{rank} u_7 \leqslant 451; \\ &\text{если } m = 11, \text{ то } 3383 \leqslant \operatorname{rank} u_3 \leqslant 5340,\ 59703 \leqslant \operatorname{rank} u_7 \leqslant 128430; \\ &\text{если } m = 31, \text{ то } 1.37 \cdot 10^7 \leqslant \operatorname{rank} u_3 \leqslant 1.53 \cdot 10^7,\ 6 \cdot 10^{10} \leqslant \operatorname{rank} u_7 \leqslant 10^{11}. \end{aligned}$$

Пусть теперь выполнены условия теоремы 23(d). Тогда

$$\begin{aligned} &\text{если } p = 5, m = 3, \text{ то } 328 \leqslant \operatorname{rank} u_3 \leqslant 3093,\ 2 \cdot 10^5 \leqslant \operatorname{rank} u_7 \leqslant 2 \cdot 10^6; \\ &\text{если } p = 5, m = 11, \text{ то } 2 \cdot 10^8 \leqslant \operatorname{rank} u_3 \leqslant 10^9,\ 10^{11} \leqslant \operatorname{rank} u_7 \leqslant 8 \cdot 10^{11}; \\ &\text{если } p = 11, m = 5, \text{ то } 10^6 \leqslant \operatorname{rank} u_3 \leqslant 2 \cdot 10^7,\ 2 \cdot 10^{10} \leqslant \operatorname{rank} u_7 \leqslant 3 \cdot 10^{11}. \end{aligned}$$

# 8 Приложения в теории кодирования

Пусть ${}_RM$ — конечный точный модуль над коммутативным кольцом $R$ с единицей $e$. Произвольный подмодуль $\mathcal{K} < {}_RM^n$ называется *линейным $n$-кодом* над ${}_RM$, его *расстояние Хэмминга* удовлетворяет равенству $d(\mathcal{K}) = \min\{\|\boldsymbol{\alpha}\| : \boldsymbol{\alpha} \in \mathcal{K} \setminus \mathbf{0}\}$, где $\|\boldsymbol{\alpha}\|$ — вес Хэмминга слова $\boldsymbol{\alpha}$.

Развитие теории линейных кодов над модулями по аналогии с классической теорией линейных кодов над полями использует определяемые далее понятия двойственного кода и проверочной матрицы [74].

Для любого идеала $I \lhd R$ и любого подмодуля $K < {}_RM$ обозначим их *аннуляторы*, соответственно в $M$ и в $R$, через $\mathrm{An}_M(I)$ и $\mathrm{An}_R(K)$. Модуль ${}_RM$ называется *квазифробениусовым* (*или $QF$-модулем*), если $\mathrm{An}_R(\mathrm{An}_M(I)) = I$ и $\mathrm{An}_M(\mathrm{An}_R(K)) = K$ для всех $I \lhd R$ и $K < {}_RM$. Существует единственный (с точностью до изоморфизма) $QF$-модуль ${}_RQ$ [47, 38].

Назовем модуль ${}_RM^* = \mathrm{Hom}_R(M, Q)$ всех гомоморфизмов ${}_RM \to {}_RQ$ *сопряженным* (или *Морита-двойственным*) к ${}_RM$, см. [70, 50, 47]. Определим произведение $\alpha \in M$ на $\varphi \in M^*$ как $\varphi\alpha = \varphi(\alpha) \in Q$. Тогда для фиксированного $\alpha \in M$ соответствие $\varphi \to \varphi\alpha$ индуцирует гомоморфизм ${}_RM^* \to Q$, принадлежащий модулю $M^{**} = \mathrm{Hom}_R(M^*, Q)$. Отождествляя этот гомоморфизм с $\alpha$, получаем равенство $M^{**} = M$. Если $R$ — QF-кольцо, и $M = R$, то $Q = R$ и $M^* = M = R$.

Представим произвольный элемент $(M^n)^* = \mathrm{Hom}_R(M^n, Q)$ как строку $\boldsymbol{\varphi} = (\varphi_1, \ldots, \varphi_n) \in (M^*)^n = \mathrm{Hom}_R(M, Q)^n$, действующую на элементы $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in M^n$ по правилу $\boldsymbol{\varphi}(\boldsymbol{\alpha}) = \boldsymbol{\varphi}\boldsymbol{\alpha} = \varphi_1\alpha_1 + \ldots + \varphi_n\alpha_n \in Q$. Тогда $(M^n)^* = (M^*)^n$. Для линейного кода $\mathcal{K} < {}_RM^n$ определим *двойственный код* $\mathcal{K}^\circ < {}_R(M^*)^n$ как $\mathcal{K}^\circ = \{\boldsymbol{\varphi} \in (M^*)^n) : \boldsymbol{\varphi}\mathcal{K} = 0\}$. Если рассматривать $\mathcal{K}$ только как подгруппу в $(M^n, +)$, то $\mathcal{K}^\circ$ — это код, двойственный коду $\mathcal{K}$ в смысле [55]. Но наша конструкция позволяет изучать $\mathcal{K}^\circ$ как $R$-модуль, если $\mathcal{K}$ — подмодуль в ${}_RM^n$. В силу [47, 55] имеем

**Предложение 13.** *Существует изоморфизм групп $\mathcal{K}^\circ \cong M^n/\mathcal{K}$, и $|\mathcal{K}^\circ| \cdot |\mathcal{K}| = |M|^n$, $\mathcal{K}^{\circ\circ} = \mathcal{K}$.*

Пусть $\varphi_i = (\varphi_{i1}, \ldots, \varphi_{in}) \in (M^*)^n$, $i \in \overline{1,l}$, — система образующих модуля ${}_R\mathcal{K}^\circ$. Матрицу $\Phi = (\varphi_{ij})_{l\times n}$ над $M^*$ назовём *проверочной матрицей* кода $\mathcal{K}$. Любой столбец $\varphi_j^\downarrow = (\varphi_{1j}, \ldots, \varphi_{lj})^T$ матрицы $\Phi$ задаёт гомоморфизм $\varphi_j^\downarrow : {}_RM \to {}_RQ^{(l)}$. Определим *гарантируемый ранг* $\varkappa_M(\Phi)$ *матрицы* $\Phi$ *относительно* $M$ как наибольшее число $k \in \mathbb{N}$ такое, что любая система $k$ столбцов $\varphi_{j_1}^\downarrow, \ldots, \varphi_{j_k}^\downarrow$ матрицы $\Phi$ линейно независима над $M$, т.е. $\varphi_{j_1}^\downarrow(\alpha_1) + \ldots + \varphi_{j_k}^\downarrow(\alpha_k) \neq 0$ для любых $(\alpha_1, \ldots, \alpha_k) \in M^k \setminus \mathbf{0}$. Как и в случае кодов над полями, справедливо

**Предложение 14.** $d(\mathcal{K}) = \varkappa_M(\Phi) + 1$.

Если код $\mathcal{K} < {}_RM^n$ имеет *проверочную матрицу над кольцом* $R$, т.е. такую матрицу $\Phi_{l\times n}$ над $R$, что $\mathcal{K} = \{\boldsymbol{\alpha} \in M^n : \Phi\boldsymbol{\alpha}^T = 0\}$, то он называется *$R$-замкнутым*. Все линейные коды над QF-модулем ${}_RQ$ являются $R$-замкнутыми [37, 72, 38].

Представим здесь конструкцию обобщенного кода Кердока над $GF(q)$, $q = 2^l$. Пусть $R = GR(q^2, 4)$ — кольцо Галуа характеристики 4 и мощности $q^2$, $q = 2^l$, $l \geqslant 1$. Обобщенный код Кердока $K_q(m+1)$ над $GF(q)$ ($m$ нечетно) — это представление Рида-Соломона так называемого базового линейного кода $\mathcal{K}_R(m)$ над кольцом $R$. Пусть $S = GR(q^{2m}, 4)$ расширение степени $m$ кольца $R$, и $\mathrm{Tr}_R^S(x)$ — след из $S$ в $R$, определяемый равенством $\mathrm{Tr}_R^S(x) = \sum_{\sigma\in \mathrm{Aut}(S/R)} \sigma(x)$.

Множество $\Gamma(S) = \{\beta \in S\colon\ \beta^{q^m} = \beta\}$ замкнуто относительно умножения и содержит $q^m$ элементов. Напомним (см. § 7 выше), что любой элемент $\beta \in S$ однозначно представляется в виде $\beta = \beta_0 + 2\beta_1$, где $\beta_t = \gamma_t(\beta) \in \Gamma(S)$, $t = \overline{0,1}$, и относительно операции $a \oplus b = \gamma_0(a+b)$ алгебра $(\Gamma(S), \oplus, \cdot)$ образует поле $GF(q^m)$, в котором $\Gamma(R) = \{\beta \in R\colon\ \beta^q = \beta\}$ — подполе $GF(q)$. Пусть $\theta$ — примитивный элемент поля $\Gamma(S)$. *Базовый код* $\mathcal{K}_R(m)$ определяется как линейный код длины $h = q^m$ над $R$, состоящий из всех слов $\boldsymbol{v} = (v(0), \ldots, v(h-1))$ таких, что для некоторых $\xi \in S$, $c \in R$

$$v(i) = \mathrm{Tr}_R^S(\xi\theta^i) + c, \quad i = \overline{0, h-2}, \quad v(h-1) = c. \tag{47}$$

Пусть теперь $\Gamma(R) = \{\omega_0 = 0, \omega_1 = e, \ldots, \omega_{q-1}\}$ и $\gamma_*\colon\ R \to \Gamma(R)^q$ — отображение, действующее на элемент $r = r_0 + 2r_1 \in R$ по правилу

$$\gamma_*(r) = (r_1, r_1 \oplus \omega_1 r_0, \ldots, r_1 \oplus \omega_{q-1} r_0). \tag{48}$$

Тогда $\gamma_*(R)$ — $[q, 2, q-1]_q$-код Рида-Соломона над $GF(q)$, поэтому $\gamma_*$ называется *RS-отображением* [75].

Код $K_q(m+1)$ определяется как конкатенация линейного над $R$ кода $\mathcal{K}_R(m)$ и линейного над $\Gamma(R)$ кода $\gamma_*(R)$. Это код длины $n = q^{m+1}$, состоящий из всех слов $\gamma_*^h(\boldsymbol{u}) = (\gamma_*(u(0)), \ldots, \gamma_*(u(h-1)))$, $\boldsymbol{u} \in \mathcal{K}_R(m)$. Если $q = 2$, т.е. $R = \mathbb{Z}_4$, это — оригинальный двоичный код Кердока [35, 62].

**Теорема 24.** *Код $K_q(m+1)$ есть $(n, n^2, \frac{q-1}{q}(n - \sqrt{n}))_q$-код с полной композиционной функцией*

$$W_{K_q(m+1)}(x_0, \ldots, x_{q-1}) = \sum_{j=0}^{q-1} x_j^n + (q^{m+2} - q) \prod_{j=0}^{q-1} x_j^{n/q} +$$

$$+ \frac{1}{2} \sum_{s \in \{-1,1\}} q(q^m - 1)(q^m + sq^{\lambda+1}) \prod_{j=0}^{q-1} x_j^{\frac{n}{q} - sq^\lambda} \sum_{j=0}^{q-1} x_j^{sq^{\lambda+1}}.$$

Рассмотрим теперь представление кодов полилинейными рекуррентами [41]. Назовём *полиэдром* произвольное конечное подмножество

$$\mathcal{F} = \{\boldsymbol{i}_1, \ldots, \boldsymbol{i}_n\} \subseteq \mathbb{N}_0^k. \tag{49}$$

Через $M^{\mathcal{F}}$ обозначим $R$-модуль функций $\delta : \mathcal{F} \to M$. Любая такая функция однозначно определяется *диаграммой значений* $\delta[\mathcal{F}] = (\delta(\boldsymbol{i}_1), \ldots, \delta(\boldsymbol{i}_n)) \in M^n$. Ясно, что модуль ${}_RM^{\mathcal{F}}$ изоморфен ${}_RM^n$. Для любой $k$-последовательности $u \in M^{\langle k \rangle}$ также можно построить диаграмму значений $u[\mathcal{F}] = (u(\boldsymbol{i}_1), \ldots, u(\boldsymbol{i}_n))$. Пусть $I \lhd R[\boldsymbol{x}]$ и

$$\mathcal{K} = L_M^{\mathcal{F}}(I) = \{u[\mathcal{F}] : u \in L_M(I)\}. \tag{50}$$

Очевидно, $\mathcal{K}$ — подмодуль $R$-модуля ${}_RM^{\mathcal{F}}$ и при нумерации 49 элементов полиэдра $\mathcal{F}$ можно рассматривать $\mathcal{K}$ как подмодуль модуля ${}_RM^n$ — линейный код длины $n$ над ${}_RM$. В общем случае не любой линейный код над ${}_RM$ представляется в виде 50, однако справедливо

**Предложение 15.** *Пусть ${}_RQ$ — $QF$-модуль. Тогда для любого линейного кода $\mathcal{K} < {}_RQ^n$ существуют $k \in \overline{1,n}$, полиэдр $\mathcal{F} \subset \mathbb{N}_0^k$ мощности $n$ и унитарный идеал $I \lhd R[\boldsymbol{x}]$ такие, что $\mathcal{K} = L_Q^{\mathcal{F}}(I)$.*

Пусть теперь полиэдр $\mathcal{F}$ является диаграммой Ферре (см. § 1). Скажем, что $\mathcal{K} < {}_RM^n$ — *рекурсивный код*, если он имеет представление 50 при подходящем выборе $k \in \overline{1,n}$, унитарного идеала $I \lhd R[\boldsymbol{x}]$, диаграммы Ферре $\mathcal{F} \subseteq \mathbb{N}_0^k$ и упорядочения 49 её элементов. Наименьшее $k$ с этим свойством назовём *рекурсивной размерностью* кода $\mathcal{K}$. Первый важный класс рекурсивных кодов даёт

**Теорема 25** (Астурийская теорема). *Любой систематический линейный код ранга $m$ над ${}_RM$ есть рекурсивный код, имеющий рекурсивную размерность не выше $m$.*

Рассмотрим рекурсивные и линейные рекурсивные МДР-коды [15, 54]. Код $\mathcal{K} \subset \Omega^n$ в алфавите $\Omega$ из $q$ элементов называется *$k$-рекурсивным*, $1 \leqslant k < n$, если существует функция $f : \Omega^k \to \Omega$ такая, что $\mathcal{K}$ состоит из всех строк

$$u(\overline{0, n-1}) = (u(0), \ldots, u(n-1)) \in \Omega^n,$$

удовлетворяющих условию $u(i+k) = f(u(\overline{i, i+k-1}))$, $i \in \overline{0, n-k-1}$. Доказательство существования МДР-кодов такого типа, т.е. рекурсивных $[n, k, n-k+1]_q$-кодов, связано с изучением следующих параметров:

$n(k,q)$ $(n^r(k,q))$ – максимум длин (рекурсивных) МДР-кодов $\mathcal{K}$ комбинаторной размерности $k$ в алфавите мощности $q$;

$l(k,q)$ $(l^r(k,q))$ – максимум длин (рекурсивных) МДР-кодов $\mathcal{K}$ комбинаторной размерности $k$, *линейных в широком смысле*,т.е. линейных над некоторой абелевой группой порядка $q$.

Для примарных чисел $q$ можно также определить $m(k,q)$ $(m^r(k,q))$ – аналог $l(k,q)$ $(m^r(k,q))$ только для кодов, *линейных в узком смысле*, т.е. над полем $\mathbf{F}_q$.

Назовем указанную выше функцию $f(\boldsymbol{x})$ *идемпотентной*, если $f(x,\ldots,x)=x$. Введём ещё три параметра: $n^{ir}(k,q), l^{ir}(k,q)$ и $m^{ir}(k,q)$ (только для примарных $q$); "ir" означает "идемпотентный рекурсивный".

Стандартные рассуждения дают для любых $x\in\{l,n\}$, $y\in\{\varnothing,r,ir\}$ и $k,q_1,q_2\in\overline{2,\infty}$ неравенство

$$x^y(k,q_1q_2)\geqslant\min\{x^y(k,q_1),x^y(k,q_2)\}. \tag{51}$$

**Предложение 16.** *Если $q$ примарное, то*

$$m^r(2,q)=n^r(2,q)=n(2,q)=q+1; \tag{52}$$

$$m^{ir}(2,q)=l^{ir}(2,q)=\begin{cases} q & \text{если } q \text{ простое;}\\ q-1 & \text{если } q \text{ не простое}\\ & (\text{А.Абашин, устное сообщение}).\end{cases} \tag{53}$$

*Для примарных $q<8$ проверяется, что $n^{ir}(2,q)=m^{ir}(2,q)$.*

**Теорема 26.** *Для любого $q>2$, кроме $q=6$ и, возможно, $q\in\{14,18,26,42\}$, $n^r(2,q)\geqslant 4$.*

В действительности, для многих значений $q$ последнее неравенство можно значительно усилить. Некоторые усиленные оценки (мы называем их *стандартными*) легко следуют из 51–53.

**Теорема 27.** *Имеют место следующие нестандартные оценки:*
$n^r(2,q)\geqslant 8$ *для* $q=80$.
$n^r(2,q)\geqslant 7$ *для* $q\in\{50,57,58,65,70,78,84,85,86,92,94,95,96,97,98\}$.
$n^r(2,q)\geqslant 6$ *для* $q\in\{54,62,66,68,69,74,75,76,82,87,90,93\}$.
$n^r(2,q)\geqslant 5$ *для* $q\in\{21,24,39,44,60\}$.
$n^{ir}(2,q)\geqslant 7$ *для* $q\in\{50,57,58,65,70,78,84,85,86,92,94,95,96,97,98\}$.
$n^{ir}(2,q)\geqslant 5$ *для* $q\in\{54,62,66,68,69,74,75,76,82,87,90,93\}$.

Рекурсивную версию некоторых известных из [51, 67] оценок для $k>2$ содержит

**Предложение 17.** *Если $q\leqslant k$, то $l^r(k,q)=n(k,q)=k+1$ и, для примарных $q$, $m^r(k,q)=k+1$.*

Для $k=3$ имеем $m^r(3,q)=q+1$ (см. [67]), и компьютерные вычисления дают

**Предложение 18.** *Для любого примарного $q\in\overline{4,128}$, число линейных рекурсивных $[q+1,3,q-1]$-кодов равно $\frac{1}{2}\varphi(q+1)(q-1)$.*

Таким образом, все коды, описанные в предложении 18, естественно эквивалентны линейным циклическим кодам, указанным в [33, гл.11, теорема 9]. Можно предположить, что это верно для всех примарных $q\geqslant 4$.

Для случая $k=3$, $q=4$ имеем

**Предложение 19.** $m^r(3,4)=5<l^r(3,4)=n^r(3,4)=m(3,4)=n(3,4)=6$.

При доказательстве последнего предложения был построен линейный в широком смысле код с рекурсивной функцией $f(x_1,x_2,x_3)=\alpha x_1^2+\alpha x_2+x_3^2$, названный *Астурийским кодом*. Астурийский код показывает, что: (1) существуют линейные в широком смысле рекурсивные коды, лучшие, чем любой линейный в классическом смысле рекурсивный код; (2) для некоторых из наилучших линейных в классическом смысле, но не рекурсивных кодов, существуют линейные в широком смысле рекурсивные коды с теми же параметрами. Однако, для $k=3$ Астурийский код является исключением, так как вычисления на компьютере дают $l^r(3,8)=9=8+1$, $\quad l^r(3,16)=17=16+1$, а результат А.Абашина (устное сообщение) утверждает, что если $t>4$, то $l^r(3,2^t)=2^t+1$.

# Литература

[1] Амбросимов А. С. О распределении частот мультиграмм в линейных рекуррентных последовательностях над кольцом вычетов. *Успехи мат. наук*, **48** (1993), № 5, 157–158.

[2] Атья М., Макдональд И. *Введение в коммутативную алгебру.* М.: Мир, 1972.

[3] Бурбаки Н. *Коммутативная алгебра.* М.: Мир, 1971.

[4] Боревич А. З., Толасов Б. А. Введение в теорию Галуа колец. Орджоникидзе, Северо-Осетинский государственный университет им. К. Л. Хетагурова, 1984.

[5] Ван дер Варден Б. Л. *Алгебра.* М.: Наука, 1979.

[6] Гилл А. *Линейные последовательностные машины. Анализ, синтез и применение.* М.: Наука, 1974.

[7] Глухов М. М., Елизаров В. П., Нечаев А. А. *Алгебра.* Часть II. М., 1991.

[8] Гонзалес С., Коусело Е., Марков В. Т., Нечаев А. А. Параметры линейных рекурсивных МДР-кодов. *Дискрет. мат.*, **12** (2000), № 4, 3–24.

[9] Елизаров В. П. *Конечные кольца.* М., 1993.

[10] Камловский О. В., Кузьмин А. С. Распределение элементов на циклах линейных рекуррентных последовательностей над кольцами Галуа. *Успехи мат. наук*, **53** (1998), № 2, 149–150.

[11] Каш Ф. *Модули и кольца.* М.: Мир, 1981.

[12] Кон П. *Свободные кольца и их связи.* М.: Мир, 1975.

[13] Коробов Н. М. Распределение невычетов и первообразных корней в рекуррентных рядах. *Докл. АН СССР*, **88** (1953), № 4, 603–606.

[14] Коробов Н. М. *Тригонометрические суммы и их приложения.* М.: Наука, 1989.

[15] Коусело Е., Гонсалес С., Марков В., Нечаев А. Рекурсивные МДР-коды и рекурсивно дифференцируемые квазигруппы. *Дискр. матем.*, **10** (1998), № 2, 3–29.

[16] Кузьмин А. С., Куракин В. Л., Нечаев А. А. Псевдослучайные и полилинейные последовательности. *Труды по дискретной математике*, том 1. М.: ТВП, 1997. С. 139–202.

[17] Лаксов Д. Линейные рекуррентные последовательности над конечными полями. *Математика* (сб. переводов), **11** (1967), № 6, 145–158.

[18] Ламбек И. *Кольца и модули.* М.: Мир, 1971.

[19] Лидл Р., Нидеррайтер Г. *Конечные поля.* М.: Мир, 1988.

[20] Кузьмин А. С., Куракин В. Л., Марков В. Т., Михалев А. В., Нечаев А. А. Коды и рекурренты над конечными кольцами и модулями. *Вестник Моск. Унив. Сер. 1. Матем. Механ.* **5** (1999), 18–31.

[21] Кузьмин А. С., Куракин В. Л., Нечаев А. А. Свойства линейных и полилинейных рекуррент над кольцами Галуа (I). *Труды по дискретной математике*, том 2. М.: ТВП, 1998. С. 191–222.

[22] Кузьмин А. С., Куракин В. Л., Нечаев А. А. Свойства линейных и полилинейных рекуррент над кольцами Галуа (II). *Обозрение прикладной и промышленной математики*, **7**, № 1, 5–59. М.: ТВП, 2000.

[23] Кузьмин А. С., Куракин В. Л., Нечаев А. А. Статистические свойства линейных рекуррент над кольцами Галуа и квазифробениусовыми модулями характеристики 4. *Труды по дискретной математике*, том 4. М.: ФИЗМАТЛИТ, 2001. С. 91–128.

[24] Куракин В. Л. Первая координатная последовательность линейной рекурренты максимального периода над кольцом Галуа. *Дискрет. мат.*, **6** (1994), № 2, 88–100.

[25] Куракин В. Л. Биномиальное представление линейных рекуррентных последовательностей. *Фундаментальная и прикладная математика*, ЦНИТ МГУ, **1** (1995), № 2, 553–556.

[26] Куракин В. Л. Алгоритм Берлекэмпа—Месси над конечными коммутативными кольцами. *Проблемы передачи информации*, **35** (1999), № 2, 38–50.

[27] Куракин В. Л. Алгоритм Берлекэмпа—Месси над конечными кольцами, модулями и бимодулями. *Дискрет. мат.*, **10** (1998), № 4, 3–34.

[28] Куракин В. Л. Полиномиальные преобразования линейных рекуррентных последовательностей над конечными коммутативными кольцами. *Дискрет. мат.*, **12** (2000), № 3, 3–36.

[29] Куракин В. Л. Линейная сложность полилинейных последовательностей. *Дискрет. мат.*, **13** (2001), № 1, 3–55.

[30] Куракин В. Л. Представление функцией след линейных рекуррент над кольцами и модулями. *Успехи мат. наук*, **56** (2001), № 6, 157–158.

[31] Куракин В. Л. Представление линейных рекуррентных последовательностей функцией след. *Мат. сборник*, **193** (2002), № 6, 123–142.

[32] Куракин В. Л. Биномиальная линейная сложность полилинейных последовательностей. *Труды по дискретной математике*, том 6. М.: ФИЗМАТЛИТ, 2003.

[33] Мак-Вилльямс Ф. Д., Слоэн Н. Д. А. Теория кодов, исправляющих ошибки. М., Связь, 1979.

[34] Нечаев А. А. Функция "след" в кольце Галуа и помехоустойчивые коды. *V Всесоюзн. симп. по теории колец, алгебр и модулей.* Новосибирск, 1982, с. 97.

[35] Нечаев А. А. Код Кердока в циклической форме. *Дискрет. мат.*, **1** (1989), № 4, 123–139.

[36] Нечаев А. А. Линейные рекуррентные последовательности над коммутативными кольцами. *Дискрет. мат.*, **3** (1991), № 4, 107–121.

[37] Нечаев А. А. Линейные рекуррентные последовательности над квазифробениусовыми модулями. *Успехи мат. наук*, **48** (1993), № 3, 197–198.

[38] Нечаев А. А. Конечные квазифробениусовы модули, приложения к кодам и линейным рекуррентам. *Фундаментальная и прикладная математика.* ЦНИТ МГУ, **1** (1995), № 1, 229–254.

[39] Нечаев А. А., Кузьмин А. С., Куракин В. Л. Структурные, аналитические и статистические свойства линейных и полилинейных рекуррент. *Труды по дискретной математике*, том 3. М.: ФИЗМАТЛИТ, 2000. С. 155–194.

[40] Нечаев А. А., Кузьмин А. С., Куракин В. Л. Вполне равномерные линейные рекурренты над кольцами Галуа и QF-модулями характеристики 4. *Труды по дискретной математике*, том 5. М.: ФИЗМАТЛИТ, 2002. С. 103–158.

[41] Нечаев А. А., Кузьмин А. С., Марков В. Т. Линейные коды и полилинейные рекурренты. *Фундаментальная и прикладная математика*, **2** (1996), № 3, 195–254.

[42] Нечаев В. И. Линейные рекуррентные сравнения с периодическими коэффициентами. *Мат. заметки*, **3** (1968), № 6, 625–632.

[43] Нечаев В. И. Рекуррентные последовательности. *Уч. зап. Моск. пед. инст. им. В. И. Ленина*, **375** (1971), 103–123.

[44] Нечаев В. И. Линейные сравнения по модулю простого идеала и линейные рекуррентные последовательности. *Уч. зап. Моск. пед. инст. им. В. И. Ленина*, **375** (1971), 124–132.

[45] Сачков В. Н. *Введение в комбинаторные методы дискретной математики.* М.: Наука, 1982.

[46] Сидельников В. М. Оценки для числа появлений знаков на отрезке рекуррентной последовательности над конечным полем. *Дискрет. мат.*, **3** (1991), № 2, 87–95.

[47] Фейс К. *Алгебра: кольца, модули, категории.* Т. 2. М.: Мир, 1979.

[48] Цирлер Н. Линейные возвратные последовательности. *Кибернетический сб.*, **6**, 55–79. Москва, ИЛ, 1963.

[49] Шпарлинский И. Е. О распределении значений рекуррентных последовательностей. *Проблемы передачи информации*, **25**, № 2, 1989, 46–53.

[50] Azumaya G. A duality theory for injective modules (Theory of quasi-Frobenius modules). *Amer. J. Math.*, **81** (1959), № 1, 249–278.

[51] Bush K. A. Orthogonal arrays of index unity. *Ann. Math. Stat.*, **23** (1952), 426–434.

[52] Carmichael R. D. On sequences of integers defined by recurrence relations. *Quart. J. Pure Appl. Math.*, **48** (1920), 343–372.

[53] Cerlienco L., Mignotte M., Piras F. Linear recurrent sequences: algebraic and arithmetical properties. *Enseign. Math.* (2), **33** (1987), № 1–2, 67–108.

[54] Couselo E., Gonzalez S., Markov V., Nechaev A. Recursive MDS-codes. *Proceedings of the WCC'99 Workshop on Coding and Cryptography.* January 11–14, 1999, Paris, France. 271–278.

[55] Delsart P. An algebraic approach to the association schemes of coding theory. *Philips research, Rep. Suppl.*, **10**, 1973.

[56] Delsarte P., Goethals J.-M. Alternating bilinear forms over $GF(q)$. *J. Combin. Theory*, **19A** (1975), 26–50.

[57] F. DeMeyer and E. Ingraham. Separable algebras over commutative rings. *Lecture Notes in Math.*, **181**. Berlin, Springer, 1971.

[58] Hammons A. R., Kumar P. V., Calderbank A. R., Sloane N. J. A., Sole P. The $\mathbf{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes. *Bull. Amer. Math. Soc.*, **29** (1993), № 2, 218–222.

[59] G. J. Janusz. Separable algebras over commutative ring. *Trans. American Math. Soc.*, **122** (1966), 461–479.

[60] Kumar P. V., Helleseth T., Calderbank A. R. An upper bound for Weil exponential sums over Galois ring and applications. *IEEE Trans. Inform. Theory*, **41** (1995), № 2, 456–468.

[61] Kurakin V. L., Kuzmin A. S., Markov V. T., Mikhalev A. V., Nechaev A. A. Linear codes and polylinear recurrences over finite rings and modules (a survey). In: Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 13-th Intern. Symp. AAECC-13, Honolulu, Hawaii, USA, November 15–19, 1999. Algebra II. Proceedings. *Lecture Notes Comput. Sci.*, **1719**, 211–220. Springer, Berlin, 1999.

[62] Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A. Linear recurring sequences over rings and modules. *J. of Math. Sciences*, **76** (1995), № 6, 2793–2915.

[63] V. L. Kurakin, A. S. Kuzmin A., and A. A. Nechaev. Codes and linear recurrences over Galois rings and QF-modules of the characteristic 4. Sixth International Workshop "Algebraic and Combinatorial Coding Theory" (ACCT-VI). Proceedings. September 6–12, 1998, Pskov, Russia. 166–171.

[64] V. L. Kurakin, A. V. Mikhalev, and A. A. Nechaev. Polylinear recurring sequences over a bimodule. In: Formal Power Series and Algebraic Combinatorics, 12-th Intern. Conf. FPSAC'00, Moscow, June 2000, Proceedings, 484–495. Springer, 2000.

[65] Kurakin V. L., Mikhalev A. V., Nechaev A. A., and Tsypyschev V. N. Linear and polylinear recurring sequences over abelian groups and modules. *J. of Math. Sciences*, **102** (2000), № 6, 4598–4627.

[66] Kurakin V. L. and Nechaev A. A. Quasi-Frobenius bimodules of functions on a semigroup. *Communications in Algebra*, **29** (2001), № 9, 4079–4094.

[67] MacWilliams F. J., Sloane N. J. A. Pseudo-random sequences and arrays. *Proc. IEEE.* **64** (1976), № 11, 1715-1729.

[68] McCoy N. H. *Rings and ideals.* Carus Mathematical Monographs, № 8. Math. Assoc. Amer., Menasha, WI: George Banta, 1962.

[69] B. R. McDonald. *Finite rings with identity.* New York, Marcel Dekker, 1974, 429 p.

[70] Morita K. Duality for modules and its applications to the theory of rings with minimum condition. *Sci. Rpts Tokyo Kyoiku Daigaku*, **A6** (1958), № 15, May, 83–142.

[71] Nathanson M. B. Difference operators and periodic sequences over finite modules. *Acta Math. Acad. Hungar.*, **28** (1976), № 3–4, 219–224.

[72] Nechaev A. A. Linear codes over finite rings and QF-modules. *Proceedings of the IV-th Int. Workshop on Algebraic and Combinatorial Coding Theory.* Novgorod, Sept. 1994, 154–157. Sofia, Zakrila, 1994.

[73] Nechaev A. A. Polylinear recurring sequences over modules and quasi-Frobenius modules. *Proc. First Int. Tainan–Moscow Algebra Workshop*, 1994, 283–298. Walter de Gruyter & Co., Berlin–N. Y., 1996.

[74] Nechaev A. A. Linear codes over modules and over spaces. Mac-Williams identity. *Proceedings of the 1996 IEEE Int. Symp. Inf. Theory and Appl.*, Victoria B. C., Canada, 1996, 35–38.

[75] Nechaev A. A., Kuzmin A. S. Linearly presentable codes. *Proceedings of the 1996 IEEE Int. Symp. Inf. Theory and Appl.*, Victoria B. C., Canada, 1996, 31–34.

[76] Nechaev A. A., Kuzmin A. S. Trace-function on a Galois ring in coding theory. *Lecture Notes Comput. Sci.*, **1255**, 277–290. Springer, Berlin, 1997.

[77] Niederreiter H. Distribution properties of feedback shift register sequences. *Probl. Control and Inform. Theory*, **15**, № 1, 1986, 19–34.

[78] Nomura T., Miyakawa H., Imai H., Fukuda A. A theory of two-dimensional linear recurring arrays. *IEEE Trans. Inform. Theory*, **18** (1972), № 6, 775–785.

[79] Sakata S. General theory of doubly periodic arrays over an arbitrary finite field and its applications. *IEEE Trans. Inform. Theory*, **24** (1978), 719–730.

[80] S. Sakata. Synthesis of two-dimensional linear feedback shift-registers and Groebner bases. *Applied algebra, algebraic algorithms and error-correcting codes* (AAECC), 1987. *Lecture Notes in Comput. Sci.*, **356**, 394–407. Springer, Berlin, 1989.

[81] S. Sakata. Extension of the Berlekamp—Massey algorithm to $N$ dimensions. *Inform. and Comput.*, **84** (1990), № 2, 207–239.

[82] S. Sakata. Two-dimensional shift register synthesis and Groebner bases for polynomial ideals over an integer residue ring. *Discr. Appl. Math.*, **33** (1991), № 1–3, 191–203.

[83] Selmer E. S. *Linear recurrence relations over finite fields.* Univ. of Bergen, Norway, 1966.

[84] Ward M. The arithmetical theory of linear recurring series. *Trans. Amer. Math. Soc.*, **35** (1933), № 3, 600–628.

[85] Ward M. Arithmetical properties of sequences in rings. *Ann. Math.*, **39** (1938), 210–219.

# Криптографические свойства дискретных функций

О. А. Логачев, А. А. Сальников, В. В. Ященко

Дискретные функции как математический объект, моделирующий преобразования информации в потоковых и блочных криптосистемах с симметричным ключом, очень удобен и позволяет привлечь разнообразный математический аппарат для анализа этих преобразований.

Как правило, дискретные функции, рассматриваемые в криптографических исследованиях, представляют собой отображения конечных алгебраических объектов (множеств, групп, колец, полей, векторных пространств и т. п.).

Исторически так сложилось, что один класс дискретных функций подвергся во второй половине XX века более систематическим и всесторонним криптографическим исследованиям. Это класс булевых функций и булевых отображений. Причиной тому явилось широкое использование этого вида преобразований в реальных криптографических системах. Результаты математических исследований криптографических свойств булевых функций и отображений являются наиболее полными и глубокими. Исследования криптографических свойств других классов дискретных функций носят фрагментарный характер и в ряде случаев служат лишь демонстрацией возможности распространения имеющихся результатов на более общие алгебраические структуры. Центральное место в обзоре уделено именно криптографическим свойствам булевых функций.

Источником исследований криптографических свойств булевых функций и отображений явились сформулированные в 1949 году Клодом Шенноном [157] принципы построения преобразований информации для криптографических систем. Важнейшими из них являются:

- принцип *«перемешивания»* — К.Шеннон дает неформальную трактовку хорошо известного в эргодической теории понятия для систем с конечным числом состояний;
- принцип *«рассеивания»* (diffusion), посредством которого «...статистическая структура сообщений, которая приводит к избыточности в сообщениях, "распыляется" в статистику больших длин, то есть в статистическую структуру, включающую длинные комбинации букв криптограмм»;
- принцип *«запутывания»* (confusion), который «состоит в том, что соотношения между простыми статистиками в пространстве криптограмм и простыми подмножествами в пространстве ключей делаются весьма сложными и беспорядочными».

К.Шеннон сформулировал свои принципы как эмпирические и не носящие формально-математического характера. Однако, эти принципы К.Шеннона вместе с постоянно развивающимися методами криптографического анализа позволили во второй половине XX века сформулировать и изучить ряд математически строго формализованных криптографических свойств дискретных функций.

Булево отображение (далее просто — отображение) $\Phi : \mathbb{F}_2^n \to \mathbb{F}_2^m$, $n > 0$, $m > 0$ — это отображение конечномерных векторных пространств над полем $\mathbb{F}_2$ из двух элементов. В частном случае, когда $m = 1$ мы получаем булеву функцию (далее — просто функцию) от $n$ переменных. Отображение $\Phi$ может в координатном виде быть представлено как система булевых функций $\Phi = (f_1, f_2, \ldots, f_m)$ от $n$ переменных, $f_i$ — $i$-тая координатная функция.

Простейшим криптографическим свойством является *уравновешенность* (balancedness) отображения $\Phi$: при $n \geqslant m$, для любого $\boldsymbol{v} \in \mathbb{F}_2^m$ выполнено условие — $\#\{\, \boldsymbol{u} \in \mathbb{F}_2^n \mid \Phi(\boldsymbol{u}) = \boldsymbol{v} \,\} = 2^{n-m}$ ($\#M$ — мощность множества $M$). Это свойство в случае $n = m$ равносильно взаимной однозначности отображения, что необходимо при реализации функций шифрования/расшифрования, а при $n > m$

Работа поддержана Российским фондом фундаментальных исследований (номера проектов 02-01-00581 и 02-01-00687).

это свойство отображений позволяет реализовывать последовательности с хорошими криптографическими качествами.

Линейность той или иной математической задачи предопределяет, как правило, наличие эффективных методов и алгоритмов ее решения. Поэтому в исследованиях по разработке и обоснованию криптографических систем «нелинейность» (как общее понятие) используемых преобразований информации является их фундаментальным и неотъемлемым качеством. Конкретная же трактовка «нелинейности» и описывающие ее параметры могут быть достаточны разнообразны.

Важнейшим криптографическим параметром функции $f$ от $n$ переменных является ее расстояние по Хэммингу до множества аффинных функций от $n$ переменных

$$\begin{aligned}&\operatorname{dist}(f,\mathcal{A}_n)=\\&\quad=\min_{l_{\boldsymbol{a},b}\in\mathcal{A}_n}\{\operatorname{dist}(f,l_{\boldsymbol{a},b})\mid l_{\boldsymbol{a},b}=\langle\boldsymbol{a},\boldsymbol{x}\rangle\oplus b\in\mathcal{A}_n,\ \boldsymbol{a}\in\mathbb{F}_2^n,b\in\mathbb{F}_2\}\ ,\end{aligned}$$

$\langle\boldsymbol{a},\boldsymbol{x}\rangle=a^{(1)}x^{(1)}\oplus\ldots\oplus a^{(1)}x^{(1)}$ — скалярное произведение. Очевидно, что этот параметр характеризует имеющуюся у криптоаналитика возможность эффективного приближения исследуемой функции ее аффинным аналогом. Это расстояние называется [112] *нелинейностью* (nonlinearity) функции $f$ и обозначается

$$N_f=\min_{l_{\boldsymbol{a},b}\in\mathcal{A}_n}\{\operatorname{dist}(f,l_{\boldsymbol{a},b})\mid l_{\boldsymbol{a},b}=\in\mathcal{A}_n\}\ .$$

Этот параметр остается инвариантным относительно группы всех аффинных преобразований пространства $\mathbb{F}_2^n$. Обычно наличие в наличие в тексте статей символа $N_f$ говорит о том, что речь идет о нелинейности функции, как расстоянии от аффинных функций, а значит не о «нелинейности» в каком-либо другом смысле. Разночтений при этом, как правило, не возникает.

Расстояние по Хэммингу от функции $f$ до множества аффинных функций связано следующим соотношением с коэффициентами преобразования Уолша-Адамара

$$\operatorname{dist}(f,\mathcal{A}_n)=2^{n-1}-\frac{1}{2}\max_{\boldsymbol{a}\in\mathbb{F}_2^n}\left|W_f(\boldsymbol{a})\right|\ ,$$

где $W_f(\boldsymbol{a})=\sum\limits_{\boldsymbol{x}\in\mathbb{F}_2^n}(-1)^{f(\boldsymbol{x})\oplus\langle\boldsymbol{a},\boldsymbol{x}\rangle}$ — преобразование Уолша-Адамара. Из равенства Парсеваля

$$\sum_{\boldsymbol{a}\in\mathbb{F}_2^n}\Big(W_f(\boldsymbol{a})\Big)^2=2^{2n}$$

следует, что для любой функции $f$ выполнено неравенство

$$\max_{\boldsymbol{a}\in\mathbb{F}_2^n}\left|W_f(\boldsymbol{a})\right|\geqslant 2^{n/2}\ .$$

Те функции, для которых последнее неравенство обращается в равенство дальше всех других функций удалены от множества аффинных функций $\mathcal{A}_n$. Функция $f$ называется *максимально нелинейной* [110, 112] (или *бент-функцией* в комбинаторной трактовке, связанной с разностными множествами [66, 67, 111, 139]), если все коэффициенты Уолша-Адамара этой функции равны $\pm 2^{\frac{n}{2}}$. Поскольку коэффициенты Уолша-Адамара являются целыми числами, то при нечетном $n$ максимально нелинейных функций не существует. В трактовке теории кодирования аффинные функции представляют собой код Рида-Маллера 1-го порядка $\mathcal{A}_n=RM_2(n,1)$. На этом языке и языке упаковок максимально нелинейные функции являются «глубокими дырами» [61] кода $RM_2(n,1)$, а нелинейность таких функций $N_f=2^{n-1}-2^{\frac{n}{2}-1}$ совпадает с радиусом покрытия $\rho(n,1)$ кода $RM_2(n,1)$. Максимально нелинейные функции являются привлекательным математическим объектом и обладают рядом интересных свойств.

- Производная [2] максимально нелинейной функции

$$D_{\boldsymbol{a}}f(\boldsymbol{x})=f(\boldsymbol{x})\oplus f(\boldsymbol{x}\oplus\boldsymbol{a})$$

по любому ненулевому направлению $\boldsymbol{a}\in\mathbb{F}_2^n$ является уравновешенной функцией.

- Функция $\widetilde{f}$, определяющая знаки коэффициентов Уолша-Адамара

$$W_f(\boldsymbol{a}) = (-1)^{\widetilde{f}(\boldsymbol{a})} \cdot 2^{n/2}$$

максимально нелинейной функции $f$, сама является максимально нелинейной.

- Степень нелинейности $\deg f$ (степень нелинейности алгебраической нормальной формы — многочлена Жегалкина, представляющего $f$) не превосходит $\frac{n}{2}$.

- Множество максимально нелинейных функций инвариантно относительно действия элементов полной аффинной группы $\mathfrak{GA}(2,n)$ на пространстве $\mathbb{F}_2^n$.

В настоящее время построен целый ряд классов максимально нелинейных функций [6, 10, 40, 41, 42, 47, 48, 49, 66, 67, 69, 111, 118, 146, 147]. Эти результаты позволяют получать нижние оценки мощности всего множества максимально нелинейных функций. Однако, подсчет точного числа максимально нелинейных функций остается на сегодня открытой проблемой.

В работах [119, 122, 134] рассмотрено обобщение свойства максимальной нелинейности на булевы отображения и построены некоторые классы таких отображений. Отметим также работы [51, 78, 101, 126, 168], в которых исследуются свойства бент-последовательностей, находящих приложения в теории связи.

Несмотря на свои привлекательные криптографические свойства, максимально нелинейные функции являются неидеальными объектами и не используются при синтезе криптосхем, поскольку не являются уравновешенными. Кроме того, как уже отмечалось, максимально нелинейные функции существуют лишь при четном числе переменных. В связи с этим в настоящее время сформировалось и активно развивается направление исследований, связанное с построением для четного $n$ уравновешенных функций, нелинейность которых удовлетворяет неравенствам

$$2^{n-1} - 2^{n/2} \leqslant N_f < 2^{n-1} - 2^{n/2-1} \ ,$$

то есть функций, нелинейность которых близка к минимально возможной $\rho(n,1)$. Некоторые результаты в этом направлении можно найти в работах [10, 11, 28, 39, 43, 73, 171, 181]. В случае нечетного $n$ вычисление радиуса покрытия кода $RM_2(n,1)$ в общем случае остается открытой проблемой. Однако известно [37, 74, 116, 136], что для нечетных $n$:

$$\rho(n,1) = 2^{n-1} - 2^{(n-1)/2}$$

при $n = 3, 5, 7$, и

$$2^{n-1} - 2^{(n-1)/2} \leqslant \rho(n,1) < 2^{n-1} - 2^{n/2-1}$$

при $n \geqslant 9$.

Эти неравенства позволяют строить и исследовать классы функций, нелинейность которых близка к $\rho(n,1)$. Необходимо также отметить, что понятия, аналогичные максимальной нелинейности (но, в ряде случаев, не полностью с ним совпадающие) имеют место для отображений над различными алгебраическими структурами: кольцами вычетов, конечными полями, кольцами Галуа, конечными группами и т.п. Результаты исследований в этом направлении можно найти в работах [1, 8, 16, 58, 89].

Понятие нелинейности функции естественным образом распространяется на случай отображений. Нелинейность $N_\Phi$ отображения $\Phi = (f_1, f_2, \ldots, f_m)$ определяется как нелинейность нетривиальной линейной комбинации координатных функций этого отображения, которая максимально близка к аффинным функциям:

$$N_\Phi = \min \Big\{ N_f \mid f = c^{(1)} f_1 \oplus \ldots \oplus c^{(m)} f_m \ , \\ \left(c^{(1)}, \ldots, c^{(m)}\right) \in \mathbb{F}_2^m \setminus \{(0, \ldots, 0)\} \Big\} \ .$$

Разработка иных концепций нелинейности булевых функций привела к идее *строго лавинного критерия* (strict avalanche criteria, SAC), родившейся при изучении проблем конструирования так называемых S-блоков [65, 75, 166]. На качественном уровне, выполнение этого критерия для некоторой функции означает, что минимальные изменения ее аргументов приводят к тому, что получающиеся значения функции не коррелируют со значениями функции на неизмененных аргументах. Более строго,

говорят, что функция $f$ удовлетворяет строгому лавинному критерию SAC, если для любого вектора $\boldsymbol{u}$ из $\mathbb{F}_2^n$, вес Хэмминга которого равен 1, производная $D_{\boldsymbol{u}}f$ функции $f$ по этому направлению является уравновешенной функцией (другими словами, автокорреляционная функция $\Delta_f(\boldsymbol{u}) = \sum\limits_{\boldsymbol{x}\in\mathbb{F}_2^n} (-1)^{D_{\boldsymbol{u}}f(\boldsymbol{x})}$ равна нулю на всех векторах веса 1). Дальнейшее развитие исследований в этом направлении привело к появлению понятия *строго лавинного критерия порядка* $k$, $1 \leqslant k < n$ (SAC($k$)) [75, 98]. Говорят, что функция $f$ удовлетворяет строгому лавинному критерию порядка $k$, если любая ее подфункция, полученная фиксацией $k$ переменных:

$$f_{i_1,\ldots,i_k}^{a^{(1)},\ldots,a^{(k)}}\left(x^{(1)},\ldots,x^{(i_1-1)},x^{(i_1+1)},\ldots,x^{(i_k-1)},x^{(i_k+1)},\ldots,x^{(n)}\right) =$$
$$= f\left(x^{(1)},\ldots,x^{(i_1-1)},a^{(1)},x^{(i_1+1)},\ldots,x^{(i_k-1)},a^{(k)},x^{(i_k+1)},\ldots,x^{(n)}\right) \ ,$$

где $1 \leqslant i_1 < \ldots < i_k \leqslant n$, $a^{(1)},\ldots,a^{(k)} \in \mathbb{F}_2$ — произвольны, удовлетворяет обычному строгому лавинному критерию SAC. Логика исследований благодаря аналогиям в строении автокорреляционных функций для максимально нелинейных функций и функций, удовлетворяющих строгим лавинным критериям SAC и SAC($k$), привела к формулировке *критерия распространения степени* $l$ (PC($l$)), $1 < l \leqslant n$ [137]. Функция $f$ удовлетворяет критерию распространения степени $l$, если ее производная $D_{\boldsymbol{u}}f$ является уравновешенной функцией для любого ненулевого направления $\boldsymbol{u} \in \mathbb{F}_2^n$ веса не больше $l$: $1 \leqslant \mathrm{wt}(\boldsymbol{u}) \leqslant l$ (другими словами, автокорреляционная функция $\Delta_f(\boldsymbol{u})$ равна нулю на всех таких векторах). Дальнейшее развитие этого понятие привело к формулировке *критерия распространения степени* $l$ *порядка* $k$ (PC($l$, $k$)), $1 < l \leqslant n$, $1 \leqslant k < n$ [91]. Функция $f$ удовлетворяет критерию распространения степени $l$ порядка $k$, если любая ее подфункция, полученная фиксацией $k$ переменных:

$$f_{i_1,\ldots,i_k}^{a^{(1)},\ldots,a^{(k)}}$$

где $1 \leqslant i_1 < \ldots < i_k \leqslant n$, $a^{(1)},\ldots,a^{(k)} \in \mathbb{F}_2$ — произвольны, удовлетворяет критерию распространения степени $l$. Очевидно, что строгий лавинный критерий SAC эквивалентен критерию распространения степени 1 PC(1), а максимальная нелинейность функции эквивалентна критерию распространения степени $n$ PC($n$).

Параллельно с формулировкой и исследованием этих критериев шло развитие способов построения высоко нелинейных уравновешенных функций, удовлетворяющих критерию распространения [150, 154]. Как правило, эти способы представляют собой достаточно простую суперпозицию функций, обладающих высокой нелинейностью от меньшего числа переменных. Пусть $f$ — максимально нелинейная функция от $n = 2k$ переменных и пусть $g$ — функция от $n+1 = 2k+1$ переменных, задаваемая соотношением

$$g\left(x^{(1)},\ldots,x^{(2k+1)}\right) =$$
$$= \left(1 \oplus x^{(1)}\right) f\left(x^{(2)},\ldots,x^{(2k+1)}\right) \oplus x^{(1)}\left(1 \oplus f\left(x^{(2)},\ldots,x^{(2k+1)}\right)\right) =$$
$$= x^{(1)} \oplus f\left(x^{(2)},\ldots,x^{(2k+1)}\right) \ ,$$

является уравновешенной и удовлетворяет критерию распространения относительно всех ненулевых векторов $\boldsymbol{u} \in \mathbb{F}_2^{2k+1}$, за исключением вектора $(1,0,\ldots,0)$. Нелинейность $N_g$ функции $g$ удовлетворяет неравенству

$$N_g \geqslant 2^{2k} - 2^k \ .$$

В качестве другого примера можно привести функцию $g$ от $n = 2k+1$ переменных, задаваемую соотношением

$$g\left(x^{(1)},\ldots,x^{(2k+1)}\right) = x^{(1)} \oplus f\left(x^{(1)} \oplus x^{(2)},\ldots,x^{(1)} \oplus x^{(2k+1)}\right) \ ,$$

где $f$ — максимально нелинейная функция от $n$ переменных. Заданная таким образом функция $g$ удовлетворяет критерию распространения степени $2k$ PC($2k$). Нелинейность $N_g$ функции $g$ также удовлетворяет неравенству

$$N_g \geqslant 2^{2k} - 2^k \ .$$

Одновременно с развитием критериев, позволяющих говорить о положительных криптографических качествах функций и отображений, естественно выделялись свойства, свидетельствующие о их

криптографических слабостях. Одним из таких свойств стало наличие у отображения (функции) *линейных структур* [9, 53, 70, 93]. Говорят, что вектор $\boldsymbol{u} \in \mathbb{F}_2^n$ является линейной структурой отображения $\Phi : \mathbb{F}_2^n \to \mathbb{F}_2^m$, если выполнено равенство

$$\Phi(\boldsymbol{x}) \oplus \Phi(\boldsymbol{x} \oplus \boldsymbol{u}) = \boldsymbol{c} = \text{const} \ , \quad \boldsymbol{c} \in \mathbb{F}_2^m \ .$$

Все линейные структуры отображения $\Phi$ образуют подпространство линейных структур $L_\Phi$ в пространстве $\mathbb{F}_2^n$. Наличие (или отсутствие) линейных структур у отображения инвариантно относительно действия на отображение полной аффинной группы. Кроме того, отображение $\Phi$, обладающее ненулевым подпространством линейных структур $L_\Phi$, $\dim L_\Phi = r$, $1 \leqslant r \leqslant n$, подходящим невырожденным линейным преобразованием $A$ может быть приведено к виду

$$\Phi'\left(x^{(1)}, \ldots, x^{(n)}\right) = \Phi\left(\left(x^{(1)}, \ldots, x^{(n)}\right) A\right) = \\ = x^{(1)}\boldsymbol{v}_1 \oplus \ldots \oplus x^{(r)}\boldsymbol{v}_r \oplus \Phi''\left(x^{(r+1)}, \ldots, x^{(n)}\right) \ ,$$

где $\boldsymbol{v}_i \in \mathbb{F}_2^m$, $1 \leqslant i \leqslant r$, а отображение $\Phi'' : \mathbb{F}_2^{n-r} \to \mathbb{F}_2^m$ не имеет ненулевых линейных структур.

Свойства корреляционной иммунности и устойчивости отображений истоками своими имеют несколько совершенно различных криптографических задач. Однако, внутренние сущностные (с точки зрения математики) особенности этих задач находят свое выражение в одинаковых вполне определенных и легко формулируемых количественных (числовых) характеристиках булевых функций и отображений.

Понятие *корреляционной иммунности* (correlation immunity) булевой функции [159, 160, 167] отражает способность противостоять корреляционному методу анализа потокового шифра, построенного на ее основе. Не вдаваясь в детали этого криптографического метода, можно сказать, что это свойство означает отсутствие какой-либо информации в известном значении функции о значениях некоторого подмножества ее аргументов, на которых это значение получено. Естественно, что это свойство формулируется в условиях определенной вероятностно-статистической модели.

Концепция *устойчивых* (resilient) отображений [29, 31, 177] была предложена при разработке отображений, связанных с такими областями исследований как распределенные вычисления, устойчивые относительно ошибок, а также с разработкой протоколов выработки общих ключей в квантово-криптографических каналах связи. Сущностным свойством устойчивых отображений является их способность сохранять свойство уравновешенности при ограничениях специального вида их области определения.

Пусть $f$ — функция от $n$ переменных, $X^{(1)}, X^{(2)}, \ldots, X^{(n)}$ — независимые одинаково распределенные равновероятные двоичные случайные величины:

$$P\left\{X^{(i)} = 1\right\} = P\left\{X^{(i)} = 0\right\} = \frac{1}{2}, \quad i = 1, 2, \ldots, n \ .$$

Тогда, несложно видеть, что двоичная случайная величина

$$Z = f\left(X^{(1)}, X^{(2)}, \ldots, X^{(n)}\right)$$

распределена следующим образом:

$$P\{Z = 1\} = \frac{\mathrm{wt}(f)}{2^n} \ , \qquad P\{Z = 0\} = 1 - \frac{\mathrm{wt}(f)}{2^n} \ .$$

Булева функция $f\left(x^{(1)}, x^{(2)}, \ldots, x^{(n)}\right)$ называется корреляционно-иммунной порядка $m$, $0 < m \leqslant n$, если для любого набора $1 \leqslant i_1 < i_2 < \ldots < i_m \leqslant n$ взаимная информация случайных величин $X^{(i_1, \ldots, i_m)} = \left(X^{(i_1)}, X^{(i_2)}, \ldots, X^{(i_m)}\right)$ и $Z$ равна нулю:

$$I\left(X^{(i_1, \ldots, i_m)}, Z\right) = 0 \ .$$

Это равносильно тому, что для любого набора $1 \leqslant i_1 < i_2 < \ldots < i_m \leqslant n$ случайные величины $X^{(i_1, \ldots, i_m)} = \left(X^{(i_1)}, X^{(i_2)}, \ldots, X^{(i_m)}\right)$ и $Z$ независимы.

Несложно видеть, что при $m = n$ корреляционно-иммунными функциями порядка $n$ являются только функции-константы: $f \equiv 0$ и $f \equiv 1$.

Это криптографическое свойство находит свое отражение в ряде числовых характеристик функций в виде критериальных утверждений. Функция $f$ является корреляционно-иммунной порядка $m$, тогда и только тогда, когда для любых наборов $1 \leqslant i_1 < i_2 < \ldots < i_m \leqslant n$, $a^{(1)}, \ldots, a^{(m)} \in \mathbb{F}_2$ выполняется равенство

$$\mathrm{wt}\left(f_{i_1,\ldots,i_k}^{a^{(1)},\ldots,a^{(k)}}\right) = \frac{\mathrm{wt}(f)}{2^m} \ .$$

Справедлива также следующая спектральная характеризация корреляционно-иммунных функций на языке коэффициентов Уолша-Адамара. Функция $f$ является корреляционно-иммунной порядка $m$, тогда и только тогда, когда $W_f(\boldsymbol{u}) = 0$ для всех векторов $\boldsymbol{u}$ из $\mathbb{F}_2^n$ таких, что $1 \leqslant \mathrm{wt}(\boldsymbol{u}) \leqslant m$. Корреляционно иммунные порядка $m$ функции являются также корреляционно иммунными и меньшего порядка. Свойство корреляционной иммунности инвариантно относительно действия на функцию группы Джевонса $\mathfrak{D}_n$. Однако, максимальная группа, относительно которой свойство корреляционной иммунности инвариантно, не известна. Корреляционная иммунность накладывает на функцию ряд ограничений. В частности, если $f$ — корреляционно-иммунная порядка $m$ функция, то выполнено неравенство

$$\deg f \leqslant n - m \ .$$

Более того, если $f$ — уравновешенная корреляционно-иммунная порядка $m$ функция, то выполнено неравенство

$$\deg f \leqslant n - m - 1 \ .$$

Единственными функциями от $n$ переменных отличными от констант, достигающими максимального порядка корреляционной иммунности $n-1$ являются функции

$$l_{1,0}\left(x^{(1)}, \ldots, x^{(n)}\right) = x^{(1)} \oplus \ldots \oplus x^{(n)} \ ,$$
$$l_{1,1}\left(x^{(1)}, \ldots, x^{(n)}\right) = x^{(1)} \oplus \ldots \oplus x^{(n)} \oplus 1 \ .$$

В настоящее время известен целый ряд конструкций [35, 54, 107, 151, 159], используемых для построения корреляционно-иммунных функций. В работе [39] показано, что можно строить устойчивые (уравновешенные корреляционно-иммунные) функции с нелинейностью строго большей $2^{n-1} - 2^{\lceil \frac{n-1}{2} \rceil}$. Кроме детерминированных конструкций использовались также и эвристические алгоритмы поиска корреляционно-иммунных функций [72, 113, 127]. Оказалось, что эти алгоритмы хорошо работают при построении таких функций от сравнительно небольшого числа переменных. В работах [143, 163, 178] с помощью различных подходов получены верхние оценки нелинейности устойчивых функций. Несколько позже были опубликованы работы [45, 50]. В работе [163] установлено, что если функция достигает верхней границы нелинейности, то она должна иметь максимально возможную алгебраическую степень нелинейности. Полученные результаты выделили класс «оптимальных» функций, т.е. функций от $n$ переменных $m$-устойчивых алгебраической степени нелинейности $d = n - m - 1$, достигающих верхней границы нелинейности. В работе [163] предложен рекурсивный алгоритм порождения «оптимальных» функций. Эта конструкция была проанализирована в [71, 164] и модифицирована в [129]. Однако, детерминированные конструкции, предложенные в [71, 129, 163, 164], не давали возможности получать некоторые классы функций от небольшого числа переменных. Комбинаторные результаты и компьютерный поиск использованы в [59, 105, 129] для получения таких функций. Перечислительные вопросы для корреляционно-иммунных функций рассматривались в работах [3, 106, 108, 114, 115, 156, 169]. Достаточно полное и сжатое изложение вопросов, связанных с исследованиями свойств корреляционно-иммунных функций можно найти в [19, 46, 140].

Отображение $\Phi = (f_1, \ldots, f_k)$ из $\mathbb{F}_2^n$ в $\mathbb{F}_2^k$ называется $(n,k,d)$-*устойчивым*, если для любых наборов $1 \leqslant j_1 < \ldots < j_d \leqslant d$, $\left(a^{(1)}, \ldots, a^{(d)}\right) \in \mathbb{F}_2^d$ отображение

$$\Phi_{j_1,\ldots,j_d}^{a^{(1)},\ldots,a^{(d)}} = \left((f_1)_{j_1,\ldots,j_d}^{a^{(1)},\ldots,a^{(d)}}, \ldots, (f_k)_{j_1,\ldots,j_d}^{a^{(1)},\ldots,a^{(d)}}\right)$$

из $\mathbb{F}_2^{n-d}$ в $\mathbb{F}_2^k$ является уравновешенным. Очевидно, что для любого $(n,k,d)$-устойчивого отображения выполняется неравенство $n - d \geqslant k$. Легко видеть, что уравновешенная функция $f$ корреляционно иммунна порядка $d$ тогда и только тогда, когда она является $(n,1,d)$-устойчивым отображением.

Существуют глубокие связи между свойством устойчивости отображения и корреляционной иммунностью координатных функций. Отображение $\Phi = (f_1, \ldots, f_k)$ из $\mathbb{F}_2^n$ в $\mathbb{F}_2^k$, $n \geqslant k \geqslant 1$ является $(n, k, d)$-устойчивым тогда и только тогда, когда для любого ненулевого набора $(b^{(1)}, \ldots, b^{(k)})$ из $\mathbb{F}_2^k$ функция $f = \bigoplus_{i=1}^{k} b^{(i)} f_i$ является $(n, 1, d)$-устойчивой, то есть уравновешенной корреляционно иммунной функцией порядка $d$. Приведем примеры устойчивых линейных отображений.

1. $k = n-1$, $d = 1$, $\Phi(\boldsymbol{x}) = \big(f_1(\boldsymbol{x}), f_2(\boldsymbol{x}), \ldots, f_{n-1}(\boldsymbol{x})\big)$, $f_i(\boldsymbol{x}) = x^{(i)} \oplus x^{(i+1)}$, $i = 1, 2, \ldots, n-1$;
2. $n = 3h$, $k = 2$, $d = 2h-1$ $\Phi(\boldsymbol{x}) = \big(f_1(\boldsymbol{x}), f_2(\boldsymbol{x})\big)$, $f_1(\boldsymbol{x}) = x^{(1)} \oplus \ldots \oplus x^{(2h)}$, $f_2(\boldsymbol{x}) = x^{(h+1)} \oplus \ldots \oplus x^{(3h)}$.

Важными и интересными являются вопросы существования устойчивых отображений для различных наборов значений параметров $n$, $k$ и $d$. В случае линейных устойчивых отображений эта проблема имеет теоретико-кодовую трактовку. Существование $(n, k, d)$-устойчивого отображения эквивалентно существованию линейного $(n, k, d+1)$-кода [29, 162]. В общем случае корреляционно иммунные функции и устойчивые отображения связаны с хорошо известным комбинаторным объектом — *ортогональными таблицами* (orthogonal array) [161, 162]. Ортогональной таблицей размера $m$ с $n$ ограничениями уровня 2 (в нашем случае), силы $t$ и индекса $\nu$ называется таблица $M$ размера $m \times n$ над полем $\mathbb{F}_2$, обладающая следующим свойством. В любом подмножестве из $t$ столбцов матрицы $M$ любой из $2^t$ векторов пространства $\mathbb{F}_2^t$ встречается как строка ровно $\nu$ раз. Такая таблица обозначается как $OA_\nu(m, n, 2, t)$. Из количественных соображений ясно, что выполнено равенство $m = \nu \cdot 2^t$, то есть параметр $m$ однозначно определяется по параметрам $\nu$ и $t$.

Для функции $f$ через $M_f$ обозначим матрицу размера $\mathrm{wt}(f) \times n$, строками которой являются наборы из $\mathbb{F}_2^n$, значение функции на которых равно 1 (так называемая таблица истинности функции $f$). Функция $f$ от $n$ переменных корреляционно иммунна порядка $t$ тогда и только тогда, когда ее таблица истинности является ортогональной таблицей $OA_\nu(\mathrm{wt}(f), n, 2, t)$.

*Покрывающим множеством ортогональных таблиц* (large set orthogonal arrays) над полем $\mathbb{F}_2$ называется множество из $\dfrac{2^{n-t}}{\nu}$ ортогональных таблиц над полем $\mathbb{F}_2$ — $OA_\nu(m, n, 2, t)$, $m = \nu \cdot 2^t$ таких, что каждый набор из $\mathbb{F}_2^n$ встречается ровно в одной таблице. Из определения видно, что $\nu$ является степенью двойки. Кроме того, ясно, что объединение таблиц из покрывающего множества дает нам тривиальную ортогональную таблицу $OA_1(2^n, n, 2, n)$, соответствующую таблице всех наборов из $\mathbb{F}_2^n$.

Отображение $\Phi$ является $(n, k, t)$-устойчивым тогда и только тогда, когда прообразы $\big\{\Phi^{-1}(\boldsymbol{y}), \boldsymbol{y} \in \mathbb{F}_2^k\big\}$ представляют собой покрывающее множество из $2^k$ ортогональных таблиц $OA_{2^{n-k-t}}(2^{n-k}, n, 2, t)$.

Необходимо отметить ряд работ, в которых понятия корреляционной иммунности и устойчивости распространяются с булева случая на случай функций над другими алгебраическими структурами [32, 33, 34, 44].

Еще одной концепцией нелинейности отображений векторных пространств является понятие индекса линейности отображения, основанное на возможности представления исходного отображения в виде разветвления линейных отображений. Хотя принцип разветвления был неявно использован при исследовании некоторых свойств булевых функций [46, 139], само понятие индекса линейности рассмотрено в [11, 22].

В работе [18] исследованы вопросы решения систем булевых уравнений вида

$$\begin{cases} y^{(i)} = f\big(x^{(i)}, \ldots, x^{(i+n-1)}\big)\,, \\ y^{(i)} \in \mathbb{F}_2\,, \quad i = 1, 2, \ldots, N \end{cases}$$

при произвольном натуральном $N$. Выделен класс булевых функций, названных «сильно равновероятными», для которых данная система разрешима при любом $N$.

Изучение этих и других криптографических свойств происходит с использованием различных представлений булевых функций, таких как алгебраическая нормальная форма, числовая нормальная форма, полиномиальное представление с помощью расширения поля из двух элементов, представление с помощью графов и др. При анализе криптографических свойств функций и отображений используются глубокие результаты математической кибернетики, комбинаторного анализа и алгебры. Важную роль играют и экспериментальные исследования с использованием возможностей вычислительной техники.

Говоря о наиболее важных направлениях исследований в этой области, отметим следующие:

- описание канонических представителей важнейших классов булевых функций при рассмотрении действия на эти функции некоторых групп преобразований. Классический образец решения проблемы этого типа — теорема Диксона о приведении квадратичной булевой функции с помощью аффинной замены переменных к каноническому виду [110]; классификация булевых функций относительно различных групп [4, 5, 17].

- направление, связанное с исследованием конкретного криптографического свойства и построением широких классов булевых функций, обладающих данным свойством, а также построением функций, обладающих экстремальными параметрами;

- исследование криптографических свойств булевых функций, реализованных в конкретных криптографических системах;

- направление, связанное с преодолением противоречивости различных криптографических свойств функций, т.е. построение классов булевых функций, обладающих двумя или более необходимыми криптографическими свойствами;

- направление, связанное с обобщением имеющихся результатов на дискретные функции над другими алгебраическими системами [6, 12, 13].

Изучение свойств дискретных функций конкретных криптографических систем стало стандартной частью любого криптографического анализа. В то же время существует ряд задач, продвижение в решении которых позволит подняться на новый уровень понимания математической природы дискретных объектов. Из более конкретных проблем мы хотим в первую очередь выделить следующие:

- аффинная классификация булевых функций от $n \geqslant 6$ переменных;

- вычисление мощностей (или их оценки) некоторых классов булевых функций, например, булевых функций, обладающих свойством корреляционной иммунности заданного порядка, бент-функций и т.п.;

- описание групп инвариантности конкретных криптографических свойств;

- разработка алгоритмов аппроксимации произвольной функции функциями из заданного класса [15];

- дальнейшее изучение внутренних связей различных криптографических свойств булевых функций [21, 22].

Имеющийся в настоящее время набор криптографических свойств булевых функций и отображений ни в коем случае нельзя считать завершенным. Практика показывает, что развитие методов криптографического анализа вводило и будет вводить в криптографический оборот новые свойства.

Библиография научной литературы по этой проблематике показывает, что во всем мире насчитывается несколько десятков математиков работающих в данном направлении и регулярно публикующих свои результаты в периодических научных изданиях. Характер публикаций показывает, что это направление остается актуальным и привлекательным для научных работников.

## Литература

[1] Амбросимов А.С. *Свойства бент-функций q-значной логики над конечными полями.* // Дискретная математика. — 1994. — **Т. 6.** — 3. — С. 50–60.

[2] Бохманн Д., Постхоф Х. *Двоичные динамические системы.* — М.: Энергоатомиздат. — 1986. — 400 с.

[3] Денисов О.В. *Асимптотическая формула для числа корреляционно-иммунных порядка k булевых функций.* // Дискретная математика. — 1991. — **Т. 3.** — 2. — С. 25–46.

[4] Клосс Б.М., Нечипорук Э.Н. *О классификации функций многозначной логики.*// Проблемы кибернетики. — 9. — 1963.

[5] Кузнецов Ю.В., Шкарин С.А. *Коды Рида-Маллера (обзор публикаций).*// Математические вопросы кибернетики. — М.: Наука. — 6. — 1996. — С. 5–50.

[6] Кузнецов Ю. В., Ященко В. В. *О частичных бент-функциях.*// Вестник МГУ. — 2000. — 5. — С. 3–6.

[7] Лабунец В. Г., Ситников О. П. *Гармонический анализ булевых функций и функций k-значной логики над конечными полями.*// Техническая кибернетика. — 1975. — 1. — С. 141–148.

[8] Логачев О.А., Сальников А.А., Ященко В.В. *Бент-функции на конечной абелевой группе.*// Дискретная математика. — 1997. — **Т. 9.** — 4. — С. 3–20.

[9] Логачев О.А., Сальников А.А., Ященко В.В. *Невырожденная нормальная форма булевых функций.*// Доклады Академии наук. — 2000. — **Т. 373.** — 2. — С. 164–167.

[10] Логачев О.А., Сальников А.А., Ященко В.В. *Бент-функции и разбиения двоичного куба.*//12-th International Conference on Formal Power Series and Algebraic Combinatorics FPSAC'00. — M.: MSU. — 2000.

[11] Логачев О.А., Сальников А.А., Ященко В.В. *Некоторые характеристики «нелинейности» групповых отображений.*// Дискретный анализ и исследование операций. Серия 1. — 2001. — **Т. 8.** — 1. — С. 40–54.

[12] Логачев О.А., Сальников А.А., Ященко В.В. *Нормальная форма отображений конечных абелевых групп.*// Дискретная математика и ее приложения. — М.: МГУ. — 2001.

[13] Логачев О.А., Сальников А.А., Ященко В.В. *Оценки некоторых параметров отображений конечных абелевых групп.*// Дискретная математика и ее приложения. — М.: МГУ. — 2001.

[14] Рязанов Б. В. *О распределении спектральной сложности булевых функций.*// Дискретная математика. — 1994. — **Т. 6.** — 2. — С. 111–119.

[15] Рязанов Б. В., Чечета С. И. *О приближении случайной булевой функции семейством квадратичных форм.*// Дискретная математика. — 1995. — **Т. 7.** — 3. — С. 129–145.

[16] Солодовников В.И. *Бент-функции из конечной абелевой группы в конечную абелеву группу.*// Дискретная математика. — 2002. — **Т. 14.** — 1. — С. 99–113.

[17] Страдзинь И. Э. *Аффинная классификация булевых функций пяти переменных.*// Автоматика и вычислительная техника. — 1975. — 1. — С. 1–9.

[18] Сумароков С. Н. *Запреты двоичных функций и обратимость для одного класса кодирующих устройств.*// Обозрение прикладной и промышленной математики. — 1994. — 1. — С. 33–55.

[19] Тарапников Ю.В. *Числовые характеристики булевых функций.* — Дискретная математика и ее приложения I. Сборник лекций. — М.: Издательство МГУ. — 2001.

[20] Ященко В.В. *Свойства булевых отображений, сводимые к свойствам их координатных функций*// Вестник МГУ, серия Математика. — 1997. — 4. — С. 11–13.

[21] Ященко В.В. *О критерии распространения для булевых функций и о бент-функциях*// Проблемы передачи информации. — 1997. — **Т. 33.** — 1. — С. 75–86.

[22] Ященко В.В. *О двух характеристиках нелинейности булевых отображений.*// Дискретный анализ и исследование операций, серия 1. — 1998. — **Т. 5.** — 2. — С. 90–96.

[23] Adams C. M. *A formal and practical design procedure for Substitution-Permutation network cryptosystem:* Dissert.... Doct. Ph. — Queen's University at Kingston. Department of Electrical Engineering. — 1990.

[24] Adams C. M. *On immunity against Biham and Shamir's differential cryptanalysis.*// Information Processing Letters. — 1992. — **Vol. 41.** — P. 77–80.

[25] Adams C. M., Tavares S. E. *Good S-boxes are Easy to Find.*// Advances in Cryptology: CRYPTO'89/ Lect. Notes in Comput. Sci. — **Vol. 435.** — New York: Springer-Verlag. — 1990. — P. 612–615.

[26] Adams C. M., Tavares S. E. *The structured design of cryptographically good S-boxes.*// Journal of Crytology. — 1990. — **Vol. 3.** — 1. — P. 27–41.

[27] Adams C. M., Tavares S. E. *Generating and Counting Binary Bent Sequences.*// IEEE Trans. on Information Theory. — 1990. — **Vol. 36.** — 5. — P. 1170–1173.

[28] Akyildiz E., Guloglu I. S., Ikeda M. *A Note on Generalized Bent Functions.*// Journal of Pure and Applied Algebra. — 1996. —**Vol. 106.** — 1. — P. 1–9.

[29] Bennet C. H., Brassard G., Robert J. M. *Privacy Amplification by Public Discussion*// SIAM Journal on Computing. — 1988. — **Vol. 17.** — P. 210–229.

[30] Beth T., Ding C. *On Almost Perfect Nonlinear Permutations.*// Advances in Cryptology: EUROCRYPT'93/ Lect. Notes in Comput. Sci. — **Vol. 765.** — New York: Springer-Verlag. — 1993. — P. 65–76.

[31] Bierbrauer J., Gopalakrishnan K., Stinson D. R. *Bounds on Resilient Functions and Orthogonal Arrays.*// Advances in Cryptology: CRYPTO'94/ Lect. Notes in Comput. Sci. — **Vol. 839.** — New York: Springer-Verlag. — 1994. — P. 247–256.

[32] Camion P., Canteaut A. *Construction of t-Resilient Functions Over a Finite Alphabet.*// Advances in Cryptology: EUROCRYPT'96/ Lect. Notes in Comput. Sci. — **Vol. 1070.** — New York: Springer-Verlag. — 1996. — P. 283–293.

[33] Camion P., Canteaut A. *Generalization of Siegenthaler Inequality and Schnorr-Vaudenay Multipermutations.*// Advances in Cryptology: CRYPTO'96/ Lect. Notes in Comput. Sci. — **Vol. 1109.** — New York: Springer-Verlag. — 1996. — P. 372–386.

[34] Camion P., Canteaut A. *Correlation Immune and Resilient Functions Over a Finite Alphabet and Their Applications in Cryptography.*// Designs Codes and Cryptography. — 1999. — **Vol. 16.** — 2. — P. 121–149.

[35] Camion P., Carlet C., Charpin P., Sendrier N. *On Correlation Immune Functions.*// Advances in Cryptology: CRYPTO'91/ Lect. Notes in Comput. Sci. — **Vol. 576.** — New York: Springer-Verlag. — 1992. — P. 86–100.

[36] Canteaut A., Carlet C., Charpin P., Fontaine C. *Propagation Characteristics and Correlation Immunity of Highly Nonlinear Boolean Functions.*// Advances in Cryptology: EUROCRYPT'00/ Lect. Notes in Comput. Sci. — **Vol. 1807.** — New York: Springer-Verlag. — 2000. — P. 507–522.

[37] Canteaut A., Carlet C., Charpin P., Fontaine C. *On Cryptographic Properties of the Cosets of* $RM(1,m)$.// IEEE Trans. on Information Theory. — 2001. — **Vol. 47.** — 4. — P. 1494–1513.

[38] Carlet C. *A transformation on Boolean Functions, its Consequences on some Problems Related to Reed-Müller Codes.*// EUROCODES'90/ Lect. Notes in Comput. Sci. — **Vol. 514.** — New York: Springer-Verlag. — 1991. — P. 42–50.

[39] Carlet C. *Partially-bent functions.*// Designs Codes and Cryptography. — 1993. — 3. — P. 135–145.

[40] Carlet C. *Two new classes of bent functions.*// Advances in Cryptology: EUROCRYPT'93/ Lect. Notes in Comput. Sci. — **Vol. 765.** — New York: Springer-Verlag. — 1994. — P. 77–101.

[41] Carlet C. *Generalized Partial Spreads.*// IEEE Trans. on Information Theory. — 1995. — **Vol. 41.** — 5. — P. 1482–1487.

[42] Carlet C. *A constraction of bent functions.*// Seventh Joint Swedish-Russian International Workshop on Information Theory. — St.-Petersburg, Russia. — 1995. — P. 57–59.

[43] Carlet C. *Hyper-bent functions.*// PRAGOCRYPT'96. — Praga. — CTV, GC UCMP. — 1996. — P. 145–155.

[44] Carlet C. *More Correlation-Immune and Resilient Functions over Galois Fields and Galois Rings.*// Advances in Cryptology: EUROCRYPT'97/ Lect. Notes in Comput. Sci. — **Vol. 1233.** — New York: Springer-Verlag. — 1997. — P. 422–433.

[45] Carlet C. *On the Coset Weight Divisibility and Nonlinearity of Resilient and Correlation Immune Functions.*// Sequences and Their Applications: SETA'2001/ Discrete Mathematics and Theoretical Computer Science. — New York: Springer-Verlag. — 2001. — P. 131–144.

[46] Carlet C. *A Large Class of Cryptographic Boolean Functions via a Study of the Maiorana-McFarland Constructions.*// Advances in Cryptology: CRYPTO'02/ Lect. Notes in Comput. Sci. — **Vol. 2442.** — New York: Springer-Verlag. — 2002. — P. 549–564.

[47] Carlet C., Charpin P., Zinoviev V. *Codes, bent functions and permutations suitable for DES-like cryptosystems.* Designs, Codes and Cryptography. — 1998. — **Vol. 15.** — P. 125–156.

[48] Carlet C., Guillot Ph. *A characterization of binary bent functions.*// Journal of Combinatorial Theory, Series A. — 1996. — **Vo. 76.** — 2. — P. 328–335.

[49] Carlet C., Guillot Ph. *An alternate characterization of the bentness of binary functions, with uniqueness.*// Designs, Codes and Cryptography. — 1998. — **Vol. 14.** — 2. — P. 33–140.

[50] Carlet C., Sarcar P. *Spectral Domain Analysis of Correlation Immune and Resilient Boolean Functions.*// Finite Fields and Its Applications. — 2001.

[51] Carlet C., Seberry J., Zhang X.M. *Comments on "Generating and counting binary bent sequences".*// IEEE Trans. on Information Theory. — 1994. — **Vol. 40.** — 2. — P. 600.

[52] Carroll J. M., Robbins L. E. *Using binary derivaties to test an enhancement of DES.*// Cryptologia. — 1988. — **Vol. 12.** — P. 193–208.

[53] Chaum, Evertse J.-H. *Cryptanalysis of DES with a Reduced Number of Rounds; Sequences of Linear Factors in Block Ciphers.*// Advances in Cryptology: CRYPTO'85/ Lect. Notes in Comput. Sci. — **Vol. 218.** — New York: Springer-Verlag. — 1986. — P. 192–211.

[54] Chee S., Lee S., Lee D., Sung S. H. *On the Correlation Immune Functions and Their Nonlinearity.*// Advances in Cryptology: ASIACRYPT'96/ Lect. Notes in Comput. Sci. — **Vol. 1163.** — New York: Springer-Verlag. — 1996. — P. 232–243.

[55] Cheon J. H. *Nonlinear Vector Resilient Functions.*// Advances in Cryptology: CRYPTO'2001/ Lect. Notes in Comput. Sci. — New York: Springer-Verlag. — 2001.

[56] Cheon J. H., Chee S. *Elliptic Curves and Resilient Functions.*// ICISC'2000/ Lect. Notes in Comput. Sci. — **Vol. 2015.** — New York: Springer-Verlag. — 2000. — P. 64–72.

[57] Chor B., Goldreich O., Hastad J., Friedman J., Rudich S., Smolensky R. *The Bit Extraction Problem or t-Resilient Functions.*// 26-th Symposium on Foundations of Computer Science. — 1985. — P. 396–407.

[58] Chung H., Kumar P.V. *A New General Construction for Generalized Bent Function.*// IEEE Trans. on Information Theory. — 1989. — **Vol. 35.** — 1. — P. 206–209.

[59] Clark J., Jacob J., Millan W., Maitra S. *Evolution of Boolean Functions Satisfying Multiple Criteria with Simulated Annealing.*// Preprint. — 2002.

[60] Cohen G. D., Karpovsky M. G., Mattson H. F., Schatz J. *Covering radius — survey and recent results.*// IEEE Trans. on Information Theory. — 1985. — **Vol. IT-31.** — P. 328–343.

[61] Conway J.H., Sloane N.J.A. *Sphere Packings, Lattices and Groups.*// Springer-Verlag. — New York. — 1988. (русский перевод: Конвэй Дж., Слоэн Н. *Сферические упаковки, решетки и группы.*// Москва, Мир, т. 1,2.)

[62] Cusick Th. W. *Boolean functions satisfying a higher order strict avalanche criterion.*// Advances in Cryptology: EUROCRYPT'93/ Lect. Notes in Comput. Sci. — **Vol. 765.** — New York: Springer-Verlag. — 1988. — P. 102–117.

[63] Dawson M. H., Tavares S. E. *An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks.*// Advances in Cryptology: EUROCRYPT'91/ Lect. Notes in Comput. Sci. — **Vol. 547.** — New York: Springer-Verlag. — 1991. — P. 352–367.

[64] Dawson E., Wu C. K. *Construction of Correlation Immune Boolean Functions.*// Information and Communications Security/ Lect. Notes in Comput. Sci. — New York: Springer-Verlag. — 1997. — P. 170–180.

[65] Desmedt Y., Quisquater J.J., Davio M. *Dependence of Output on Input DES: Small Avalanche Characteristics.*// Advances in Cryptology: CRYPTO'84/ Lect. Notes in Comput. Sci. — **Vol. 196.** — New York: Springer-Verlag. — 1985. — P. 359–376.

[66] Dillon J.F. *A survey of bent functions.*// The NSA Technical Journal (unclassified). — 1972. — P. 191–215.

[67] Dillon J.F. *Elementary Hadamard Difference sets:* Dissert.... Doct. Ph. — University of Maryland. — 1974.

[68] Ding C., Xiao G., Shan W. *The Stability Theory of Stream Ciphers.*// Lect. Notes in Comput. Sci. — **Vol. 561.** — New York: Springer-Verlag. — 1991.

[69] Dobbertin H. *Constraction of Bent Functions and Balanced Boolean Functions with High Nonlinearity.*// Fast Software Encryption — Second International Workshop, Leuven (1994)/ Lect. Notes in Comput. Sci. — New York: Springer-Verlag. — 1995. — P. 61–74.

[70] Evertse J.-H. *Linear Structures in Blockciphers.*// Advances in Cryptology: EUROCRYPT'87/ Lect. Notes in Comput. Sci. — **Vol. 304.** — New York: Springer-Verlag. — 1988. — P. 249–266.

[71] Fedorova M., Tarannikov Y. V. *On the Constructing of Highly Nonlinear Resilient Boolean functions by Means of Special Matrices.*// Progress in Cryptology: INDOCRYPT'2001/ Lect. Notes in Comput. Sci. — **Vol. 2247.** — New York: Springer-Verlag. — 2001. — P. 254–266.

[72] Filiol E., Fontaine C. *Highly Nonlinear Balanced Boolean Functions with a Good Correlation-Immunity.*// Advances in Cryptology: EUROCRYPT'98/ Lect. Notes in Comput. Sci. — **Vol. 1403.** — New York: Springer-Verlag. — 1998. — P. 475–488.

[73] Fontaine C. *The Nonlinearity of a Class of Boolean Functions with Short Representation.*// PRAGOCRYPT'96. — Praga. — CTV, GC UCMP. — 1996. — P. 129–144.

[74] Fontaine C. *On Some Cosets of the First-Order Reed-Müller Code with High Minimum Weight.*// IEEE Trans. on Information Theory. — 1999. — **Vol. 45.** — 4. — P. 1237–1243.

[75] Forré R. *The Strict Avelanche Criterion: Spectral Properties of Boolean Functions and an Extended Definition.*// Advances in Cryptology: CRYPTO'88/ Lect. Notes in Comput. Sci. — **Vol. 403.** — New York: Springer-Verlag. — 1989. — P. 450–468.

[76] Forré R. *Methods and instruments for designing S-boxes.*// Journal of Crytology. — 1990. — **Vol. 3.** — 2. — P. 115–130.

[77] Friedman J. *On the Bit Extraction Problem.*// 33-rd IEEE Symposium on Foundations of Computer Science. — 1982. — P. 314–319.

[78] Gold R. *Optimal binary sequences for spread-spectrum multiplexing.*// IEEE Trans. on Information Theory. — 1967. — **Vol. 13.** — 4. — P. 619–621.

[79] Golić J. Dj. *Fast Low Order Approximation of Cryptographic Functions.*// Advances in Cryptology: EUROCRYPT'96/ Lect. Notes in Comput. Sci. — **Vol. 1070.** — New York: Springer-Verlag. — 1996. — P. 268–282.

[80] Golomb S.W. *On classification of Boolean functions.*// IRE Trans. on circuit theory. — 1959. — 6. — P. 176–186.

[81] Gong G., Golomb S.W. *Transform domain analysis of DES.*// IEEE Trans. on Inform. Theory. — 1999. — **Vol. IT-45.** — 6. — P. 2065–2073.

[82] Gopalakrisnan K., *A Study of Correlation-Immune, Resilient and Related Cryptographic Functions:* Dissert.... Doct. Ph. — University of Nebraska. — 1994.

[83] Gopalakrisnan K., Hoffman D.G., Stinson D. R. *A Note on a Conjecture Concerning Symmetric Resilient Functions.*// Information Processing Letters. — 1993. — **Vol. 47.** — 3. — P. 139–143.

[84] Gordon J., Retkin H. *Are big S-boxes best?.*// Advances in Cryptology: EUROCRYPT'82/ Lect. Notes in Comput. Sci. — New York: Springer-Verlag. — 1983. — P. 257–262.

[85] Guo-Zhen X., Massey J. *A Spectral Characterization of Correlation Immune Combining Functions.*// IEEE Trans. on Inform. Theory. — 1988. — **Vol. 34.** — 3. — P. 569–571.

[86] Johansson T., Pasalic E. *A Constraction of Resilient Functions with High Nonlinearity.*// IEEE International Symposium on Information Theory: ISIT'2000.// http://www.eprint.iacr.org No. 2000/053.

[87] Kim K. *A study on the construction and analysis of substitution boxes for symmetric cryptosystems:* Dissert.... Doct. Ph. — Yokohama National Univeristy. Division of Electrical and Computer Engineering. — 1990.

[88] Kim K., Matsumoto T., Imai H. *On generating cryptographically desirable substitutions.*// Transactions of the IEICE, E. — 1990. — **Vol. 73.** — 7. — P. 1031–1035.

[89] Kumar P.V., Scholts R.A., Welch L.R. *Generalized bent functions and their properties.*// Journal of Combinatorial Theory. Series A. — 1985. — **Vol. 40.** — 1. — P. 90–107.

[90] Kurosawa K., Satoh T. *Generalization of higher order SAC to vector output Boolean Functions.*// Advances in Cryptology: ASIACRYPT'96/ Lect. Notes in Comput. Sci. — **Vol. 1163.** — New York: Springer-Verlag. — 1996. — P. 218–231.

[91] Kurosawa K., Satoh T. *Design of SAC/PC(l) of Oder k Boolean Functions and Three other Cryptographic Criteria.*// Advances in Cryptology: EUROCRYPT'97/ Lect. Notes in Comput. Sci. — **Vol. 1233.** — New York: Springer-Verlag. — 1998. — P. 434–449.

[92] Kurosawa K., Satoh T., Yamamoto K. *Highly Nonlinear t-Resilient Functions.*// Journal of Universal Computer Science. — 1997, — **Vol. 3.** — 6. — P. 721–729.

[93] Lai X. *Additive and Linear Structures of Cryptographic Functions.*// Fast Software Encryption, Second International Workshop/ Lect. Notes in Comput. Sci. — **Vol. 1008.** — New York: Springer-Verlag. — 1995. — P. 75–85.

[94] Lechner R. J. *A Transform Approach to Logic Design.*// IEEE Trans. on Computers. — 1970. — **Vol. C-19.** — 10. — P. 627–640.

[95] van Leekwijck W., van Linden L. *Crytografische eigenschappen van Boolean functies:* Thesis grad.. — ESAT Katholieke Universiteit Leuven. — 1990.

[96] Lloyd S. A. *Balance, uncorrelatedness and the Strict Avalanche Criterion.*// Techical Report of Hewlett-Packard Research Laboratories, Bristol, HPL-ISC-TM-89-012. — 1989.

[97] Lloyd S. A. *Characterising and counting functions satisfying Strict Avalanche Criterion of order* $(n - 3)$.// 2nd IMA Conference on Cryptography and Coding. — 1989.

[98] Lloyd S. A. *Counting functions satisfying a higher order strict avalanche criterion.*// Advances in Cryptology: EUROCRYPT'89/ Lect. Notes in Comput. Sci. — **Vol. 434.** — New York: Springer-Verlag. — 1990. — P. 63–74.

[99] Lloyd S. *Properties of Binary Functions.*// Advances in Cryptology: EUROCRYPT'90/ Lect. Notes in Comput. Sci. — **Vol. 473.** — New York: Springer-Verlag. — 1991. — P. 124–139.

[100] Lloyd S. A. *Counting binary functions with certain cryptographic properties.*// Journal of Cryptology. — 1992. — **Vol. 5.** — 2. — P. 107–131.

[101] Lempel A., Cohn M. *Maximal Families of Bent Sequences.*// IEEE Trans. on Information Theory. — 1982. — **Vol. 28.** — 6. — P. 865–868.

[102] Maitra S. *Correlation Immune Boolean Functions with Very High Nonlinearity.*// http://www.eprint.iacr.org No. 2000/054.

[103] Maitra S. *Autocorrelation Properties of Correlation Immune Boolean Functions.*// Progress in Cryptology: INDOCRYPT'2001/ Lect. Notes in Comput. Sci. — **Vol. 2247.** — New York: Springer-Verlag. — 2001. — P. 242–253.

[104] Maitra S. *Boolean Functions with Important Cryptographic Properties:* Dissert.... Doct. Ph. — Indian Statistical Institute. — 2001.

[105] Maitra S., Pasalic E. *Further Construction of Resilient Boolean Functions with Very High Nonlinearity.*// IEEE Trans. on Information Theory. — 2002.

[106] Maitra S., Sarkar P. *Enumeration of Correlation Immune Boolean Functions.*// 4-th Australasian Conference on Information, Security and Privacy/ Lect. Notes in Comput. Sci. — **Vol. 1587.** — New York: Springer-Verlag. — 1999. — P. 12–15.

[107] Maitra S., Sarkar P. *Highly Nonlinear Resilient Functions Optimizing Siegenthaler's Inequality.*// Advances in Cryptology: CRYPTO'99/ Lect. Notes in Comput. Sci. — **Vol. 1666.** — New York: Springer-Verlag. — 1999. — P. 198–215.

[108] Maitra S., Sarkar P. *Hamming Weights of Correlation Immune Boolean Functions.*// Information Processing Letters. — 1999. — **Vol. 71.** — 3–4. — P. 149–153.

[109] Maitra S., Sarkar P. *Cryptographically Significant Boolean Functions with Five Valued Walsh Spectra.*// Theoretical Computer Science. — 2002.

[110] MacWilliams F.J., Sloane N.J.A. *The Theory of Error-Correcting Codes.*// North-Holland Publishing Company. — Amsterdam–New York–Oxford — 1977. (русский перевод: Мак-Вильямс Ф.Дж., Слоэн Н.Дж. *Теория кодов, исправляющих ошибки.*// М.: Связь, 1979.)

[111] McFarland R.L. *A Family of Difference Sets in Non-cyclic Groups.*// Journal of Combinatorial Theory (A). — 1973. — **Vol. 15.** — 1. — P. 1–10.

[112] Meier W., Staffelbach O. *Nonlinearity Criteria for Cryptographic Functions.*// Advances in Cryptology: EUROCRYPT'89/ Lect. Notes in Comput. Sci. — **Vol. 434.** — New York: Springer-Verlag. — 1990. — P. 549–562.

[113] Millan W., Clark A., Dawson E. *Heuristic Design of Cryptographicaly Strong Balanced Boolean Functions.*// Advances in Cryptology: EUROCRYPT'98/ Lect. Notes in Comput. Sci. — **Vol. 1403.** — New York: Springer-Verlag. — 1998. — P. 489–499.

[114] Mitchell C.J. *Enumerating Boolean Functions of Cryptographic Significance.*// Journal of Crytology. — 1990. — **Vol. 2.** — 3. — P. 155–170.

[115] Mo S.P., Sangjin L., Kwangjo K. *Improving Bound for the Number of Correlation Immune Boolean Functions.*// Information Processing Letters. — 1997. — **Vol. 61.** — 4. — P. 209–212.

[116] Mykkeltveit J. J. *The Covering Radius of the* $(128, 8)$ *Reed-Müller Code is 56.*// IEEE Trans. on Information Theory. — 1983. — **Vol. IT-26.** — 3. — P. 358–362.

[117] Mulan L., Peizhong L., Mullen G. L. *Correlation-Immune Functions over Finite Fields.*// IEEE Trans. on Information Theory. — 1998. — **Vol. 44.** — 3. — P. 1273–1278.

[118] Nyberg K. *Constructions of Bent Functions and Difference Sets.*// Advances in Cryptology: EUROCRYPT'90/ Lect. Notes in Comput. Sci. — **Vol. 473.** — New York: Springer-Verlag. — 1991. — P. 151–160.

[119] Nyberg K. *Perfect nonlinear S-boxes.*// Advances in Cryptology: EUROCRYPT'91/ Lect. Notes in Comput. Sci. — **Vol. 547.** — New York: Springer-Verlag. — 1991. — P. 378–386.

[120] Nyberg K. *On the Construction of Higly Nonlinear Permutations.*// Advances in Cryptology: EUROCRYPT'92/ Lect. Notes in Comput. Sci. — **Vol. 658.** — New York: Springer-Verlag. — 1993. — P. 92–98.

[121] Nyberg K. *Differentially Uniform Mappings for Cryptography.*// Advances in Cryptology: EUROCRYPT'93/ Lect. Notes in Comput. Sci. — **Vol. 765.** — New York: Springer-Verlag. — 1994. — P. 55–64.

[122] Nyberg K. *New Bent Mappings Suitable for Fast Implementation.*// Fast Software Encryption'93/ Lect. Notes in Comput. Sci. — **Vol. 809.** — New York: Springer-Verlag. — 1994. — P. 179–184.

[123] Nyberg K. *S-Boxes and Round Functions with controllable Linearity and Differential Uniformity.*// Fast Software Encryption, Second International Workshop/ Lect. Notes in Comput. Sci. — **Vol. 1008.** — New York: Springer-Verlag. — 1995. — P. 111–130.

[124] O'Connor L.J. *Enumeration Nondegenerate Permutations.*// Advances in Cryptology: EUROCRYPT'91/ Lect. Notes in Comput. Sci. — **Vol. 547.** — New York: Springer-Verlag. — 1992. — P. 368–377.

[125] O'Connor L.J. *An Analysis of Product Ciphers based on the Properties of Boolean Functions:* PhD Dissertation. — University of Waterloo. — Waterloo, Ontario, Canada. — 1992. — 171 p.

[126] Olsen J. D., Scholtz R. A., Welch L. R. *Bent-Function Sequences.*// IEEE Trans. on Information Theory. — 1982. — **Vol. 28.** — 6. — P. 858–864.

[127] Pasalic E., Johansson T. *Further Results on the Relation Between Nonlinearity and Resiliency of Boolean Functions.*// IMA Conference on Cryptography and Coding/ Lect. Notes in Comput. Sci. — **Vol. 1746.** — New York: Springer-Verlag. — 1999. — P. 35–45.

[128] Pasalic E., Maitra S. *Linear Codes in Constructing Resilient Functions With High Nonlinearity.*// Selected Areas in Cryptography: SAC'2001/ Lect. Notes in Comput. Sci. — **Vol. 2259.** — New York: Springer-Verlag. — 2001. — P. 60–74.

[129] Pasalic E., Maitra S., Johansson T., Sarkar P. *New Constructions of Resilient and Correlation Immune Boolean Functions Achieving Upper Bounds on Nonlinearity.*// Workshop on Coding and Cryptography: WCC'2001, Paris/ Electronic Notes in Discrete Mathematics — **Vol. 6.** — New York: Elsevier Science. — 2001.

[130] Patterson N. J., Wiedemann D. H. *The Covering Radius of the* $(2^{15}, 16)$ *Reed-Müller Code is at least 16276.*// IEEE Trans. on Information Theory. — 1983. — **Vol. IT-29.** — 3. — P. 354–356.

[131] Patterson N. J., Wiedemann D. H. *Correction to — The Covering Radius of the* $(2^{15}, 16)$ *Reed-Müller Code is at least 16276.*// IEEE Trans. on Information Theory. — 1990. — **Vol. IT-36.** — 2. — P. 443.

[132] Pieprzyk J. P. *Error Propagation Property and Application in Cryptography .*// Proc. IEE, Pt. E. — 1989. — **Vol. 136.** — 4. — P. 262–270.

[133] Pieprzyk J. P. *Nonlinearity of exponent permutations.*// Advances in Cryptology: EUROCRYPT'89/ Lect. Notes in Comput. Sci. — **Vol. 434.** — New York: Springer-Verlag. — 1990. — P. 80–92.

[134] Pieprzyk J. P. *On bent permutations.*// Techical Report: Department of Computer Science, The University of NewSouthWales. — CS91/11. — 1991.

[135] Pieprzyk J. P., Finkelstein G. *Towards effective nonlinear cryptosystem design.*// IEE Proceedings, part E: Computers and Digital Techniques. — 1988. — **Vol. 135.** — 6, November, series E, Department of Computer Science, University of New South Wales, Australian Defence Force Academy, Canberra, ACT 2600, Australia. — P. 325–335.

[136] *Handbook of Coding Theory.* **Vol. I, II.**, Eds. Pless V.S., Huffman W.C.// Elsevier. — 1998.

[137] Preneel B., VanLeekwijck W., VanLinden L., Govaerts R., VanDewalle J. *Propagation Characteristics of Boolean Functions.*// Advances in Cryptology: EUROCRYPT'90/ Lect. Notes in Comput. Sci. — **Vol. 473.** — New York: Springer-Verlag. — 1991. — P. 161–173.

[138] Preneel B., Govaerts R., VanDewalle J. *Boolean Functions Satisfying Higher Order Propagation Criteria.*// Advances in Cryptology: EUROCRYPT'91/ Lect. Notes in Comput. Sci. — **Vol. 541.** — New York: Springer-Verlag. — 1991. — P. 141–152.

[139] Rothaus O.S. *On "Bent" Functions.*// Journal of Combinatorial Theory (A). — 1976. — **Vol. 20.** — 3. — P. 300–305.

[140] Roy B. *A Brief Outline of Research on Correlation Immune Functions.*// ACISP'2002/ Lect. Notes in Comput. Sci. — **Vol. 2384.** — New York: Springer-Verlag. — 2002.

[141] Sarkar P. *A Note on the Spectral Characterization of Correlation Immune Boolean Functions.*// Information Processing Letters. — 2000. — **Vol. 74.** — 5–6. — P. 191–195.

[142] Sarkar P. Maitra S., *Construction of Nonlinear Boolean Functions with Important Cryptographic Properties.*// Advances in Cryptology: EUROCRYPT'2000/ Lect. Notes in Comput. Sci. — **Vol. 1807.** — New York: Springer-Verlag. — 2000. — P. 485–506.

[143] Sarkar P. Maitra S., *Nonlinearity Bounds and Constructions of Resilient Boolean Functions with Important Cryptographic Properties.*// Advances in Cryptology: CRYPTO'2000/ Lect. Notes in Comput. Sci. — **Vol. 1880.** — New York: Springer-Verlag. — 2000. — P. 515–532.

[144] Sarkar P. Maitra S., *Balancedness and Correlation Immunity of Symmetric Boolean Functions.*// preprint. — 2000.

[145] Sarkar P. Maitra S., *Cross-Correlation Analysis of Cryptographically Useful Boolean Functions and S-boxes.*// Theory of Computing Systems. — 2002.

[146] Savicky P. *On the bent Boolean functions that are symmetric.*// European Journal of Combinatorics. — 1994. — **Vol. 15.** — 4. — P. 407–410.

[147] Savicky P. *Bent functions and random Boolean formulas.*// Discrete Mathematics. — 1995. — **Vol. 147.** — P. 1–3.

[148] Schneider M. *On the Construction and Upper Bounds of Balanced and Correlation Immune Functions.*// Selected Areas in Cryptography: SAC'1997/ Lect. Notes in Comput. Sci. — New York: Springer-Verlag. — 1997.

[149] Seberry J., Zhang X.-M. *Highly nonlinear* $0-1$ *balanced Boolean functions satisfying strict avalanche criterion.*// Advances in Cryptology: AUSCRYPT'92/ Lect. Notes in Comput. Sci. — **Vol. 718.** — New York: Springer-Verlag. — 1993.

[150] Seberry J., Zhang X.-M., Zheng Y. *Nonlinearly Balanced Boolean Functions and Their Propagation Characteristics.*// Advances in Cryptology: CRYPTO'93/ Lect. Notes in Comput. Sci. — **Vol. 773.** — New York: Springer-Verlag. — 1994. — P. 49–60.

[151] Seberry J., Zhang X.-M., Zheng Y. *On the Constructions and Nonlinearity of Correlation Immune Boolean Functions.*// Advances in Cryptology: EUROCRYPT'93/ Lect. Notes in Comput. Sci. — **Vol. 765.** — New York: Springer-Verlag. — 1994. — P. 181–199.

[152] Seberry J., Zhang X.-M., Zheng Y. *Relationships Among Nonlinearity Criteria.*// Advances in Cryptology: EUROCRYPT'94/ Lect. Notes in Comput. Sci. — **Vol. 950.** — New York: Springer-Verlag. — 1995. — P. 376–388.

[153] Seberry J., Zhang X.-M., Zheng Y. *Improving the Strict Avalanche Characteristics of Cryptographic Functions.*// Information Processing Letters. — 1994, — **Vol. 50.** — P. 37–41.

[154] Seberry J., Zhang X.-M., Zheng Y. *Nonlinearity and propagation characteristics of balanced boolean functions.*// Information and Computation. — 1995. — **Vol. 119**. — P. 1–13.

[155] Seberry J., Zhang X.-M., Zheng Y. *The relationship Between Propagation Characteristics and Nonlinearity of Cryptographic Functions.*// Journal of Universal Computer Science. — 1995, — **Vol. 1.** — 2. — P. 136–150.

[156] Shan W. *The Structure and the Construction of Correlation Immune Functions:* MS Thesis. — NTE Institute, Xian. — 1987.

[157] Shannon C. *Communication Theory of Secrecy Systems.*// Bell System Technical Journal. — 1949, — **Vol. 28.** — 4. — P. 656–715. (Русский перевод: *Теория связи в секретных системах*, в сборнике Шеннон К.// Работы по теории информации и кибернетике/ Москва, Иностранная литература, 1963, С. 333–402.)

[158] Shen V.Y., McKellar A. Weiner P. *A Fast Algorithm for the Disjunctive Decomposition on Switching Functions.*// IEEE Trans. on Computers. — 1971, — **Vol. 20.** — 3. — P. 304–309.

[159] Siegentaler T. *Correlation-immunity of Nonlinear Combining Functions for Cryptographic Applications.*// IEEE Trans. on Information Theory. — 1984. — **Vol. IT-30.** — 5. — P. 776–780.

[160] Siegentaler T. *Decrypting a Class of Stream Ciphers Using Ciphertext Only.*// IEEE Trans. on Computers. — 1985. — **Vol. C-34.** — 1. — P. 81–85.

[161] Stinson D. R. *Resilient Functions and Large Sets of Orthogonal Arrays.*// Congressus Numerantium/ — **Vol. 92.** — 1993. — P. 105–110.

[162] Stinson D. R., Massey J. L. *An Infinite Class of Counterexamples to a Conjecture Concerning Nonlinear Resilient Functions.*// Journal of Cryptology. — 1995, — **Vol. 8.** — 3. — P. 167–173.

[163] Tarannikov Y. V. *On Resilient Boolean Functions with Maximum Possible Nonlinearity.*// Progress in Cryptology: INDOCRYPT'2000/ Lect. Notes in Comput. Sci. — **Vol. 1977.** — New York: Springer-Verlag. — 2000. — P. 19–30.

[164] Tarannikov Y. V. *New Constructions of Resilient Boolean Functions with Maximal Nonlinearity.*// Fast Software Encryption: FSE'2001/ Lect. Notes in Comput. Sci. — New York: Springer-Verlag. — 2001. — P. 70–81.

[165] Tarannikov Y. V., Korolev P., Botev A. *Autocorrelation Coefficients and Correlation Immunity of Boolean Functions.*// Advances in Cryptology: ASIACRYPT'2001/ Lect. Notes in Comput. Sci. — New York: Springer-Verlag. — 2001.

[166] Webster A. F., Tavares S. E. *On the Design of S-Boxes.*// Advances in Cryptology: CRYPTO'85/ Lect. Notes in Comput. Sci. — New York: Springer-Verlag. — 1986. — P. 523–534.

[167] Xiao G.Z., Massey J.L. *A Spectral Characterization on Correlation-Immune Functions.*// IEEE Trans. on Information Theory. — 1988. — **Vol. 34.** — 3. — P. 569–571.

[168] Yarlagadda R., Hershey J.E. *Analysis and synthesis of bent sequences.*// Proc. IEE, Pt. E. — 1989. — **Vol. 136.** — 2. — P. 112–123.

[169] Yang Y. X., Guo B. *Further Enumerating Boolean Functions of Cryptographic Significance.*// Journal of Crytology. — 1995. — **Vol. 8.** — 3. — P. 115–122.

[170] Youssef A. M., Cusick T. W., Stănică P., Tavares S. E. *New bounds on the number of functions satisfying strict avalanche criterion.*// Third Annual Workshop on Selected Areas in Cryptography. — 1996.

[171] Youssef A., Gong G. *Hyper-bent functions.*// Advances in Cryptology: EUROCRYPT'2001/ Lect. Notes in Comput. Sci. — **Vol. 2045.** — New York: Springer-Verlag. — 2001. — P. 406–419.

[172] Zhang X.-M., Zheng Y. *GAC — the Criterion for Global Avalanche Characteristics of Cryptographic Functions.*// Journal of Universal Computer Science. — 1995, — **Vol. 1.** — 5. — P. 320–337.

[173] Zhang X.-M., Zheng Y. *Auto-Correlations and New Bounds on the Nonlinearity of Boolean Functions.*// Advances in Cryptology: EUROCRYPT'96/ Lect. Notes in Comput. Sci. — **Vol. 1070.** — New York: Springer-Verlag. — 1996. — P. 294–305.

[174] Zhang X.-M., Zheng Y. *Characterizing the structures of cryptographic functions satisfying the propagation criterion for almost all vectors.*// Designs, Codes and Cryptography. — 1996. — **Vol. 7**. — P. 111–134.

[175] Zhang X.-M., Zheng Y. *On the Difficulty of Constructing Cryptographically Strong Substitution Boxes.*// Journal of Universal Computer Science. — 1996, — **Vol. 2.** — 3. — P. 147–162.

[176] Zhang X.-M., Zheng Y. *New Lower Bounds on Nonlinearity and a Class of High Nonlinear Functions.*// Information Security and Privacy: ACISP'97/ Lect. Notes in Comput. Sci. — **Vol. 1270.** — New York: Springer-Verlag. — 1998. — P. 147–158.

[177] Zhang X.-M., Zheng Y. *Cryptographically Resilient Functions.*// IEEE Trans. on Information Theory. — 1997. — **Vol. 43.** — 5. — P. 1740–1747.

[178] Zheng Y., Zhang X.-M. *Improved Upper Bounds on Nonlinearity of High Order Correlation Immune Functions.*// Selected Areas in Cryptography: SAC'2000/ Lect. Notes in Comput. Sci. — **Vol. 2012.** — New York: Springer-Verlag. — 2000. — P. 264–274.

[179] Zheng Y., Zhang X.-M. *On Relationships among Propagation Degree, Nonlinearity and Correlation Immunity.*// Advances in Cryptology: ASIACRYPT'2000/ Lect. Notes in Comput. Sci. — New York: Springer-Verlag. — 2000.

[180] Zheng Y., Zhang X.-M. *New Results on Correlation Immune Functions.*// International Conference on Information Security and Cryptology: ICISC'2000/ Lect. Notes in Comput. Sci. — **Vol. 2015.** — New York: Springer-Verlag. — 2001. — P. 49–63.

[181] Zheng Y., Zhang X.-M. *Plateaued Function.*// http://www.pscit.monas.edu.au/~yuliang/.

# Датчики псевдослучайных чисел и их применения

А. М. Зубков

Теория вероятностей, как и другие области математики, изучает модели некоторых свойств или явлений реального мира. Случайными явлениями можно считать изменения погоды, турбулентные движения жидкостей или газов, радиоактивный распад, квантовые эффекты и т. п. В отличие от детерминированных явлений, типичных для классической механики и физики, моделируемые теорией вероятностей явления имеют вид закономерностей, которые проявляются не в каждом конкретном случае, а лишь в больших совокупностях однородных экспериментов. Главным неформальным признаком случайности является непредсказуемость; разумеется, степень непредсказуемости часто зависит от имеющейся информации и от уровня знаний. Этот признак дает основания говорить о случайности в идеальных детерминированных объектах: последовательности простых чисел, знаках десятичных разложений иррациональных чисел, поведении динамических систем и т. п.

Первые исследования случайных явлений были связаны с деятельностью человека: азартными играми, лотереями и страховым делом. Азартные игры и лотереи можно рассматривать как исторически первые примеры практической реализации и применения «датчиков случайных чисел», т. е. устройств, которые могут порождать непредсказуемые последовательности объектов (символов или чисел при бросании монет или игральных кубиков, наборов игральных карт, номеров шаров при их извлечении из барабана и т. п.).

Область применения датчиков случайных чисел существенно расширилась в середине XX века. При этом одновременно сформировались два различных направления ее расширения: вычислительные методы (включая статистическое моделирование) и криптография. Возможность реализации таких применений была обеспечена, с одной стороны, развитием теории вероятностей, а с другой стороны — созданием ЭВМ, позволивших быстро проводить вычисления по сложным формулам. Уже в первых ЭВМ использовались быстрые программные датчики нерегулярных числовых последовательностей, наряду с которыми существовали и разрабатывались более медленные физические датчики случайных чисел.

Законность применения датчиков случайных чисел к вычислению интегралов, решению дифференциальных уравнений с частными производными и т. п., как правило, обосновывается законом больших чисел или центральной предельной теоремой. Позднее стали интенсивно развиваться методы построения рандомизированных алгоритмов решения комбинаторных и оптимизационных задач, использующие более тонкие результаты теории вероятностей.

Теория вероятностей стала одной из математических основ криптографии после того, как во время второй мировой войны Клод Шеннон в работе «Теория связи в секретных системах» [6] доказал теорему о возможности построения совершенного шифра. Конструктивная часть этой теоремы в качестве примера совершенного шифра предлагала процедуру познакового сложения открытого текста и ключевой (известной только отправителю и получателю) последовательности, образованной независимыми равномерно распределенными знаками того же алфавита (отождествляемого, например, с множеством наименьших неотрицательных вычетов). После доказательства этой теоремы одной из основных задач создателей систем шифрования стало приближение свойств ключевых последовательностей и шифрованного текста к свойствам последовательности независимых равномерно распределенных случайных величин, т. е. по сути дела — построение датчиков псевдослучайных чисел, трудно отличимых от «идеальных» случайных чисел.

Критерий близости псевдослучайной последовательности к «настоящей случайной» последовательности зависит от области применения псевдослучайных чисел. Например, в методе Монте-Карло обычно используются лишь закон больших чисел и центральная предельная теорема, и в таких ситуациях, как правило, достаточна лишь некоррелированность псевдослучайных чисел. Даже если окажется, что использованный датчик неудовлетворителен, можно повторить вычисления с другим датчиком и сравнить полученные результаты. С другой стороны, в криптографии пользователь с

помощью датчика псевдослучайных чисел пытается защитить важную информацию от активного злоумышленника, и исправить последствия использования некачественного датчика, как правило, невозможно. Поэтому в криптографии используются наиболее жесткие критерии близости псевдослучайных последовательностей к случайным.

Применения случайных чисел в алгоритмах вычисления, статистического моделирования и в криптографии стимулировали как разработку теоретических основ методов построения детерминированных быстро порождаемых числовых последовательностей, не обладающих заметной регулярностью, так и попытки построить строгое и удобное определение понятия случайности, не противоречащее интуитивным представлениям о ней.

Подавляющее большинство датчиков случайных чисел порождают детерминированные рекуррентные последовательности $\{x_n\}$ большого, но конечного периода. Примерами соотношений, определяющих такие последовательности, являются

$$\begin{aligned} x_{n+1} &\equiv ax_n + b \pmod N, \\ x_{n+1} &\equiv ax_n^2 + b \pmod N, \\ x_{n+1} &\equiv ax_n^{-1} + b \pmod N, \\ x_{n+r} &\equiv a_0x_n + a_1x_{n+1} + \ldots + a_{r-1}x_{n+r-1} \pmod N, \end{aligned}$$

где под $x^{-1}$ понимается как обратный к $x$ элемент в мультипликативной группе вычетов $\mathbb{Z}_N^*$ по модулю $N$; здесь и далее всегда рассматриваются наименьшие неотрицательные вычеты. Многие свойства таких последовательностей, характеризующие как их сходство с последовательностями случайных чисел, так и отличия, довольно детально изучены (см., например, [2]). В частности, очевидно, что любая рекуррентная последовательность, элементы которой принимают значения из конечного множества, асимптотически периодична.

Рекуррентные последовательности с простыми функциональными зависимостями между знаками обладают рядом свойств регулярности, которые обнаруживаются даже на их сравнительно коротких отрезках, что может быть допустимо в вычислительных алгоритмах и процедурах статистического моделирования, но для криптографии неприемлемо.

Для скрытия зависимостей структуру таких последовательностей иногда усложняют детерминированными нелинейными преобразованиями, рассматривая, например, вместо рекуррентной последовательности $\{x_n\}$ последовательность

$$y_n = f(x_n, x_{n+1}, \ldots, x_{n+k}),$$

где $f$ — достаточно сложная нелинейная функция, отображающая $\mathbb{Z}_N^{k+1}$ в $\mathbb{Z}_N$.

Другой класс способов устранения явных зависимостей состоит в усложнении правила перехода от одного знака рекуррентной последовательности к следующему. Примерами являются датчики, основанные на использовании теоретико-числовых операций, обращение которых является трудно решаемой алгоритмической задачей. Приведем два примера таких датчиков псевдослучайных битов.

а) Пусть $k$ — большое натуральное число; выберем нечетные простые числа $p_1$ и $p_2$ из интервала $[2^k, 2^{k+1})$ и положим $N = p_1p_2$. Выберем большое целое $e \in \{2, \ldots, N-2\}$, взаимно простое с $\varphi(N) = (p_1-1)(p_2-1)$. По начальному значению $z_0 \in \{2, \ldots, N-1\}$ построим последовательности

$$z_{n+1} = z_n^e \pmod N, \quad y_n \equiv z_n \pmod 2, \quad n \geqslant 0.$$

Тогда полиномиально растущее вместе с $k$ количество значений $y_n \equiv z_n \pmod 2$ можно рассматривать как последовательность псевдослучайных битов, которую трудно отличить от последовательности независимых случайных битов.

б) Выберем $k > 2$ и $N$ так же, как в п. а), при дополнительном условии $p_1 \equiv p_2 \equiv 3 \pmod 4$. По начальному начальному значению $z_0 \in \{2, \ldots, N-1\}$ построим последовательность $\{z_n\}$, полагая $z_{n+1} \equiv z_n^2 \pmod N$, если этот наименьший неотрицательный вычет лежит в $[0, N/2)$, и $z_{n+1} = N - (z_n^2 \pmod N)$ в противном случае. Таким образом, всегда $0 < z_{n+1} < N/2$. Положим теперь $y_n = z_n \pmod 2$. Аналогично примеру а) полиномиально зависящее от $k$ количество значений $y_n$ можно рассматривать как последовательность псевдослучайных битов. Условие $p_1 \equiv p_2 \equiv 3 \pmod 4$ гарантирует, что $-1$ является квадратичным невычетом как для $p_1$, так и для $p_2$.

Разные начальные значения порождают разные рекуррентные последовательности, и их «случайность» порождается выбором начального значения. Описание ряда идей, используемых при построении датчиков псевдослучайных чисел и критериев проверки их качества, можно найти в книге Д.Кнута [2]. В частности, простыми и распространенными характеристиками качества последовательностей псевдослучайных чисел являются длина периода и наличие (или отсутствие) легко обнаруживаемых регулярностей. Равномерность распределения знаков псевдослучайных последовательностей и наличие зависимостей между ними можно проверять, например, с помощью основанного на свойствах тригонометрических сумм критерия Вейля (см., например, [1]), а также с помощью различных стандартных статистических критериев.

Однако даже если несколько критериев не обнаруживают отличия свойств детерминированной последовательности от свойств случайной последовательности, то это не значит, что критерия, обнаруживающего такие различия, не существует. В качестве примера можно привести способ построения нормальной последовательности знаков, предложенный Чемперноуном ([7], см. также [4]). Для двоичных последовательностей он выглядит следующим образом: последовательность нулей и единиц $\{s_n\}$ состоит из блоков; длина $r$-го блока равна $r2^r$, и $r$-й блок состоит из $2^r$ цепочек длины $r$, представляющих собой записи чисел $0, 1, \ldots, 2^r - 1$ в двоичной системе счисления. Эта последовательность непериодична и является нормальной в следующем смысле: если $N(\Delta_v, T)$ — число появлений цепочки $\Delta_v = (\delta_1, \ldots, \delta_v)$ из $v$ нулей и единиц в отрезке $s_1, \ldots, s_{T+v-1}$, то $\lim_{T\to\infty} T^{-1}N(\Delta, T) = 2^{-v}$ при любых $v$ и $\Delta_v$. Очевидно, однако, что структура этой последовательности очень жестко детерминирована, и ее нельзя считать случайной.

Указанный пример показывает нетривиальность принципиальных вопросов, связанных с формализацией интуитивных представлений о случайности, в соответствии с которыми под «настоящими» случайными числами мы понимаем числовые характеристики реальных явлений, не определяющихся контролируемыми начальными условиями.

Областью математики, изучающей модели случайных явлений, является теория вероятностей. Современная теория вероятностей основана на разработанной А. Н. Колмогоровым в начале 30-х годов XX века системе аксиом, которая сводит теорию вероятностей к теории меры [3].

В колмогоровской аксиоматике модель случайных явлений или наблюдений — это случайные величины, т. е. измеримые функции $\xi_1, \xi_2, \ldots$, определенные на измеримом пространстве $(\Omega, \mathcal{F})$ с вероятностной мерой $\mathsf{P}$. Типичные теоремы теории вероятностей и математической статистики описывают свойства меры $\mathsf{P}$ множеств тех $\omega \in \Omega$, при которых конечная или бесконечная последовательность чисел $\xi_1(\omega), \xi_2(\omega), \ldots$ (реализация случайных величин $\xi_1, \xi_2, \ldots$) обладает тем или иным свойством. Можно сказать, что в теории вероятностей изучаются лишь общие закономерности случайности, а не свойства отдельных реализаций случайных последовательностей. Иными словами, в теории вероятностей вопрос о природе исходной случайности сводится к выбору точки в пространстве элементарных событий. Механизм этого выбора теорию вероятностей не интересует; требуется лишь, чтобы он соответствовал заданной вероятностной мере $\mathsf{P}$ (и формально определяемому условию независимости при повторении испытаний).

Например, при построении статистического критерия для проверки гипотезы $H$ о том, что наблюдаемые значения $x_1, x_2, \ldots, x_T$ являются реализацией случайных величин $\xi_1, \xi_2, \ldots, \xi_T$ с распределением $\mathsf{P}$, в множестве всех возможных реализаций $x_1, x_2, \ldots, x_T$ выделяют множество $C$ с небольшой $\mathsf{P}$-мерой и считают, что значения $x_1, x_2, \ldots, x_T$ не противоречат гипотезе $H$, если $(x_1, x_2, \ldots, x_T) \in C$.

Принято считать, что детерминированная последовательность конечной длины $T$ обладает хорошими псевдослучайными качествами, если совокупность статистических критериев не может отличить ее от реализации последовательности случайных чисел.

Однако это определение не является математически строгим. Был предложен ряд других подходов к более формализованному определению понятия случайности. В них используются понятия вычислимости и алгоритмической сложности. Подробное описание основных подходов можно найти в [5], поэтому здесь они будут только кратко намечены.

Исторически первый — частотный — подход был предложен фон Мизесом в начале XX века. Его основная идея состоит в том, что частоты событий в случайной последовательности не должны изменяться при переходе от нее к «правильно» выбираемым подпоследовательностям. Впоследствии этот подход развивался Черчем, Колмогоровым и Ловеландом. Понятию «правильности» выбора подпоследовательности трудно придать четкий и не противоречащий интуитивным представлениям смысл.

Другой подход — сложностной — был предложен А. Н. Колмогоровым и основан на том, что описание реализации случайной последовательности не может быть заметно короче самой этой реализации

(при любом заранее фиксированном способе описания).

Третий — количественный — подход развивался П. Мартин-Лефом; он состоит в использовании классической конструкции вероятностного пространства $(\Omega, \mathcal{F}, \mathsf{P})$ и определении конструктивных подмножеств эффективно нулевой меры. Оказалось, что в отличие от множеств нулевой меры Лебега в классе подмножеств эффективно нулевой меры существует «максимальное» подмножество $D$, что позволяет называть все последовательности, не принадлежащие $D$, «случайными».

Наконец, в последние десятилетия в связи с развитием представлений о том, какие свойства случайных последовательностей нужны для их применений в криптографии, возник новый — криптографический — подход к определению понятия случайности. На неформальном уровне согласно этому подходу последовательность называется случайной, если она удовлетворяет всем таким статистическим критериям случайности, для которых сложность вычисления используемых в них статистик не выше заданной. Приведем немного более детальное описание этого подхода из [8], [9].

В качестве математической модели датчика псевдослучайных чисел, порождающего по начальному значению длинную последовательность, выбирается полиномиально вычислимый ансамбль функций $g\colon \{0,1\}^n \to \{0,1\}^{k(n)}$, где $k(n) > n$ — функция, растущая не быстрее некоторого полинома. Пусть, далее, $X$ имеет равномерное распределение на $\{0,1\}^n$, $Z$ имеет равномерное распределение на $\{0,1\}^{k(n)}$ и $A_n\colon \{0,1\}^{k(n)} \to \{0,1\}$ — статистики, которыми может воспользоваться злоумышленник для того, чтобы отличить случайную величину $g(X)$ (последовательность, выработанную датчиком) от случайной величины $Z$ (идеальной случайной последовательности той же длины). Вероятность успеха для злоумышленника в этом случае измеряется величиной

$$\delta(n) = |\mathsf{P}(A_n(g(X)) = 1) - \mathsf{P}(A_n(Z) = 1)|.$$

Говорят, что ансамбль $g$ определяет $S(n)$-стойкий датчик псевдослучайных битов (где $S(n)$ — функция, стремящаяся к бесконечности при $n \to \infty$, если для любой статистики $A$ выполняется условие $T(n) > S(n)/\delta(n)$, где $T(n)$ — сложность вычисления $A_n$ в наихудшем случае.

## Литература


[1] Кейперс Л., Нидеррайтер Г. Равномерное распределение последовательностей. М.: Наука, 1985.

[2] Кнут Д. Искусство программирования для ЭВМ. Т. 2. Получисленные алгоритмы. М.: Мир, 1977 (второе издание: М.: изд. дом «Вильямс», 2000).

[3] Колмогоров А. Н. Основные понятия теории вероятностей. М.: Наука, 1974.

[4] Постников А. Г. Арифметическое моделирование случайных процессов. Труды Матем. ин-та АН СССР, 1960, **57**.

[5] Успенский В. А., Семенов А. Л., Шень А.Х. Может ли (индивидуальная) последовательность нулей и единиц быть случайной? Успехи математических наук, 1990, **45**, вып. 1, 105–162.

[6] Шеннон К. Э. Теория связи в секретных системах. В кн.: Шеннон К. Э. Работы по теории информации и кибернетике. М.: ИЛ, 1963.

[7] Champernowne D. G. The construction of decimal normal in the scale of ten. J. London Math. Soc., 1933, **8**, 254–260.

[8] Goldreich O. Modern Cryptography, Probabilistic Proofs and Pseudorandomness. Berlin e.a.: Springer-Verlag, 1999.

[9] Luby M. Pseudorandomness and Cryptographic Applications. Princeton: Princeton Univ. Press, 1996.

# Проблемы теории сложности квантовых вычислений

Н. П. Варновский, М. Н. Вялый

С середины 80-х годов XX века началось теоретическое исследование вычислительных устройств, подчиняющихся законам квантовой механики (квантовые компьютеры). Уже в первых работах Р. Фейнмана и Д. Дойча [29, 30, 24] было отмечено, что моделирование квантовых систем на классических компьютерах существующими методами приводит к большим (экспоненциальным) затратам ресурсов. Интерес к квантовым компьютерам резко вырос после появления эффективных квантовых алгоритмов для задач факторизации целых чисел и нахождения дискретного логарифма, которые принято считать трудными для классических компьютеров [53]. Эти результаты стимулировали и теоретические, и прикладные исследования в данной области.

Реальных квантовых компьютеров пока нет. Задача создания полноценного квантового компьютера, оперирующего большим количеством квантовых битов, представляется необычайно трудной. Её решение, скорее всего, возможно только при значительных затратах сил и средств, сопоставимых по порядку с затратами на космическую программу и программу термоядерного синтеза.

Поэтому по-прежнему остаются актуальными два основных вопроса:

1) Существуют ли фундаментальные препятствия на пути физической реализации квантовых компьютеров?

2) Насколько широк класс задач, при решении которых квантовые компьютеры имеют принципиальное превосходство над классическими?

Оба эти вопроса весьма трудны. Первый оказался легче и в настоящее время считается решенным. Большинство специалистов как в физике, так и в теории вычислений сходятся на том, что никаких фундаментальных препятствий для создания квантовых компьютеров не существует. Вместе с тем, хотя это менее известно, одновременно с положительными результатами в анализе проблемы физической реализации квантового компьютера были получены и некоторые отрицательные результаты, которые заставляют сомневаться в возможности реализации квантовых компьютеров в сколь-нибудь обозримом будущем, по крайней мере в рамках той стандартной модели, реализация которой обычно и рассматривается как задача построения квантового компьютера.

Основные трудности возникают при учете воздействия шума на процесс квантового вычисления. Любая практически реализуемая схема вычислений должна обеспечивать надежное вычисление при наличии помех. Напомним, что переход от аналоговых вычислений к цифровым во многом был связан именно с большей надежностью цифровых вычислений. Для классических вычислений задача надежности вычисления в условиях помех и ошибок в работе базисных элементов была решена фон Нейманом [49].

Что касается квантовых вычислений, то возможность компенсировать воздействие помех кажется далеко не очевидной. Помимо ошибок классического типа, квантовое вычисление подвержено ошибкам иного рода, связанным с разрушением суперпозиции состояний. Важный класс таких ошибок, называемый потерей когерентности (decoherence) был описан в работах [57, 58, 70]. Потеря когерентности, если её не компенсировать, приводит к тому, что квантовое вычисление перестаёт отличаться по вычислительным возможностям от классического вероятностного. Кроме того, в квантовом случае невозможно копирование состояний [67] — простейший приём, который обеспечивает надежность

Частично работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (коды проектов № 02-01-00547 и № 00-15-96064).

классического вычисления. Всё это сделало проблему *надежного* квантового вычисления центральной проблемой для всего направления исследований, связанных с квантовыми вычислениями. К настоящему моменту можно сказать, что как теоретическая проблема она решена [55, 56, 2, 9, 11], причём ответ положительный: надёжное квантовое вычисление возможно. Впрочем, условия, при которых возможно надёжное квантовое вычисление, оказываются весьма жёсткими. Во-первых, надёжное квантовое вычисление возможно только при достаточно низком уровне шума. Во-вторых, показана невозможность надёжного *последовательного* квантового вычисления [10], т. е. физические реализации квантовых вычислителей должны обеспечивать массированный параллелизм. В-третьих, надёжное квантовое вычисление невозможно в чисто унитарной модели. Как минимум [12], требуется в процессе вычисления приготавливать кубиты в известном состоянии (скажем, $|0\rangle$) и удалять кубиты (и та, и другая операции будут постоянно использоваться в процессе надёжного квантового вычисления).

Что касается второго из сформулированных выше вопросов, по существу относящегося к области теории сложности вычислений, то довольно быстро выяснилось, что он связан с известными нерешенными вопросами в этой теории. Поэтому окончательное решение этого вопроса в обозримом будущем представляется сомнительным. Однако модель квантовых вычислений можно исследовать методами теории сложности вычислений и получать, пусть косвенные, результаты, свидетельствующие о возможностях этой модели. Такой подход с успехом применялся ко многим математическим задачам за последние 30 лет, модель квантовых вычислений не стала исключением.

В этом обзоре мы попытаемся кратко охарактеризовать результаты, полученные в теории сложности квантовых вычислений. Учитывая, что сейчас уже появилось довольно много книг и обзоров общего характера, посвященных теории квантовых вычислений (например, книги [3, 50, 37], обзоры [2, 11]), мы не даем подробного введения в основы этой теории.

Дальнейшее изложение построено следующим образом. В разд. 1 кратко описана стандартная модель квантового вычисления. На основе этой модели можно определять квантовые аналоги многих классических сложностных классов, в разд. 2 приводятся основные примеры. В разд. 3 приводятся результаты о взаимосвязи этих классов и их соотношениях с классическими сложностными классами. Разд. 4 содержит описание результатов, относящихся к моделям с оракулами.

Обзор не претендует на полноту: в каждом из упомянутых направлений исследования показаны наиболее типичные результаты.

# 1 Стандартные модели квантового вычисления

Основными вычислительными моделями в теории сложности классических вычислений являются машины Тьюринга и булевы схемы. Поэтому неудивительно, что в первых работах по квантовым вычислениям [30, 24, 25] были построены квантовые аналоги именно этих моделей. Довольно быстро была показана их полиномиальная эквивалентность [68] при естественном условии однородности семейства схем (описания схем должны эффективно порождаться некоторой классической машиной Тьюринга).

Дадим краткое описание схемной модели. Квантовая схема $U$, использующая $N$ *кубитов*, описывает унитарное преобразование пространства состояний, которое является тензорной степенью $\mathcal{B}^{\otimes N}$ *пространства состояний одного кубита* $\mathcal{B} = \mathbb{C}^2$. Как и в случае классических схем, для задания квантовой схемы нужно прежде всего задать *базис*: некоторое множество унитарных операторов. Обычным и физически осмысленным требованием является *условие локальности*: операторы из базиса действуют на $O(1)$ кубитов (т. е. задают преобразования пространств $\mathcal{B}^{\otimes r}$ в себя, где $r = O(1)$). Схема *размера* $s$ задается последовательностью операторов $U_1[A_1], U_2[A_2], \ldots, U_s[A_s]$ длины $s$, каждый из которых является тензорным произведением одного из базисных операторов, действующих на подмножестве кубитов $A$, и тождественного оператора, действующего на остальных кубитах.

Преобразование, описываемое схемой, — это произведение

$$U = U_l[A_l] \cdot \ldots \cdot U_1[A_1]. \tag{1}$$

Среди кубитов схемы выделены $n$ входных битов и $m$ выходных. Схема, описывающая оператор $U$, *вычисляет* частично определенную функцию $f_U$, которая задается следующим образом:

$$f_U(x) = y, \quad \text{если } |\Pi_y U |x0^{N-n}\rangle| > 1 - \varepsilon, \tag{2}$$

где $\Pi_y$ — проектор на подпространство $|y\rangle \otimes \mathcal{B}^{N-m}$. В противном случае $f_U$ не определена. Величина $\varepsilon$, которая называется *точностью* вычисления, имеет смысл вероятности ошибки при вычислении. Без ограничения общности можно считать, что $\varepsilon = 1/3$.

Имея в виду класс вычисляемых схемами функций и рассматривая размер схемы с точностью «до полинома», можно ограничиться рассмотрением конечных базисов. Стандартным примером полного конечного базиса является *базис Шора* [56, 2], он содержит операторы $\{H, K, \mathrm{CNOT}, \mathrm{CCNOT}\}$, где первые два однобитовых оператора задаются матрицами

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad K = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \tag{3}$$

оператор CNOT определяется как

$$\mathrm{CNOT}\colon |a, b\rangle \mapsto |a, a \oplus b\rangle, \tag{4}$$

где $\oplus$ обозначает сложение по модулю 2, а последний — *элемент Тоффоли* — действует на трёх кубитах по правилу

$$\mathrm{CCNOT}\colon |a, b, c\rangle \mapsto |a, b, c \oplus ab\rangle. \tag{5}$$

## 2 Квантовые аналоги классических сложностных классов

Наиболее близким классическим аналогом квантового вычисления является вероятностное вычисление. В обоих случаях определена лишь вероятность $p$ правильного решения вычислительной задачи (скажем, если речь идёт о машине Тьюринга, распознающей некоторый язык, $p$ равно вероятности принимающего финального состояния). Стандартным способом перевода результата вычисления в детерминированную форму является задание пороговых вероятностей $0 \leqslant p_0 \leqslant 1/2 \leqslant p_1 \leqslant 1$. Результат считается достигнутым, если $p > p_1$ (или $p = 1$ при $p_1 = 1$), а если $p < p_0$ (или $p = 0$ при $p_0 = 0$), то считается, что результат не получен. Таким образом, и вероятностными, и квантовыми устройствами вычисляются вообще говоря частично определённые предикаты и функции.

Приведём основные примеры квантовых аналогов классических сложностных классов.

### 2.1 Класс BQP

Класс BQP [22, 8, 20] — квантовый аналог класса BPP, введённого в [33] для формализации понятия эффективного вероятностного вычисления. Приведем определение класса BQP, использующее схемную модель квантового вычисления (определение, использующее квантовые машины Тьюринга см., например, в [21]). Предварительно заметим, что квантовую схему в базисе Шора размера $s$ можно описать последовательностью $W = (u_j, a_j, b_j, c_j)$, $j = 1, \ldots, s$, каждый элемент которой описывает $j$-й оператор схемы: $u_j$ указывает на выбор одного из базисных операторов, а $a_j$ (как и $b_j, c_j$, если они применимы для выбранного базисного оператора) указывает на номер (или номера) кубитов, к которым применяется выбранный оператор. Итак, последовательности $W$ соответствует квантовая схема, которая описывает некоторый унитарный оператор, этот оператор обозначим через $U(W)$.

**Определение 1.** Предикат $L$ (возможно, частично определённый) принадлежит классу BQP, если существует такая машина Тьюринга $M$ (классическая), которая работает на любом входном слове $x$ полиномиальное время (существует такой многочлен $q(\cdot)$, что вероятность работы $M$ дольше $q(|x|)$ шагов равна 0), и результатом ее работы на входе $x$ является описание $W_x$ некоторой квантовой схемы, что при $L(x) = 1$ вероятность успешного вычисления на входе $|0^m\rangle$ (значение первого кубита равно 1), задаваемая формулой

$$p = \langle 0^m | U(W_x)^\dagger \Pi_1^{(1)} U(W_x) | 0^m \rangle, \tag{6}$$

больше $2/3$, а при $L(x) = 0$ вероятность успешного вычисления меньше $1/3$. Используя введенные выше обозначения, можно сказать, что $p_0 = 1/3$, $p_1 = 2/3$.

Пороговые вероятности можно выбрать экспоненциально близкими к 0 и 1 [21], добиваясь сколь угодно высокой надежности полученного результата, поскольку в случае класса BQP применима стандартная техника усиления вероятностей. Здесь имеется в виду зависимость от длины входа $n$. Более

того, тот же класс BQP получается, если в определении 1 выбрать пороговые вероятности с полиномиальным зазором: $p_1 - p_0$ порядка $n^{-c}$, где $c$ — константа. Это следует из того, что вероятность $p$ успешного завершения работы можно оценить с такой точностью за полиномиальное число шагов.

Как показали Нилл и Лафламм [40], ещё одно определение для класса BQP можно получить, если рассматривать вместо вероятности, задаваемой формулой (6), квадрат модуля любого наперёд заданного матричного элемента оператора $U_x$, задаваемого однородной по $x$ последовательностью квантовых схем (ещё один вариант формулировки см. ниже, теорема 4).

Варьируя в определении 1 пороговые вероятности, можно получить сложностные классы, отличные от BQP.

Если взять $p_0 = 0, p_1 = 1$, получится определение класса EQP. У этого класса нет вероятностного аналога, так как при таком выборе пороговых вероятностей в классическом случае получится просто класс P. О классе EQP известно довольно мало. Релятивизированные результаты [23, 21, 59] показывают, что маловероятно совпадение EQP с P. Однако никаких естественных задач, принадлежащих EQP, в настоящее время неизвестно.

Противоположный предельный случай получается, если выбрать пороговые вероятности равными $1/2$: $p_0 = p_1 = 1/2$. В вероятностных вычислениях этот случай отвечает классу PP. Оказывается, что определенный таким образом квантовый класс также совпадает с PP (лёгкое следствие из доказательства теоремы 2, см. ниже).

Если $p_0 = p_1 = 0$, то получается класс, который в [8] был назван классом недетерминированного полиномиального квантового вычисления (обозначение NQP).

## 2.2 Интерактивные квантовые доказательства

В силу вероятностной природы квантового вычисления невозможно дать разумное определение квантовых аналогов полиномиальной иерархии (определение классов иерархии см. в [1, 3, 5]). Вероятностный аналог классов полиномиальной иерархии приводит к играм Артура — Мерлина, которые ввёл в теорию сложности Л. Бабаи [16]. Их естественным обобщением являются системы интерактивных доказательств, введённые Голдвассер, Микали и Ракоффом [34] — одно из центральных понятий современной теории сложности вычислений. В классическом варианте система интерактивных доказательств состоит из двух игроков — проверяющего и доказывающего. Проверяющий и доказывающий обмениваются сообщениями. Проверяющий игрок по вычислительным возможностям является полиномиально ограниченной вероятностной машиной Тьюринга. Возможности доказывающего игрока ничем не ограничены. Его цель — убедить проверяющего в справедливости некоторого утверждения.

Квантовый аналог интерактивных доказательств устроен так же, только игроки могут использовать квантовую информацию. Часть данных каждого из игроков недоступна для его партнера. Точное определение квантовых интерактивных доказательств выполнимости предиката $L(x)$ дадим в модели квантовых схем, следуя [39].

Квантовый проверяющий с параметрами $k, q_V, q_M$ (где $k(\cdot)$, $q_V(\cdot)$, $q_M(\cdot)$ — полиномиально ограниченные функции из $\mathbb{N}$ в $\mathbb{N}$) — это полиномиально вычислимая (на классической машине Тьюринга) функция $V\colon \{0,1\}^* \to \{0,1\}^*$, значение $V(x)$ которой интерпретируется как набор $(V(x)_1, \ldots, V(x)_{k(|x|)})$ описаний квантовых схем, действующих на $q_V(|x|) + q_M(|x|)$ кубитах, причём указано, какие кубиты являются кубитами проверяющего (всего их $q_V(|x|)$ штук), а какие — кубитами, предназначенными для обмена сообщениями. Схема, описывающая $V(x)_j$, составлена в базисе Шора и имеет полиномиальный от $|x|$ размер. Один из кубитов проверяющего объявляется битом результата (туда проверяющий вносит свой вердикт).

Квантовый доказывающий с параметрами $l, q_P, q_M$ определяется аналогично, но теперь это произвольная функция $P\colon \{0,1\}^* \to \{0,1\}^*$, значение $P(x)$ которой интерпретируется как набор $(P(x)_1, \ldots, P(x)_{l(|x|)})$ описаний квантовых схем, действующих на $q_P(|x|) + q_M(|x|)$ кубитах, причём указано, какие кубиты являются кубитами доказывающего. Никаких ограничений на схемы $P(x)_j$ нет.

Квантовая система интерактивных доказательств с параметром $m$, где $m(\cdot)$ — некоторая функция из $\mathbb{N}$ в $\mathbb{N}$ (количество сообщений между игроками), задаётся указанием пары $(V, P)$ из квантового проверяющего и квантового доказывающего, согласованных в том смысле, что

- количество общих для обоих игроков кубитов во всех схемах $V(x)_i$, $P(x)_j$ одинаково;
- $k(|x|) = \lfloor m(|x|)/2 + 1 \rfloor$, $l(|x|) = \lfloor m(|x|)/2 + 1/2 \rfloor$.

Для каждого входного слова $x$ квантовая система доказательств определяет квантовую схему $(V(x), P(x))$, которая получается последовательным применением схем

$$P(x)_1, V(x)_1, \ldots P(x)_{(m(|x|)+1)/2}, V(x)_{(m(|x|)+1)/2},$$

если $m(|x|)$ нечетно, и схем

$$V(x)_1, P(x)_1, \ldots P(x)_{m(|x|)/2}, V(x)_{m(|x|)/2+1},$$

если $m(|x|)$ четно.

Вероятность того, что $(V, P)$ принимает входное слово $x$, равна вероятности значения 1 в кубите результата после применения схемы $(V(x), P(x))$ к кубитам, первоначально установленным в 0.

**Определение 2.** Пусть $m\colon \mathbb{N} \to \mathbb{N}$, $a, b\colon \mathbb{N} \to [0,1]$. Тогда класс $\mathrm{QIP}(m, a, b)$ состоит из таких языков $L$, для которых существует такой проверяющий $V$, что

- существует доказывающий $P$, образующий вместе с $V$ квантовую систему интерактивного доказательства за $m$ раундов, такой что для любого $x \in L$ система $(V, P)$ принимает $x$ с вероятностью по крайней мере $a(|x|)$;
- для любой системы $(V, P')$ и любого $x \notin L$ вероятность того, что $(V, P')$ принимает $x$, не превосходит $b(|x|)$.

Через QIP обозначается объединение классов $\mathrm{QIP}(m, 2/3, 1/3)$ по всем полиномиально ограниченным функциям $m$, а через $\mathrm{QIP}(k)$, $k$ константа, — класс с односторонней ошибкой $\mathrm{QIP}(k, 1, 1/2)$. Заметим, что класс $\mathrm{QIP}(1, 2/3, 1/3)$ обозначается в [3] через BQNP и является наиболее точным квантовым аналогом класса NP — см. соответствующие результаты в п. 3.6.

Аналогично определению 2 даётся определение квантовых доказательств с несколькими доказывающими и соответствующего класса QMIP, который обобщает классический класс MIP [63]. При этом не только не разрешается взаимодействие между доказывающими во время работы, но и никакого предварительного взаимодействия между ними также не допускается: как и в определении 2 мультиинтерактивная система доказательств (точнее, определяемая ею схема) применяется к кубитам, установленным в 0.

## 2.3 Другие примеры квантовых аналогов

Для формализации эффективного параллельного вычисления в теории сложности используется класс NC (см. [5]). Этот класс описывается однородными семействами схем полиномиального размера и полилогарифмической глубины. Квантовый аналог этого класса введён К. Муром и М. Нильсоном в [48]. Для его определения необходимо лишь определить глубину квантовой схемы. Сделать это можно так. Назовём квантовую схему однослойной, если она представляется в виде тензорного произведения локальных операторов (другими словами, базисные операторы в схеме действуют на непересекающие множества кубитов). Тогда схема глубины $d$ есть композиция $d$ однослойных схем. Класс QNC определяется аналогично схемному определению класса BQP, только на схемы, которые участвуют в определении накладывается дополнительное условие: их глубина должна быть полилогарифмической.

Аналогичным образом в [46] определяются квантовые аналоги QAC, QACC, QACC[$q$] классов AC, ACC, ACC[$q$] (в этих классах допускаются базисные элементы с неограниченным количеством входов). Заметим, что в квантовом случае оказывается существенным ограничение на степень ветвления кубита, поскольку операторы в одном слое должны применяться к непересекающимся множествам кубитов. Поэтому даже включение $\mathrm{AC}^0 \subseteq \mathrm{QAC}^0$ (схемы глубины $O(1)$) требует доказательства (приводится в [46]).

В работе [47] построены квантовые аналоги конечных автоматов и контекстно-свободных грамматик. Последние определяются через квантовый аналог автоматов с магазинной памятью (стеком). Квантовый аналог конечного автомата получается заменой конечного множества состояний на конечномерное пространство. Каждому символу входного алфавита теперь приписывается унитарное преобразование на пространстве состояний. После прочтения входного слова происходит измерение: проекция на подпространство принимающих состояний. Таким образом определяется вероятность

того, что квантовый автомат принимает входное слово. Используя пороговые вероятности, можно определить класс языков, принимаемых квантовыми конечными автоматами.

В работах [15, 44] рассмотрены квантовые аналоги двусторонних автоматов (допускается движение по ленте в обе стороны), причём в [15] рассматривается смешанная модель, в которой имеются как классические, так и квантовые состояния.

# 3 Сравнение с классическими сложностными классами

Наиболее важен вопрос о месте класса BQP в общей иерархии сложностных классов. По сути это вопрос о возможностях квантовых компьютеров, сформулированный на языке теории сложности.

## 3.1 Включения в BQP

Какие классы сложности содержаться в BQP? Прогресс в этом вопросе пока крайне незначителен.

**Теорема 1** (Бернштейн, Вазирани [20]). $\mathrm{BPP} \subseteq \mathrm{BQP}$.

Сам по себе этот результат почти очевиден, поскольку не представляет никакого труда создать запас случайных кубитов с помощью оператора

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

Ни про какие другие классы, естественным образом возникающие в теории классической сложности, неизвестно их включение в BQP.

Знаменитый алгоритм Шора [53, 54] показывает, что класс BQP содержит задачи, принадлежность которых классу BPP сомнительна (факторизация целых чисел, дискретный логарифм). Но про эти задачи неизвестны результаты о полноте в каких-либо классических классах.

## 3.2 Включения BQP

В той же работе [20] Бернштейн и Вазирани установили включение $\mathrm{BQP} \subseteq \mathrm{PSPACE}$. Уже из этого результата видно, что сравнение классической и квантовой сложности — очень трудная задача: если было бы доказано строгое включение $\mathrm{P} \subset \mathrm{BQP}$, то из него следовало бы включение $\mathrm{P} \subset \mathrm{PSPACE}$, которое является одной из основных недоказанных гипотез теории вычислительной сложности.

В работе [8] установлено более сильное включение.

**Теорема 2** (Адлеман, Демарье, Хуанг [8]). $\mathrm{BQP} \subseteq \mathrm{PP}$.

В работе [31] получено усиление этого результата, а именно, установлено включение класса BQP в некоторый подкласс PP, который обозначается AWPP. Этот класс формализует представление о задачах, для которых возможно так называемое «усиление вероятностей» (amplification). Поскольку включение $\mathrm{BQP} \subset \mathrm{AWPP}$ — самое сильное из известных в настоящее время включений, дадим описание этого класса. Для этого необходимо переформулировать определение класса PP в терминах классов перечислительной сложности.

Основной класс перечислительной сложности #P был введён Валиантом [62] по аналогии с классом P.

**Определение 3.** Класс #P образован функциями $f\colon \{0,1\}^* \to \mathbb{N}$, которые удовлетворяют следующему условию: существуют такой предикат от двух переменных $Q(\cdot,\cdot) \in \mathrm{P}$ и полином $q(\cdot)$, что для любого $x$ выполнено

$$f(x) = \bigl|\{y : Q(x,y) \ \&\ |y| = q(|x|)\}\bigr|. \tag{7}$$

Феннер, Фортнау и Курц [26] ввели естественное обобщение класса #P, замкнутое относительно вычитания.

**Определение 4.** Класс GapP образован функциями $f\colon \{0,1\}^* \to \mathbb{Z}$, которые удовлетворяют следующему условию: существует такие два предиката от двух переменных $Q_1(\cdot,\cdot) \in \mathrm{P}$, $Q_2(\cdot,\cdot) \in \mathrm{P}$ и полином $q(\cdot)$, что для любого $x$ выполнено

$$f(x) = \bigl|\{y : Q_1(x,y) \ \&\ |y| = q(|x|)\}\bigr| - \bigl|\{y : Q_2(x,y) \ \&\ |y| = q(|x|)\}\bigr|. \tag{8}$$

Класс GapP в перечислительной сложности является аналогом класса PP:

**Утверждение 1** ([26]). *Язык $L$ принадлежит* PP *тогда и только тогда, когда есть такая функция $f \in$ GapP, что*

$$x \in L \implies f(x) > 0, \quad x \notin L \implies f(x) < 0. \tag{9}$$

Теперь дадим определение класса AWPP [26, 27].

**Определение 5.** Язык $L$ принадлежит классу AWPP если и только если выполнено следующее условие: для любого полинома $q$ найдутся такие GapP-функция $f$ от двух аргументов и вычислимая за полиномиальное время функция $g$, что для любого слова $x$ и числа $m \geqslant |x|$ выполнено

$$\begin{aligned} &0 < f(x, 1^m) < g(1^m), \\ &x \in L \implies f(x, 1^m) \geqslant \left(1 - 2^{-q(m)}\right) g(1^m), \\ &x \notin L \implies f(x, 1^m) \leqslant 2^{-q(m)} g(1^m). \end{aligned}$$

**Теорема 3** (Фортнау, Рожерс [31]). BQP $\subseteq$ AWPP.

Это наиболее сильное известное в настоящее время ограничение сверху класса BQP. Теорема 3 допускает более или менее прямые доказательства как в модели квантовых машин Тьюринга, так и в модели однородных квантовых схем.

## 3.3 Полные задачи

Для класса BQP, как и для класса BPP, неизвестны полные относительно полиномиальной сводимости задачи (определение полиномиальной сводимости см. в книге [1]).

Однако, если рассматривать частично определенные предикаты, то полные задачи появляются для обоих этих классов. Как и следует ожидать, полной является задача предсказания результата работы квантовой машины Тьюринга за указанный промежуток времени (при условии, что вероятности положительного и отрицательного ответа $p_1$ и $p_0$ соответственно удовлетворяют неравенству $p_1 - p_0 = \Omega(n^{-\alpha})$, где $\alpha > 0$ — константа) или результата работы квантовой схемы (при тех же ограничениях).

Более интересные примеры BQP-полных (в указанном выше смысле) задач найдены Ниллом и Лафламмом. В работе [40] они показали, что задача оценки величины заданного матричного элемента оператора, реализированного заданной квантовой схемой, является BQP-полной.

**Теорема 4** (Нилл, Лафламм [40]). *Пусть $U = U_m \cdot \ldots \cdot U_1$ — унитарный оператор на $\mathcal{B}^{\otimes n}$, заданный как произведение операторов из некоторого полного квантового базиса. Тогда следующая задача является* BQP*-полной:*

сравнить $\mathrm{Re}\langle 0^n|U|0^n\rangle$ с $1/2$, если известно, что выполнено условие $|\,\mathrm{Re}\langle 0^n|U|0^n\rangle - 1/2| > 1/4$.

Еще более интересная BQP-полная задача приведена в [41].

**Теорема 5** (Нилл, Лафламм [41]). *Следующая задача является* BQP*-полной:*

Оценить знак суммы

$$S = \sum_{Ax=0, x\in\{0,1\}^n} (-1)^{x^T B x} 4^{\|x\|} 3^{n-\|x\|}, \tag{10}$$

при условии, что $|S| > 5^n/2$.

*Здесь $A$ — $(0,1)$-матрица размера $n \times n$, на диагонали которой стоят единицы ($a_{ii} = 1$), а матрица $B$ получается из матрицы $A$ заменой на нули всех элементов, стоящих на главной диагонали и выше нее, $\|x\|$ — количество единиц в записи $x$.*

## 3.4 Известны ли все быстрые квантовые алгоритмы?

Неформальный вопрос, вынесенный в название этого подраздела, допускает более точную формулировку. Прежде чем перейти к ней, сделаем общее замечание. Несмотря на интенсивные исследования в данной области, за последние 8 лет не появилось никаких эффективных квантовых алгоритмов, принципиально отличающихся от алгоритма Шора. Это даёт основания выдвинуть гипотезу об универсальном характере алгоритма Шора. Может оказаться, что вся вычислительная сила квантовых алгоритмов исчерпывается задачами, которые решил Шор, или найденными к настоящему времени их обобщениями. Самым простым таким обобщением является задача нахождения стабилизатора элемента при эффективно заданном действии абелевой группы.

Приведем формулировку этой задачи. Пусть $G$ — группа, действующая на конечном множестве $M$. Предположим, что это действие, а также групповые операции в $G$ эффективно вычислимы. Требуется вычислить стабилизатор данного элемента $a \in M$. Всякая конечно порожденная абелева группа гомоморфна $\mathbb{Z}^k$, так что при рассмотрении действия абелевых групп без ограничения общности можно считать, что $G = \mathbb{Z}^k$. Предполагая заданной некоторую эффективно вычислимую кодировку множества $M$, можно также считать, что $M$ — некоторое подмножество булева куба $\{0,1\}^n$.

Задача об абелевом стабилизаторе определяется следующими параметрами:

- Два натуральных числа $k$ и $n$. Пара $(k,n)$ называется размером задачи.
- Элемент $a \in \{0,1\}^n$.
- Функция $F\colon \mathbb{Z}^k \times M \to M$ $(a \in M \subseteq \{0,1\}^n)$, такая, что

$$F(0,x) = x, \quad F(g+h,x) = F(g,F(h,x))$$
$$\text{для любых } g,h \in \mathbb{Z}^k,\ x \in M.$$

Стабилизатором элемента $a$ относительно функции $F$ называется множество $\mathrm{Stab}_F(a) = \{g \in \mathbb{Z}^k : F(g,a) = a\}$. Это — подгруппа группы $\mathbb{Z}^k$ индекса $\leqslant |M| \leqslant 2^n$. Следовательно, $\mathrm{Stab}_F(a)$ изоморфна $\mathbb{Z}^k$ и имеет базис $(g_1,\ldots,g_k)$ полиномиального размера, т. е. $\sum_{j=1}^k \mathrm{size}(g_j) \leqslant \mathrm{poly}(n+k)$. Любой такой базис может служить решением задачи о стабилизаторе.

Теперь можно строго сформулировать вопрос, вынесенный в название раздела.

**Проблема 1.** Верно ли, что задача о нахождении абелева стабилизатора BQP-полна относительно сводимости по Тьюрингу?

Это означает, что любой язык из класса BQP распознается за полиномиальное время на машине Тьюринга с оракулом, который по описанию задачи об абелевом стабилизаторе выдаёт одно из её решений.

Положительное решение проблемы 1 означало бы, что класс BQP содержится в полиномиальной иерархии. Действительно, ответ в задаче об абелевом стабилизаторе может быть сформулирована как $\Sigma_2$-условие. А именно, существуют такие $g_1,\ldots,g_k \in \mathbb{Z}^k$, что

- для любого набора показателей $\alpha_1,\ldots,\alpha_k$, $0 \leqslant \alpha_j < 2^n$, элемент $\sum_j \alpha_j g_j$ принадлежит $\mathrm{Stab}_F(a)$;
- для любого представителя $g$ ненулевого класса смежности $\mathbb{Z}^k$ по подгруппе, порождённой $(g_1,\ldots,g_k)$, $F(g,a) \neq a$.

## 3.5 Положение BQP в PP

Наиболее сильные результаты, относящиеся к положению класса BQP в иерархии классов сложности, принадлежат Фортнау и Роджерсу. В работе [31] они показали, опираясь на более ранние результаты Л. Ли [45] и теорему 3, что $\mathrm{PP}^{\mathrm{BQP}} = \mathrm{PP}$. Если $X^Y = X$, то говорят, что класс $Y$ низок для класса $X$.

Ясно, что если $Y$ низок для $X$, то $Y \subseteq X$. Но, опираясь на косвенные доводы, можно сказать и бóльшее. Например, из результатов С. Тода [60] следует, что равенство $\mathrm{PP} = \mathrm{PP}^{\mathrm{PP}}$ маловероятно, т. е., по-видимому, класс PP не слаб относительно самого себя. Таким образом, получаем косвенный довод в пользу строгого включения $\mathrm{BQP} \subset \mathrm{PP}$.

С другой стороны, этот же результат можно использовать и для выделения задач, потенциально допускающих эффективные квантовые алгоритмы. Например, в работе [43] показано, что задача

распознавания изоморфизма графов GI лежит в AWPP (на самом деле, там установлено даже более сильное включение). Поэтому шансы построить эффективный квантовый алгоритм для GI выше, чем для задач, вхождение которых в AWPP не установлено.

## 3.6 Классы интерактивных квантовых доказательств

В характеризации квантовых аналогов интерактивных доказательств за последние два года были достигнуты наиболее значительные успехи.

Вначале приведем основные результаты, относящиеся к квантовым доказательствам с одним доказывающим.

**Теорема 6** ([66]). PSPACE $\subseteq$ QIP(3).

Этот результат показывает, что квантовые интерактивные доказательства, по-видимому, гораздо сильнее классических: напомним, что известные интерактивные доказательства для языков из PSPACE требуют полиномиального числа раундов: PSPACE = IP(poly) [52]. В дальнейшем было установлено, что квантовое доказательство за полиномиальное число раундов имитируется за 3 раунда:

**Теорема 7** ([39]). QIP $\subseteq$ QIP(3).

В той же работе было показано, что один квантовый доказывающий, скорее всего, не может заменить нескольких классических. Известно, что MIP = NEXPTIME [32]. С другой стороны, имеет место следующий результат.

**Теорема 8** ([39]). QIP(3) $\subseteq$ EXPTIME.

Поэтому из MIP $\subseteq$ QIP следовало бы NEXPTIME = EXPTIME, что представляется сомнительным.

Совсем недавно получен результат, полностью описывающий класс QMIP.

**Теорема 9** ([42]). QMIP = NEXPTIME = MIP.

Итак, интерактивные доказательства с несколькими доказывающими уже нечувствительны к дополнительным возможностям, предоставляемым квантовыми компьютерами.

Меньше известно про квантовые интерактивные доказательства с ограниченным количеством сообщений.

**Теорема 10** ([3]). QIP$(1, 2/3, 1/3)$ = BQNP $\subseteq$ PP.

Доказательство этого результата опирается на полноту задачи о локальном гамильтониане в BQNP. (При этом, как и для класса BQP рассматриваем частично определённые предикаты и функции.)

Оператор $H\colon \mathcal{B}^{\otimes n} \to \mathcal{B}^{\otimes n}$ называется *$k$-локальным гамильтонианом*, если он выражается в виде

$$H = \sum_j H_j[S_j],$$

где каждое слагаемое — эрмитов оператор, действующий на множестве кубитов $S_j$, $|S_j| \leqslant k$, на остальных кубитах он действует тождественно.

При этом выполнено условие нормировки $0 \leqslant H_j \leqslant 1$ (другими словами, и $H_j$, и $I - H_j$ — положительно полуопределённые).

Задача о локальном гамильтониане задается частично определённой булевой функцией $F$, определенной на множестве троек $Z$ вида

$$(\langle\text{описание } k\text{-локального гамильтониана } H\rangle, a, b),$$

где $k = O(1)$, $0 \leqslant a < b$, $b - a = \Omega(n^{-\alpha})$, $(\alpha > 0)$. Для $z \in Z$

$$F(z) = 1 \iff \text{если у } H \text{ есть собственное число, не большее } a,$$
$$F(z) = 0 \iff \text{если все собственные числа } H \text{ больше } b.$$

**Утверждение 2** ([3]). *Задача о локальном гамильтониане принадлежит* BQNP *и любая задача из* BQNP *сводится к задаче о локальном гамильтониане.*

Оценка собственного числа гамильтониана может быть сделана путём вычисления следа достаточно большой степени этого гамильтониана.

## 3.7 Характеризации классов квантовой сложности

Наряду с теоремой 9 известны ещё две точные характеризации квантовых классов сложности в терминах классических классов.

Первая найдена Яо и Ямаками. Она выражает класс NQP через ещё один класс перечислительной сложности, обозначаемый co-$C_=P$.

**Определение 6.** Класс co-$C_=P$ составляют те языки $L$, для которых существует такая GapP-функция $f$, что

$$x \in L \implies f(x) \neq 0, \quad x \notin L \implies f(x) = 0. \tag{11}$$

**Теорема 11** ([69]). NQP = co-$C_=P$.

Напомним, что NQP определяется нулевыми пороговыми вероятностями. Таким образом, этот результат можно понимать как указание на то, что проверка равенства нулю вероятности успеха квантового вычисления является вычислительно трудной. Обобщением этого наблюдения является следующая теорема.

**Теорема 12** ([28]). *Для любой функции* $f \in$ GapP *существуют такие полиномиально ограниченная квантовая машина Тьюринга* $M$, *элементы матрицы переходов которой принадлежат* $\{0, \pm 1/\sqrt{2}, \pm 1\}$, *и многочлен* $p$, *что*

$$\mathsf{P}(M \text{ принимает } x) = \frac{f(x)}{2^{p(|x|)}}. \tag{12}$$

Ещё одна точная характеризация описывает класс языков, вычислимых квантовыми машинами Тьюринга на полиномиальной памяти [64, 65].

**Теорема 13.** *Класс языков, распознаваемых квантовыми машинами Тьюринга на полиномиальной памяти, совпадает с* PSPACE.

## 3.8 Вычислительные возможности квантовых аналогов слабых вычислительных моделей

Обратимость (унитарность) квантового вычисления, вообще говоря, является ограничением на возможности вычислителя. Эта ограниченность проявляется при рассмотрении квантовых автоматов. Как показано в [44] языки, распознаваемые квантовыми автоматами, являются строгим подмножеством класса регулярных языков (т. е. языков, распознаваемых обычными конечными автоматами). Ограниченность возможностей модели квантовых автоматов позволяет также устанавливать количественные соотношения между сложностью классических и квантовых автоматов, распознающих один и тот же язык [14, 7].

Уже на следующем уровне вычислительной иерархии — в схемах конечной глубины — ситуация меняется. В работе [46] доказана цепочка включений

$$\mathrm{AC}^0 \subset \mathrm{ACC}^0[2] \subset \mathrm{ACC}^0 \subseteq \mathrm{QAC}^0_{\mathrm{wf}} = \mathrm{QACC}^0[2] = \mathrm{QACC}^0 \tag{13}$$

(первые два включения давно известны из работ А. Разборова и Р. Смоленского по классической схемной сложности). Здесь $\mathrm{QAC}^0_{\mathrm{wf}}$ обозначает класс схем, в которых добавлены элементы, размножающие данный кубит (обратимое копирование в несколько мест). Этот результат резко контрастирует с известным из классической теории неравенством $\mathrm{ACC}^0[p] \neq \mathrm{ACC}^0[q]$.

В работах [35, 36] получен ряд дополнительных результатов об этих классах, в частности, доказано, что $\mathrm{QACC}[q] = \mathrm{QACC}$.

Следующий уровень классической иерархии представляет класс $\mathrm{NC}^1$, которому принадлежат функции, вычислимые однородными семействами схем полиномиального размера и логарифмической глубины. Хорошо известная теорема Баррингтона [17] характеризует класс $\mathrm{NC}^1$ как класс функций, вычислимых полиномиальными по размеру перестановочными бинарными программами ограниченной ширины (достаточна ширина 5). Недавно получена аналогичная характеризация класса $\mathrm{NC}^1$ в терминах квантовых бинарных программ [6]. Оказывается, что класс $\mathrm{NC}^1$ характеризуется как класс функций, вычислимых полиномиальными бинарными программами ширины 2.

### 3.9 Квантовые вычисления с малым объёмом квантовой памяти

Вполне можно ожидать, что сложность реализации квантового вычислителя будет сильно зависеть от объёма используемой этим вычислителем памяти. Поэтому представляется важным вопрос о силе квантовых вычислений на небольшой квантовой памяти. Здесь рассматривается смешанная, квантово-классическая модель вычислений, в которой допускаются классические биты, измерения квантовых битов, порождающие классические биты, а также классическое управление операторами над квантовыми битами.

Возможна ли реализация алгоритма Шора, или даже универсального квантового вычисления, с небольшим (полилогарифмическим от размера входа) числом квантовых битов? Такая реализация предполагает построение «генератора псевдоквантовых битов» — алгоритма, который используя небольшое число «затравочных» истинно квантовых битов, организует так работу с ними, чтобы моделировать алгоритмы, использующие гораздо большее число квантовых битов.

Заметим также, что возможность моделирования универсального квантового вычисления на полилогарифмической квантовой памяти означает, что квантовое вычисление моделируется классическим за время $2^{\log^{O(1)} n}$. С одной стороны это само по себе означало бы возможность более быстрого решения задачи факторизации, чем в существующих в настоящее время алгоритмах ($2^{n^{O(1)}}$), что представляет определённый интерес с точки зрения математической криптографии. С другой стороны, такой результат был бы косвенным подтверждением гипотезы о том, что $\mathrm{NP} \not\subseteq \mathrm{BQP}$, которая представляется правдоподобной большинству исследователей.

Сформулируем наиболее перспективный на настоящий момент подход к решению этой проблемы. Как и в классическом случае, можно определить глубину квантовой схемы как наименьшее число слоев, в которые можно разместить элементы схемы так, чтобы вычисление в одном слое можно было произвести одновременно (одновременно можно применять базисные операторы к непересекающимся квантовым регистрам). Малая глубина схемы показывает, что вычисления по этой схеме поддаются массивному распараллеливанию.

**Проблема 2.** Возможно ли моделирование квантовых схем глубины $d$ на памяти $\mathrm{poly}(d)$?

Более точно, существует ли квантово-классическая машина Тьюринга, которая по описанию квантовой схемы $U$ глубины $d$ определяет результат измерения в классическом базисе результата применения схемы $U$ ко входу $|0^m\rangle$ с той же по порядку вероятностью ошибки, что и вероятность ошибки в схеме $U$. При этом моделирующая квантово-классическая машина Тьюринга может использовать не более $\mathrm{poly}(d)$ квантовых битов и должна работать за полиномиальное (от длины описания схемы $U$) общее время.

## 4 Результаты о сравнении релятивизированных классов

В теории сложности весьма популярным направлением является исследование соотношений между релятивизированными классами сложностей. Суть данного подхода проще всего объяснить на следующем примере. Как известно, проблема $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$ является одной из важнейших нерешенных на сегодняшний день математических проблем. Но что будет, если полиномиальному детерминированному (класс P) и полиномиальному недетерминированному (класс NP) алгоритмам дозволяется в процессе своей работы получать дополнительную помощь от оракула? В любой момент времени алгоритм может за один шаг вычисления узнать у оракула, принадлежит ли данная (выбранная алгоритмом) строка $x$ данному фиксированному языку (множеству) $A$. Существуют также функциональные оракулы: за один шаг вычисления алгоритм может получить от оракула значение $F(x)$ данной фиксированной функции $F$. Здесь опять $x$ — значение, выбираемое алгоритмом. Если в определение произвольного класса сложностей $C$ внести единственное изменение, разрешающее алгоритмам, которые определяют этот класс, обращаться к оракулу для некоторого языка $A$, то получим определение нового класса сложностей. Этот класс обозначается через $C^A$ и называется релятивизированным. Обычно оракул для языка $A$ отождествляют с самим этим языком и говорят, что $C^A$ — это класс $C$, релятивизированный к оракулу $A$.

Интерес к релятивизированным классам сложностей вызван, в первую очередь, отсутствием на данный момент методов, позволяющих устанавливать соотношения между их нерелятивизированными «двойниками». Если неизвестно, совпадают ли классы сложностей $C_1$ и $C_2$, то что можно сказать о классах $C_1^A$ и $C_2^A$ для различных оракулов $A$? Так, в связи с проблемой $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$ построены оракулы $A$

и $B$ такие, что $\mathrm{P}^A \neq \mathrm{NP}^A$, но $\mathrm{P}^B = \mathrm{NP}^B$. Эти результаты в совокупности демонстрируют, главным образом, сложность самой проблемы $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$.

Вообще говоря, из существования оракула такого, что, скажем, $C_1^A = C_2^A$ следует только тот факт, что если на самом деле $C_1 \neq C_2$, то этот результат весьма нетривиален, поскольку он должен доказываться методом, не допускающим релятивизации.

Имеются веские основания считать, что гораздо более достоверную информацию о соотношении нерелятивизированных классов сложностей можно получить, если исследовать релятивизации не к произвольным, а к случайным или генерическим оракулам. Например, Беннетт и Джилл [19] доказали, что относительно случайного оракула $A$ с вероятностью 1, $\mathrm{P}^A \neq \mathrm{NP}^A$, и этот результат рассматривается как весьма серьезный аргумент в поддержку гипотезы, что $\mathrm{P} \neq \mathrm{NP}$.

В исследованиях квантовых классов сложностей и их соотношений с классическими также широко используется подход, основанный на релятивизации. Общая методология здесь аналогична классическому случаю, но имеется одно существенное отличие, которое обычно совершенно упускается из виду. Остановимся на этом более подробно.

В классическом случае алгоритмы всех типов (детерминированные, недетерминированные, вероятностные) получают от оракула одинаковую помощь. Каждый из них передает оракулу в качестве запроса единственную строку $x$ и получает в ответ либо один бит ($x \in A$ или $x \notin A$), либо значение функции $F$ на этом входе. Квантовый алгоритм (под которым всюду в данном разделе мы понимаем квантовую машину Тьюринга) может передавать оракулу суперпозицию запросов $\sum_x \alpha_x |x\rangle$ и получать в ответ суперпозиции вида $\sum_x \alpha_x |x \circ A(x)\rangle$. Здесь $A(x)$ — ответ оракула на запрос $x$, $\circ$ обозначает конкатенацию. Такой квантовый оракул представляется значительно более мощным, чем классический. Но классические алгоритмы не могут работать с квантовыми оракулами. Поскольку не доказано (и это представляется неправдоподобным), что помощь, получаемая от квантового и классического оракулов для одного и того же языка $A$ (одной и той же функции $F$) равноценна, все результаты о соотношениях между релятивизированными классическими и квантовыми классами сложностей должны интерпретироваться следующим образом. Пусть $C_1$ — классический класс сложностей, а $C_2$ — квантовый. Если для некоторого оракула $A$ доказано, что $C_2^A \subset C_1^A$ (строгое включение), то этот результат несколько сильнее, чем аналогичное утверждение в классическом случае: квантовый алгоритм, даже с более мощной поддержкой со стороны оракула, не достигает вычислительной мощности классического алгоритма. Если же доказано обратное включение $C_1^A \subset C_2^A$, то это — довольно слабый результат. Возможно, он отражает не преимущества квантовых алгоритмов над классическими, а лишь различие в мощности оракулов.

На первый взгляд может показаться, что приведенные выше рассуждения справедливы лишь для детерминированных и вероятностных алгоритмов и не относятся к недетерминированным. Ведь в последних количество вычислительных путей может быть экспоненциальным, а значит и количество различных запросов к оракулу также может быть экспоненциальным. Однако, рассмотрим определение класса NP: полиномиальная недетерминированная машина Тьюринга распознает язык $L$, если для всякого входного слова $x \in L$ существует вычислительный путь, приводящий в принимающее состояние, а для всякого $x \notin L$ такого пути нет. Именно это экзистенциальное условие приема слов из языка и доставляет недетерминированным алгоритмам гипотетическое преимущество над детерминированными. Всякий вычислительный путь, приводящий к успеху, рассматриваемый отдельно, представляет собой детерминированное вычисление и работает с оракулом так же, как детерминированный алгоритм. И все действия, выполняемые алгоритмом в данном вычислительном пути, никоим образом не зависят от ответов оракула на запросы, выданные в других вычислительных путях. В этом и состоит принципиальное отличие недетерминированных и квантовых вычислений с оракулами.

Резюмируя, подчеркнем, что вопреки утверждениям, встречающимся во многих работах по квантовым вычислениям, нам на данный момент не известно ни одного результата, даже релятивизированного, который доказывал бы, что квантовые машины Тьюринга мощнее классических.

Перейдем теперь к определению квантовой машины Тьюринга с оракулом [18]. Такая машина имеет специальную ленту для запросов к оракулу и два специальных состояния $q_q$ и $q_a$. Все ячейки ленты запросов содержат пробелы, за исключением одного непрерывного блока, содержащего строку вида $x \circ b$. Здесь $x \in \Sigma^*$ — запрос к оракулу, $b \in \Sigma$ — бит ответа, $\Sigma = \{0, 1\}$, а $\circ$, как и выше, обозначает конкатенацию строк. Если квантовая машина Тьюринга находится в состоянии $q_q$, то это означает, что выдан запрос к оракулу, который выполняется следующим образом, В случае, когда лента запросов пуста (содержит только пробелы), машина переходит в состояние $q_a$ и никаких других

изменений в ее конфигурации не происходит. Если же содержимое ленты запросов имеет вид $|x \circ b\rangle$, то машина переходит в состояние $q_a$, а на ленту запросов записывается $|x \circ (b \oplus A(x))\rangle$. Все остальные составляющие конфигурации машины при этом не меняются. Всякое обращение к оракулу считается одним тактом работы квантовой машины Тьюринга.

Если кубит ответа $|b\rangle$ изначально находился в состоянии $|0\rangle$, то в результате обращения к оракулу он будет содержать $|A(x)\rangle$, как и в классическом случае. Если же кубит ответа уже находился в состоянии $|A(x)\rangle$, то обращение к оракулу вернет его в состояние $|0\rangle$. Такая возможность весьма полезна в свете необходимости обеспечивать обратимость квантовых вычислений с оракулами.

Как уже отмечалось выше, квантовые машины Тьюринга могут выполнять суперпозиции запросов к оракулу. Если в момент обращения к оракулу $A$ лента запросов находилась в состоянии $\sum_{x,b} \alpha_{x,b}|x \circ b\rangle$, то в результате выполнения запроса будет получено состояние $\sum_{x,b} \alpha_{x,b}|x \circ (b \oplus A(x))\rangle$. Примером использования запросов к оракулу, в которых кубит ответа находится в суперпозиции состояний, может служить алгоритм Гровера. В самом деле, выполняемое этим алгоритмом условное инвертирование фазы может быть реализовано просто путем обращения к оракулу с кубитом ответа в суперпозиции $(|0\rangle - |1\rangle)/\sqrt{2}$.

В связи с использованием оракулов в квантовых вычислениях возникает одна проблема, не имеющая аналога в классическом случае. Предположим, что для функции, реализуемой оракулом (характеристическая функция языка $A$ или функция $F$) у нас есть квантовый алгоритм. Можно ли его использовать в качестве оракула, или, говоря иными словами, вызывать этот алгоритм в качестве подпрограммы? Ясно, что ответ на этот вопрос важен не только с теоретической, но и с практической точки зрения. Суть же проблемы состоит в следующем. Допустим, мы вызываем подпрограмму, которая вычисляет функцию $f$, и передаем ей строку $x$ в качестве аргумента. Поскольку подпрограмма может вызываться на суперпозиции различных $x$'ов, она должна стирать весь мусор в своей рабочей памяти и возвращать на ленте только значение $f(x)$. В противном случае различное содержимое рабочей памяти для различных $x$'ов может воспрепятствовать правильной интерференции вычислительных путей в вызывающей программе. Хорошо известно, что стирание содержимого памяти не является унитарной операцией. Столь же хорошо известно и решение указанной проблемы в том случае, если функция $f$ вычисляется детерминированным алгоритмом: на первом шаге вычисляется $f(x)$, на втором значение $f(x)$ копируется, а на третьем выполняется обращение вычислений первого шага, в результате чего первая копия значения $f(x)$ и содержимое рабочей памяти стираются.

Однако, в том случае, когда подпрограмма сама является квантовым алгоритмом (например, машиной из класса BQP), только часть ее вычислительных путей дает корректное значение $f(x)$. Поэтому, при попытке применить указанную выше процедуру получится следующее. На втором шаге в различных вычислительных путях будут скопированы различные выходные значения, и при попытке выполнить третий шаг эти значения могут воспрепятствовать правильной интерференции вычислительных путей (здесь речь идет о вычислительных путях подпрограммы).

Тем не менее, в работе [18] доказана теорема технического характера, из которой следует, например, что всякую машину из класса BQP, вычисляющую функцию $f$, можно преобразовать в машину из того же класса, у которой почти все (по вероятности) состояния заключительной суперпозиции содержат чистую ленту, на которой записаны лишь аргумент $x$ и значение $f(x)$. Формулировка этой теоремы требует следующих определений.

**Определение 7.** Функция $T\colon \mathbb{N} \to \mathbb{N}$ называется конструируемой (time-constructible), если существует детерминированная машина Тьюринга, которая на всяком входе $n \in \mathbb{N}$ останавливается через не более чем $T(n)$ шагов и вычисляет значение $T(n)$.

Заметим, что все обычно используемые в теории сложности и теории алгоритмов функции, характеризующие временну́ю сложность (степенные, показательные и т. п.) являются конструируемыми.

**Определение 8.** BQTime($T(n)$) обозначает класс языков, для каждого из которых существует квантовая машина Тьюринга со следующими свойствами:

1) время работы машины на любом входе длины $n$ не превосходит $T(n)$;

2) машина распознает данный язык с вероятностью по крайней мере $2/3$, т. е. вероятность принятия каждого слова из языка не меньше $2/3$, а вероятность принятия каждого слова, не принадлежащего языку, не больше $1/3$.

**Теорема 14.** *Если* $L \in \mathrm{BQTime}(T(n))$, *где* $T(n) > n$ *и* $T(n)$ *конструируема, то для всякого* $\varepsilon > 0$ *существует квантовая машина Тьюринга* $M$, *которая принимает язык* $L$ *с вероятностью* $1 - \varepsilon$, *и при этом:*

1) *на входах длины* $n$ *машина* $M$ *работает за время* $cT(n)$, *где* $c$ — *полином от* $\log 1/\varepsilon$;

2) *в заключительной суперпозиции машины* $M$ *вероятность состояния* $|x\rangle|L(x)\rangle$, *где* $L(x) = 1$, *если* $x \in L$ *и* $L(x) = 0$ *в противном случае, не меньше* $1 - \varepsilon$.

Для дальнейшего нам необходимо следующее определение.

**Определение 9.** Пусть $\mathrm{C}_1$ и $\mathrm{C}_2$ — классы сложностей. Тогда $\mathrm{C}_1^{\mathrm{C}_2} = \cup_{A \in \mathrm{C}_2} \mathrm{C}_1^A$.

**Следствие 1.** $\mathrm{BQP}^{\mathrm{BQP}} = \mathrm{BQP}$.

Основной же результат работы [18] — это исследование соотношения между классом NP и квантовыми классами сложностей в релятивизированном мире. После открытия Шором полиномиальных алгоритмов для задач факторизации и дискретного логарифмирования естественным образом возник вопрос о существовании таких алгоритмов для NP-полных задач. Как показывает следующая теорема, таких алгоритмов скорее всего нет.

**Теорема 15.** *Для любой функции* $T(n) \in o(2^{n/2})$ *и для случайного оракула* $A$ *с вероятностью* 1, $\mathrm{BQTime}^A(T(n)) \not\supseteq \mathrm{NP}^A$.

Из оценки сложности алгоритма Гровера следует, что граница $2^{n/2}$ — точная.

В работе [18] есть еще один результат, который показывает, что эффективных квантовых алгоритмов скорее всего не существует и для более узкого (гипотетически) класса, чем NP.

**Определение 10.** Функциональный оракул называется оракулом-перестановкой, если для каждого $n$ его ограничение на множество $\Sigma^n$ является перестановкой.

Напомним, что для произвольного класса сложностей C класс coC определяется следующим образом: $\mathrm{coC} = \{L : \Sigma^* \setminus L \in \mathrm{C}\}$.

**Теорема 16.** *Для любой функции* $T(n) \in o(2^{n/3})$ *и для случайного оракула-перестановки* $A$ *с вероятностью* 1, $\mathrm{BQTime}^A(T(n)) \not\supseteq \mathrm{NP}^A \cap \mathrm{coNP}^A$.

**Следствие 2.** *Для случайного оракула-перестановки с вероятностью* 1 *существует квантовая односторонняя перестановка.*

Такая перестановка эффективно вычислима с помощью оракула даже на детерминированной машине Тьюринга, но не имеет эффективных квантовых алгоритмов инвертирования (также имеющих доступ к оракулу). Подчеркнем, что здесь речь идет о так называемой некриптографической односторонней перестановке. Она может эффективно инвертироваться почти всюду; определение гарантирует лишь существование для любого эффективного алгоритма бесконечной последовательности значений, на которой он этого сделать не сможет.

В работе [31] получено несколько интересных результатов о соотношениях между релятивизированными классами сложностей, включающих класс BQP. Так, например, доказано, что класс BQP является низким в классе PP, т. е. $\mathrm{PP}^{\mathrm{BQP}} = \mathrm{PP}$. Это означает, что BQP-алгоритмы являются в определенном смысле слабыми для класса PP, т. к. использование их в качестве оракулов не расширяет этот класс.

Вопрос о существовании в классе BQP полных языков на данный момент остается открытым. В работе [31] построен оракул $A$ такой, что в классе $\mathrm{BQP}^A$ нет полных множеств.

Построен также оракул $A$ такой, что $\mathrm{P}^A = \mathrm{BQP}^A$, но $\mathrm{P}^A \neq \mathrm{UP}^A \cap \mathrm{coUP}^A$ и существуют односторонние функции. Здесь опять речь идет о некриптографических односторонних функциях. Класс UP определяется аналогично классу NP с той лишь разницей, что входное слово принимается тогда и только тогда, когда существует в точности одно принимающее вычисление на этом слове.

## Литература


[1] Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

[2] Китаев А. Ю. Квантовые вычисления: алгоритмы и исправление ошибок. УМН, № 6, 1997. 53–112.

[3] Китаев А. Ю., Шень А., Вялый М. Н. Классические и квантовые вычисления. М: МЦНМО, 1999.

[4] МакВильямс Ф. Дж., Слоэн Н. Дж. Теория кодов, исправляющих ошибки. М.: Связь, 1979.

[5] Стокмейер Л. Сложность вычислительных проблем. Киб. сборник. Вып. 26. М.: Мир, 1989. С. 20–83.

[6] Ablayev F., Moore Ch., Pollett Ch. Quantum and stochastic branching programs of bounded width. 2002. E-version: quant-ph/0201139.

[7] Ablayev F., Gainutdinova A. On the lower bounds for one-way quantum automata. Proc. of 25th Int. Symp. MFCS 2000, Bratislava. Springer-Verlag, 2000. 132–140.

[8] Adleman L., DeMarrais J., Huang M. Quantum computability. SIAM J. on Comput. 1997. **26**. № 5. 1524–1540.

[9] Aharonov D., Ben-Or M. Fault-tolerant quantum computation with constant error. 1996. E-version: quant-ph/9611025.

[10] Aharonov D., Ben-Or M. Polynomial simulations of decohered quantum computers. FOCS'37, 1996. 46–55.

[11] Aharonov D., Ben-Or M. Fault-tolerant quantum computation with constant error rate. 1999. E-version: quant-ph/9906129.

[12] Aharonov D., Ben-Or M., Impagliazzo R., Nisan N. Limitations of noisy reversible computation. 1996. E-version: quant-ph/9611028.

[13] Aharonov D., Kitaev A., Nisan N. Quantum Circuits with Mixed States. STOC'29, 1997. E-version: quant-ph/9806029.

[14] Ambainis A., Freivalds R. 1-way quantum automata: strengths, weaknesses and generalization. FOCS'39. 1998. 332–342.

[15] Ambainis A., Watrous J. Two-way finite automata with quantum and classical states. E-version: cs.cc/9911009.

[16] Babai L. Trading group theory for randomness. STOC'17. 1985. 421–429.

[17] Barrington D. A. Bounded-width polynomial-size branching programs recognize exactly those languages in $NC^1$. Journal of Computer and System Sciences, **38**, 1989, 150–164.

[18] Bennett C. H., Bernstein E., Brassard G., Vazirani U. Strengths and weaknesses of quantum computing. SIAM J. on Comput. 1997. **26** 1510–1523. E-version: quant-ph/9701001.

[19] Bennett C. H., Gill J. Relative to a random oracle $A$, $P^A \neq NP^A \neq co\text{-}NP^A$ with probability 1. SIAM J. on Comput., 1981, **10**, № 1, 96–113.

[20] Bernstein E., Vazirani U. Quantum complexity theory. STOC'25. 1993, 11–20.

[21] Bernstein E., Vazirani U. Quantum complexity theory. SIAM J. on Comput. 1997. **26**. 1411–1473.

[22] Berthiaume A., Brassard G. The quantum challenge to structural complexity theory. Proc. of 7th IEEE Conf. on Structure in Complexity Theory. 1992. 132–137.

[23] Berthiaume A., Brassard G. Oracle quantum computing. J. of Modern Optics. 1994. V.41. 1411–1473.

[24] Deutsch D. Quantum theory, the Church–Turing principle and the universal quantum computer. Proc. R. Soc. Lond. **A 400**, 1985. 97.

[25] Deutsch D. Quantum computational networks. Proc. Roy. Soc. Lond. **A 425**,1989. 73.

[26] Fenner S., Fortnow L., Kurtz S. Gap-definable counting classes. J. of Comp. and Sys. Sci. 1994. **48**. 116–148.

[27] Fenner S., Fortnow L., Kurtz S., Li L. An oracle builder's toolkit. Proc. of 8th IEEE Conf. on Structure in Complexity Theory. 1993. 120–131.

[28] Fenner S., Green F., Homer S., Pruim R. Determining acceptance possibility for a quantum computation is hard for the polinomial hierarchy. Proc. of the Royal Society London. Ser. A, 1999. **455**. 3953–3966.

[29] Feynman R. P. Simulating physics with computers. International Journal of Theoretical Physics. 1982. **21** № 6/7. 467–488.

[30] Feynman R. P. Quantum mechanical computers. Optics News, February 1985. **11**. 11.

[31] Fortnow L., Rogers J. Complexity limitations on Quantum Computation. Proc. 13th Conference on Computational Complexity. 1998. 202–209. E-version: cs.CC/9811023.

[32] Fortnow L., Rompel J., Sipser M. On the power of multi-prover interactive protocols. Theoretical Computer Science. Vol 134. 1994. 545–557.

[33] Gill J. Computational complexity of probabilistic complexity classes. SIAM J. on Comput. 1977. **6**. 675–695.

[34] Goldwasser S., Micali S., Rackoff Ch. The knowledge complexity of interactive proof systems. SIAM J. on Comp. 1989. **18**. 186–208.

[35] Green F., Homer S., Moore C., Pollett C. Counting, fanout, and the complexity of quantum ACC. 2001. E-version: quant-ph/0106017.

[36] Green F., Homer S., Pollett C. On the complexity of quantum ACC. Proc. 15th Conf. on Computational Complexity. 2000. 250–262.

[37] Gruska J. Quantum Computing. McGraw-Hill, London, 1999.

[38] Kitaev A. Yu. Unpaired Majorana fermions in quantum wires. Proc. of the Mesoscopic and Strongly Correlated Electron Systems Conference. 2000. E-version: quant-ph/00010440.

[39] Kitaev A., Watrous J. Parallelization, amplification, and exponential time simulation of quantum interactive systems. STOC'32, 2000. 608–617.

[40] Knill E., Laflamme R. On the Power of One Bit of Quantum Computation. E-version: quant-ph/9802037.

[41] Knill E., Laflamme R. Quantum Computation and Quadratically Signed Weight Enumerators. E-version: quant-ph/9909094.

[42] Kobayashi H., Matsumoto K. On the Power of Quantum Multi-Prover Intractive Proof Systems. E-version: cs.CC/0102013.

[43] J. Köbler, U. Schöning, J. Torán. Graph isomorphism is low for PP. Computational Complexity. , 1992. **2**. 301–330.

[44] Kondacs A., Watrous J. On the power of quantum finite state automata. FOCS'38. 1997. 66–75.

[45] Li L. On the counting functions. PhD thesis, University of Chicago, 1993. Department of Computer Science, TR 93-12.

[46] Moore C. Quantum curcuits: fanout, parity and counting. E-version: quant-ph/9903046.

[47] Moore C., Crutchfield J. P. Quantum automata and quantum grammars. 1997. E-version: quant-ph/9707031.

[48] Moore C., Nilsson M. Parallel Quantum Computation and Quantum Codes. E-version: quant-ph/9808027.

[49] von Neumann J. Probabilistic logic and the synthesis of reliable organisms from unreliable components. Automata studies, 1956.

[50] Nielsen M. A., Chuang I. L. Quantum computation and quantum information. Cambridge University Press, 2000.

[51] Nissan N., Wigderson A. Hardness vs. randomness. FOCS'29, 1988. 2–11.

[52] Shamir A. IP = PSPACE. Journal of the ACM. 1992. **39**. 869–877.

[53] Shor P. W. Algorithms for quantum computation: discrete log and factoring. FOCS'35. 1994. 124–134.

[54] Shor P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. of Comput. 1997. **26**. 1484. E-version: quant-ph/9508027.

[55] Shor P. W. Scheme for reducing decoherence in quantum computer memory. Phys. Rev. A, 1995, **52**, R2493.

[56] Shor P. W. Fault-tolerant quantum computation. FOCS'37. 1996. 56–65. E-version: quant-ph/9605011.

[57] Stern A., Aharonov Y., Imry Y. Phase uncertainty and loss of interference: a general picture. Phys. Rev. A, **41**, 1995. 34–36.

[58] Stern A., Aharonov Y., Imry Y. Dephasing of interference by a back reacting environment. Quantum coherence, 1990. (Ed. J. Anandan)

[59] Tamon C., Yamakami T. Quantum computation relative to oracles. 2000. E-version: quant-ph/0010002.

[60] Toda S. PP is as hard as the polynomial-time hierarchy. SIAM J. on Comput. 1991. **20**. 865–877.

[61] Unruh W. G. Maintaining coherence in quantum computers. Phys. Rev. A, **51**, 1995. 992–997.

[62] Valiant L. G. The complexity of computing the permanent. Theoretical Computer Science. 1979. **8**. 189–202.

[63] Ben-Or M., Goldwasser S., Kilian J., Wigderson A. Multi-prover interactive proofs: how to remove the intractability assumptions. STOC'20. 1988. 113–131.

[64] Watrous J. Relationships between quantum and classical space-bounded complexity classes. Proc. of the 13th IEEE Conf. on Computational Complexity. 1998. 210–227.

[65] Watrous J. Space-bounded quantum complexity. J. of Comp. and Sys. Sci. 1999. **59**. 281–326.

[66] Watrous J. PSPACE has 2-round quantum interactive proof system. E-version: cs.CC/9901015.

[67] Wootters W. K., Zurek W. H. A single quantum cannot be cloned. Nature, 1982, **299**, 802.

[68] Yao A. C-C. Quantum circuit complexity. FOCS'34. 1993. 352–361.

[69] Yamakami T., Yao A. C-C. $NQP_C$ = co-$C_=P$. Information Processing Letters. 1999. **71**. 63–69. Preliminary E-version: quant-ph/9812032.

[70] Zurek W. H. Decoherence and the transition from quantum to classical. Physics Today **44**, № 10, 1991. 36–44.

# Проблемы развития теории квантовых коммуникаций

В. В. Белокуров, В. А. Садовничий, О. Д. Тимофеевская, О. А. Хрусталев

## 1 Введение

Любая передача информации представляет собой, прежде всего, физический процесс, обязательной частью которого является обмен между отправителем и адресатом некоторой физической системой. Улучшение качества передачи информации связано с возможностью наиболее точного описания передающего информацию объекта и управления этим объектом. Последовательное осуществление этой программы приводит к обсуждению таких коммуникационных схем, в которых проявляются квантовые свойства носителя информации. Наиболее привлекательным здесь представляется то обстоятельство, что о надежности передачи и возможности контроля в этом случае непосредственно позаботились фундаментальные законы природы, поскольку квант неделим и его нельзя клонировать.

Применительно к наиболее широко распространенному в настоящее время способу обмена информацией с помощью электромагнитных импульсов, это соответствует созданию схем, в которых информация передается с помощью отдельных квантов электромагнитного поля — фотонов.

## 2 Квантовое описание фотона

Физические величины, связанные с фотоном, можно реализовать как линейные операторы, действующие в гильбертовом пространстве квадратично интегрируемых функций $\psi(\vec{q},\sigma)$, где $\vec{q}=(q_1,q_2,q_3)$ — совокупность трех непрерывных переменных (это могут быть, например, координаты, импульсы и т. д.), а $\sigma$ — дискретная переменная, принимающая два значения, $\sigma=\pm1$.

Состояние фотона определяется в терминах *матрицы плотности* — оператора $\widehat{\rho}$ с ядром $\rho(q,q')$. Среднее значение величины $F$ в состоянии $\rho$ вычисляется по формуле

$$\langle F\rangle_\rho = \mathrm{Tr}\left(\widehat{F}\widehat{\rho}\right).$$

В задачах, связанных с коммуникациями, ядро $\rho(q,q')$ факторизуется:

$$\rho(q,q') = \rho_c(\vec{q},\vec{q}')\rho_{\mathrm{pol}}(\sigma,\sigma').$$

Поляризационную матрицу плотности можно представить в форме

$$\widehat{\rho}=\frac{1}{2}\left(\widehat{E}+r\vec{n}\widehat{\vec{\sigma}}\right),$$

где $\vec{n}\widehat{\vec{\sigma}}=n_\alpha\widehat{\sigma}_\alpha$, $n_\alpha$ — составляющие единичного вектора, $\vec{n}^2=1$, $\widehat{\sigma}_\alpha$ — матрицы Паули, а число $r$ ограничено неравенствами

$$0\leqslant r\leqslant 1.$$

Параметр $r$ называют *степенью поляризации фотона*. Если $r<1$, то говорят, что *фотон поляризован частично*, а при $r=0$ называют его *полностью неполяризованным*.

Если $r = 1$, то поляризационная матрица плотности оказывается проекционной. В этом случае фотон обладает определенной поляризацией, т. е. равна нулю дисперсия величины

$$\widehat{S}_n = \frac{1}{2}\vec{n}\widehat{\vec{\sigma}}.$$

В оптике принято задавать поляризацию в терминах параметров Стокса, определяя их как составляющие вектора

$$\vec{\xi} = r\vec{n}.$$

Если длина вектора Стокса равна единице, его составляющие можно задать двумя параметрами:

$$\xi_1 = \sin 2\alpha \cos\beta, \quad \xi_2 = \sin 2\alpha \sin\beta, \quad \xi_3 = \cos 2\alpha.$$

Содержащиеся в этих формулах углы совпадают с представлением вектора поляризации в форме

$$\vec{e} = \vec{\chi}_1 \cos\alpha + \vec{\chi}_2 e^{i\beta} \sin\alpha,$$

в которой векторы $\vec{\chi}_{1,2}$ образуют базис в плоскости, перпендикулярной к направлению распространения.

# 3 Переписка Алисы и Боба

Коммуникационная система безопасных квантовых сообщений была изобретена в 1970 году Виснером. Идеи Виснера, по-видимому, настолько опередили время, что представленная им работа была опубликована лишь в 1983 году [21]. В 1984 году появилась работа Беннета и Брассара [1] (в настоящее время принята аббревиатура *BB84* ), положившая начало современным исследованиям в этой области. Систему Беннета и Брассара часто называют *схемой четырех состояний*.

Обычно ее описывают, используя терминологию, применяемую в теории частиц со спином 1/2, но она применима при описании любой системы с двумя состояниями (или двухуровневой системы). Здесь будет говориться о двух независимых поляризациях фотона.

В классической физике подобным системам соответствуют бистабильные системы, в которых существует два состояния равновесия. В классических вычислительных схемах эти системы используются для записи битов. При этом каждой отдельной системе соответствует один бит.

Положение меняется при переходе в квантовую область. Квантовая двухуровневая система — это система, свойства которой описываются линейными операторами в двухмерном гильбертовом пространстве. Произвольное состояние такой системы описывается тремя действительными параметрами, а наиболее важные для квантовых коммуникаций *чистые состояния* — двумя параметрами. Существенно, что эти параметры изменяются непрерывно в отведенных для них областях. Это определяет бóльшую возможность выбора состояний. Математические образы, связанные с квантовыми двухмерными системами, называют *кубитами* (квантовыми битами). Каналы связи, по которым передаются кубиты, обычно, называют *квантовыми каналами*. Кроме того, по установившейся традиции о схемах квантовых коммуникаций рассказывают как об обмене посланиями между двумя молодыми людьми — Алисой и Бобом, а подслушивает разговор обычно лучшая, но очень любопытная подруга Алисы — Ева.

Для определенности предположим, что Алиса посылает Бобу поляризованные фотоны. Канал, по которому эти фотоны пересылаются, обычно называют *квантовым каналом*. Процедуру отправления писем можно описать следующим образом.

Алиса посылает Бобу последовательность отдельных фотонов. Каждый из них может быть поляризован или линейно или циркулярно, т. е. всего рассматривается четыре сорта фотонов. Поляризации фотонов позволяют Алисе создать квантовый алфавит. Последовательность букв превращается в письмо, состоящее из двоичных чисел. С этими числами сопоставляются поляризации фотонов, а чтобы поместить это письмо в конверт, Алиса выбирает поляризации своих фотонов случайным образом. Точнее говоря, она создает последовательность случайных чисел и поляризует свои фотоны по предписанию этой последовательности.

Боб узнает о поляризации каждого из фотонов, используя один из четырех поляризационных фильтров. Выбор каждого из фильтров также определяется случайной последовательностью чисел, которую Боб строит независимо от Алисы.

Вообще говоря, таким способом разговор поддержать трудно, но если Алиса и Боб воспользуются одинаковыми поляризатором и анализатором, то Боб прочитает соответствующую букву правильно.

Чтобы выяснить соответствие этих устройств, Алиса и Боб пользуются каналом, который по традиции называют *классическим*. Это не значит, что существуют какие-то каналы различной природы. Чтобы избежать недоразумений, следует помнить, что существует только квантовая физика, а то что принято называть физикой классической — это совокупность явлений, в которых реализуются те или иные предельные случаи квантовых состояний. Например, состояния, в которых по общепринятой терминологии присутствует электромагнитное поле, достигаются тогда, когда система содержит неопределенное число фотонов. В этом случае средние значения квантовых *операторов* электромагнитных потенциалов не равны нулю, и именно эти величины обладают свойствами, которые приписываются классическим полям. Создавать такие состояния и управлять ими (при не чрезмерных требованиях к точности) проще, чем состояниями, в которых явственно проявляются квантовые свойства. Поэтому Алиса и Боб, создавая устройство передачи сообщений, дополняют односторонний квантовый канал (по нему передаются сообщения) двухсторонним помехоустойчивым классическим каналом. Поскольку передаваемые по этим каналам сведения без квантового канала не имеют никакой ценности, они не пытаются защитить этот канал от подслушивания.

Таким образом, пересылка послания от Алисы к Бобу происходит примерно так: квантовый канал используется для обмена алфавитами, а классический канал используется для проверки, не возникают ли при передаче послания ошибки (в частности, нет ли подслушивания). Позднее по классическому каналу можно будет послать нужный текст.

В принципе этого достаточно, чтобы обеспечить безопасность коммуникаций: Алиса и Боб могут обменяться бóльшим количеством кубитов, чем необходимо для передачи алфавита, используя избыток для проверки того, подслушиваются их переговоры, или нет. Если они не находят ошибок, то считают, канал пригоден для передачи сообщения. Наличие ошибки свидетельствует о том, что разговор подслушивается.

## 3.1 Пример BB84-протокола

При сообщениях по квантовому каналу Алиса и Боб используют фотоны, векторы состояний которых образуют два базиса в пространстве $\mathcal{H}_2$:

a) Базис из состояний с *вертикальной* и *горизонтальной* поляризациями. Это векторы

$$|\uparrow\rangle \quad \text{или} \quad |\rightarrow\rangle.$$

b) Базис из состояний, в которых поляризация образует с осью $Ox$ углы $\pi/4$ и $3\pi/4$ (фотон распространяется вдоль оси $Oz$) — векторы

$$|\nearrow\rangle \quad \text{или} \quad |\nwarrow\rangle.$$

Квантовые алфавиты можно построить путем следующего сопоставления векторов с битами

$$\begin{array}{lll} \text{a)} & 1 \longleftrightarrow |\uparrow\rangle, & 0 \longleftrightarrow |\rightarrow\rangle; \\ \text{b)} & 1 \longleftrightarrow |\nearrow\rangle, & 0 \longleftrightarrow |\nwarrow\rangle. \end{array}$$

После этого BB84-протокол сводится к последовательности операций.

**Стадия 1. Квантовая часть протокола BB84**

1) Алиса создает *случайную последовательность* нулей и единиц $S_A$. Эта последовательность позволит перевести общепринятый алфавит в квантовый.

2) Для каждого бита случайной последовательности Алиса случайным образом выбирает тот квантовый алфавит, которым собирается пользоваться. После этого она пересылает Бобу фотоны, поляризованные тем или иным способом.

3) Боб измеряет поляризации полученных фотонов. Поскольку Боб, получая фотоны, ничего не знает об алфавитах, выбранных Алисой, он создает *свою случайную последовательность*, которая определяет его выбор алфавитов. После всех измерений Боб получает свою случайную последовательность нулей и единиц $S_B$.

### Стадия 2. Классическая часть протокола BB84

Здесь можно выделить две фазы.

*Фаза 1. Создание сырого ключа*

1) Боб по открытому классическому каналу сообщает Алисе, какие фильтры он использовал при анализе поляризаций фотонов, не сообщая о полученных результатах.

2) Алиса сообщает Бобу по открытому же каналу, совместимы ли состояния отправленных ею фотонов с анализаторами Боба.

3) Алиса и Боб исключают все несовместимые состояния. В результате получается *предварительный алфавит*. Если при передаче послания не было ни помех, ни ошибок, все буквы ключа Алисы и Боба должны совпасть. В противном случае их ключи будут согласованы не полностью.

*Фаза 2. Оценка ошибки*

1) По открытому каналу Алиса и Боб сравнивают малые порции их предварительных алфавитов, чтобы оценить уровень ошибки $R$, и затем удаляют несогласующиеся биты, чтобы получить *просеянный алфавит*. Если при анализе сырых ключей Алиса и Боб не обнаружили ошибок ($R = 0$), то они принимают просеянные ключи в качестве окончательных.

2) Если будет обнаружена хотя бы одна ошибка, то Алиса и Боб отказываются от просеянного ключа и начинают все сначала.

Алиса переводит биты в поляризованные фотоны:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ \times & + & \times & \times & \times & \times & \times & + & \times & \times & + & + \\ \nearrow & - & \nearrow & \nearrow & \nearrow & \searrow & \searrow & - & \searrow & \nearrow & | & | \end{pmatrix}.$$

Боб переводит поляризованные фотоны в биты:

$$\begin{pmatrix} \nearrow & - & \nearrow & \nearrow & \nearrow & \searrow & \searrow & - & \searrow & \nearrow & | & | \\ + & + & \times & + & \times & \times & + & \times & + & \times & + & + \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Алиса и Боб сравнивают биты:

$$\begin{pmatrix} 1 & 1 & & 0 & & 1 & 0 \\ + & \times & & \times & & \times & + \\ + & \times & & \times & & \times & + \\ 1 & 1 & & 0 & & 1 & 0 \end{pmatrix}.$$

После этого происходит обмен ключами:

$$\begin{pmatrix} \times & & \times & \times & & \times & + & \times & & + & \\ + & & + & \times & & + & \times & + & & + & \\ 0 & & 1 & 1 & & 0 & 0 & 1 & & 0 & \\ & & & 1 & & & & & & 0 & \end{pmatrix}.$$

Впервые предложенная схема передачи сообщений была реализована в 1989 году в лаборатории IBM [2] (см. также [3], [4]). Продемонстрированное устройство передавало сообщения на расстояние 30 cm.

То обстоятельство, что Алиса и Боб пользуются на этой стадии протокола «открытыми каналами», обычно считается характерной особенностью криптопротоколов. Эти каналы не обязаны быть конфиденциальными, но должны быть аутентичными. Поэтому Ева может слушать все переговоры по открытому каналу, но не может его модифицировать.

Очевидно, что Алиса и Боб могут использовать одно и то же устройство для реализации и квантового, и классического каналов.

## 4 B92-протокол

В B92-протоколе Алиса распоряжается фотонами с двумя неортогональными поляризациями, например, вертикальной $|\uparrow\rangle$ и образующей положительный угол в 45° градусов с осью $Ox$ — $|\nearrow\rangle$. Устройства Боба позволяет выделять фотоны с поляризациями, перпендикулярными этим, а именно с образующей угол в $-45°$ — $|\searrow\rangle$ с осью $Ox$ и горизонтальной — $|\rightarrow\rangle$. Алиса создает случайную последовательность двоичных чисел и сопоставляет с ними поляризации фотонов по следующим правилам.

Алиса:

$$0 \longleftrightarrow |\uparrow\rangle, \quad 1 \longleftrightarrow |\nearrow\rangle.$$

Боб создает свою случайную последовательность и сопоставляет с ними ориентации фильтров, определяющих поляризацию фотонов, которые он фиксирует.

Боб:

$$0 \longleftrightarrow |\searrow\rangle, \quad 1 \longleftrightarrow |\rightarrow\rangle.$$

Боб регистрирует результаты наблюдений по правилам: Y — удача, если ему удалось зафиксировать фотон, и N — неудача, если фотона зафиксировать не удалось. Если биты Алисы и Боба различны, то заведомо будет зафиксирована неудача. В случае удачи бит Боба всегда совпадает с битом Алисы. Удача регистрируется для половины одинаковых битов. Приведем пример распределения битов.

$$\begin{pmatrix} \text{Биты Алисы} & 1 & 0 & 1 & 0 \\ \text{Поляризация ее фотонов} & |\nearrow\rangle & |\uparrow\rangle & |\nearrow\rangle & |\uparrow\rangle \\ \text{Биты Боба} & 0 & 0 & 1 & 1 \\ \text{Поляризаторы Боба} & |\searrow\rangle & |\searrow\rangle & |\rightarrow\rangle & |\rightarrow\rangle \\ \text{Результаты Боба} & \text{N} & \text{N} & \text{Y} & \text{N} \end{pmatrix}$$

Первый и четвертый биты Алисы и Боба имеют различные значения, так что в каждом из этих случаев результат Боба равен $N$. Во втором и третьем случаях значения битов совпадают, и с вероятностью 0.5 результат Боба будет равен Y. Конечно, нельзя предсказать заранее результат каждого измерения.

Чтобы закончить протокол, Боб посылает свои результаты Y или N Алисе, не сообщая значений поляризации своих анализаторов. Это сообщение посылается по открытому каналу.

После этого Алиса и Боб оставляют только те биты, для которых результаты Боба равны Y, именно эти биты соответствуют совпадению алфавитов. В приведенном примере только третий бит передает одинаковые буквы алфавита.

Таким образом, эффективность идеальной процедуры обмена, $\eta_Q$, равна 0.25.

В практических системах возникают дополнительные потери при передаче сигнала, величина этих потерь характеризуется коэффициентом $\eta_T$, потери при детектировании можно оценить коэффициентом $\eta_D$. Эти потери влияют на скорость передачи сообщений, но не искажают их смысла. Ошибки, искажающие смысл, как и утечка информации, могут возникать в тех случаях, когда Ева перехватывает фотон, выясняет его поляризационное состояние и посылает Бобу свой фотон. Здесь относительная ошибка может достичь 0.25 (когда анализаторы Евы поляризованы так же, как фотоны Алисы). В этом случае правильно идентифицируется лишь 0.75 битов. Конечно, это настолько большой источник ошибок, что Алиса и Боб обнаружат его без труда. Однако, Ева может перехватывать только часть сигналов. Для борьбы с этим нужно изобретать особые приемы, но для восстановления отправляемого текста можно применить стандартную процедуру исправления ошибок.

## 5 Надежность криптографических схем

Естественно, что простое описание схемы коммуникаций должно быть дополнено анализом ее надежности. Этому было посвящено много работ и была доказана надежность только что разобранных и аналогичных им протоколов (например, [16]). Была доказана надежность этих схем против весьма изобретательных и объединенных атак квантового канала. Однако, экспериментальная устойчивость некоторых из коммуникаций рассмотренного типа была доказана лишь недавно [15].

# 6 Источники фотонов

Оптические квантовые коммуникации основаны на использовании однофотонных состояний. К несчастью, эти состояния трудно реализовать экспериментально. В настоящее время их получают или с помощью слабых лазерных импульсов или коррелированных фотонных пар, когда как отдельные фотоны, также как и фотонные пары распределены по закону Пуассона. Таким образом, достоинства и того, и другого способа страдают от обязательного наличия состояний со многими фотонами или парами. Эти состояния передаются, как и однофотонные, по квантовому каналу и при больших потерях в канале могут быть причиной помех. Поэтому имеет смысл несколько подробнее обсудить достоинства и недостатки различных источников фотонов.

**Слабые лазерные импульсы.** В этом случае задача получения однофотонного состояния (приближенно) решается весьма просто: нужно получить когерентное состояния с предельно малым *средним числом фотонов* $\mu$. Такие состояния легко реализовать, используя стандартные полупроводниковые лазеры и аттенюаторы.

Вероятность найти $n$ фотонов в когерентном состоянии равна

$$P(n,\mu) = \frac{\mu^n}{n!}e^{-\mu},$$

поэтому вероятность того, что слабый когерентный импульс содержит более одного фотона, равна

$$P(n>1,\mu) = \frac{1-P(0,\mu)-P(1,\mu)}{1-P(0,\mu)} = \frac{1-e^{-\mu}-\mu e^{-\mu}}{1-e^{-\mu}} \approx \frac{\mu}{2}.$$

и может быть сколь угодно малой.

Таким образом, использование слабых лазерных импульсов вполне практично, и они действительно применяются в большинстве экспериментов. Однако этот метод имеет и большой недостаток: поскольку вероятность того, что импульс не содержит ни одного фотона, равна $P(0,\mu) = 1-\mu$, большинство импульсов оказываются пустыми.

Связанное с уменьшением $\mu$ убывание скорости счета можно скомпенсировать за счет модуляции лазерных импульсов. Однако при этом возникают дополнительные трудности, связанные с «темным счетом» детекторов. Детекторы должны сохранять свою активность для всех импульсов, в том числе и для пустых. Поэтому полное число темных отсчетов будет увеличиваться. Таким образом, *отношение зарегистрированных фотонов к числу темных отсчетов уменьшается вместе с уменьшением* $\mu$.

**Рождение пар фотонов с помощью параметрической конверсии.** Другой способ рождения псевдоединичных фотонных состояний состоит в рождении пар и использования одного из фотонов в качестве триггера для другого [11], [12]. В этом случае детектор, который должен регистрировать фотон, активизируется только в том случае, когда регистрируется триггерный фотон, следовательно, когда выясняется, что $\mu = 1$. Это не имеет никакого отношения к импульсу накачки, поэтому трудности, связанные с темным счетом, просто-напросто не возникают. Фотонные пары обычно рождаются при спонтанной параметрической конверсии в $\chi^{(2)}$ нелинейных кристаллах. В этом процессе, обратном к хорошо известному процессу удвоения длины волны — один фотон спонтанно расщепляется на два дочерних фотона — *сигнальный* и *ленивый* (этот фотон приходит к адресату после сигнального). При этом сохраняются полные импульс и энергия фотонов. Процесс рождения пар весьма неэффективен. Как правило одна пара заданной моды рождается примерно на $10^{10}$ фотонов (недавно при использовании световодов в периодически расположенных кристаллах $LiNbO_3$ достигнута скорость конверсии порядка $10^{-6}$ ). Число фотонных пар на моду в масштабе времени когерентности фотонов имеет тепловое распределение, следовательно, для больших масштабов времени пары распределены по закону Пуассона. Помпа мощностью в 1 mW может накопить в световоде примерно $10^6$ пар. Условная вероятность найти вторую пару в промежутке времени около 1 ns — величина порядка $10^6 \cdot 10^{-9} \approx 0.01\%$.

# 7 Передача сообщений с помощью коррелированных фотонных пар

В протоколах типа BB84 Боб не знает, как расшифровать бит, доставленный ему очередным фотоном. Для того, чтобы найти ключ, ему необходимо получить, как минимум, два фотона. Эта

тенденция сохраняется и при обработке более длинных посланий. Лишь несколько протоколов превосходят 50%-ный порог эффективности (например, [14]). Протоколы такого типа естественно назвать *недетерминистскими.*

Можно предложить и *детерминистские* схемы, когда Боб получает ключ вместе с каждым фотоном. Впервые такая схема рассматривалась в работе [6]. В ней предлагалось использовать пары фотонов, рождающихся в антисимметричных поляризационных состояниях (т. е., фактически, один фотон). Если в качестве одного такта работы генерирующего фотоны устройства использовать двухкратное прохождение жесткого излучения вдоль нелинейного кристалла, то рождение пары фактически эквивалентно рождению одного фотона. Каждый такт в работе передающего устройства определяется рождением двух пар фотонов в состоянии

$$\begin{aligned}\rho(\sigma,\sigma') &= \Psi(\sigma)\Psi^*(\sigma'),\\ \Psi(\sigma) &= \chi(\sigma_1,\sigma_2)\chi(\sigma_3,\sigma_4),\\ \chi(\sigma_1,\sigma_2) &= -\chi(\sigma_2,\sigma_1).\end{aligned}$$

Если поляризовать фотоны 2 и 4 вдоль направлений $\vec{m}$ и $\vec{s}$, то фотоны 1 и 3 окажутся поляризованными вдоль ортогональных к этим векторам $\vec{m}$ и $\vec{s}$ направлений. Волновая функция системы четырех фотонов, после того как фотоны 2 и 4 пройдут сквозь поляризационный фильтр, окажется равной

$$\Phi(\sigma) = \varphi_{\vec{n}}(\sigma_1)\varphi_{\vec{m}}(\sigma_2)\varphi_{\vec{r}}(\sigma_3)\varphi_{\vec{s}}(\sigma_4).$$

Состояние системы, состоящей из фотонов 1 и 3, определяется условной матрицей плотности

$$\rho_{(1,3)/(2,4)} = \upsilon(\sigma_1,\sigma_3)\upsilon^*(\sigma_1,\sigma_3),$$

где

$$\upsilon(\sigma_1,\sigma_2) = \varphi_{\vec{n}}(\sigma_1)\varphi_{\vec{r}}(\sigma_2).$$

В этом случае можно довольно просто реализовать квантовый вариант коммуникационной схемы Вернама [20]. Векторы $\vec{m}$ и $\vec{s}$ выбираются случайно, поэтому случайными оказываются и векторы $\vec{n}$ и $\vec{r}$, определяющие поляризации фотонов, которые Алиса направляет Бобу. Перехват одного из фотонов пары не приносит никакой информации Еве, но является для Алисы и Боба сигналом о том, что их разговор подслушивается. Результатом этого обстоятельства является абсолютная надежность квантовой коммуникационной схемы.

Экспериментально наблюдаемое рождение фотонных пар в таких состояниях, когда сумма поляризаций имеет определенное значение, представляет собой еще одну возможность для квантовых коммуникаций. Возможность такого способа передачи информации была предсказана в 1992 году [9]. (Обзор этой проблемы см. в [22].)

В 1999 году три группы продемонстрировали экспериментально возможность квантовых коммуникаций, использующих находящиеся в таких состояниях фотоны [13], [17], [19].

Все перечисленные схемы используют следующее обстоятельство: если в матрице плотности пары фотонов спиновые переменные факторизуются, то поляризационные свойства пары должны слабо изменяться при увеличении расстояния. Если сумма поляризаций двух фотонов имеет определенное значение, то поляризационное состояние одного фотона зависит от поляризации другого фотона.

Таким образом, даже после того, как принадлежащие одной паре фотоны расходятся на макроскопические расстояния, корреляции поляризаций не проявляют склонности к ослаблению. Поэтому пары фотонов можно использовать как средство квантовой коммуникации.

На несколько необычные с классической точки зрения корреляции импульсов и координат двух частиц, находящихся в чистом состоянии с равным нулю полным импульсом, обратили внимание еще в 1935 году Эйнштейн, Подольский и Розен [8]. Они видели в существовании таких корреляций невозможность описания свойств каждой из частиц с помощью волновой функции, что ставило под сомнение саму возможность использования общепринятого математического аппарата для полного описания квантовых явлений.

Это создавало вокруг состояний, построенных Эйнштейном, Подольским и Розеном, ореол таинственности, создававший им особую популярность. В научной литературе появилась даже особая аббревиатура EPR-состояния. В развернувшейся дискуссии, среди участников которой были Бор, Паули, Фок, было выяснено, что все явления в системе двух частиц укладываются в общую схему

описания состояний квантовых систем в терминах матрицы плотности, открытой Нейманом еще в 1927 году. На возможность использования EPR-состояний в квантовых коммуникациях впервые обратил внимание Дойч [7]. Пригодный для непосредственного использования математический аппарат был создан Экертом [10] и усовершенствован Беннетом, Брассаром и Мермином [5]. Однако полное отсутствие ссылок на основополагающие работы затуманивает содержание этих работ. Квалифицированные исследования в этой области невозможны без изучения работ фон Неймана [18].

Упомянем об опыте, демонстрирующем возможность квантовых коммуникаций с помощью коррелированных фотонных пар, выполненном в Инсбруке [13].

Послание Алисы к Бобу содержало гордость музея Вены — фотографию «Вилендорфской Венеры» — статуэтки, вырезанной из известняка примерно за 24000–22000 лет до Рождества Христова. Для передачи изображения была использована матрица, содержащая $60 \times 90$ точек, 8 битов цветной информации на точку: 432000 битов информации, кодирующей изображение. Файл содержал дополнительную информацию, включая таблицу цветов — всего 51840 битов. Боб воспроизвел только ту информацию, которая относилась к изображению. В результате получилось изображение, которое содержало лишь несколько ошибок, которые были вызваны ошибками, оставшимися в квантовом алфавите.

Результаты эксперимента привели авторов к убеждению, что несмотря на необходимость дальнейших теоретических и экспериментальных исследований, квантовая передача сообщений с помощью коррелированных фотонов вполне может стать частью завтрашней технологии.

## 8 Попытка взгляда в будущее

В докладе на рабочем совещании, посвященном квантовым сообщениям, один из ведущих специалистов в этой области профессор Ло [14], оценивая квантовые коммуникации как новую технологию, попытался ответить на вопрос — станут ли квантовые коммуникации успешной технологией. Не имея возможности обсудить здесь все положения этого доклада, остановимся лишь на наиболее близких к нашей теме.

В числе наиболее серьезных аргументов, не способствующих популяризации идеи квантовых коммуникаций, Ло отмечает следующие:

1. Невозможность безусловной надежности во многих приложениях квантовых коммуникаций.
2. Неуверенность в распространении нынешнего способа квантовых сообщений на большие (по сравнению с десятками километров) расстояниями.
3. Малая скорость передачи сообщений. Современные скорости передачи квантовых сообщений — величины порядка Kbits/sec. Рекорд передачи сообщений по одномодовому световоду — это 160 Gbits/sec.
4. Оборудование для квантовых сообщений слишком громоздко. Создание аппаратуры, умещающейся в чемоданчике, было бы великим достижением.
5. Слишком высокие цены. Стоимость отдельных узлов устройств для квантовых коммуникаций — от сотен до тысяч долларов.
6. Отсутствие действительно надежных систем передачи кубитов.
7. Ожидание будущих трудностей — каждый анализ надежности квантовых коммуникаций содержит те или иные идеализации.

Нетрудно заметить, что полностью справедливая критика слабых мест схемы квантовых коммуникаций лишь подчеркивает масштаб задач, связанных с новой концепцией коммуникаций.

Столь же очевидны способы преодоления трудностей:

Создание новых схем квантовых коммуникаций, например, объединения методов квантовых коммуникаций и квантовых вычислений. По существу, это означает необходимость более глубокого внедрения квантовой механики в новые технологии. В частности, здесь были бы полезны поиски сочетания методов обычных коммуникаций с квантовыми технологиями.

Решение задачи миниатюризации — вплоть до умещения всех квантовых устройств на компакт-диске.

Необходимость строжайшего пересмотра — главным образом экспериментального — способов обеспечения надежности квантовых каналов.

## Литература


[1] Bennet C., Brassard C. Quantum cryptography: public key distribution and coin tossing. Int. Conf. Computer, Systems and Signal Processing, 1984 India, 172–174.

[2] Bennet C., Brassard C. The Dawn of a New Era for Quantum Cryptography: The Experimental Prototype is Working! SIGACT News, 1989, **20**, 78–82.

[3] Bennet C., Brassard G., Ekert A. Quantum Cryptography. Scientific American, October 1992, 50–70.

[4] Bennet C., Bessete G., Brassard G., Salvail L., Smolin J. Experimental Quantum Cryptograpny. J. Cryptology, 1992, **5**, 3–28.

[5] Bennet C., Brassard G., Mermin N. Quantum cryptography without Bell's theorem. Phys. Rev. Lett., 1992, **68**, 557–559.

[6] Belokurov V. V, Khrustalev O. A., Sadovnichy V. A., Timofeevskaya O. D. Systems and subsystems in Quantum Communication. ArXiv: quant-ph/0111164, 2001.

[7] Deutsch D. Quantum theory, the Church–Turing principle and universal quantum computer. Proc. Royal Soc. London, Ser. A, 1985, **400**, 97–105.

[8] Einstein A., Podolsky B., Rosen N. Can quantum-mechanical description of physical reality be considered complete? Phys. Rev., 1935, **47**, 777–780.

[9] Ekert A. K., Rarity P. R., Tapster P. R., Palma G. M. Practical quantum cryptography based on two-photon interferometry. Phys. Rev. Lett., 1992, **69**, 1293–1296.

[10] Ekert A. K. Quantum cryptography based on Bell's theorem. Phys. Rev. Lett., 1991, **67**, 661–663.

[11] Hong C. K., Mandel L. Theory of parametric frequency down conversion of light. Phys. Rev., 1985, **A31**, 2409–2418.

[12] Hong C. K., Mandel L. Experimental realization of a localized one-photon state. Phys. Rev. Lett., 1986, **56**, 58–60.

[13] Jennewein T., Simon G., Weihs G., Weinfurter H., Zeilinger A. Quantum cryptography with entangled photons. Phys. Rev. Lett., 2000, **84**, 4729–4732.

[14] Lo H. K. Will quantum cryptography ever become a successful technology in the marketplace?, ArXiv: quant-ph/9912011, 1999.

[15] Lutkenhaus M. Security against individual attacks for realistic quantum key distribution. ArXiv: quant-ph/9910093, 1999.

[16] Mayers D. Unconditional security in quantum Cryptography. ArXiv: quant-ph/9802025, 1998.

[17] Naik D., Peterson C., White A., Berglund A., Kwiat P. Entangled state quantum cryptography: eavesdropping on the Ekert protocol. Phys. Rev. Lett., 2000, **84**, 4733–4736.

[18] von Neumann J. Mathematische Grundlagen der Quantenmechanik. Berlin.: 1932. Русский перевод: фон Нейман И.. Математические основы квантовой механики. М.: 1964.

[19] Tittel W., Brendel J., Zbinden H., Gisin N. Quantum cryptography using energy-time entangled photons. Phys. Rev., 2000, **A59**, 4150–4163.

[20] VERNAM G. Gipher printer telegraph systems for secret wire and radio telegraph communications. J. Am. Institute of Electrical Engineers, 1926, **45**, 109–115.

[21] WIESNER S. Conjugate coding. SIGACT News, 1983, **15**, № 1, 78.

[22] ZEILINGER A. Experiment and foundations of quantum physics. Rev. Mod. Phys., 1999, **71**, 288–297.

# Вклад выпускников МГУ в развитие теоретической криптографии в России во второй половине XX века

В. Н. Сачков

Целью настоящего доклада является краткое изложение научного и научно-организационного вклада выпускников Московского государственного университета в становление и развитие отечественной криптографической службы во второй половине XX века и в достижение криптографической наукой нашей страны передовых позиций в мировой криптографии.

Хорошо известно, что история развития криптографии в России насчитывает не одно столетие. Однако, шифровальная служба как государственный орган впервые была организована при Петре I. К началу XX века в России в ряде ведомств существовали специальные подразделения, занимавшиеся проблемами, связанными с криптографией.

После 1917 г. возникла необходимость создания новой криптографической службы для решения задач разработки шифров для защиты отечественных линий связи и анализа иностранных шифров. Образованная в мае 1921 года криптографическая служба прошла длительный путь своего становления и развития до уровня, обеспечившего паритет с передовыми шифрслужбами Запада. В настоящее время преемником ее является Федеральное агентство правительственной связи и информации при Президенте Российской Федерации.

В Великой Отечественной войне 1941–1945 годов отечественные шифры на основных линиях связи надежно противостояли атакам криптографов противника. В то же время нашим дешифровальщикам, среди которых были и выпускники мехмата МГУ, удавалось получать ценную разведывательную информацию.

К этому же времени относятся и первые достижения отечественной теоретической криптографии. Так, в 1941 году Котельниковым Владимиром Александровичем была доказана теоретическая стойкость шифра гаммирования при одноразовом использовании случайной и равновероятной гаммы. Отметим, что работа К. Шеннона, содержащая такой результат, была опубликована в 1945 году.

В послевоенные годы в связи с резким увеличением информационного обмена и необходимостью его надежной защиты на основе последних достижений науки и техники, а также для повышения эффективности дешифровальной работы возникла потребность существенного усиления криптографических служб ведущих держав. С этой целью в Советском Союзе в 1949 году было создано Главное управление специальной службы (ГУСС), а в США в 1952 году — Агентство национальной безопасности (АНБ). Деятельность как ГУСС, так и АНБ протекала в условиях строгой секретности.

Образование ГУСС сыграло огромную роль для существенной перестройки всей криптографической службы страны и дальнейшего ее развития. Еще в 1946 году к работе в криптографической службе была привлечена группа научных и инженерных работников из Московского университета и других учебных заведений, которые внесли значительный вклад в решение актуальных задач отечественной криптографии и повысили ее научный уровень. Это обстоятельство определило направление дальнейшего комплектования подразделений криптографической службы.

С созданием ГУСС было образовано закрытое отделение механико-математического факультета МГУ и Высшая школа криптографов (ВШК), в которой обучавшиеся в течение двух лет получали второе высшее специальное образование. Правопреемником Высшей школы в настоящее время является Институт криптографии, связи и информатики (ИКСИ) Академии ФСБ. В 1951 году при Высшей школе была организована аспирантура.

Большую роль в создании закрытого отделения мехмата МГУ сыграли выпускники мехмата Копытцев А. И. и Пондопуло Г. И.

С большой признательностью мы отмечаем сегодня активное участие в разработке математических учебных программ для закрытого отделения и в чтении лекций таких известных ученых как Колмогоров А. Н., Хинчин А. Я., Смирнов Н. В., Мальцев А. И., Линник Ю. В., Марджанишвили К. К., Гельфонд А. О., Марков А. А., Курош А. Г. В Высшей школе и на закрытом отделении мехмата лекции читали Козлов В. Я., Верченко И. Я., Узков А. И., Севастьянов Б. А., Санов И. Н., Блинов А. А.

В программу закрытого отделения мехмата входили курсы по дополнительным разделам теории вероятностей и математической статистики, высшей алгебры, теории групп, теории чисел, теории конечных разностей, специальных применений вычислительной техники и курсы по криптографии. За время своего функционирования с 1949 года по 1957 год на закрытом отделении мехмата МГУ прошли обучение около 200 человек. Но и после закрытия этого отделения выпускники мехмата МГУ составляли значительную долю научных работников криптографической службы, внося существенный вклад в ее развитие. В частности, большая группа выпускников мехмата была принята на работу в криптографическую службу в начале 60-х годов.

К началу 50-х годов криптография накопила большой опыт в построении разнообразных шифров и имела значительный набор разнообразных, подчас весьма изощренных методов их дешифрования. Однако, недостаточная связь криптографии с исследованиями в различных областях науки и достижениями в технике, бедность арсенала общих методов криптографического анализа и синтеза делали ее близкой скорее к искусству, чем к науке. К середине XX века ситуация стала изменяться. С одной стороны, с накоплением опыта криптографического анализа конкретных шифрсистем наряду с дальнейшим развитием экспериментальных методов начали ставиться общие криптографические задачи с использованием математического аппарата. С другой стороны, в связи с бурным развитием электронной вычислительной техники и средств обработки информации дискретного принципа действия значительно повысился интерес математиков к изучению дискретных явлений.

В связи с этим получили существенное развитие такие разделы дискретной математики как комбинаторный анализ, теория функций алгебры логики, теория графов, теория релейно-контактных схем, теория автоматов. Методы и результаты в этих и других областях дискретной математики оказались весьма полезными для решения криптографических задач.

Широкое применение в криптографии нашли теоретико-вероятностные и статистические методы, что объясняется, с одной стороны, случайным характером открытых и шифрованных текстов и применяемых для шифрования ключей, а с другой стороны, широким использованием для изучения сложных детерминированных процессов различных теоретико-вероятностных моделей.

Применение алгебраических и теоретико-числовых методов в криптографии для изучения процессов шифрования основано на использовании функциональных особенностей элементной базы для построения шифраторов, которая реализует ряд алгебраических операций. Это позволяет проводить анализ шифрсистем на основе применения методов теории групп, теории конечных полей и колец, линейной алгебры, а в последние годы — и методов алгебраической геометрии и алгебраической теории чисел.

Для изучения разнообразных дискретных моделей шифраторов широкое применение в криптографии нашли комбинаторные методы. При этом в криптографии возникают как задачи построения комбинаторных конфигураций с заданными свойствами, так и задачи их перечисления, при решении которых используются теоретико-вероятностные методы и методы асимптотического анализа.

Интенсивное использование в криптографии ЭВМ предопределило существенную роль алгоритмических методов в решении криптографических задач.

Наряду с методами математической логики, теории информации и теории автоматов значительную роль в криптографии играет теория кодирования. В этой области можно отметить результаты Сидельникова В. М.

Приход на работу в начале 50-х годов в криптографическую службу выпускников закрытого отделения мехмата МГУ в значительной мере способствовал процессу «математизации» отечественной криптографии. Наряду с разработкой новых методов криптографического анализа шифрсистем существенное развитие получила теоретическая криптография, в которой одну из ведущих ролей стал играть математический аппарат.

Одной из важнейших задач этого периода стало создание более совершенных датчиков случайных чисел и строгое математическое обоснование случайности и равновероятности получаемых с их помощью последовательностей, а также методов статистического контроля их криптографического качества. Эта задача была успешно решена коллективом криптографов и инженеров под руководством Козлова В. Я. В дальнейшем большой вклад в развитие этого направления внесли Беляев П. Ф.

и Пярин В. А. Отметим, что в связи с решением этой задачи были получены первые результаты в получившей в дальнейшем достаточно широкое развитие теории вероятностных распределений на группах.

Большую роль сыграли выпускники мехмата и в решении другой важной задачи криптографической службы по созданию нового поколения отечественных шифраторов.

В их работах было дано аналитическое описание функционирования действовавших в то время шифраторов, разработаны методы их криптографического анализа. Основополагающий вклад в решение этих вопросов внесли выпускники МГУ старшего поколения Верченко И. Я., Козлов В. Я., Блинов А. А., Бобылев В. И., Бороздкин К. Г., Головин О. Н., Марджанишвили К. К., Пондопуло Г. И., Соколов М. И.

Существенные научные результаты в этой области получили выпускники закрытого отделения мехмата Горчинский Ю. Н., Сачков В. Н., Медведев Ю. И., Голованов П. Н., Волков И. С. и др. В их работах, в частности, на основе специального вида неоднородных цепей Маркова были построены теоретико-вероятностные модели шифраторов, а также решен ряд сложных комбинаторных задач, возникающих в их криптоанализе.

В этот же период в криптографической службе интенсивно проводилась разработка высокопроизводительной по тому времени вычислительной техники. Группой инженеров-изобретателей в составе Полина В. С., Левина В. К. и др. и криптографов Бежаева И. О., Подколзина А. Т., Тихоновой Г. П., Воскресенского В. А. была разработана специализированная ЭВМ, которая обладала производительностью $10^6$ операций в секунду. Отметим, что в это время при создании первых отечественных электронных цифровых машин общего назначения «БЭСМ», «Стрела» было достигнуто быстродействие $10^4$ операций в секунду.

При построении специализированных ЭВМ большое значение имело создание критериев на открытый текст. Такие критерии были разработаны в работах Санова И. Н. и выпускника спецотделения мехмата Боровкова А. А. на основе результатов по предельным теоремам о больших уклонениях сумм случайных величин.

В 60-х годах наступил новый этап в мировом шифраторостроении. В анализе и синтезе криптографических схем шифраторов нового поколения выпускники мехмата МГУ и Высшей школы приняли активное участие с самого начала работ.

Анализ и синтез шифраторов нового поколения сопровождался глубокими теоретическими исследованиями в совершенно новой области криптографии. Были определены основные принципы построения их криптосхем и исследованы их типовые узлы и блоки, разработаны основные методы математического расчета шифрующих автоматов и оценки их статистических свойств с использованием ЭВМ.

В создание отечественных шифраторов нового поколения значительный вклад внесли криптографы старшего поколения Блинов А. А., Калачев К. Ф., Козлов В. Я., Узков А. И. В разработке и обосновании специальных свойств этих шифраторов приняли непосредственное участие выпускники мехмата МГУ Горчинский Ю. Н., Сачков В. Н., Степанов В. Е., Медведев Ю. И., Башев В. А., Емельянов Г. В., Максимов Ю. И. и др.

В их исследованиях совместно с другими криптографами были получены важные научные и практические результаты, позволившие обосновать высокие специальные качества отечественных шифров и найти подходы к дешифрованию некоторых иностранных шифраторов. Одновременно эти результаты составили существенный вклад в развитие теоретической криптографии.

Наряду с математизацией и компьютеризацией отечественной криптографии особо важную роль сыграло развитие физико-технического направления. Исследования в этой области позволили на основе синтеза математических и инженерных идей с криптографией получить решения ряда трудных криптографических задач.

Большой вклад в развитие этого направления внесли выпускник Высшей школы криптографов Николай Николаевич Андреев, ныне президент Академии криптографии Российской Федерации, а также выпускники МГУ Владимир Георгиевич Матюхин — ныне генеральный директор ФАПСИ, Владислав Петрович Шерстюк — ныне первый заместитель секретаря Совета безопасности Российской Федерации. Все они являются сопредседателями настоящей конференции.

В области теоретической криптографии в этот период большой цикл математических работ в интересах криптографии был выполнен в связи с исследованиями характеристик булевых функций и отображений конечных множеств. В настоящее время это направление исследований получило значительное развитие и ему посвящена обширная открытая литература.

Значительные результаты были получены в области разработки методов решения систем линейных и нелинейных булевых уравнений, в том числе систем случайных уравнений в работах Степанова В. Е., Коваленко И. Н. , Прохорова Ю. В., Балакина Г. В.

Для оценки качества гамм, вырабатываемых шифраторами, и решения других задач были разработаны новые статистические критерии.

Получила дальнейшее развитие теория распределений на группах. Группой выпускников МГУ была изучена так называемая схема авторегрессии на абелевой группе. Новые результаты были получены в изучении предельных распределений композиций случайных величин на некоммутативных группах в работах выпускников закрытого отделения мехмата МГУ Клосса Б. М. и Горчинского Ю. Н.

Для обоснования специальных качеств шифраторов нового поколения были успешно применены теоретико-групповые методы, в том числе в работах Глухова М. М. В частности, были исследованы вопросы строения групп подстановок, заданных системами образующих. В работах Сачкова В. Н. с помощью методов теоретико-вероятностной комбинаторики было изучено асимптотическое поведение математических моделей некоторых узлов и блоков шифраторов.

Говоря о связях между криптографией и современной математикой, следует подчеркнуть, что эти связи двусторонние: в настоящее время не только криптография использует готовые математические результаты для своих целей, но все чаще задачи, возникающие в криптографии, становятся источником развития ряда областей математики.

Так, выпускники МГУ внесли значительный вклад в развитие и ряда направлений, находящихся на стыке алгебры и теории вероятностей, в частности, в изучение конечных групп и полугрупп, заданных системами образующих, случайных многочленов над конечными полями, анализ нерегулярных выборок от псевдослучайных генераторов, уравнений в конечных кольцах и др.

В значительной мере исследованиями математиков-криптографов было развито направление, получившее название вероятностной комбинаторики. Оно включает в себя исследования случайных размещений частиц в ячейки, случайных подстановок и отображений с ограничениями, общие методы перечисления комбинаторных конфигураций и многое другое. Для решения этих задач использовался глубокий аппарат предельных теорем теории вероятностей, теории функций комплексного переменного, методы производящих и характеристических функций.

Существенное развитие получили основные направления математической статистики — разработка общих методов исследования широкого класса дискретных вероятностных моделей, предельные теоремы для различных типов статистик, включая такие статистики, как «хи-квадрат», наибольшего правдоподобия, первых и вторых частот полиномиальной схемы, U-статистики, разделимые статистики.

В развитие этих направлений большой вклад внесли Севастьянов Б. А., Колчин В. Ф., Чистяков В. П., Степанов В. Е., Сачков В. Н., Медведев Ю. И., Ивченко Г. И., Зубков А. М., Михайлов В. Г., Тараканов В. Е. и др.

Теоретико-автоматный подход разрабатывался в криптографии вначале в связи с исследованием периодичности автоматов прежде всего в работах Горчинского Ю. Н., Башева В. А. В дальнейшем это направление обогатилось исследованиями многозначных функций и универсальных алгебр, а также результатами изучения и построения классов функций с заданными параметрами.

Методы теории чисел, конечных полей и колец широко используются для решения задач дискретного логарифмирования и задач факторизации целых чисел. Кстати, задача дискретного логарифмирования в конечных полях возникла в криптографической службе в конце 50-х годов и первую нетривиальную оценку сложности ее решения получил Гельфонд А. О. в начале 60-х годов задолго до известных открытых публикаций.

Таков далеко не полный перечень направлений математики, развитие которых связано с проблемами современной криптографии.

Возросший за прошедшие годы научный потенциал отечественной криптографической службы и уровень развития криптографии привели к необходимости создания в начале 90-х годов Академии криптографии Российской Федерации, которая решает сегодня важнейшие проблемы в интересах информационной безопасности страны. Отметим, что в состав Академии криптографии входят ученые и Российской Академии наук: Котельников В. А., Козлов В. Я., Прохоров Ю. В., Севастьянов Б. А., Дианов Е. М., Левин В. К.

В тесном контакте с Академией криптографии работает лаборатория МГУ (руководитель Сидельников В. М.), созданная при активном участии сопредседателя этой конференции ректора МГУ

Садовничего Виктора Антоновича, который в настоящее время руководит коллективом сотрудников МГУ, участвующих в проведении научных исследований по квантовым вычислениям в Академии криптографии.

Вклад математиков-криптографов в развитие ряда направлений отечественной математики аккумулирован в целом ряде монографий и сотнях журнальных публикаций в ведущих математических изданиях страны. Статьи отечественных криптографов-математиков, публикуемые в «Трудах по дискретной математике», издаваемых Российской Академией наук и Академией криптографии Российской Федерации, являются вкладом в решение задач, актуальных для мировой криптологии.

В последние годы круг задач, стоящих перед отечественными криптографами, существенно расширился. Появление новых информационных и телекоммуникационных технологий, возрастание объемов и скоростей передаваемой информации поставило новые задачи перед криптографической наукой, в решении которых и в дальнейшем будут принимать активное участие выпускники Московского государственного университета.

# Влияние выпускников Московского университета на становление криптографического образования в России

П. Н. Голованов

Отечественная криптография прошла большой исторический путь. Еще в дореволюционной России работе шифровальных органов (шифровальным отделениям, «черным кабинетам») придавалось исключительно большое значение. На работу в эти подразделения направлялись наиболее подготовленные и способные работники. После революции криптографическая служба была создана фактически заново. Соответствующий отдел при ВЧК был создан постановлением Совнаркома РСФСР 5 мая 1921 года. В работе Спецотдела возникли большие трудности в связи с нехваткой квалифицированных специалистов. Из ветеранов старой шифровальной службы в отделе работали единицы, в том числе замечательные криптографы-практики Б. А. Аронский, С. С. Толстой и некоторые другие, много сделавшие для решения практических задач и подготовки молодых специалистов. Для пополнения рядов криптографов, повышения уровня их подготовки создавались разнообразные краткосрочные курсы. Однако кардинально решить кадровую проблему этим путем не удавалось. Криптографам явно не хватало математических знаний. Положение дел начало улучшаться, когда в Специальную службу стали направлять специалистов с университетским образованием, окончивших аспирантуру, защитивших диссертацию.

Еще в предвоенные годы на работу в Специальную службу был направлен выпускник Московского университета А. И. Копытцев. В дальнейшем А. И. стал первым генералом, занимавшим должность одного из руководителей Службы. На этом посту он вел активную работу по повышению уровня теоретической подготовки криптографов. Под его руководством и при личном участии в 1939 году был издан первый отечественный учебник по криптографии, в котором обобщался накопленный практический опыт и систематизировались разрозненные криптографические факты.

Выпускники Московского университета кандидаты наук М. И. Соколов, Г. В. Чуриков, Л. А. Тихонов пришли на работу в Службу в тяжелые военные годы. Занимаясь практической работой, решая сложные задачи, они в то же время уделяли внимание научной деятельности, подготовке кадров криптографов, развитию и совершенствованию криптографического образования.

М. И. Соколов был первым начальником кафедры криптографии. Им написан оригинальный учебник по криптографии, в котором обобщен опыт практической работы по различным видам так называемых ручных шифров. Эта книга до сих пор является обязательным пособием при подготовке криптографов-математиков любого уровня.

Оригинальным и самобытным специалистом зарекомендовал себя Г. В. Чуриков. Его поразительная криптографическая интуиция помогала разрабатывать и потом теоретически обосновывать сложные методы криптографического анализа. В последние годы своей жизни он также много внимания уделял преподаванию и воспитательной работе среди слушателей Института криптографии, связи и информатики (ИКСИ).

Л. А. Тихонов помимо практической работы и теоретических исследований (например, известна его работа по изучению свойств реверсивности сложных шифрсистем) занимался педагогической деятельностью, читая лекции при подготовке молодых специалистов и на курсах усовершенствования инженерного состава. Он обладал прекрасными педагогическими данными, его лекции были живыми и остроумными и всегда вызывали большой интерес у слушателей.

Новый этап развития криптографической службы, а вместе с ней и криптографической науки, начался после окончания Великой Отечественной войны 1941–1945 гг. Победоносное окончание войны и разгром фашизма породили большие надежды на новую бесконфликтную жизнь. В войне участвовали многие страны, которые действительно были союзниками, объединившимися в борьбе против общего

врага. Но прошло совсем немного времени после окончания войны и стало очевидно, что мир разделился на два противостоящих друг другу лагеря. Знаменательной вехой в формировании этих лагерей была речь У. Черчилля, произнесенная им в Фултоне (США) 5 марта 1946 г. С этого времени охлаждение в отношениях между нашей страной и западными странами стало усиливаться и постепенно наступила эпоха «холодной войны». В этих условиях перед нашей страной, помимо восстановления разрушенного войной хозяйства, стала задача усиления обороноспособности. Важным элементом защиты государственных интересов было обеспечение надежной связи государственных и партийных органов. Руководство страны придавало этому вопросу исключительно большое значение, поэтому были приняты масштабные решения организационного, технического, кадрового плана. Стало ясно, что решение задач безопасности связи в новых условиях потребует новых кадров — высококвалифицированных специалистов-криптографов с хорошей математической подготовкой. Именно в середине XX века были приняты исторические решения, определившие развитие отечественной криптографии на многие десятилетия вперед , вплоть до настоящего времени.

Знаменательным событием в жизни криптографической службы стало решение Политбюро от 19 октября 1949 года о создании Главного управления Специальной службы, знаменитого ГУСС при ЦК ВКП(б). Одной из первых и важнейших задач, поставленных перед Службой, была задача кадрового обеспечения. При этом к кадрам предъявлялись самые высокие требования. Прежде всего, это должны быть высококвалифицированные специалисты, обладающие глубокими математическими знаниями и имеющие склонность к криптографическим исследованиям. Фактически в этот период родилась новая специальность — криптограф-математик. Решение этой кадровой задачи проходило по нескольким направлениям. Важным направлением было привлечение к работе в Специальной службе уже готовых кадров специалистов, в первую очередь преподавателей и выпускников Университета, сотрудников Академии наук и Математического института им. В. А. Стеклова. Именно в эти годы к решению криптографических задач были привлечены видные математики, зарекомендовавшие себя в научном мире своими оригинальными работами.

Воспитанник Лузинской школы математиков, ученик Д. Е. Меньшова, выпускник Московского университета (окончил аспирантуру и защитил кандидатскую диссертацию в 1937 г.), доктор физико-математических наук И. Я. Верченко начал работать в Специальной службе с 1947 года. В период с 1962 г. по 1963 г. был начальником кафедры математики, потом начальником технического факультета Высшей школы КГБ, на котором готовились в том числе и кадры криптографов-математиков. Совместно с А. И. Узковым и Г. П. Толстовым поставил обновленный курс математического анализа. И. Я. Верченко сыграл выдающуюся роль в организации учебного процесса по подготовке кадров криптографов и вообще в деле становления Специальной службы в новых условиях, проявив незаурядные организаторские способности, твердость и принципиальность в отстаивании своих взглядов. Будучи руководителем технического факультета, И. Я. привлек к педагогической работе ряд крупных математиков из Университета или окончивших Университет. При нем на факультете работали Н. П. Жидков, В. Я. Козлов, Л. Я. Окунев, А. И. Узков, Г. П. Толстов и другие. Это обеспечивало высокий, практически университетский, уровень математической подготовки слушателей. За успехи в педагогической деятельности И. Я. был избран членом-корреспондентом АПН.

В 1951 году на работу в ГУСС пришел В. Я. Козлов, выпускник Московского университета, также воспитанник Лузинской школы, ученик Н. К. Бари, доктор физико-математических наук, впоследствии член-корреспондент АН. В. Я. с большим энтузиазмом включился в новую работу и быстро сплотил вокруг себя молодых и талантливых ученых. Научная школа В. Я. Козлова оказала и продолжает оказывать определяющее влияние на развитие современной отечественной криптографии.

В 50-е годы к активному сотрудничеству со Специальной службой (в основном, на правах совместительства) были привлечены такие выдающиеся математики, как А. А. Марков (мл.), Ю. В. Линник, Л. Я. Куликов и другие. Запомнился также постоянно действующий семинар в МИАН по вопросам математической статистики, который вели выдающиеся ученые-математики Н. В. Смирнов и Л. Н. Большев. Молодые криптографы, недавно пришедшие из Университета и Высшей школы, с большим интересом и пользой посещали этот семинар.

Кандидаты физико-математических наук И. Н. Санов, И. О. Бежаев, А. Т. Подколзин пришли на работу практически одновременно в 1951 году. Как старшие, более опытные и подготовленные специалисты они возглавили наиболее ответственные участки работы и достаточно быстро добились значительных успехов. Уже в 1952 году эти три автора подготовили научный отчет, в котором дали обоснование и детальный расчет одного принципиального метода криптографического анализа. Этот метод в будущем послужил основой для разработки специализированных средств вычислительной

техники.

Производственные группы, которые возглавляли старшие специалисты, постоянно пополнялись молодыми сотрудниками, среди которых было много выпускников мехмата МГУ. Всех их перечислить не представляется возможным, хотя все они этого заслуживают. Назовем лишь некоторых. Это Г. П. Башарин, Т. П. Тихонова, З. Н. Зайцева, З. С. Волобуева, Е. И. Кузьминова, Г. И. Лужкова и многие, многие другие. Перед молодыми сотрудниками было необозримое поле деятельности, где они могли быть первооткрывателями, поэтому с большим рвением они брались за решение самых сложных задач и нередко добивались впечатляющих результатов, многие из которых заложили фундамент будущих успехов в работе Специальной службы.

Еще одно важное направление в подготовке криптографов-математиков связано с созданием закрытого отделения на механико-математическом факультете МГУ. Решение о создании такого отделения было принято Советом Министров СССР 23 сентября 1949 года. Мехмат находился в это время в старом здании Университета на Моховой. Была выделена небольшая аудитория с «предбанником» и дежурным постом. Дверь в аудиторию была постоянно заперта и имела звонок. Эта дверь «с кнопкой» постоянно рождала среди студентов всевозможные легенды. В то время самыми популярными направлениями были атомная энергетика и ракетная техника, криптография как возможная область деятельности практически не упоминалась. Отбор в спецгруппу был весьма тщательный. Помимо хорошей успеваемости, были строгие требования по дисциплине, анкетным данным, состоянию здоровья. Беседы с каждым кандидатом проходили на достаточно высоком уровне, в том числе с инструкторами ЦК на Старой площади. От предложения к зачислению в спецгруппу, как правило, невозможно было отказаться. Мне известен один случай, когда мой товарищ, очень не хотевший попасть в спецгруппу, на беседе простодушно сказал, что он разговаривает во сне и вообще любит выпивать. Таких откровений кадровые работники не ожидали, но в группу его все-таки не взяли.

Руководителем закрытого отделения в ранге заместителя декана механико-математического факультета МГУ был Г. И. Пондопуло, кандидат физико-математических наук, выпускник мехмата 1937 года. Г. И. вложил много душевных сил и организаторских способностей в становление закрытого отделения, налаживание учебного процесса, проявляя при этом большую заботу о студентах. Одновременно он работал на руководящей должности в Специальной службе. Поэтому некоторые выпускники, приходя на работу, снова попадали под его заботливое руководство. Это способствовало адаптации бывших студентов к новым, очень строгим условиям работы, да и всей внеслужебной жизни. С 1953 года Г. И. Пондопуло в течение 23 лет был бессменным руководителем кафедры криптографии. Именно при нем преподавание криптографических дисциплин было поднято на высокий уровень, что было обусловлено тем, что в педагогическом процессе участвовали ведущие специалисты Службы.

К преподаванию на закрытом отделении были также привлечены лучшие педагогические кадры мехмата. Дополнительные главы теории вероятностей читал А. Я. Хинчин — крупнейший советский математик и выдающийся педагог. Его лекции отличались высоким методическим мастерством, ясностью изложения, изяществом в проведении математических доказательств. Примерно в это время А. Я. опубликовал свои работы по теории энтропии вероятностных схем, в которых развивал и уточнял идеи К.Шеннона. Шенноновский подход к оценке стойкости шифров, основанный на понятии энтропии, явился крупным достижением теоретической криптографии. Молодые специалисты, криптографы-практики с большим энтузиазмом осваивали новые идеи. Большую роль сыграли в этом деле ученые, привлеченные к работе в Специальной службе.

Теорию чисел, некоторые дополнительные вопросы алгебры читал А. О. Гельфонд. А. О. всегда поражал своей эрудицией, умением предвидеть результаты сложных исследований. Мне очень повезло в том, что дипломную работу я выполнял под его руководством. Как руководитель А. О. отличался доброжелательностью и внимательностью к своим ученикам. Он уделял им много времени, часто принимал у себя дома в своей небольшой квартире у Курского вокзала.

В последние годы функционирования закрытого отделения теорию вероятностей и математическую статистику читал доктор физико-математических наук, профессор Б. А. Севастьянов, один из ведущих специалистов-математиков в этих областях, воспитанник Московского университета, ученик академика А. Н. Колмогорова.

Вопросы высшей алгебры и некоторых ее приложений к криптографическим задачам преподавал кандидат физико-математических наук И. Н. Санов, который одновременно работал в Специальной службе. И. Н. внес также большой вклад в становление и развитие вероятностных методов в криптографии. В этой области он плодотворно сотрудничал с академиком Ю. В. Линником.

Следует вообще отметить, что студентам первых послевоенных лет выпало счастье слушать лекции выдающихся ученых и педагогов, таких как А. Н. Колмогоров, Б. Н. Делоне, А. Г. Курош, А. И. Маркушевич, П. К. Рашевский, А. П. Минаков, Л. Н. Сретенский и многих других. Каждый из них был неповторимой личностью, блестящим лектором, обладал большим педагогическим мастерством. Неудивительно, что вокруг них всегда группировались студенты, аспиранты, молодые ученые. Интерес к научным исследованиям, дух творчества был отличительной чертой учебы в Московском университете.

Для преподавания криптографических дисциплин студентам закрытого отделения были привлечены ведущие специалисты службы. Общий курс криптографии читал М. С. Одноробов, выпускник МГУ 1941 года. Используя богатый практический материал, имеющуюся довольно скудную литературу, опираясь на собственные проработки, М. С. подготовил большой 4-х томный курс по криптографии, изданный в 1951 году. Это была первая попытка изложения теоретического материала с использованием математических моделей и соответствующих расчетов. Особенно следует отметить его интерес к новым идеям, в частности, к шенноновскому подходу к оценке свойств шифров. Запомнились его содержательные научные дискуссии по этим вопросам с выпускником закрытого отделения 1952 года Н. Н. Ченцовым, впоследствии известным математиком, автором многих статей и монографий по теории вероятностей и математической статистике.

Теорию дисковых шифраторов, в том числе теорию подстановочных уравнений, читали выпускники МГУ кандидат физико-математических наук А. А. Блинов и В. И. Бобылев, впоследствии также защитивший диссертацию, уже находясь на работе в Специальной службе. А. А. принимал активное участие в развитии и совершенствовании криптографического образования как на закрытом отделении МГУ, так и на кафедре криптографии технического факультета Высшей школы.

Основы вычислительных устройств и технических средств, используемых в криптографии, преподавал кандидат наук В. С. Полин, один из ведущих специалистов Службы, стоявший у истоков создания специальных технических средств в интересах решения криптографических задач.

Первый выпуск закрытого отделения мехмата состоялся в 1951 году. Среди его выпускников особо следует отметить В. Е. Степанова и Ю. Н. Горчинского. В. Е. был одаренным математиком. Его работы по критериям для цепей Маркова, по исследованию некоторых специальных систем уравнений не только внесли большой вклад в аналитические методы криптографии, но и послужили толчком, открыли перспективу для новых исследований, в том числе и многих его учеников. В. Е. был блестящим педагогом, пользовался большим авторитетом и уважением слушателей технического факультета и коллег по работе. Его лекции всегда были глубоки по содержанию, а его требовательность и научная принципиальность снискали ему большое уважение и авторитет в коллективе. В. Е. воспитал целую плеяду молодых ученых, кандидатов и докторов наук. Он один из первых выпускников закрытого отделения, защитивший кандидатскую диссертацию. Среди представленных им результатов был и такой, в котором исправлялся результат одного американского автора. Этот факт произвел неизгладимое впечатление на руководство Специальной службы, поскольку в то время Служба была строго замкнутой организацией и никаких внешних контактов, тем более с американцами, не имела. В апреле 1964 года В. Е. один из первых защитил докторскую диссертацию и стал признанным лидером теоретических исследований в криптографии.

Ю. Н. Горчинский вскоре после окончания закрытого отделения также стал ведущим криптографом-математиком. По его инициативе и при его личном участии разрабатывались сложные вопросы современной теоретической криптографии. Он много и плодотворно работал в области теории шифрующих автоматов, применения алгебраических методов для изучения свойств шифров и оценки их стойкости. Многие его исследования имеют не только теоретическое, но и большое практическое значение, в частности, легли в основу разработки системы требований к стойкости шифрсистем и их классификации. Ю. Н. также уделял большое внимание подготовке кадров, преподавал на техническом факультете и в ИКСИ, воспитал многих кандидатов и докторов наук.

Первый выпуск закрытого отделения дал также таких известных криптографов-математиков, как О. Ю. Приходов, Ю. А. Веретенников, С. А. Казаков, Л. С. Михайлов, Н. М. Петрова и другие.

Среди выпускников 1952 года впоследствии также оказался ряд крупных криптографов, сыгравших важную роль в развитии теоретической криптографии и ее приложениях.

Так В. Н. Сачков с первых дней учебы на закрытом отделении зарекомендовал себя исключительно способным и настойчивым студентом, отличался большим трудолюбием и упорством в достижении поставленной цели. На работе эти качества позволили ему достаточно быстро найти свое оригинальное направление криптографических исследований, связанное с применением методов комбинаторно-

вероятностного анализа для исследования свойств современных шифров. Дар научного предвидения у него проявился даже в том, что из всех популярных в то время видов спорта, таких как волейбол, баскетбол или гимнастика, он отдал предпочтение единственному доступному тогда виду единоборств — это самбо. Его результаты математического характера опубликованы им в нескольких монографиях, известных во всем мире. В. Н. также постоянно уделяет внимание подготовке кадров, долгие годы ведет преподавательскую деятельность сначала на техническом факультете, в настоящее время в ИКСИ. Среди его учеников также много кандидатов и докторов наук. В. Н. является вице-президентом Академии криптографии. За заслуги в научной и педагогической деятельности и в первую очередь в области криптографии ему присвоено звание Почетного выпускника Московского Университета.

Выпускник этого же года Э. Ф. Скворцов еще на студенческой скамье увлекся алгебраическими исследованиями под руководством А. И. Узкова. Придя на работу, он продолжил исследования в области теории структур линейных преобразований. Эта тематика имела исключительно большое значение для оценки свойств и криптографического качества новых шифрующих устройств. Работы Э. Ф. положили начало многочисленным последующим исследованиям и по праву могут быть названы пионерскими работами в этой области.

Еще один выпускник 1952 года Л. Я. Савельев уже в студенческие годы показал себя вдумчивым исследователем, стремящимся в любом вопросе докопаться до самой сути, придать даже известным результатам оригинальную и нестандартную трактовку. В 1958 году он защитил кандидатскую диссертацию и вскоре перешел на работу в Сибирское отделение АН. Работая там, он подготовил и издал оригинальную книгу по комбинаторике и теории вероятностей, а также (совместно с М. М. Лаврентьевым) монографию по теории операторов и некорректным задачам.

Упоминавшийся уже Н. Н. Ченцов, также выпускник 1952 года, после окончания закрытого отделения перешел на работу в Институт прикладной математики и быстро вырос в крупного специалиста, пользовавшегося большим авторитетом в научном мире.

Среди выпускников 1953 года выделялся Ю. И. Медведев. Придя на работу в Специальную службу, он возглавил новое направление по исследованию свойств шифрсистем при наличии ограниченной информации об их устройстве. Его теоретические исследования в этой области легли в основу кандидатской, а потом и докторской диссертаций. Он также принимал активное участие в преподавательской деятельности. Совместно с Г. И. Ивченко (также выпускником мехмата) издал в 1984 году учебник по математической статистике.

Выпуск 1953 года был последним, который целиком проходил в старом здании МГУ на Моховой. Следующий выпуск 1954 года был уже в новом здании МГУ на Воробьевых (тогда Ленинских) горах.

Среди выпускников закрытого отделения этого года были А. А. Боровков и И. С. Волков, оба поступившие в аспирантуру сразу после окончания мехмата, их научным руководителем был академик А. Н. Колмогоров. А. А. недолго работал в Специальной службе. В 1959 году он перешел на работу (как и Л. Я. Савельев) в Сибирское отделение АН и переехал в Новосибирск. Но даже за короткий срок он оставил яркий след в теоретических исследованиях по криптографии, внес значительный вклад в разработку практических задач. Его дипломная работа, посвященная линейным статистическим критериям в криптографии, оказала заметное влияние на дальнейшие исследования в этой области. Характерной особенностью работ А. А. является сочетание тонких и оригинальных методов исследования с доведением полученных результатов до практического применения и получения расчетных формул. В дальнейшем А. А. много и плодотворно работает в разных областях теории вероятностей и математической статистики. Им выпущены учебники по теории вероятностей и математической статистики, имевшие ряд переизданий. Эти учебники активно используются в учебном процессе при подготовке криптографов-математиков в ИКСИ.

И. С. Волков, придя в Специальную службу, свои глубокие знания по теории вероятностей и вообще широкий кругозор во многих областях математики, заложенный университетским образованием и воспитанием, с большим успехом применил в практической работе по принципиально новым направлениям теоретической криптографии. Его заслуги в этой деятельности отмечены Ленинской премией. Среди коллег по работе И. С. известен как знающий специалист, твердо и непреклонно отстаивающий свои принципиальные убеждения. Он также принимал участие в педагогической деятельности на техническом факультете. И. С. многие годы является членом ученого совета по защите диссертаций.

Ю. И. Максимов окончил закрытое отделение мехмата в 1956 году, доктор физико-математических наук, является крупным специалистом в области теоретико-вероятностных и статистических методов

исследования сложных современных шифрсистем. Ю. И. активно участвует в подготовке специалистов высшей квалификации, 13 аспирантов под его руководством успешно защитили кандидатские диссертации.

В этом же году закрытое отделение мехмата окончил В. П. Елизаров, который является одним из старейших преподавателей кафедры дискретной математики ИКСИ, кандидатскую диссертацию защитил в 1961 году. В. П. подготовил лично и в соавторстве несколько учебных пособий по алгебраическому профилю, которые используются как основной учебный материал при подготовке математиков-криптографов.

Особую роль в подготовке кадров высшей квалификации — докторов и кандидатов наук — сыграл Ученый совет, созданный в рамках ГУССа в 1949 году. В его состав вошли авторитетные ученые и специалисты-практики того времени. В первом составе совета были академик А. Н. Колмогоров и член-корреспондент АН А. О. Гельфонд. В состав совета входили также И. Я. Верченко, Г. И. Пондопуло, А. А. Блинов, Г. В. Чуриков, В. С. Полин и другие. В 1951 году было утверждено Положение о Совете и Положение об аспирантуре (очной и заочной). С этого времени началась регулярная работа по подготовке кадров высшей квалификации, которая плодотворно продолжается и по сей день.

Среди первых аспирантов-очников были выпускники мехмата, в том числе закрытого отделения, Г. П. Башарин, В. Н. Сачков, Л. Я. Савельев, П. Н. Голованов, Е. И. Кузьминова, Е. И. Веретенникова и другие. Защиты кандидатских диссертаций начались с 1954 года. В числе первых кандидатами наук стали Г. П. Башарин, Е. В. Павловский, В. К. Левин, П. Ф. Беляев.

Длительное время ученым секретарем Совета был В..И. Егоров. Его стараниям и заботам обязаны многие кандидаты и доктора наук в области криптографии, ставшие впоследствии видными учеными-криптографами. С 1980 года по 1990 год на посту ученого секретаря находился С. Н. Сумароков, выпускник мехмата 1963 года. Его высокая требовательность и педантичность запомнились многим соискателям на долгие годы. Вместе с тем эта требовательность и принципиальность в оценке представленных диссертаций создали Совету высокую репутацию и большой авторитет в ученых кругах, о чем свидетельствует четкое и безотказное прохождение работ в ВАКе. Сам С. Н. успешно работал в области теории булевых функций и защитил кандидатскую диссертацию. Его пионерские исследования некоторых криптографических свойств булевых функций послужили мощным толчком для дальнейших работ в этом направлении.

Преподавание криптографических дисциплин на закрытом отделении мехмата проводилось до 1954 года. После этого было расширено преподавание математических дисциплин по наиболее актуальным направлениям, важным для Специальной службы. В новом качестве закрытое отделение продолжало функционировать вплоть до 1957 года, когда было принято решение о его ликвидации.

Следует отметить, что и в последующие годы выпускники мехмата направлялись на работу в Специальную службу. Многие из них и по сей день успешно работают в практических подразделениях, а также ведут преподавательскую работу в ИКСИ.

Выпускник мехмата 1958 года В. А. Башев стал одним из ведущих криптографов Специальной службы. Его работы по алгебраическому и теоретико-автоматному направлению исследований в области криптографии внесли существенный вклад в развитие аналитических методов анализа сложных современных шифрсистем. В. А. успешно руководит работой аспирантов, активно участвует в проведении занятий на курсах повышения квалификации криптографов, является соавтором крупной монографии по теории шифрующих автоматов. За заслуги в научной деятельности и вклад в развитие криптографического образования удостоен звания Почетного выпускника Московского Университета.

В. А. Носов окончил мехмат в 1963 году и в этом же году начал работу в Специальной службе, получил хорошие результаты в практической деятельности и теоретических исследованиях, защитил в 1970 году кандидатскую диссертацию, потом перешел на преподавательскую работу. Долгое время был руководителем кафедры дискретной математики, подготовил несколько учебных пособий по теории сложности вычислительных алгоритмов и другим разделам дискретной математики.

Выпускник мехмата 1962 года, доктор физико-математических наук, профессор Г. В. Балакин является инициатором исследований систем уравнений специального вида. Это направление тесно связано не только с теоретическими вопросами криптографии, но и имеет важное прикладное значение. По этому вопросу Г. В. подготовил обстоятельную монографию и значительное число открытых публикаций. Он длительное время ведет педагогическую работу в ИКСИ, имеет много учеников и последователей.

М. П. Кривенко окончил мехмат в 1969 году, защитил докторскую диссертацию в 1994 году, в

настоящее время является начальником кафедры ИКСИ по прикладной математике и информатике. М. П. активно участвует в подготовке специалистов по автоматизации информационно-аналитической деятельности, имеет большое число научных и научно-методических работ, успешно руководит работой аспирантов.

Одна из причин решения о ликвидации закрытого отделения мехмата состояла в том, что в Специальной службе была создана и набрала полную силу собственная система подготовки кадров, в том числе и криптографов-математиков. Эта система развивалась параллельно с функционированием закрытого отделения мехмата. Еще при образовании ГУССа была создана Высшая школа криптографов, позже в 1960 году преобразованная в технический факультет Высшей школы (ВШ) КГБ, а в 1992 году на его базе создан Институт криптографии, связи и информатики (ИКСИ), вошедший в состав Академии ФСБ России.

Как уже отмечалось, у истоков системы подготовки криптографов-математиков стояли ученые и преподаватели из Университета или окончившие Университет. Традиции Университета и уровень подготовки привлеченных специалистов были восприняты системой подготовки кадров в Специальной службе и успешно продолжаются до настоящего времени. Профиль подготовки в ИКСИ значительно расширился, но, тем не менее, подготовка криптографов-математиков составляет одно из главных направлений его деятельности. В педагогической и воспитательной работе по подготовке новых высококвалифицированных кадров важное место занимает использование опыта и знаний специалистов старшего поколения, в том числе воспитанников Московского Университета. Именно по этому пути идет развитие и совершенствование учебного процесса в ИКСИ.

К настоящему времени в ИКСИ, как преемнике традиций и опыта предшествующих форм подготовки, сложился высококвалифицированный профессорско-преподавательский коллектив. Важное место в этом коллективе занимают выпускники Университета разных лет. Следует также отметить, что и собственные выпускники ИКСИ выросли в крупных специалистов и руководителей, успешно работающих как в Специальной службе, так и в самом ИКСИ. Ряд выпускников ИКСИ по разным причинам перешли на работу в другие отрасли народного хозяйства и успешно трудятся в новых условиях, что говорит об их широкой и всесторонней подготовке.

В заключение можно отметить, что роль Московского университета в становлении и развитии отечественной криптографии, в деле подготовки высококвалифицированных кадров криптографов-математиков была и остается очень высокой. Большое значение имело созданное в свое время закрытое отделение механико-математического факультета МГУ. Эстафету системы подготовки кадров криптографов-математиков, заложенную в те годы, с успехом продолжает и развивает коллектив ИКСИ, опираясь на традиции научно-педагогической деятельности Университета и сочетая их с традициями Специальной службы.

Многие подготовленные за прошедшие годы специалисты заняли ведущее место в современной криптографической науке, ряд выпускников стали руководителями разного ранга.

Криптографы-математики, работая на ответственных участках и решая сложные задачи, обеспечивают высокий уровень криптографической науки и вносят тем самым свой вклад в укрепление могущества и обороноспособности нашей Родины.

## Литература

[1] 50 лет Институту криптографии, связи и информатики (исторический очерк). М.: 1999.

[2] Соболева Т. А. История шифровального дела в России. М.: ОЛМА-ПРЕСС, 2002.

[3] Бабаш А. В., Шанкин Г. П. История криптографии. М.: Гелиос-АРВ, 2002.