**Федеральное государственное бюджетное учреждение науки**
**МАТЕМАТИЧЕСКИЙ ИНСТИТУТ ИМ. В. А. СТЕКЛОВА РАН**

На правах рукописи



Трушечкин Антон Сергеевич

# СВОЙСТВА МОДЕЛЕЙ НЕОБРАТИМОЙ КВАНТОВОЙ ДИНАМИКИ И КВАНТОВОЙ КРИПТОГРАФИИ

01.01.03 — Математическая физика

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
доктора физико-математических наук

**Москва — 2019**

Работа выполнена в федеральном государственном бюджетном учреждении науки Математический институт им. В. А. Стеклова РАН

Научный консультант: **Игорь Васильевич Волович**,
доктор физико-математических наук, член-корреспондент РАН, главный научный сотрудник отдела математической физики ФГБУН Математический институт им. В. А. Стеклова РАН (специальность — 01.01.03)

Официальные оппоненты: **Андрей Игоревич Кириллов**,
доктор физико-математических наук, пенсионер (специальность — 01.01.03)

**Василий Никитич Колокольцов**,
доктор физико-математических наук, главный научный сотрудник Международной лаборатории стохастического анализа и его приложений ФГАОУ ВО «Национальный исследовательский университет «Высшая школа экономики» (специальность — 01.01.03)

**Андрей Игоревич Шафаревич**,
доктор физико-математических наук, член-корреспондент РАН, профессор кафедры дифференциальной геометрии и приложений механико-математического факультета ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова» (специальность — 01.01.03)

Ведущая организация: ФГБУН Санкт-Петербургское отделение Математического института им. В. А. Стеклова РАН

Защита состоится 9 апреля 2020 г. в 14 часов на заседании совета по защите диссертаций Д 002.022.02 при Математическом институте им. В.А. Стеклова РАН по адресу: 119991, г. Москва, ул. Губкина, д. 8.

С диссертацией можно ознакомиться в библиотеке Математического института им. В.А. Стеклова РАН и на сайте института по адресу http://www.mi-ras.ru/dis/ref19/trushechkin/dis.pdf

Автореферат разослан “____” декабря 2019 г.

Ученый секретарь Диссертационного совета,
доктор физико-математических наук Ю.Н. Дрожжинов

## ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Актуальность и степень разработанности темы исследования.**

1. Изучение необратимой динамики имеет давнюю историю. Одним из простейших и, возможно, исторически первых примеров необратимой динамической системы можно считать уравнение движения Ньютона в присутствии силы трения. Другой пример необратимой динамики предоставляет гидродинамика, а именно уравнение Навье–Стокса движения вязкой жидкости. В термодинамике представление о необратимых процессах восходит к работам Р. Клаузиуса, который ввёл понятие энтропии для количественной характеристики степени необратимости динамики. Теория необратимых процессов в классической термодинамике и статистической физике получила развитие в работах Дж. Максвелла, Л. Больцмана, Дж. Гиббса, А. Пуанкаре, Л. Онсагера, И.Р. Пригожина, А.Н. Колмогорова, А.Я. Хинчина, Д.Н. Зубарева и других. В частности, для данной диссертации важно упомянуть кинетическое уравнение Больцмана, описывающее необратимое поведение газа в терминах функции плотности распределения частиц в фазовом пространстве.

Исследование необратимых процессов в квантовой механике восходит к работам В. Паули, Л.Д. Ландау, Дж. фон Неймана. Для описания необратимой квантовой динамики чаще всего прибегают к формализму открытых квантовых систем, т.е. систем, взаимодействующих с резервуаром. В некоторых случаях динамику состояния системы (т.е. положительного ядерного оператора в гильбертовом пространстве с единичным следом) можно описать при помощи квантовой динамической полугруппы. Соответствующее дифференциальное уравнение называется квантовым кинетическим уравнением (quantum master equation). Общий вид генератора квантовой динамической полугруппы (в конечномерном случае и, более общо, в случае ограниченного генератора) выведен в работах В. Горини (V. Gorini), А. Коссаковски (A. Kossakowski) и Э. Сударшана (E. Sudarshan) и независимо от них — Г. Линдблада (G. Lindblad). Поэтому квантовое кинетическое уравнение, в правой части которого стоит данный генератор, называется уравнением Горини–Коссаковски–Сударшана–Линдблада (ГКСЛ). Это уравнение играет фундаментальную роль в теории открытых квантовых систем.

Обычно факт необратимости динамики, описываемой кинетическим уравнением, выражается в виде той или иной $H$-теоремы, т.е. невозрастания некоторого функционала ($H$-функции, в некоторых случаях является функцией Ляпунова). В частности, для упомянутого выше кинетического уравнения Больцмана роль $H$-функции играет величина энтропии, взятая со знаком «минус», введённая самим Больцманом.

Однако для уравнения ГКСЛ энтропия фон Неймана (энтропия квантовой

системы) не является подходящим функционалом, поскольку в общем случае энтропия на решениях уравнения ГКСЛ может и убывать, что связано с тем, что система не изолирована, а взаимодействует с резервуаром. Однако в соответствии со вторым началом термодинамики неотрицательной должна быть величина, состоящая из двух слагаемых: производной по времени от энтропии системы и потока энтропии из системы в резервуар в единицу времени. Эта величина называется производством энтропии и широко используется в неравновесной термодинамике и статистической механике.

В диссертации сделан уклон на математическое значение функционала производства энтропии, а именно на нахождение с его помощью стационарных решений уравнения ГКСЛ. Как и для других уравнений движения, нахождение всех стационарных решений (стационарных состояний) — одна из важнейших задач для уравнения ГКСЛ. В простейшем случае уравнение ГКСЛ имеет одно стационарное решение. Но уравнения с множеством стационарных решений представляют интерес ввиду того, что в этом случае возникают нетривиальные эффекты, важные в том числе и для практики, такие как, например, «пленение» квантовых когерентностей, сверхперенос энергии и другие. Общая структура стационарных решений уравнения ГКСЛ активно изучается на протяжении нескольких десятков лет, с того времени как это уравнение появилось. Однако информация об общей структуре не всегда позволяет найти всё множество стационарных решений для конкретного уравнения.

Также для квантовой термодинамики важны системы, взаимодействующие с несколькими резервуарами, находящимися при различных температурах. В этом случае аналитическое нахождение стационарных состояний даже в простых случаях и даже когда из общей теории следует, что стационарное состояние единственно, часто представляет трудности. Например, до сих пор не был известен общий аналитический вид стационарного состояния пары взаимодействующих двухуровневых квантовых систем, одна из которых также взаимодействует с «горячим» резервуаром, а другая — с «холодным». Известен был лишь ответ для частного случая.

Одним из методов нахождения стационарных состояний кинетических уравнений, восходящий к Больцману, является исследование $H$-функции этого уравнения. $H$-функция для уравнения Больцмана позволила последнему доказать сходимость решений этого уравнения к распределению Максвелла. Впрочем, строго этот факт был доказан только сравнительно недавно С. Виллани (C. Villani).

Изучение открытых квантовых систем важно в том числе в связи с развитием квантовых технологий. Наибольший интерес представляет перспектива создания квантового компьютера, который бы позволил эффективно решать некоторые за-

дачи, не решаемые эффективно (за приемлемое время) на обычных (классических) компьютерах. В частности, Нобелевская премия по физике 2012 г. была присуждена С. Арошу (S. Haroche) и Д. Вайнленду (D. Weinland) «за создание прорывных технологий манипулирования квантовыми системами, которые сделали возможными измерение отдельных квантовых систем и управление ими».

2. Квантовая система, взаимодействующая с резервуаром, — не единственная модель необратимой квантовой динамики. В настоящее время в работах В.В. Козлова, Д.В. Трещёва, О.Г. Смолянова и других развивается подход (восходящий к Пуанкаре), связанный с так называемым слабым пределом решений эволюционных уравнений. Для ряда случаев доказывается, что, несмотря на обратимость уравнения Лиувилля в классической механике и уравнений Шрёдингера и фон Неймана — в квантовой, предельная функция плотности в фазовом пространстве при бесконечно больших временах обладает большей энтропией, нежели начальная плотность, что является свойством необратимой динамики. К теории слабого предела примыкает также так называемая функциональная механика, предложенная И.В. Воловичем, в которой предлагается принять именно уравнения для функции плотности в качестве основных уравнений механики для обоснования необратимой динамики макроскопических систем исходя из обратимой динамики частиц.

Простейшая модель в этих рассмотрениях — это модель бесстолкновительной сплошной среды в прямоугольном ящике, которая сводится к движению на торе. Если для случая классической динамики удаётся доказать существование слабого предела (теоремы о диффузии), то непосредственное обобщение этих результатов на квантовый случай наталкивается на трудности. Эти трудности связаны с тем, что свободная квантовая динамика в ограниченном пространстве или на компактном многообразии является почти периодической, что связано с интерференцией волн, движущихся с разными скоростями. Данные интерференции проявляют себя на временах за пределами так называемого времени Эренфеста, когда квантовая динамика волновых функций (квадратично интегрируемых функций на торе), изначально локализованных и в координатном, и в импульсном пространствах (такие волновые функции называются когерентными состояниями), начинает отклоняться от классической.

Квантовая динамика за пределами времени Эренфеста представляет интерес сама по себе и активно изучается в настоящее время в математической физике. Один из подходов здесь связан с квазиклассическими мерами — квазиклассическим пределом мер Вигнера или (эквивалентно) Хусими. Поэтому результаты соответствующей части работы интересны не только в связи с исследованиями необратимой динамики и слабого предела, но и в связи с изучением квантовой динамики за пределами времени Эренфеста и с теорией квазиклассических мер.

3. Особым видом квантового необратимого процесса является квантовое измерение. В результате взаимодействия с измерительным прибором система необратимо меняет своё состояние, даже если результат измерения не считывается наблюдателем (такое измерение называется неселективным). В известном курсе теоретической физики Л.Д. Ландау и Е.М. Лифшица выделяется именно роль измерения в появлении необратимости в квантовых явлениях. С точки зрения теории открытых квантовых систем измерительный прибор представляет собой резервуар особого вида. Теория квантовых измерений восходит к работам фон Неймана и развивалась затем во многих исследованиях. В настоящее время квантовые измерения рассматриваются как одно из средств управления квантовыми системами, чему и посвящена одна из глав диссертации. Метод квантового управления посредством неселективных измерений был предложен и теоретически развит в работах А.Н. Печеня, Х. Рабица (H. Rabitz) и соавторов.

В диссертации рассматривается квантовое управление посредством неселективных измерений в системе Ландау–Зинера. Система Ландау–Зинера представляет собой простую (но фундаментальную) модель неадиабатического перехода в двухуровневой системе с переменным гамильтонианом и так называемым квазипересечением уровней энергии. С математической точки зрения речь идёт об определённой системе из двух линейных дифференциальных уравнений с переменными коэффициентами. Эта модель находит широкое применение в физике, химии и биохимии.

Бесконечно частые повторения одного и того же измерения над системой приводят, как известно, к так называемому квантовому эффекту Зенона, когда система «замораживается» в своём начальном состоянии и динамики не происходит. Однако бесконечно частые измерения — это математическая абстракция, на практике же можно осуществить только конечное число измерений (или же приближаться к квантовому эффекту Зенона иначе, например, путём рассмотрения не мгновенных, а непрерывных измерений, что также изучается). Поэтому возникает естественный вопрос об оптимальном приближении к квантовому эффекту Зенона при конечном числе измерений, т.е. о нахождении оптимальных моментов этих измерений.

4. Замечательным свойством некоторых классических кинетических уравнений, описывающих необратимую динамику, является то, что для них существуют так называемые микроскопические решения в виде суммы дельта-функций, соответствующие обратимой динамике микроскопических частиц. Точки, входящие в носитель таких сингулярных распределений, соответствуют частицам. Термин «микроскопические решения» предложен Н.Н. Боголюбовым. Более распространённое название таких решений — «решения в виде эмпирических мер». К таким уравнениям относятся уравнение Власова (что показано

самим А.А. Власовым), а также, как показано Н.Н. Боголюбовым, уравнение Больцмана–Энскога. К сожалению, доказательство Н.Н. Боголюбова этого интересного факта об уравнении Больцмана–Энскога выполнено лишь на «физическом» уровне строгости. Строгое доказательство наталкивается на трудности ввиду возникновения произведений дельта-функций.

5. Математически строгий вывод квантовых кинетических уравнений вида ГКСЛ для открытой квантовой системы осуществлён для пределов слабой связи системы с резервуаром (в физической литературе этот предельный случай называется теорией Редфилда, или стандартной теорией Редфилда), низкой плотности частиц резервуара и повторяющихся взаимодействий. Однако при изучении открытых квантовых систем интересны и другие предельные режимы. Так, например, в теории переноса энергии возбуждённого состояния в молекулярных (в том числе биологических, фотосинтетических) системах широко используются теория Фёрстера и модифицированная теория Редфилда. Но, к сожалению, в отличие от стандартной теории Редфилда, в настоящем виде эти теории не позволяют получить полный оператор плотности системы, а лишь только его диагональную часть в фиксированных базисах. В физической литературе диагональные матричные элементы оператора плотности называются также «населённостями», потому что соответствуют вероятностям нахождения системы на определённых энергетических уровнях, или, иными словами, населённостям уровней. Внедиагональные элементы называются «когерентностями» и отвечают за собственно квантовые эффекты. Невозможность вычислить динамику внедиагональных элементов оператора плотности (когерентностей) — это серьёзное ограничение указанных двух теорий. Несмотря на некоторые имеющиеся работы, в которых предлагается феноменологичекий вывод выражений для когерентности, проблема оставалась открытой.

6. Необратимые преобразования квантовых состояний часто рассматриваются в квантовой теории информации (одном из разделов современной математической физики). Так, например, с необратимым рассеянием квантовой информации в окружение мы сталкиваемся в квантовых коммуникациях и, более конкретно, в квантовой криптографии. Задача теоретической квантовой криптографии заключается в математическом доказательстве стойкости протоколов (алгоритмов) квантовой криптографии. Теоретическая квантовая криптография — один из разделов квантовой теории информации и, соответственно, современной математической физики. К математической физике она также примыкает и по используемым методам (которые имеют мало общего с обычной, классической криптографией).

Наиболее развитый раздел квантовой криптографии носит название квантового распределения ключей, поэтому эти два понятия часто употребляются

как синонимы. Квантовое распределение ключей позволяет двум сторонам, соединённых квантовым каналом, сгенерировать общий секретный ключ, то есть общую строку из двоичных символов (0 и 1), неизвестную никому более. Особенность квантовой криптографии заключается в том, что стойкость обеспечивается даже тогда, когда противник обладает неограниченными вычислительными возможностями.

Концепция квантового распределения ключей была предложена в 1984 г. Ч. Беннеттом (C. Bennett) и Ж. Брассаром (G. Brassard), которые разработали протокол, названный впоследствии BB84. Вскоре после этого последовали первые экспериментальные реализации этого протокола. В настоящее время реализованы коммерческие системы квантовой криптографии на основе протокола BB84. Разработки систем квантовой криптографии проводятся во многих странах и целым рядом крупных корпораций. Несмотря на то что предложено множество протоколов квантового распределения ключей, BB84 остаётся наиболее распространённым.

Первое полное математическое доказательство стойкости протокола BB84 было получено в работе Д. Майерса (D. Mayers) в 1996 г. Далее последовали другие доказательства. Общая математическая теория квантового распределения ключей, основанная на теории информации и энтропийных характеристиках, построена Р. Реннером (R. Renner) и затем развита в последующих работах разных авторов.

Упомянутые доказательства стойкости протоколов квантовой криптографии предполагают идеальную физическую аппаратуру. Одна из задач, стоящих перед теоретической квантовой криптографией сегодня, — это доказательство стойкости протоколов квантовой криптографии, которые учитывают то, что аппаратура работает неидеально, и получение соответствующих оценок достижимых скоростей генерации секретного ключа. Один из примеров неидеальности аппаратуры — это несовпадение квантовых эффективностей однофотонных детекторов, т.е. вероятностей регистрации ими фотона. Упомянутые выше доказательства неприменимы в этом случае.

Отметим, что система квантовой криптографии также может быть представлена как своеобразная открытая квантовая система, взаимодействующая с резервуаром. Роль системы здесь исполняет квантовый носитель информации (фотон), пересылаемый по каналу связи. Роль окружения играет противник, который взаимодействует с этим носителем, пытаясь считать эту информацию. С точки зрения «легитимных» отправителя и получателя этот процесс выглядит как необратимое рассеяние квантовой информации в окружение.

Тематику квантовой криптографии с тематикой производства энтропии в открытых квантовых системах объединяет и то, что и в том и в другом случае

одну из ключевых ролей играет минимизация квантовой относительной энтропии. В открытых квантовых системах так называемый неадиабатический вклад в производство энтропии выражается в монотонном уменьшении квантовой относительной энтропии между состоянием, зависящим от времени, и стационарным состоянием. При больших временах эта величина принимает минимально возможное значение при фиксированных линейных ограничениях (законах сохранения). В квантовой криптографии решается задача минимизации квантовой относительной энтропии между квантовым состоянием, возникающим в ходе протокола квантовой криптографии, и результатом действия на это состояние неселективного измерения одного из регистров, также при линейных ограничениях. Задача, решаемая в квантовом распределении ключей, также близка к задаче квантовой томографии: оценить информационные характеристики неизвестного квантового состояния по наблюдаемым данным.

**Цели и задачи.** Цель работы состоит в углублении понимания необратимой динамики квантовых систем и её соотношения с обратимой динамикой. Для осуществления этой цели ниже сформулированы задачи, связанные с различными моделями необратимой динамики: динамикой открытых квантовых систем, слабым пределом и квазиклассическими мерами, необратимой динамикой под воздействием квантовых измерений, существованием обратимых микроскопических решений кинетических уравнений и, наконец, необратимой динамикой квантовой информации на примере квантовой криптографии.

1. Построить функционал производства энтропии, являющийся неотрицательным для как можно более широкого класса уравнений ГКСЛ, а также его разложение на слагаемые, неотрицательные по отдельности, соответствующие адиабатическому и неадиабатическому вкладам. При помощи введённого функционала разработать метод нахождения стационарных решений уравнения ГКСЛ.

2. Описать квазиклассические меры, соответствующие свободной квантовой динамике когерентных состояний на торе на различных масштабах времени. Показать, что усреднение по времени приводит к выравниванию пространственной плотности, что соответствует обобщению результатов теории слабого предела на случай квантовой динамики на торе.

3. Осуществить оптимальное приближение к квантовому эффекту Зенона для модели Ландау–Зинера посредством конечного числа повторений неселективного измерения фиксированной наблюдаемой.

4. Доказать существование микроскопических решений (решений в виде сумм дельта-функций и соответствующих микроскопической динамике частиц) кинетического уравнения Больцмана–Энскога.

5. Вывести формулы зависимости от времени внедиагональных элементов

матрицы плотности в рамках двух теорий возмущений для динамики открытых квантовых систем: теории Фёрстера и модифицированной теории Редфилда, что позволит рассчитывать необратимую динамику всей матрицы плотности, а не только её диагональной части.

6. Получить выражение для предельной скорости генерации секретного ключа в протоколе квантовой криптографии BB84 в зависимости от наблюдаемых данных при детекторах с несовпадающими эффективностями.

**Научная новизна.** Ранее были известны некоторые определения функционала производства энтропии в открытых квантовых системах, динамика которых описывается уравнением ГКСЛ. Но обобщающий эти определения функционал, представленный в данной работе, определённый на языке операторов, без обращения к концепции квантовых стохастических траекторий, построен впервые. Адиабатический и неадиабатический вклады в производство энтропии также впервые определены для квантового случая на языке операторов, без обращения к концепции квантовых стохастических траекторий. Использование этой концепции ограничивало общность определений. Впервые доказано, что адиабатический вклад в производство энтропии неотрицателен в малой окрестности стационарного состояния при тех же предположениях, при которых неотрицательно производство энтропии в целом.

Впервые показано, как функционал производства энтропии можно использовать для нахождения стационарных решений уравнения ГКСЛ для систем, взаимодействующих с несколькими резервуарами с разными температурами, т.е. для неравновесных систем.

Впервые построено полное семейство квазиклассических мер, соответствующих эволюции когерентных состояний на торе, без сглаживания по времени.

Впервые рассмотрена и решена задача оптимального приближения к квантовому эффекту Зенона в модели Ландау–Зинера посредством конечного числа неселективных измерений фиксированной наблюдаемой.

Впервые строго доказано существование микроскопических решений (имеющих вид сумм дельта-функций и соответствующих микроскопической динамике частиц) у кинетического уравнения Больцмана–Энскога.

Выражения для динамики внедиагональных элементов матрицы плотности в теории Фёрстера и модифицированной теории Редфилда впервые получены в рамках строгого метода. До этого были известны только эвристические выражения для внедиагональных элементов матрицы плотности в модифицированной теории Редфилда, которые не учитывают важные эффекты и потому в некоторых случаях приводят к большим погрешностям.

Впервые доказана теорема о предельной скорости генерации секретного ключа в протоколе квантовой криптографии BB84 при детекторах с несовпадающи-

ми эффективностями. Для этого было использовано известное сведение задачи вывода формулы предельной скорости генерации к задаче минимизации квантовой относительной энтропии (выпуклой функции) при линейных ограничениях. До этого данная задача минимизации решалась только численно. В данной работе впервые продемонстрировано аналитическое решение этой задачи. Это позволяет говорить о новом методе вывода формул предельных и достижимых скоростей генерации секретного ключа в квантовой криптографии.

**Теоретическая и практическая значимость работы.** Работа носит теоретический характер. Один из основных результатов, связанный с доказательством теоремы о предельной скорости генерации секретного ключа в системах квантовой криптографии при детекторах с несовпадающими эффективностями, имеет и практическую ценность, поскольку соответствующая формула может быть использована в практических системах квантового распределения ключей.

Результаты, связанные с построением и исследованием функционала производства энтропии для решений уравнения ГКСЛ, могут быть использованы в квантовой термодинамике при анализе эффективности квантовых тепловых машин. Разработанный метод нахождения стационарных решений уравнения ГКСЛ может быть использован при анализе так называемых подпространств, свободных от декогеренции, изучаемых в теории помехоустойчивых квантовых вычислений.

Исследование квазиклассических мер квантовой динамики, доказательство выравнивания пространственной плотности при сглаживании по времени важно как для теории квазиклассических мер, так и для теории слабого предела, который, в свою очередь, является одним из современных направлений исследований фундаментальной проблемы необратимости. Эта проблема заключается в согласовании обратимых по времени уравнений микроскопической динамики с необратимой динамикой макросостояния физической системы, состоящей из большого числа частиц.

Решение задачи выбора оптимальных моментов измерений (воздействия специального вида) на систему Ландау–Зинера можно использовать для управления квантовыми системами, что важно, в частности, для создания квантовых компьютеров.

Доказательство существования микроскопических решений уравнения Больцмана–Энскога, т.е. доказательство того факта, что кинетическое уравнение, описывающее необратимую динамику и рост энтропии, содержит в себе также и обратимые решения, соответствующие микроскопической динамике частиц, также важно для углубления нашего понимания соотношения между обратимой и необратимой динамикой, возникновением необратимости при описании макроскопических систем.

Получение выражений для внедиагональных элементов матрицы плотности в теории Фёрстера и модифицированной теории Редфилда важно для более широкого применения этих теорий и более детального исследования роли квантовых эффектов в переносе энергии возбуждения в биологических системах.

**Методология и методы исследования.** В работе используются различные методы математической физики и функционального анализа.

Неотрицательность функционала производства энтропии, адиабатического и неадиабатического вкладов в производство энтропии доказана с помощью свойств выпуклости функций, входящих в определения этих функционалов. С помощью этих функционалов разработан метод нахождения стационарных решений уравнения ГКСЛ.

Для нахождения квазиклассических мер на торе использовались распределения Хусими (один из способов сопоставления квантовому состоянию классического распределения вероятностей на фазовом пространстве) и разложение функций Хусими в ряд Фурье по координатам и в интеграл Фурье по импульсам с последующим вычислением гауссовых интегралов.

Для решения задачи оптимального приближения к квантовому эффекту Зенона в модели Ландау–Зинера, т.е. подбора оптимальных моментов неселективных измерений, использовался метод динамического программирования и приближённые выражения для функций параболического цилиндра в различных предельных случаях.

Для доказательства существования микроскопических решений уравнения Больцмана–Энскога использовались методы теории обобщённых функций, а также регуляризации дельта-функций и интеграла столкновений.

Для вывода выражений для внедиагональных элементов матрицы плотности в теории Фёрстера и модифицированной теории Редфилда использовался метод проекционных операторов Цванцига.

Для доказательства теоремы о предельной скорости генерации секретного ключа при детекторах с разными эффективностями было использовано сведение задачи нахождения предельной скорости генерации к задаче выпуклой оптимизации — минимизации квантовой энтропии когерентности с линейными ограничениями — и аналитическое решение этой задачи. Поскольку аналитическое решение этой задачи продемонстрировано впервые, можно говорить о том, что предложен новый метод вывода формул предельных и достижимых скоростей генерации секретного ключа в квантовой криптографии.

**Положения, выносимые на защиту:**

1. Для широкого класса уравнений Горини–Коссаковски–Сударшана–Линдблада (ГКСЛ) построен функционал производства энтропии и доказана его неотрицательность. Доказана также неотрицательность по отдельности адиаба-

тического и неадиабатического вкладов в производство энтропии в окрестности стационарного состояния и, при определённых предположениях, для произвольных квантовых состояний.

2. Предложен метод поиска стационарных решений уравнения ГКСЛ в теории открытых квантовых систем, основанный на свойствах функционала производства энтропии. С помощью этого метода найден общий вид стационарных решений для нескольких моделей, для которых до этого общий вид стационарных решений в аналитическом виде известен не был.

3. Доказано существование обратимых по времени микроскопических решений нелинейного интегро-дифференциального кинетического уравнения Больцмана–Энскога для газа из твёрдых шаров, открытых Н.Н. Боголюбовым на физическом уровне строгости.

4. Полностью описаны квазиклассические меры, соответствующие свободной квантовой динамике когерентных состояний на торе на различных масштабах времени. Показано, что сглаживание по времени приводит к выравниванию плотности пространственного распределения.

5. Выведены формулы для внедиагональных элементов матрицы плотности в рамках двух теорий возмущений для динамики открытых квантовых систем: теории Фёрстера и модифицированной теории Редфилда. Это позволяет рассчитывать динамику всей матрицы плотности, а не только её диагональной части, и потому устраняет существенное ограничение этих теорий, широко используемых в теории переноса энергии в молекулярных системах.

6. Решена задача оптимального приближения к квантовому эффекту Зенона для модели Ландау–Зинера, то есть задача выбора оптимальных моментов неселективных измерений определённой наблюдаемой при фиксированном их числе.

7. Доказана теорема о предельной скорости генерации секретного ключа в протоколе квантовой криптографии BB84 при несовпадающих эффективностях однофотонных детекторов. Предложен новый метод доказательства подобных теорем на основе аналитической минимизации квантовой относительной энтропии когерентности.

**Степень достоверности и апробация результатов.** Достоверность результатов глав 1–4 и 6 обеспечивается их строгими математическими доказательствами. Результаты главы 5 получены на «физическом» уровне строгости, их достоверность обеспечивается следованием систематическому методу (методу проекционных операторов Цванцига) и сравнением расчётов по выведенным формулам с расчётами по точному (но алгоритмически затратному и потому непригодному для больших систем) методу.

Результаты диссертации докладывались на общеинститутском семинаре «Математика и её приложения» МИАН им. В.А. Стеклова, семинарах отделов

математической физики и теоретической физики МИАН, семинаре «Квантовая вероятность, статистика и информация» МИАН, семинаре «Асимптотические методы в математической физике» ИПМех им. А.Ю. Ишлинского РАН, семинаре «Дифференциальные операторы на сингулярных пространствах, алгебраически интегрируемые системы и квантование» механико-математического факультета МГУ им. М.В. Ломоносова, семинаре «Квантовая физика и квантовая информация» МФТИ, семинаре по математической физике им. М.В. Масленникова ИПМ им. М.В. Келдыша РАН, на Международном конгрессе по математической физике (Ольборг, Дания, 2012), на следующих международных научных конференциях: QBIC V (международная конференция по квантовой биоинформатике и квантовым вычислениям, Токио, Япония, 2011), ICSSUR 2013 (международная конференция по сжатым состояниям и соотношениям неопределённостей, Нюрнберг, Германия, 2013), Statphys 25 (25-я международная конференция по статистической физике, Сеул, Корея, 2013), «Математическая статистическая физика» (Киото, Япония, 2013), QP 34 (международная конференция по квантовой вероятности и смежным вопросам, Москва, 2013), «Геометрия и управление» (Москва, 2014), «Случайная геометрия и физика» (Москва, 2014), «Квантовые эффекты в биологических системах» (Сингапур, 2014; Иерусалим, Израиль, 2017; Вильнюс, Литва, 2018), «Международная конференция по математической теории управления и механике» (Суздаль, 2015), ICQT 2015 (международная конференция по квантовым технологиям, Москва, 2015), «Новые направления в математической и теоретической физике» (Москва, 2016), «Декабрьские чтения» (Новосибирск, 2017), «Квантовая информация, статистика, вероятность» (Москва, 2018), «Современная математическая физика. Владимиров-95» (Москва, 2018), «Бесконечномерный анализ и математическая физика» (Москва, 2019), «Математическая физика, динамические системы, бесконечномерный анализ» (Москва, 2019), ICQT 2019 (Москва, 2019). Часть результатов была прочитана на лекции в рамках Первой научно-образовательной школы по квантовым коммуникациям (Сочи, 2019).

**Публикации.** Основные результаты диссертации опубликованы в 15 печатных работах в рецензируемых научных изданиях, входящих в международные реферативные базы данных и системы цитирования Web of Science, Scopus, MathSciNet, zbMATH. В публикациях, в которых имеются соавторы, вклад автора данной диссертации определяющий.

**Личный вклад автора.** Все результаты, представленные в диссертационной работе и выносимые на защиту, получены её автором лично.

## ОСНОВНОЕ СОДЕРЖАНИЕ

Диссертация состоит из введения, шести глав, заключения, списка публикаций автора и списка литературы. Объём диссертации составляет 306 страниц.

**Введение** представляет собой расширенную версию представленной выше общей характеристики работы.

**Глава 1** посвящена исследованию необратимой динамики открытых квантовых систем, подчиняющихся уравнению ГКСЛ. В разделе 1.1 этой главы вводятся основные определения и обозначения для всей работы. Мы используем обозначения Дирака: $|\psi\rangle$ — элементы гильбертова пространства, $\langle\psi|$ — соответствующие элементы двойственного пространства (линейные функционалы), $\langle\,\cdot\,|\,\cdot\,\rangle$ — скалярное произведение.

В разделе 1.2 вводится функционал производства энтропии для уравнения ГКСЛ и доказывается его неотрицательность. Рассмотрим уравнение ГКСЛ в пространстве $\mathbb{C}^n$ для состояния $\rho(t)$ (положительного оператора в $\mathbb{C}^n$ со следом единица, также называемого оператором плотности), зависящего от времени $t$:

$$\dot\rho(t) = -i[H,\rho(t)] + \sum_{k=1}^{K}\left(L_k\rho(t)L_k^\dagger - \frac{1}{2}\{L_k^\dagger L_k,\rho(t)\}\right) \equiv \mathcal{L}(\rho(t)),$$

где $H$ и $L_k$ — линейные операторы в $\mathbb{C}^n$, причём оператор $H$ — самосопряжённый (называется оператором Гамильтона или гамильтонианом), $[A,B] = AB - BA$, $\{A,B\} = AB + BA$, $K$ — некоторое натуральное число. Точкой над буквой в этой работе будет обозначаться производная по времени.

Будем предполагать, что существуют такие вещественные числа $\Delta s_k$, $k = 1,\ldots,K$, и отображение $k \mapsto \tilde k$, являющееся инволюцией (т.е. для которого выполнено $\tilde{\tilde k} = k$), для которых выполнены равенства:

$$\Delta s_{\tilde k} = -\Delta s_k, \quad L_{\tilde k} = L_k^\dagger e^{-\Delta s_k/2}. \tag{1}$$

Определим функционал (функционал производства энтропии):

$$\Pi(\rho) = -\operatorname{Tr}\mathcal{L}(\rho)\ln\rho + \sum_{k=1}^{K}\operatorname{Tr}(L_k^\dagger L_k\rho)\Delta s_k. \tag{2}$$

Первое слагаемое здесь соответствует приращению энтропии системы, второе — потоку энтропии из системы в резервуар. Примем соглашение, что операция взятия следа Tr действует на всё, что записано справа от неё.

**Теорема 1.** *При выполнении условий (1) функционал (2) неотрицателен.*

Отдельные слагаемые в (2) могут быть отрицательными. В разделе 1.3 рассматривается разбиение производства энтропии на два слагаемых (адиабатический и неадиабатический вклады), которые при некоторых условиях неотрицательны по отдельности, доказывается несколько теорем об этом. В разделе 1.4 приводятся примеры функционалов производства энтропии для системы, взаимодействующей с резервуаром в режиме слабой связи и в режиме повторяющихся взаимодействий.

Функционал производства энтропии можно использовать для нахождения стационарных решений уравнения ГКСЛ. Этому посвящён раздел 1.5, где доказывается следующая

**Теорема 2.** *Пусть*
*а) выполнено условие (1),*
*б) операторы $L_k$ и $H$ в уравнении ГКСЛ таковы, что из равенства $L_k\rho = \rho L_k e^{-\Delta s_k}$ для всех $k$ следует $[H,\rho]=0$,*
*в) адиабатический вклад в производство энтропии равен нулю, то есть функционал $\Pi$ можно представить в виде*

$$\Pi(\rho) = -\frac{d}{dt} D\left(e^{t\mathcal{L}}\rho \| \rho^{\mathrm{st}}\right)\Big|_{t=0} = -\operatorname{Tr}\mathcal{L}(\rho)[\ln\rho - \ln\rho^{\mathrm{st}}], \tag{3}$$

*где $\rho^{\mathrm{st}}$ — некоторое стационарное решение уравнения ГКСЛ. Тогда оператор плотности $\rho$ — стационарное решение (необязательно совпадающее с $\rho^{\mathrm{st}}$) тогда и только тогда, когда он удовлетворяет уравнениям $L_k\rho = \rho L_k e^{-\Delta s_k}$ для всех $k$.*

Здесь $D(\rho\|\sigma) = \operatorname{Tr}\rho\ln\rho - \operatorname{Tr}\rho\ln\sigma$ — квантовая относительная энтропия.

Далее в разделе 1.5 приводятся примеры применения теоремы 2 для нахождения стационарных решений. Приведём здесь один из них. Рассмотрим следующее уравнение ГКСЛ в пространстве $\mathbb{C}^4$:

$$\dot\rho(t) = -i[H,\rho(t)] + \sum_{R=A,B}\sum_{f=a,b}\gamma_{Rf}\mathcal{D}_{Rf}(\rho(t)), \tag{4}$$

$$\mathcal{D}_{Rf}(\rho) = L_{Rf}\rho L_{Rf}^\dagger - \frac{1}{2}\{L_{Rf}^\dagger L_{Rf},\rho\} + e^{-\beta_R\omega_f}\left(L_{Rf}^\dagger\rho L_{Rf} - \frac{1}{2}\{L_{Rf}L_{Rf}^\dagger,\rho\}\right),$$

$$L_{Aa} = \cos\alpha(|e_{01}\rangle\langle e_{11}| + |e_{00}\rangle\langle e_{10}|), \quad L_{Ab} = \sin\alpha(|e_{10}\rangle\langle e_{11}| - |e_{00}\rangle\langle e_{01}|),$$
$$L_{Bb} = \cos\alpha(|e_{10}\rangle\langle e_{11}| + |e_{00}\rangle\langle e_{01}|), \quad L_{Ba} = \sin\alpha(-|e_{01}\rangle\langle e_{11}| + |e_{00}\rangle\langle e_{10}|),$$

$\gamma_{Rf},\omega_f,\beta_A,\beta_B>0$, $\alpha\in(0,2\pi)$, $H$ диагонален в базисе $\{|e_{00}\rangle, |e_{01}\rangle, |e_{10}\rangle, |e_{11}\rangle\}$ (некоторый ортонормированный базис).

Уравнение (4) возникает в квантовой термодинамике как модель пары двухуровневых систем, взаимодействующих друг с другом и с резервуарами при разных температурах ($\beta_A$ и $\beta_B$ — обратные температуры). Аналитический вид (единственного) стационарного решения этого уравнения не был известен, поскольку попытка решения соответствующей системы линейных уравнений «в лоб» приводит к очень громоздким выражениям. При помощи теоремы 2 удаётся получить искомое стационарное решение:

$$\rho^{\mathrm{st}} = Z^{-1}(P_{00} + \pi_b P_{01} + \pi_a P_{10} + \pi_a\pi_b P_{11}),$$

где $P_{xy}$ — проектор на $|e_{xy}\rangle$, $Z = (1+\pi_a)(1+\pi_b)$,

$$\pi_a = \frac{\gamma_{Aa} e^{-\beta_A \omega_a} \cos^2\alpha + \gamma_{Ba} e^{-\beta_B \omega_a} \sin^2\alpha}{\gamma_{Aa} \cos^2\alpha + \gamma_{Ba} \sin^2\alpha},$$

$\pi_b$ определяется по той же формуле с точностью до замены индексов $A$ на $B$, $a$ на $b$ и наоборот. Представляет интерес величина потока энергии из резервуара $A$ в резервуар $B$ в стационарном состоянии:

$$J^{\mathrm{st}}_{A\to B} = \frac{\gamma_{Aa}\omega_a}{1+\pi_a}(e^{-\beta_A\omega_a} - \pi_a^{-1})\cos^2\alpha + \frac{\gamma_{Ab}\omega_b}{1+\pi_b}(e^{-\beta_A\omega_b} - \pi_b^{-1})\sin^2\alpha.$$

Знак $J^{\mathrm{st}}_{A\to B}$ совпадает со знаком $\Delta\beta = \beta_B - \beta_A$, что находится в согласии со вторым началом термодинамики: тепло течёт из горячего резервуара в холодный.

В **главе 2** строится полное семейство квазиклассических мер, соответствующих эволюции квантовых когерентных состояний на торе на всех масштабах времени (классическое движение, расплывание пространственной плотности вероятности, дробные и полные возрождения исходного состояния). В связи с исследованиями по теории слабого предела показано, как при усреднении по времени возникает равновесное (а именно, равномерное) пространственное распределение.

Свободная квантовая эволюция на плоском торе $\mathbb{T}^d = \mathbb{R}^d/(2\pi\mathbb{Z}^d)$ задаётся гамильтонианом (самосопряжённым оператором) $H = -\hbar^2\Delta$ с областью определения $W_2^2(\mathbb{T}^d)$ (пространство Соболева). Здесь $\Delta$ — оператор Лапласа, $\hbar > 0$ — постоянная Планка (в данной главе — не столько физическая константа, сколько формальный математический параметр).

В этой главе под состоянием понимается чистое состояние, т.е. вектор из $L^2(\mathbb{T}^d)$. Если $\psi(x)$ — функция из $L^2(\mathbb{T}^d)$, то мы будем писать как $\psi$, так и $|\psi\rangle$. Рассмотрим гладкую быстро убывающую функцию $\varphi(x)$, $x \in \mathbb{R}^d$, с единичной $L^2(\mathbb{R}^d)$-нормой и семейство функций из $L^2(\mathbb{R}^d)$ вида

$$\eta^{(\hbar)}_{qp}(x) = \frac{1}{\sqrt{\alpha^d_\hbar}}\varphi\left(\frac{x-q}{\alpha_\hbar}\right)\exp\left\{\frac{ip(x-q)}{\hbar}\right\},$$

где $(q,p) \in \mathbb{R}^{2d}$ и $\alpha_\hbar > 0$ — такая константа, зависящая от $\hbar$, что $\alpha_\hbar \to 0$ и $\hbar/\alpha_\hbar \to 0$ при $\hbar \to 0$ (например, $\alpha_\hbar = \sqrt{\hbar}$), и соответствующее когерентное состояние (или волновой пакет) на торе:

$$\upsilon^{(\hbar)}_{qp}(x) = \sum_{n\in\mathbb{Z}^d} \eta^{(\hbar)}_{qp}(x - 2\pi n),$$

где $(q,p) \in \Omega$. Функции на торе отождествляются с периодическими функциями в $\mathbb{R}^d$. Операторы $|\upsilon^{(\hbar)}_{qp}\rangle\langle\upsilon^{(\hbar)}_{qp}|$ образуют непрерывное операторное разложение единицы.

Рассмотрим проэволюционировавший во времени волновой пакет $\upsilon^{(\hbar)}_{q_0p_0,t} = e^{i\hbar t\Delta}\upsilon^{(\hbar)}_{q_0p_0}$ и соответствующее распределение Хусими

$$H_{q_0,p_0,t}(q,p) = \frac{1}{(2\pi\hbar)^d}|\langle \upsilon_{qp}|\upsilon_{q_0p_0,t}\rangle|^2.$$

Мы будем рассматривать непрерывную, зависимую от $\hbar$ функцию $t_\hbar$ с различными вариантами асимптотического поведения. Сформулируем здесь общее почти для всех вариантов условие, на которое часто будем ссылаться:

$$\hbar(t_\hbar - AT_\hbar) \to 0, \quad \frac{\hbar}{\alpha_\hbar}(t_\hbar - AT_\hbar) \to B \tag{5}$$

для некоторых $A \in \mathbb{R}$ и $B \in [-\infty, +\infty]$. Здесь $T_\hbar = 2\pi/\hbar$.

**Теорема 3.** *1. Пусть $t_\hbar$ удовлетворяет одному из следующих условий: а) (5) с иррациональным $A$ и произвольным $B$, б) (5) с $B = \infty$ и произвольным $A$ или в) $\hbar t_\hbar \to +\infty$. Тогда*

$$\lim_{\hbar\to 0} H_{q_0,p_0,t_\hbar}(q,p) = \frac{1}{(2\pi)^d}\,\delta(p-p_0).$$

*2. Пусть $t_\hbar$ удовлетворяет (5) с $|B| < \infty$ и рациональным $A$, которое выражается в виде несократимой дроби как $A = \frac{M}{N}$ (если $A = 0$, то полагаем по определению $M = 0$ и $N = 1$). Тогда*

$$\lim_{\hbar\to 0}\Big\{H_{q_0,p_0,t_\hbar}(q,p) - \frac{1}{N'}\sum_{k\in[N']^d}\delta_B\left(q - q_0 - 2p_0(t_\hbar - AT_\hbar) - \Delta q_0 + \frac{2\pi k}{N'}\right)\delta(p-p_0)\Big\} = 0.$$

*Здесь* $\delta_B(q) = \dfrac{1}{(2\pi)^d}\sum_{j\in\mathbb{Z}^d}\sigma_{Bj}e^{ijq}$, $\sigma_R = \displaystyle\int_{\mathbb{R}^d}\varphi(x)\overline{\varphi(x-2R)}\,dx$,

$$N' = \begin{cases} N & \textit{для чётных } N,\\ \frac{N}{2} & \textit{для нечётных } N,\end{cases} \qquad \Delta q_0 = \begin{cases} \frac{2\pi}{N}I, & N \equiv 2 \pmod 4,\\ 0, & \textit{в противном случае},\end{cases}$$

$I = (1,1,\dots,1) \in \mathbb{Z}^d$, $[N'] = \{0,1,2,\dots,N'-1\}$.

Квазиклассическими мерами для семейства $\{\psi_\hbar\}$ ограниченных функций из $L^2(\mathbb{T}^d)$ называются меры Радона $\mu$, которые могут быть получены как пределы распределений Хусими $H_{\psi_\hbar}(q,p) = (2\pi\hbar)^{-d}|\langle \upsilon_{qp}|\psi_{\psi_\hbar}\rangle|^2$:

$$\lim_{n\to\infty}\int_\Omega H_{\psi_{\hbar_n}}(q,p)a(q,p)\,dqdp = \int_\Omega a(q,p)\mu(dqdp) \tag{6}$$

для некоторой бесконечно малой последовательности $\{\hbar_n\}$ и для всех функций $a \in C_0^\infty(\Omega)$ (бесконечно дифференцируемых функций с компактным носителем). В разделе 2.5.1 доказывается эквивалентность определений квазиклассических мер через распределение Вигнера и через распределение Хусими для случая тора. Как простое следствие теоремы 3 (в диссертации — теоремы 2.1) в теореме 2.2 диссертации перечисляются все квазиклассические меры, соответствующие семейству $\upsilon^{(\hbar)}_{q_0p_0,t}$. В теореме 2.3 рассматриваются пределы выражений типа (6) с дополнительным интегрированием с пробной функцией времени. Такие предельные меры также называются квазиклассическими. Приведём эту теорему здесь.

**Теорема 4.** *Рассмотрим функцию $t_\hbar = \lambda_\hbar t$, где $\lambda_\hbar \to \infty$ при $\hbar \to 0$.*

*1. Если $\hbar\lambda_\hbar/\alpha_\hbar \to \infty$ при $\hbar \to 0$, то для всех функций $a \in C_0^\infty(\Omega)$ и $b \in L^1(\mathbb{R})$ существует предел*

$$\lim_{\hbar\to 0} \int\limits_{\Omega\times\mathbb{R}} a(q,p)b(t)H_{q_0,p_0,\lambda_\hbar t}(q,p)\,dqdpdt = \langle a\rangle(p_0) \int\limits_{\mathbb{R}} b(t)\,dt, \tag{7}$$

*где* $\quad \langle a\rangle(p_0) = \dfrac{1}{(2\pi)^d} \displaystyle\int\limits_{\mathbb{T}^d} a(q,p_0)\,dq.$

*2. Если $\hbar\lambda_\hbar/\alpha_\hbar \to B \in [0,+\infty)$, то для всех функций $a \in C_0^\infty(\Omega)$ и $b \in L^1(\mathbb{R})$, существует предел*

$$\lim_{\hbar\to 0} \int\limits_{\Omega\times\mathbb{R}} a(q,p)b(t)H_{q_0,p_0,\lambda_\hbar t}(q,p)\,dqdpdt = \lim_{T\to\infty} \frac{1}{T} \int\limits_0^T a^{(b,B)}(q+p_0t,p_0)\,dt, \tag{8}$$

*где* $\quad a^{(b,B)}(q,p) = \dfrac{1}{(2\pi)^{\frac{d}{2}}} \displaystyle\sum_{j\in\mathbb{Z}^d} a_j(p) \left[\int\limits_{\mathbb{R}^d} dx \int\limits_{-\infty}^{+\infty} b(t)\varphi(x)\overline{\varphi(x-2Btj)}\,dt\right] e^{ijq}.$

*В частности, если $B = 0$, то*

$$\lim_{\hbar\to 0} \int\limits_{\Omega\times\mathbb{R}} a(q,p)b(t)H_{q_0,p_0,\lambda_\hbar t}(q,p)\,dqdpdt = \lim_{T\to\infty} \frac{1}{T} \int\limits_0^T a(q+p_0t,p_0)dt \int\limits_{-\infty}^{+\infty} b(t)dt. \tag{9}$$

*Если $p_0$ не принадлежит «резонансному» множеству*

$$R = \{p \in \mathbb{R}^d \mid jp = 0 \text{ для некоторых } j \in \mathbb{Z}^d\backslash\{0\}\},$$

*то пределы (8) и (9) сводятся к (7).*

Раздел 2.3 посвящён обсуждению результатов главы. В частности, теорема 4 говорит о выравнивании пространственной плотности при дополнительном сглаживании по времени. В этом смысле их можно уподобить теоремам Козлова о диффузии в теории слабого предела.

**Глава 3** посвящена оптимальному приближению к квантовому эффекту Зенона в модели Ландау–Зинера. Представим зависящий от времени вектор из $\mathbb{C}^2$ в виде $|\psi(t)\rangle = a(t)\,|0\rangle + b(t)\,|1\rangle$, где $\{|0\rangle, |1\rangle\}$ — ортонормированный базис. Динамика двухуровневой системы в модели Ландау–Зинера задаётся системой уравнений

$$i\dot{a} = -\frac{t}{2}\,a + \sqrt{\gamma}\,b, \quad i\dot{b} = \sqrt{\gamma}\,a + \frac{t}{2}\,b,$$

где $\gamma > 0$. Эта система уравнений задаёт унитарную эволюцию $U(t, t_0)\,|\psi(t_0)\rangle = |\psi(t)\rangle$. Обозначим $u_{jk}(t, t_0)$, $j, k = 0, 1$, матричные элементы $U$ в базисе $\{|0\rangle, |1\rangle\}$. Они явно выражаются через функции параболического цилиндра. Неселективное измерение в базисе $\{|0\rangle, |1\rangle\}$ соответствует квантовому динамическому отображению

$$\rho \mapsto |0\rangle\langle 0|\rho|0\rangle\langle 0| + |1\rangle\langle 1|\rho|1\rangle\langle 1| \equiv \mathcal{P}\rho,$$

действующему на состояние (оператор плотности) $\rho$. Рассмотрим начальное состояние $\rho(-\infty) = |0\rangle\langle 0|$ и будем интересоваться вероятностью в момент времени $+\infty$ остаться в состоянии $|0\rangle\langle 0|$. Если проводится $N$ измерений в моменты времени $t_1 \leqslant t_2 \leqslant \ldots \leqslant t_N$, то искомая вероятность равна

$$\begin{aligned}\langle 0|\rho(+\infty)|0\rangle &= \mathrm{Tr}[|0\rangle\langle 0|\,\mathcal{U}(+\infty, t_N)\mathcal{P}\ldots\mathcal{P}\mathcal{U}(t_2, t_1)\mathcal{P}\mathcal{U}(t_1, -\infty)\rho(-\infty)] = \\ &= \sum_{j_1,\ldots,j_N\in\{0,1\}}\prod_{k=0}^{N}|u_{j_{k+1},j_k}(t_{k+1}, t_k)|^2, \qquad (10)\end{aligned}$$

где $\mathcal{U}(t, t_0)\rho = U(t, t_0)\rho\,U(t, t_0)^\dagger$, $t_0 = -\infty$, $t_{N+1} = +\infty$, $j_0 = j_{N+1} = 0$.

Рассмотрим задачу выбора моментов $t_1, \ldots, t_N$, максимизирующих эту вероятность. В пределе $N \to \infty$ можно выбрать моменты измерения таким образом, что $\langle 0|\rho(+\infty)|0\rangle \to 1$, что соответствует квантовому эффекту Зенона: если над системой проводить бесконечно частые измерения, то она «замораживается» в своём начальном состоянии. Таким образом, поставленную задачу можно рассматривать как оптимальное приближение к квантовому эффекту Зенона при конечном числе измерений. Отметим также, что при отсутствии измерений, т.е. при $N = 0$, искомая вероятность равна $e^{-2\pi\gamma}$ — знаменитая формула Ландау–Зинера.

Матричные элементы $u_{jk}(t, t_0)$ быстро осциллируют, поэтому целевая функция (10) имеет множество локальных экстремумов. По этой причине попытки

решить задачу глобальной оптимизации (т.е. поиска глобального, а не локального максимума) в представленном виде известными методами оптимизации, такими как случайный поиск, имитация отжига, эволюционные алгоритмы и другие, не приводят к успеху. Воспользуемся хорошо известным методом динамического программирования. Он заключается в том, что сложная задача оптимизации сводится к последовательности более простых.

**Теорема 5.** *Максимальное значение целевой функции (10) можно представить в виде* $\langle 0|\rho(+\infty)|0\rangle = f_N^0(-\infty)$, *где функции* $f_n^j(t)$, $n \geqslant 0$, $j = 0, 1$, *удовлетворяют следующей системе рекуррентных соотношений (задач оптимизации):*

$$f_n^j(t) = \max_{t'>t}\{|u_{0j}(t',t)|^2 f_{n-1}^0(t') + |u_{1j}(t',t)|^2 f_{n-1}^1(t')\}, \quad n \geqslant 1,$$
$$f_0^j(t) = |u_{0j}(+\infty, t)|^2.$$

Алгоритм, основанный на этой теореме, позволяет численно решить задачу максимизации величины (10). Для предельного случая малых $\gamma$ удаётся разработать вычислительно более простой алгоритм, также на основе метода динамического программирования — теорема 3.2 в диссертации.

Предел больших $\gamma$ (адиабатический предел), при котором в отсутствие измерений искомая вероятность стремится к нулю, удаётся разобрать аналитически. А именно, элементы унитарной матрицы можно в этом случае приближённо представить в виде

$$|u_{jl}(2\sqrt{\gamma}\,t, 2\sqrt{\gamma}\,t_0)|^2 = \frac{1 \pm \tau(t)\tau(t_0)}{2} + \frac{1}{2}\sqrt{[1-\tau(t_0)^2][1-\tau(t)^2]}\cos(\gamma\Delta\omega_{t,t_0}), \tag{11}$$

где знаки «плюс» и «минус» в $\pm$ соответствуют $l = j$ и $l = 1 - j$,

$$\tau(t) = \frac{t}{\sqrt{1+t^2}}, \quad \Delta\omega_{t,t_0} = \omega(t) - \omega(t_0),$$
$$\omega(t) = \operatorname{sgn}(t)\ln(|t| + \sqrt{1+t^2}) + t\sqrt{1+t^2}.$$

**Теорема 6.** *Если в качестве элементов унитарной матрицы в задаче максимизации величины (10) взять приближённую формулу (11), то максимальное значение целевой функции в пределе* $\gamma \to \infty$ *составит*

$$\langle 0|\rho(+\infty)|0\rangle = \frac{1}{2}\left\{1 + \left(\cos\frac{\pi}{N+1}\right)^{N+1}\right\}. \tag{12}$$

*Решение, доставляющее это значение (вообще говоря, не единственное), имеет вид*

$$t_k = -2\sqrt{\gamma}\operatorname{ctg}\left(\frac{\pi k}{N+1}\right) + O\left(\frac{2\pi}{\sqrt{\gamma}\omega'(t_k)}\right), \tag{13}$$

*где* $k = 1, \ldots, N$, $\omega'(t)$ — *производная от* $\omega(t)$.

Таким образом, аналитически можно найти максимальное значение целевой функции и приблизительные значения оптимальных моментов измерений. Точные значения можно найти численно с помощью любого алгоритма поиска локального максимума с начальной точкой $(t_1, \ldots, t_N)$, заданной формулой (13). Разработанный на основе теоремы 6 алгоритм также предусматривает корректировку малых $t_i$ в найденном решении, когда приближённые формулы (11), строго говоря, перестают работать. Предел при $N \to \infty$ правой части (12) даёт единицу, что соответствует квантовому эффекту Зенона.

Решение (12)–(13) можно осуществить на практике, только если длительность реального измерения не превышает $2\pi/\sqrt{\gamma}\omega'(t_k)$ (мгновенное измерение — это математическая идеализация). В противном случае из-за быстрых осцилляций целевой функции погрешность в моменте измерения может привести к значению целевой функции, далёкому от оптимального. В разделе 3.6.3 рассматривается задача на максимин, при которой предполагается, что в пределах погрешности реализуется наихудший возможный момент. В этом случае показывается (теорема 3.4), что оптимально провести одно измерение в момент времени 0, что даёт значение искомой вероятности 1/2 (вместо нулевой вероятности при отсутствии измерений в пределе $\gamma \to \infty$).

**Глава 4** посвящена строгому доказательству существования микроскопических решений у уравнения Больцмана–Энскога, найденных Н.Н. Боголюбовым на физическом уровне строгости. Уравнение Больцмана–Энскога, описывающее кинетику газа из твёрдых шаров диаметра $a$, имеет вид

$$\frac{\partial f}{\partial t} = -v_1 \frac{\partial f}{\partial r_1} + Q(f, f), \tag{14}$$

$$Q(f,f)(r_1, v_1, t) = na^2 \int\limits_{\Omega_{v_1}} (v_{21}, \omega)[f(r_1, v_1', t) f(r_1 + a\omega, v_2', t) - \\ - f(r_1, v_1, t) f(r_1 - a\omega, v_2, t)] d\omega dv_2.$$

Здесь $f = f(r_1, v_1, t) \geqslant 0$ — функция плотности распределения шаров в фазовой точке $(r_1, v_1)$, где $r_1 \in \mathbb{T}^3 = \mathbb{R}^3/(\alpha\mathbb{Z} \times \beta\mathbb{Z} \times \gamma\mathbb{Z})$ — пространственные координаты шара (т.е. координаты его центра), $v_1 \in \mathbb{R}^3$ — скорость шара, $\alpha, \beta, \gamma > a$, $\frac{\partial}{\partial r_1}$ — градиент по переменной $r_1$. К динамике твёрдых шаров на торе может быть сведена динамика в прямоугольном параллелепипеде с упругим отражением от стенок. Если $f$ нормирована на объём $V$ ёмкости, в которую заключён газ (в нашем случае $V = \alpha\beta\gamma$), то $n = \frac{N}{V}$ — концентрация шаров. Такую нормировку и будем предполагать в дальнейшем. Далее,

$$v_1' = v_1 + (v_{21}, \omega)\omega, \quad v_2' = v_2 - (v_{21}, \omega)\omega,$$

$v_{21} = v_2 - v_1$, $\omega \in S^2$ ($S^2$ — единичная сфера в $\mathbb{R}^3$), $(\cdot,\cdot)$ — скалярное произведение. $v_1$ и $v_2$ имеют смысл скоростей первого и второго шара до столкновения, $v_1'$ и $v_2'$ — после столкновения. $\omega$ имеет смысл единичного вектора, направленного из центра второго шара в центр первого шара. Выражение $Q(f,f)$ называется интегралом столкновений. Интегрирование в нём ведётся по области

$$\Omega_{v_1} = \{(\omega, v_2) : \omega \in S^2, v_2 \in \mathbb{R}^3, (v_{21}, \omega) \geqslant 0\} \subset S^2 \times \mathbb{R}^3.$$

Микроскопические решения, открытые Н.Н. Боголюбовым, имеют вид

$$f(r_1, v_1, t) = n^{-1} \sum_{i=1}^{N} \delta(r_1 - q_i(t), v_1 - w_i(t)), \tag{15}$$

где $\delta(r,v) \equiv \delta(r)\delta(v)$ — шестимерная дельта-функция, $q_i(t)$, $w_i(t)$ — координаты и скорости $N$ твёрдых шаров в момент $t$. Зависимость от времени определяется динамикой твёрдых шаров, т.е. микроскопической динамикой (в противоположность макроскопической динамике, задаваемой кинетическим уравнением). Непосредственная подстановка этих функций в интеграл столкновений приводит к формально некорректным произведениям дельта-функций. Строгий смысл удаётся придать, вводя регуляризацию дельта-функций и интеграла столкновений.

**Теорема 7.** *Рассмотрим семейство функций*

$$f_\varepsilon(r_1, v_1, t) = n^{-1} \sum_{i=1}^{N} \delta_\varepsilon(r_1 - q_i(t), v_1 - w_i(t))$$

*в предположении, что динамика твёрдых шаров $\{q_i(t), w_i(t)\}_{i=1}^N$ определена корректно. Здесь $\delta_\varepsilon \in L_0^\infty(\mathbb{T}^3 \times \mathbb{R}^3)$, $\varepsilon > 0$, — дельта-образное семейство ограниченных функций с компактным носителем, $\delta_\varepsilon \to \delta$ при $\varepsilon \to 0$ в пространстве обобщённых функций $C'(\mathbb{T}^3 \times \mathbb{R}^3)$ (т.е. в пространстве линейных непрерывных функционалов над пространством непрерывных функций $C(\mathbb{T}^3 \times \mathbb{R}^3)$). Также потребуем, чтобы диаметр носителя $\delta_\varepsilon$ стремился к нулю при $\varepsilon \to 0$. Тогда в $C'(\mathbb{T}^3 \times \mathbb{R}^3)$ для всех $t \in \mathbb{R}$ имеет место предел*

$$\lim_{\varrho \to +0} \lim_{\varepsilon \to +0} \int_0^t Q_\varrho(f_\varepsilon, f_\varepsilon)[r_1 - v_1(t-s), v_1, s]\, ds = f(r_1, v_1, t) - f(r_1 - v_1 t, v_1, 0),$$

*где*

$$Q_\varrho(f_\varepsilon, f_\varepsilon) = na^2 \int_{\Omega_{v_1}} (v_{21}, \omega)[f_\varepsilon(r_1, v_1', t) f_\varepsilon(r_1 + (a+\varrho)\omega, v_2', t) - \\ - f_\varepsilon(r_1, v_1, t) f_\varepsilon(r_1 - (a+\varrho)\omega, v_2, t)] d\omega dv_2.$$

За основу в этой теореме взято понятие «мягкого» (“mild”) решения уравнения Больцмана–Энскога:

$$f(r_1, v_1, t) = f(r_1 - v_1 t, v_1, 0) + \int_0^t Q(f, f)(r_1 - v_1(t-s), v_1, s)\, ds.$$

Также в разделе 4.5 этой главы рассматривается другой подход к приданию строгого смысла микроскопическим (и, более общо, мерозначным) решениям на основе представления решений в виде рядов по историям столкновений. Этот подход не требует регуляризации дельта-функций, но использует регуляризацию в определении членов ряда.

**Глава 5** посвящена выводу формул зависимости от времени внедиагональных элементов матрицы плотности в рамках двух теорий возмущений для динамики открытых квантовых систем: теории Фёрстера и модифицированной теории Редфилда. Вывод осуществляется при помощи метода проекционных операторов Цванцига.

Гамильтониан, описывающий процесс переноса энергии возбуждения в молекулярных системах, называемый гамильтонианом экситона Френкеля, имеет следующий вид:

$$H = H^{\mathrm{el}} + H^{\mathrm{Coul}} + H^{\mathrm{ph}} + H^{\text{el-ph}} + H^{\mathrm{reorg}},$$

$$H^{\mathrm{el}} = \sum_{n=1}^{N} |n\rangle\, \varepsilon_n^0\, \langle n|\,, \qquad H^{\mathrm{Coul}} = \sum_{n=1}^{N} \sum_{m>n}^{N} (J_{nm}\, |n\rangle\, \langle m| + \text{э.с.}),$$

$$H^{\mathrm{ph}} = \sum_{n=1}^{N} H_n^{\mathrm{ph}}, \qquad H_n^{\mathrm{ph}} = \int_{-\infty}^{+\infty} \omega_n(\xi) c_n^\dagger(\xi) c_n(\xi)\, d\xi,$$

$$H^{\text{el-ph}} = \sum_{n=1}^{N} |n\rangle\, u_n\, \langle n|\,, \qquad u_n = \int_{-\infty}^{+\infty} h_n(\xi)[c_n(\xi) + c_n^\dagger(\xi)]\, d\xi,$$

$$H^{\mathrm{reorg}} = \sum_{n=1}^{N} |n\rangle\, \lambda_n\, \langle n|\,, \qquad \lambda_n = \int_{-\infty}^{+\infty} \frac{h_n(\xi)^2}{\omega_n(\xi)}\, d\xi,$$

где «э.с.» означает эрмитово сопряжение. Здесь слагаемые $H^{\mathrm{el}}$ и $H^{\mathrm{Coul}}$ представляют электронные степени свободы молекул — открытую квантовую систему: $N$ есть число молекул, $|n\rangle$ соответствует возбуждённому состоянию $n$-й молекулы, тогда как остальные находятся в основном состоянии. Т.е. каждая молекула рассматривается как двухуровневая система, причём в каждый момент времени

ровно одна молекула находится в возбуждённом состоянии (разумеется, с точностью до суперпозиций). Таким образом, $H^{\mathrm{el}}$ и $H^{\mathrm{Coul}}$ действуют в пространстве $\mathbb{C}^N$, где векторы $|n\rangle$, $n = 1, \ldots, N$, образуют ортонормированный базис. Далее, $\varepsilon_n^0$ — энергия возбуждения $n$-й молекулы, $J_{nm}$ — дипольная кулоновская связь между $n$-й и $m$-й молекулами. Обычно эти величины вещественны, но мы будем предполагать, что они комплексные, причём $J_{mn} = J_{nm}^*$. Эти дипольные связи отвечают за перенос энергии возбуждения: $H^{\mathrm{Coul}}$ — единственное слагаемое, содержащее внедиагональные элементы в базисе локальных возбуждений $\{|n\rangle\}$.

Электронные степени свободы каждой молекулы взаимодействуют со своим собственным резервуаром, состоящим из континуума одномерных гармонических осцилляторов (индексируемых параметром $\xi$), которые отражают колебания ядер атомов вокруг своих положений равновесия, а также влияние окружения молекулярной системы. Гильбертово пространство каждого такого резервуара — бозонное фоковское пространство над $L^2(\mathbb{R})$, $\xi \in \mathbb{R}$. Далее, $c_n^\dagger(\xi)$ и $c_n(\xi)$ — операторы рождения и уничтожения кванта (фонона) в моде $\xi$ для резервуара $n$-й молекулы (операторнозначные обобщённые функции), удовлетворяющие бозонным каноническим коммутационным соотношениям. Наконец, $h_n(\xi)$ — непрерывные вещественные функции, стремящиеся к нулю при $|\xi| \to \infty$, $\omega_n(\xi)$ — гладкие положительные функции, производная которой нигде не обращается в нуль. Предполагаем, что интегралы, определяющие величины $\lambda_n$, сходятся.

Изложение в главе 5 — на «физическом» уровне строгости, поскольку теория Фёрстера и модифицированная теория Редфилда не выведены на математическом уровне строгости. В диссертации эта проблема также не находит решения, но в ней выводятся новые формулы в рамках этих теорий, а также приводятся некоторые соображения в направлении разработки строгой теории. Результаты этой главы подытожены в теореме 5.1. Для краткости изложим здесь результаты только для теории Фёрстера. Она соответствует теории возмущений по $H^{\mathrm{Coul}}$, т.е. малым дипольным связям между молекулами. Остальную часть гамильтониана обозначим $H_0$.

Введём проекционный оператор $\mathcal{P}$ на пространстве операторов, действующий на произвольный оператор $X$ следующим образом:

$$\mathcal{P}X = \sum_{n=1}^{N} \mathrm{Tr}_R(X_{nn})\, |n\rangle \langle n| \otimes \rho_n, \quad X_{nn} = \langle n|X|n\rangle\,, \tag{16}$$

где $\mathrm{Tr}_R$ — частичный след по пространству резервуаров. Также обозначим $\mathcal{Q} = \mathrm{Id} - \mathcal{P}$ ($\mathrm{Id}$ — тождественный оператор). Рассмотрим начальное состояние

$$\rho(0) = \sigma(0) \otimes \rho_g, \tag{17}$$

где $\rho_g = e^{-\beta H^{\mathrm{ph}}}/\mathrm{Tr}\, e^{-\beta H^{\mathrm{ph}}}$, $\beta > 0$ — обратная температура резервуара. Строго

говоря, след оператора $e^{-\beta H^{\rm ph}}$ не имеет определённого значения. Однако этот след и оператор плотности $\rho_g$ корректно определены, если интеграл по $\xi$ в $H^{\rm ph}$ и в выражениях для $u_n$ и $\lambda_n$ заменить на сумму по конечному количеству значений $\xi$. Будем понимать состояние $\rho_g$ в предельном смысле: если $B$ — оператор в пространстве резервуара, то выражение $\mathrm{Tr}\, B\rho_g$ следует понимать как предел выражений с конечным числом колебательных мод $\xi$ при этом числе, стремящемся к бесконечности. Говоря иначе, состояние $\rho_g$ — не оператор плотности (если количество гармонических осцилляторов — континуум), а линейный функционал, действующий на $C^*$-алгебре классических коммутационных соотношений.

Обозначим $p_n(t) = \langle n|(\mathrm{Tr}_R\, e^{-iHt}\rho(0)e^{iHt})|n\rangle$. Во втором порядке теории возмущений $p_n(t)$ удовлетворяют кинетическому уравнению

$$\dot p_n(t) = \sum_{m\neq n}\big(K_{nm}p_m(t) - K_{mn}p_n(t) - 2\,\mathrm{Im}\{\sigma_{nm}(0)J_{mn}A_n(t)A_m^*(t)\}\big), \qquad (18)$$

где

$$K_{nm} = 2|J_{nm}|^2\,\mathrm{Re}\int\limits_0^\infty d\tau\, F_m^*(\tau)A_n(\tau)$$

— коэффициенты переноса,

$$F_m(\tau) = \exp\{-i(\varepsilon_m^0 - \lambda_m)\tau - g_m^*(\tau)\}, \quad A_n(\tau) = \exp\{-i(\varepsilon_n^0 + \lambda_n)\tau - g_n(\tau)\}$$

— функции, преобразования Фурье которых — спектры испускания и поглощения соответствующих молекул (т.е. экспериментально доступные функции), $g_n(t) = \int\limits_0^t d\tau_1 \int\limits_0^{\tau_1} d\tau_2\, C_n(\tau_2)$ — функция спектральной линии, $C_n(t) = \mathrm{Tr}[u_n(t)u_n\rho_g]$ — корреляционная функция $n$-го резервуара, $u_n(t) = e^{-iH_0t}u_ne^{iH_0t}$. Отметим, что получение последнего слагаемого в (18), которое учитывает начальные когерентности (внедиагональные элементы) $\sigma_{nm}(0) = \langle n|\sigma(0)|m\rangle$, и аналогичного слагаемого для модифицированной теории Редфилда также является результатом этой главы.

Считалось, что, поскольку проекционный оператор $\mathcal{P}$ уничтожает информацию о когерентностях, в рамках теории Фёрстера можно вычислить только динамику населённостей (диагональных элементов матрицы плотности системы) по уравнению (18) без последнего слагаемого. Результат главы 5 состоит в том, что можно вычислить и динамику внедиагональных элементов.

В первом порядке теории возмущений по $H^{\rm Coul}$ в представлении взаимодействия относительно $H_0$ справедлива формула

$$\mathcal{Q}\rho(t) = \mathcal{Q}\rho(0) - i\int\limits_0^t d\tau\mathcal{L}(\tau)\mathcal{P}\rho(\tau) - i\int\limits_0^t d\tau\mathcal{Q}\mathcal{L}(\tau)\mathcal{Q}\rho(0), \qquad (19)$$

где $\mathcal{L}(t) = [H^{\mathrm{Coul}}(t), \cdot]$, $H^{\mathrm{Coul}}(t) = e^{iH_0 t} H^{\mathrm{Coul}} e^{-iH_0 t}$. Определим $A = |n\rangle\langle m|$, $A(t) = e^{iH_0 t} A e^{-iH_0 t}$. Нас интересует величина

$$\sigma_{mn}(t) = \operatorname{Tr} A(t)\mathcal{P}\rho(t) + \operatorname{Tr} A(t)\mathcal{Q}\rho(t). \tag{20}$$

**Теорема 8.** *Пусть в правой части (20) $\mathcal{P}\rho(t)$, $t \geqslant 0$, определяется формулой (16) и кинетическим уравнением (18), а $\mathcal{Q}\rho(t)$ — формулой (19) и начальным состоянием (17). Тогда для $\sigma_{mn}(t)$ справедлива формула*

$$\sigma_{mn}(t) = \sigma_{mn}^{\mathrm{eq}}(t) + \sigma_{mn}^{\mathrm{noneq}}(t) + \sigma_{mn}^{\mathrm{init}}(t), \tag{21}$$

$$\sigma_{mn}^{\mathrm{neq}}(t) = ip_m(t)J_{mn}\int_0^t d\tau\, A_n^*(\tau)F_m(\tau) - ip_n(t)J_{mn}\int_0^t d\tau\, F_n^*(\tau)A_m(\tau),$$

$$\sigma_{mn}^{\mathrm{noneq}}(t) = ip_m(0)J_{mn}\int_0^t d\tau\, A_n^*(\tau)[F_m(\tau,t) - F_m(\tau)] -$$

$$- ip_n(0)J_{mn}\int_0^t d\tau\, [F_n(\tau,t) - F_n(\tau)]^* A_m(\tau),$$

$$\sigma_{mn}^{\mathrm{init}}(t) = \sigma_{mn}(0)A_n^*(t)A_m(t) + i\sum_{l\neq n,m}\int_0^t d\tau\, \{\sigma_{ml}(0)J_{ln}A_n^*(\tau)A_m(t)A_l^*(t-\tau) -$$

$$- \sigma_{ln}(0)J_{ml}A_n^*(t)A_m(\tau)A_l(t-\tau)\},$$

$$F_m(\tau,t) = \exp\{-i(\varepsilon_m^0 + \lambda_m)\tau - g_m^*(\tau) - 2i\operatorname{Im}[g_m(t) - g_m(t-\tau)]\}.$$

Модифицированная теория Редфилда соответствует теории возмущений по $H' = \sum_{k\neq k'} |k\rangle\langle k|H|k'\rangle\langle k'|$, где $|k\rangle$, $|k'\rangle$ — элементы базиса из собственных векторов оператора $H^{\mathrm{el}} + H^{\mathrm{Coul}} + H^{\mathrm{reorg}}$. Это приводит к более громоздким, но аналогичным формулам.

В **главе 6** доказывается стойкость протокола квантовой криптографии (квантового распределения ключей) BB84 в случае однофотонных детекторов с несовпадающими эффективностями. Сформулируем здесь основной математический результат этой главы.

Рассмотрим пространство $\mathbb{C}^2 \otimes \mathbb{C}^3$. Первому пространству (пространству отправителя) в этом тензорном произведении соответствует индекс $A$, второму (пространству получателя) — $B$; $I_A$ и $I_B$ — тождественные операторы в соответствующих пространствах. Базис первого пространства — $\{|0\rangle, |1\rangle\}$, базис второго — $\{|0\rangle, |1\rangle, |\mathrm{vac}\rangle\}$. Базисные векторы $|0\rangle$ и $|1\rangle$ могут соответствовать, например, двум перпендикулярным поляризациям фотона, $|\mathrm{vac}\rangle$ — вакуумному

состоянию (фотон может поглотиться в процессе передачи). Также введём состояния $|\pm\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Один детектор имеет эффективность единица, т.е. всегда срабатывает при прилёте фотона, второй — эффективность $\eta \in (0, 1]$, т.е. срабатывает с вероятностью $\eta$. Общий случай, когда эффективности обоих детекторов меньше единицы, может быть сведён к этому.

Рассмотрим задачу оптимизации

$$\min_{\rho_{AB}\in\mathbf{S}} D\big(\mathscr{G}(\rho_{AB})\|\mathscr{Z}(\mathscr{G}(\rho_{AB}))\big), \tag{22}$$

где $\mathbf{S}$ — множество положительных операторов на пространстве $\mathbb{C}^2 \otimes \mathbb{C}^3$, $D$ — определённая выше квантовая относительная энтропия с заменой натурального логарифма на двоичный (что не имеет значения для задачи оптимизации),

$$\mathscr{G}(\rho_{AB}) = G\rho_{AB}G, \qquad G = I_A \otimes \begin{pmatrix} 1 & 0 & 0 \\ 0 & \sqrt{\eta} & 0 \\ 0 & 0 & 0 \end{pmatrix} = I_A \otimes (|0\rangle\langle 0| + \sqrt{\eta}\,|1\rangle\langle 1|),$$

$$\mathscr{Z}(\rho_{AB}) = \sum_{a\in\{0,1\}} (|a\rangle_A\langle a| \otimes I_B)\,\rho_{AB}\,(|a\rangle_A\langle a| \otimes I_B),$$

и линейные ограничения

$$\mathrm{Tr}[(I_A \otimes |0\rangle_B\langle 0|)\rho_{AB}] = p_0, \tag{23}$$

$$\mathrm{Tr}[(I_A \otimes |1\rangle_B\langle 1|)\rho_{AB}] = p_1/\eta, \tag{24}$$

$$\mathrm{Tr}[(|+-\rangle\langle +-| + |-+\rangle\langle -+|)\rho_{AB}] = tQ_x, \tag{25}$$

где $t = p_0 + p_1/\eta$. Здесь $p_0$, $p_1$ и $Q_x$ — заданные величины, принадлежащие отрезку $[0, 1]$, причём $0 < p_0 + p_1 \leqslant 1$. Относительная энтропия в (22) характеризует нехватку информации противника, которую необходимо оценить снизу, линейные ограничения — наблюдаемую отправителем и получателем статистику регистраций фотонов. Оценка информации противника на основе наблюдаемой статистики — ключевая математическая задача в квантовой криптографии, выражающая её суть, которая заключается в том, что попытка подслушивания информации, закодированной в квантовые состояния, ведёт к изменению этих состояний и, следовательно, статистики наблюдений. Монотонное невозрастание квантовой относительной энтропии на решениях уравнения ГКСЛ (см. (3)) и минимизация квантовой относительной энтропии в квантовой криптографии объединяет эти две, казалось бы, несвязанные тематики.

**Теорема 9.** *Задача оптимизации (22) на множестве положительных операторов с линейными ограничениями (23)–(25) имеет допустимые решения (т.е. решения, удовлетворяющие ограничениям) тогда и только тогда, когда*

$$Q_x \geqslant \frac{1}{2} - \frac{1}{t}\sqrt{\frac{p_0 p_1}{\eta}}.$$

*В этом случае оптимальное значение целевой функции есть*

$$p_{\mathrm{det}}\left[h\left(\frac{1-\delta_z}{2}\right)-h\left(\frac{1-\sqrt{\delta_z^2+\delta_x^2}}{2}\right)\right],$$

*где* $h(x)=-x\log_2 x-(1-x)\log_2(1-x)$ *— двоичная энтропия,*

$$p_{\mathrm{det}}=p_0+p_1,\qquad \delta_z=\frac{p_0-p_1}{p_{\mathrm{det}}},\qquad \delta_x=\frac{(1-2Q_x)\sqrt{\eta}}{p_{\mathrm{det}}}.$$

Раздел 6.8 посвящён адаптации так называемого метода обманных состояний (состояний-ловушек, decoy-state method) к ситуации несовпадающих эффективностей детекторов. Этот метод обеспечивает обобщение теоремы 9 на случай, когда пространство отправителя — не $\mathbb{C}^2$, а бозонное пространство Фока над $\mathbb{C}^2$, и посылки отправителя с некоторой вероятностью содержат более одного фотона. Доказывается теорема 6.2 о сведении многофотонной ситуации к однофотонной.

В **заключении** перечислены основные результаты диссертации, т.е. положения, выносимые на защиту, и указаны дальнейшие перспективы разработки темы. **Список публикаций автора** содержит 15 публикаций автора, в которых опубликованы основные результаты диссертации. **Список литературы** содержит 328 наименований.

## СПИСОК ПУБЛИКАЦИЙ АВТОРА, В КОТОРЫХ ОПУБЛИКОВАНЫ ОСНОВНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИИ


1. Трушечкин А. С. Нахождение стационарных решений уравнения Линдблада посредством исследования функционала производства энтропии // Тр. МИАН. 2018. Т. 301. С. 276–286.
2. Trushechkin A. Semiclassical evolution of quantum wave packets on the torus beyond the Ehrenfest time in terms of Husimi distributions // J. Math. Phys. 2017. V. 58, N. 6. P. 062102.
3. Трушечкин А. С. Микроскопические решения кинетических уравнений и проблема необратимости // Тр. МИАН. 2014. Т. 285. С. 264–287.
4. Волович И. В., Трушечкин А. С. Асимптотические свойства квантовой динамики в ограниченных областях на различных масштабах времени // Изв. РАН. Сер. матем. 2012. Т. 76, № 1. С. 43–84.
5. Trushechkin A. S. Microscopic and soliton-like solutions of the Boltzmann–Enskog and generalized Enskog equations for elastic and inelastic hard spheres // Kinetic and Related Models. 2014. V. 7, N. 4. P. 755–778.

6. Bochkov M. K., Trushechkin A. S. Security of quantum key distribution with detection-efficiency mismatch in the single-photon case: Tight bounds // Phys. Rev. A. 2019. V. 99, N. 3. P. 032308.
7. Pechen A., Trushechkin A. Measurement-assisted Landau-Zener transitions // Phys. Rev. A. 2015. V. 91, N. 5. P. 052316.
8. Trushechkin A. S. Calculation of coherences in Förster and modified Redfield theories of excitation energy transfer // J. Chem. Phys. 2019. V. 151, N. 7. P. 074101.
9. Trushechkin A. S. Derivation of the particle dynamics from kinetic equations // p-Adic Numbers, Ultrametic Analysis and Applications. 2012. V. 4, N. 2. P. 130–142.
10. Trushechkin A. S. Derivation of the Boltzmann equation and entropy production in functional mechanics // p-Adic Numbers, Ultrametic Analysis and Applications. 2011. V. 3, N. 3. P. 225–235.
11. Trushechkin A. S., Volovich I. V. Perturbative treatment of inter-site couplings in the local description of open quantum networks // EPL. 2016. V. 113, N. 3. P. 30005.
12. Трушечкин А. С. Об общем определении производства энтропии в марковских открытых квантовых системах // Итоги науки и техн. Сер. Соврем. мат. и ее прил. 2017. Т. 138. С. 82–98.
13. Трушечкин А. С. О строгом определении микроскопических решений уравнения Больцмана–Энскога // Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки. 2013. № 1(30). С. 270–278.
14. Трушечкин А. С. Уравнение Больцмана и H-теорема в функциональной формулировке классической механики // Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки. 2011. № 1(22). С. 158–164.
15. Трушечкин А. С. Необратимость и роль измерительного прибора в функциональной формулировке классической механики // ТМФ. 2010. Т. 164, № 3. С. 435–440.

Автор считает своим приятным долгом выразить глубочайшую признательность и благодарность своему учителю, члену-корреспонденту РАН, доктору физико-математических наук Игорю Васильевичу Воловичу за постоянное внимание к работе и поддержку, а также всем сотрудникам отдела математической физики МИАН им. В. А. Стеклова и участникам спецсеминара «Квантовая математическая физика», действующего в рамках Научно-образовательного центра при МИАН, за внимание и полезные обсуждения.

Подписано в печать 21.11.2019 г.
Тираж 100 экз.

Отпечатано в (название, адрес типографии)