Московский государственный университет
им. М.В. Ломоносова
физический факультет
кафедра общей физики и волновых процессов

На правах рукописи

Сыч Денис Васильевич

Совместимая информация как инструмент анализа квантовых информационных каналов

Специальность 01.04.02 — теоретическая физика

Диссертация на соискание ученой степени
кандидата физико-математических наук

Научный руководитель
кандидат физико-математических наук,
доцент В.Н. Задков

Москва — 2005

Оглавление

Введение

Одним из наиболее значительных научных событий XX века в области физики стало, несомненно, создание квантовой теории. Основные ее положения настолько сильно отличаются от привычных представлений о мире, что вызывали не только споры у основоположников квантовой теории (достаточно вспомнить известную дискуссию Эйнштейн — Бор [1,2]), но и все новые и новые попытки интерпретации её оснований, продолжающиеся до сих пор [3]. Другим значительным научным событием XX века стало создание теории информации. Если квантовая теория явилась продуктом коллективного творчества целого ряда ученых, то основные положения теории информации были сформулированы в работе Шеннона [4].

На стыке квантовой теории и теории информации в последнее время начала активно развиваться *теория квантовой информации*, которая, возможно, станет одной из самых интересных областей науки XXI века. Ее предметом является создание, передача и обработка информации, с той особенностью, что носителями информации выступают не классические, а сугубо квантовые объекты, с присущей им квантовой спецификой.

Переход к квантовому характеру носителей информации первоначально стимулировался необходимостью учёта ограничений, накладываемых квантовым характером устройств преобразования информации, например, в задачах обработки электромагнитных сигналов. В грубой форме их учёт может быть выполнен и без использования явных математических обобщений соответствующих понятий классической теории, что является достаточным для многих практических приложений [5]. Тем не менее, необходимость таких обобщений является очевидной вследствие их важности для более глубокого понимания самой физики процессов в квантовых каналах, потребности в явном и математически экономном описании множества преобразований, физически возможных в квантовых системах, а также в установлении точных пределов качества функционирования квантовых информационных систем. Активные исследования в этом направлении были начаты в 60–70-х г.г. прошлого века.

Из наиболее ранних работ в этом направлении можно отметить исследования информационной пропускной способности квантовых информационных каналов, выполненные Гордоном, Лебедевым, Левитиным и Стратоновичем [5–10]. Начало исследований проблемы квантового обобщения классической теории оптимального обнаружения сигналов и оценивания параметров может быть связано с работами Хелстрома и других авторов в конце 60-х — начале 70-х годов (более детальный список соответствующих литературных ссылок содержится в монографии [11]).

Наиболее общей для данного круга задач является терминология, использующая вместо относительно более частного понятия оценки $\tilde{\lambda}$

неизвестного параметра (параметров) λ понятия оптимального решения, которое в теории принятия оптимальных решений [12] в общем случае описывается статистической (рандомизированной) решающей функцией — распределением вероятностей $\mu(d\tilde{\lambda})$ (в теории обнаружения и измерения оптимум достигается на нерандомизированных решениях, поэтому во многих случаях рассмотрение рандомизации не обязательно). В работах Гришанина [13, 14] было показано, что адекватным сокращённым математическим представлением квантовой процедуры принятия решения, иначе, обобщённого измерения, является его представление в форме неортогонального разложения $\hat{E}(d\tilde{\lambda}) \geq 0$ единичного оператора, удовлетворяющего условию нормировки $\int \hat{E}(d\tilde{\lambda}) = \hat{I}$. В настоящее время это разложение более известно под названием положительной операторной меры (ПОМ), или POVM (positive operator-valued measure). В работе Холево [15] была установлена — как было показано впоследствии, физически достижимая [16, 17] — верхняя граница для количества информации в квантовом канале с классическим входом, известная в настоящее время как *информация Холево*. Обобщённое изложение некоторых математических результатов исследований данного периода содержится в монографии Холево [18], а современное состояние — в монографии [19].

Можно сказать, что сегодня теория квантовой информации переживает свое второе рождение. Бурное развитие современных теоретических исследований в этой области во многом обусловлено возросшими возможностями экспериментальных методов в таких областях, как квантовая оптика, атомная физика, физика твердого тела. Если раньше роль экс-

периментатора ограничивалась контролем макроскопических параметров системы, то теперь стало возможным создание, манипулирование и измерение индивидуальных квантовых состояний объектов на микроскопическом уровне, что открывает новые горизонты во многих фундаментальных вопросах.

Особенный интерес научного сообщества к теории квантовой информации представляет и тот факт, что классическая теория информации находится с теорией квантовой информации приблизительно в том же соотношении, что и классическая ньютоновская механика с квантовой — некоторые объекты и результаты квантовой теории в частном случае дают классическую теорию, а некоторые совсем не имеют классического аналога, и, помимо интереснейших фундаментальных результатов, дают принципиально новые возможности решения важных прикладных задач. К последнему случаю относятся такие разделы теории квантовой информации, как квантовые вычисления, квантовая криптография, квантовая телепортация, в которых уже экспериментально продемонстрированы новые возможности практического использования специфических особенностей квантовой информации.

Так, например, в квантовых вычислениях переход к квантовому носителю информации — кубиту (от английского qubit — quantum bit) дает возможность построения *квантовых алгоритмов*, решающих некоторые математические задачи за меньшее число шагов, чем лучшие классические алгоритмы. На это впервые указал Фейнман [20], предложивший использовать квантовые компьютеры (т.е. такие компьютеры, носителя-

ми информации в которых являются кубиты) для моделирования динамики квантовых систем. Тогда еще было не ясно, могут ли квантовые компьютеры ускорить решение каких-либо других задач, но сейчас для ряда практически важных проблем квантовые алгоритмы уже найдены: разложение n-значного числа на простые множители — пожалуй, самая важная на сегодняшний день задача для прикладной криптографии, решается классическими алгоритмами за число шагов порядка $e^{\sqrt[3]{n}}$, а квантовый алгоритм Шора выполняет эту же задачу за число шагов порядка n^2 [21]; поиск элемента в несортированной базе данных объемом N элементов выполняется классическим компьютером за число шагов порядка N, а квантовый алгоритм Гровера решает эту задачу за число шагов порядка $\sqrt{N}$ [22]. На сегодняшний день уже известен целый ряд задач, решаемых на квантовом компьютере асимптотически быстрее, чем на классическом, и проблема экспериментального создания квантового компьютера интенсивно разрабатывается во многих лабораториях мира. Уже достигнут значительный прогресс в данной области, и можно сказать, что проблема экспериментального создания полноценного квантового компьютера — это лишь вопрос времени [23, 24].

Другая сфера практического применения теории квантовой информации, гораздо более успешная в плане экспериментальной реализации — это квантовая криптография. Центральная идея квантовой криптографии — идея некопируемости квантовой информации — была осознана в конце 70-х — начале 80-х годов и выражена в принципе неклонируемости квантовых состояний [25–27], который обсуждается в разделе 3.1.

Суть этого принципа состоит в том, что для произвольного неизвестного заранее квантового состояния нельзя создать его точную копию, не изменив при этом само копируемое состояние, т.е. неизвестное заранее квантовое состояние нельзя клонировать. Такое свойство квантовых состояний используется в процедуре квантового распределения ключа — передаче небольшого сообщения, которое служит паролем для дальнейшего шифрования больших объемов данных средствами классической криптографии.

Отметим, что процедура классического распределения ключа теоретически не является абсолютно секретной, т.к. основана на математической сложности решения ряда задач (например задачи разложения большого числа на простые множители). Обоснованием секретности служит лишь большое время решения этих задач, в среднем существенно превосходящее разумное время, в течение которого имеет значение секретность шифруемой информации. Процедура квантового распределения ключа, напротив, обеспечивает *абсолютно* секретную передачу информации, т.к. обоснованием секретности служат уже физические законы.

В 1984 году в работе [28] был предложен первый протокол квантовой криптографии, названный в честь его создателей BB84 (от первых букв в фамилиях Bennet и Brassard), а спустя три года он уже был реализован экспериментально [29]. Позже было предложено еще несколько протоколов квантовой криптографии [30–33]. К настоящему времени экспериментальные схемы, реализующие протоколы квантовой криптографии, уже выпускаются как коммерческие продукты [34, 35].

Детальное обсуждение проявлений квантовой специфики физических систем, лежащей в основе перечисленных приложений, можно найти в современных обзорах [23, 36–42] и монографиях [24, 43–46]. Несмотря на все многообразие эффектов и необычность приложений теории квантовой информации, все они связаны тесно связаны между собой и могут быть описаны единым образом как процессы передачи и обработки квантовой информации, посредством *квантовых информационных каналов*. В общем случае преобразование информации в информационном канале $\mathcal{M}$ можно определить как некоторое преобразование состояний на входе канала A в состояния на выходе B:

$$A \xrightarrow{\mathcal{M}} B. \tag{1}$$

Отметим, что вход и выход информационного канала, да и сам канал могут иметь совершенно различный характер: это может быть как специально созданный канал для целенаправленной передачи данных, например, в классических линиях связи или в квантовой криптографии, так и канал, спонтанно реализованный в природе, например, в результате временной эволюции одной физической системы, где входом и выходом канала являются разновременные состояния этой системы, или в результате взаимодействия двух физических систем, представляющих вход и выход некоторого абстрактного канала связи. С этой точки зрения любые физические взаимодействия в принципе можно рассматривать как процессы обмена информацией. Подобное *информационное* описание взаимодействия физических систем будет давать более абстрактную карти-

ну по сравнению с описанием взаимодействия в терминах выбранных конкретных динамических переменных.

С фундаментальной точки зрения одной из центральных проблем в теории информации является определение количественной меры информации и связанной с ней пропускной способностью информационного канала. В классической теории объем информации определяется информационным функционалом Шеннона, имеющим смысл логарифма числа сообщений, передаваемых безошибочно при оптимальном кодировании в асимптотическом пределе больших последовательностей сообщений [4].

По сравнению с теорией информации Шеннона в приложении к физике роль квантовой информации представляется значительно более существенной, не позволяющей выделить её в качестве независимой от физики чисто математической дисциплины [47, 48]. В отличие от классических систем, в квантовом случае проблема введения количественной меры квантовой информации не допускает единого решения, а зависит от физического содержания квантового информационного канала.

Качественное отличие квантовых систем от классических состоит в *некоммутативности* квантовых переменных, которая эквивалентна *неортогональности* их собственных квантовых состояний и связанной с этим невозможности рассмотрения произвольного набора квантовых событий в рамках классической логики — т. н. *несовместимости* элементарных квантовых событий, проявляющейся в возникновении специфической *квантовой неопределенности*, что будет подробно рассмотрено в разделе 1.1 главы 1.

С учетом этого факта наиболее общее деление типов квантовых каналов и соответствующих информационных мер основано на внутренней и взаимной коммутативности/некоммутативности проекторов–индикаторов событий на входе и выходе информационного канала, или, другими словами, внутренней и взаимной совместимости или несовместимости элементарных событий на входе и выходе информационного канала [48].

В результате можно выделить следующие четыре основных типа информационных каналов:

- *Классический канал* — элементарные события на входе и выходе канала внутренне и взаимно совместимы. В исходной форме теории информации Шеннона "по умолчанию" рассматриваются именно такие классические состояния [4, 49]. Классический канал задаётся условным распределением вероятностей $p(y|x)$ состояний выхода y при фиксированных состояниях входа x. Отметим, однако, что классическая информация всегда может быть передана по квантовому каналу и также представляет определённый интерес в квантовой физике. Адекватной количественной мерой классического канала является классическая взаимная информация Шеннона.

- *Полуклассический канал* — элементарные события на входе канала внутренне совместимы и автоматически взаимно совместимы с элементарными событиями на выходе канала, но, в отличие от предыдущего случая, элементарные события на выходе канала внутренне

несовместимы. Полуклассический канал в общем случае описывается ансамблем смешанных квантовых состояний выхода $\hat{\rho}_\lambda$, зависящих от классического параметра λ на входе [14, 15, 50]. Состояния на входе канала задаются классическими параметрами λ, которые эквивалентны входным переменным x в классическом канале; состояния на выходе задаются множеством всех волновых функций $\psi \in H$, аналогичным переменным y; матрица плотности $\hat{\rho}_\lambda$ аналогична условному распределению вероятностей $p(y|x)$ классического канала. Адекватной количественной мерой полуклассического канала является информация Холево, представляемая как обобщение классического информационный функционала Шеннона с использованием для энтропии её квантового обобщения в форме $S[\hat{\rho}] = -\mathrm{Tr}\hat{\rho}\log\hat{\rho}$.

- *Некоммутативный канал* — элементарные события на входе и выходе канала внутренне и взаимно несовместимы. Некоммутативный канал описывается супероператором канала $\mathcal{N}$, преобразующим матрицу плотности входа в матрицу плотности выхода: $\hat{\rho}_B = \mathcal{N}\hat{\rho}_A$ [51, 52]. Преобразование $\mathcal{N}$ определяет поток квантово несовместимых состояний от входа канала к его выходу и является полностью квантовым аналогом классического условного распределения $p(y|x)$, которое осуществляет аналогичное линейное преобразование классического входного распределения вероятностей $p(x)$ в выходное распределение $p(y)$. Адекватной количественной мерой

некоммутативного канала является объем когерентной информации [51]. Физически некоммутативный канал реализуется, например, при временной эволюции динамически замкнутой квантовой системы, которая в начальный момент времени играет роль входа, а в конечный — роль выхода информационного канала.

- *Коммутативный канал* — элементарные события на входе и выходе канала внутренне несовместимы, но, в отличие от предыдущего случая, взаимно совместимы. Коммутативный канал, вообще говоря, реализуется в случае, когда пространство состояний канала H_{AB} представимо в виде тензорного произведения пространств состояний входа и выхода ($H_{AB} = H_A \otimes H_B$), и существует совместная матрица плотности входа и выхода $\hat{\rho}_{AB}$. Такая ситуация появляется, например, при рассмотрении одновременных состояний двух различных нерелятивистских физических систем, играющих роль входа и выхода информационного канала.

В то время как три первых типа информационных каналов и соответствующих им информационных мер хорошо известны и в той или иной степени изучены, совместимая информация как особый тип информационной меры коммутативного канала в явной форме введена лишь относительно недавно [53]. В связи с этим представляется весьма актуальным анализ общих свойств совместимой информации, разработка математических методов информационного анализа коммутативных каналов и применение анализа, основанного на расчете совместимой информа-

ции, к общеупотребительным моделям реальных физических систем.

Совместимая информация связана с возникновением корреляций в состояниях входа и выхода канала, проявляющихся в форме совместного распределения вероятностей $P_{AB}(x, y)$ результатов двух независимых обобщенных измерений, выполняемых на входе A и выходе B квантового канала. Естественной количественной мерой совместимой информации является классический информационный функционал Шеннона. Отметим, что совместимую информацию можно рассматривать и безотносительно процесса измерения, как потенциально заложенную меру классического "знания" выхода канала о состоянии входа.

С точки зрения качественного содержания совместимая информация является обобщением классической взаимной информации на случай квантовых систем, т.к. учитывает как чисто классические, так и специфически квантовые корреляции состояний входа и выхода. Она характеризует информационную связь между входом и выходом в декванто-ванной, классической форме, допускающей копирование, в отличие от когерентной информации, которая должна быть уничтожена в одной физической системе, чтобы быть переданной в другую.

Цель данной диссертации состоит в анализе общих свойств совместимой информации и применение разработанного формализма к информационному анализу некоторых важных типов совместимых информационных каналов, что имеет существенное значение для теории квантовой информации.

Диссертация состоит из введения, трех глав, заключения, списка ли-

тературы и двух приложений.

В первой главе диссертации рассмотрены общие понятия теории классической и квантовой информации и специфика квантовых систем с информационной точки зрения. Изучены общие свойства совместимой информации и проанализирована их связь со свойствами классической взаимной информации. Выполнен детальный качественный и количественный информационный анализ максимально перепутанных и сепарабельных двухкубитных квантовых каналов.

Во второй главе диссертации на примере двухкубитного информационного канала, образованного двумя двухуровневыми атомами, взаимодействующими в рамках модели Дике, рассмотрены свойства описания динамики взаимодействия квантовых систем на языке обмена совместимой информацией. Проведен расчет зависимости совместимой информации в задаче Дике от физических параметров системы.

В третьей главе диссертации общая идеология совместимой информации примененяется к анализу информационных каналов в задачах квантовой криптографии. Изучена зависимость помехоустойчивости протоколов квантовой криптографии от алфавитов, выбранных для кодирования классической информации при ее передаче по квантовому каналу. Предложен ряд новых протоколов квантовой криптографии, основанных на квантовых алфавитах, образующих правильные многогранники на сфере Блоха. Изучена их стабильность против помех в квантовом канале, вызванных перехватом информации с помощью стратегии перехвата—пересылки и стратегии оптимального подслушивания при индивидуаль-

ных атаках. Рассмотрена возможность реализации секретной связи при произвольном уровне ошибок за счет увеличения размерности гильбертова пространства в протоколе с континуальным алфавитом, использующем все квантовые состояния гильбертова пространства. Рассчитаны верхние оценки эффективности протоколов квантовой криптографии, основанных на многомерных алфавитах. Предложена экспериментальная схема реализации рассмотренных протоколов квантовой криптографии.

В Заключении обсуждаются результаты диссертационной работы, делаются выводы и формулируются защищаемые положения.

В приложении А дано описание представления состояния кубита вектором на сфере Блоха. В приложении Б приведена программа на языке Mathematica для расчета основных полученных в работе величин.

Глава 1

Передача классической информации по квантовым каналам

1.1 Информационное содержание основных положений квантовой теории

Одним из центральных понятий квантовой теории является понятие *состояния* квантовой системы. Рассмотрим его на простейшем примере двухуровневой квантовой системы, или *кубита*, имеющего два классических состояния $|1\rangle$ и $|2\rangle$, которые образуют ортогональный базис в гильбертовом пространстве состояний кубита. Согласно принципу суперпозиции, любое чистое состояние кубита может быть представлено как

$$|\psi\rangle = \alpha\,|1\rangle + \beta\,|2\rangle, \tag{1.1}$$

где квадраты модулей комплексных коэффициентов α и β связаны соотношением нормировки $|\alpha|^2 + |\beta|^2 = 1$ и согласно вероятностной интерпретации Борна [54] определяют *вероятности обнаружения* кубита в состояниях $|1\rangle$ и $|2\rangle$.

Довольно широко распространена такая интерпретация принципа суперпозиции, согласно которой квантовая система, находясь в суперпозиционном состоянии $|\psi\rangle$, одновременно находится сразу в двух классических состояниях $|1\rangle$ и $|2\rangle$. Однако такое высказывание, рассматриваемое в рамках классической логики, внутренне противоречиво. Действительно, утверждение *"квантовая система находится в состоянии* $|\psi\rangle$*"* означает, что вероятность обнаружения системы в другом произвольном состоянии $|\varphi\rangle$ равна его проекции $|\langle\varphi\,|\psi\rangle\,|^2$ на состояние $|\psi\rangle$. Если же говорить, что система в состоянии $|\psi\rangle$ находится одновременно в двух

(или даже нескольких) других состояниях, то вероятностный смысл последних теряется, т.к. они дают ненулевую проекцию на ортогональное к $|\psi\rangle$ состояние $|\tilde{\psi}\rangle$, вероятность обнаружения в котором должна была бы быть равной нулю. Таким образом, понятие "истинного состояния" квантовой системы, т.е. такого состояния, в котором система находится в классическом понимании, существенно отличается от понятия остальных "состояний, в которых система может быть обнаружена", т.е. в которых она *как бы* находится.

Полученное противоречие решается в т.н. логико–алгебраическом подходе в квантовой теории адекватным введением понятия *события* в физической системе и соответствующей *квантовой логики* событий, непосредственно связанной с алгеброй физических переменных и отображаемой с её помощью динамики (в форме соответствующей группы динамических преобразований). Для раскрытия смысла этих понятий рассмотрим сначала их классические аналоги.

В классической теории понятие "события" принимается "по умолчанию", и в явной форме определяется лишь в теории вероятностей [55]. Несмотря на это, понятие события является более первичным в физике, чем понятие физической переменной или ее величины, т.к. именно на уровне *логики* событий закладываются основные правила оперирования с физическими величинами.

В классической теории совокупность всех физических событий образует *σ-алгебру событий* B как множество подмножеств множества элементарных событий Ω с определенными на ней операциями сложения и

умножения в виде объединения и пересечения множеств:

$$\forall A_1, A_2 \in B \quad A_1 \cdot A_2 \equiv A_1 \cap A_2, \quad A_1 + A_2 \equiv A_1 \cup A_2. \tag{1.2}$$

Геометрическое представление σ-алгебры было дано еще Аристотелем в виде "кругов Аристотеля" — множества всех подмножеств геометрического множества на плоскости. На этом примере был формализован основной закон классической логики — закон дистрибутивности

$$(A_1 + A_2) \cdot A_3 = A_1 \cdot A_3 + A_2 \cdot A_3, \tag{1.3}$$

который легко проверяется с помощью геометрических построений на плоскости.

В частном случае, когда $A_3 = \omega$, где ω — произвольное элементарное событие, а $A_2 = \overline{A}_1$, где $\overline{A}_1$ обозначает событие, дополнительное к A_1, т.е. дополняющее его до максимального, достоверного события E, и не перекрывающее A_1 ($A_1 + \overline{A}_1 = E, \quad A_1 \cdot \overline{A}_1 = 0$), получается закон исключенного третьего:

$$\omega = (A_1 + \overline{A}_1) \cdot \omega = A_1 \cdot \omega + \overline{A}_1 \cdot \omega, \tag{1.4}$$

выражающий тот факт, что любое элементарное событие ω представляется в виде "либо A_1, либо не-A_1".

В квантовой теории роль элементарных событий ω играют волновые функции $|\psi\rangle$, или векторы состояний квантовой системы [56]. Множество всех элементарных событий образует гильбертово пространство H. На алгебре квантовых событий B, образованной совокупностью всех подпространств в H, операции умножения и сложения определяются как

пересечение и линейное объединение подпространств, соответственно. В описываемой такой алгеброй квантовой логике закон дистрибутивности (1.3) не выполняется, в чем легко убедится уже на примере двумерного гильбертова пространства, взяв в качестве элементов A_1, A_2 и A_3 три произвольных неортогональных и неколлинеарных вектора на плоскости. В левой части (1.3) сумма $A_1 + A_2$, согласно определению сложения как линейной оболочки на A_1 и A_2, будет давать все двумерное пространство как единичный элемент алгебры, и, после умножения (определенного как пересечение подпространств) на A_3, левая часть будет равна A_3. Правая часть (1.3) равна нулю, т.к. каждое из слагаемых в нем равно нулю. Таким образом, в квантовой логике закон дистрибутивности, а вместе с ним и закон исключенного третьего, вообще говоря, не выполняются. Однако, в частном случае, когда в квантовой алгебре рассматривается только подалгебра, построенная на ортогональных подпространствах, закон дистрибутивности выполняется, что и делает возможным существование классической логики в нашем мире.

Отметим, что классический наблюдатель, мыслящий в рамках классической логики, может однозначно интерпретировать лишь классический, ортогональный набор событий. В этом смысле все наборы событий делятся на два класса: *совместимые* и *несовместимые*. Первые описываются ортогональным набором событий и подчиняются законам классической логики (они взаимно совместимы в ней), вторые описываются неортогональным набором и классической логике не подчиняются — они несовместимы в рамках классической логики. Здесь важно понимать, что

понятие совместимости в приведенном выше смысле относится только к набору событий, а не к событиям самим по себе.

Физически выбор набора рассматриваемых событий определяется через *обобщенное измерение* квантовой системы и математически выражается положительно определенной операторнозначной мерой (ПОМ), или, другими словами, обобщенным разложением единичного оператора [14, 57, 58]:

$$\hat{1} = \sum_k \hat{E}(k). \tag{1.5}$$

Составляющие ПОМ $\hat{E}(k)$, вообще говоря, могут не коммутировать: $[\hat{E}(k_1), \hat{E}(k_2)] \neq 0$. Вероятности элементарных событий как исходов обобщенного измерения равны среднему значению соответствующих ПОМ: $P(k) = \mathrm{Tr}\hat{E}_k\hat{\rho}$.

Выбор ПОМ фактически представляет собой обобщённый аналог полной группы классических случайных событий, вероятности которых нормированы на равную единице вероятность достоверного события, представляемого в квантовом случае единичным оператором:

$$\sum P(k) = \sum \mathrm{Tr}\hat{E}_k\hat{\rho} = \mathrm{Tr}\hat{\rho}\sum \hat{E}_k = \mathrm{Tr}\hat{\rho}\hat{1} = 1. \tag{1.6}$$

Совместимый набор элементарных событий описывается набором коммутирующих ортопроекторов $\hat{P}(k) = |k\rangle\langle k|$, $([\hat{P}(k_1), \hat{P}(k_2)] = 0)$, разложение (1.5) принимает при этом частный вид

$$\hat{1} = \sum_k \hat{P}(k) \tag{1.7}$$

и физически реализуется как прямое, ортогональное измерение рассматриваемой квантовой системы.

Произвольное обобщенное измерение, связанное с произвольной ПОМ $\hat{E}(k)$, реализуется как прямое измерение в расширенном пространстве $H_{Aa} = H_A \otimes H_a$ составной системы "рассматриваемая система A + вспомогательная система a" с последующим усреднением по степеням свободы вспомогательной системы [14, 59, 60]:

$$\hat{E}_A(k) = \mathrm{Tr}_a \hat{P}_{Aa}(k)\hat{\rho}_a. \tag{1.8}$$

Отметим, что процедура обобщенного измерения не означает возможности одновременного точного измерения неортогонального набора состояний. При реализации обобщенного измерения квантовой системы как прямого измерения в расширенном пространстве внутренняя квантовая неопределенность рассматриваемого несовместимого набора событий просто переходит в обычную статистическую неопределенность классических результатов измерения в составной системе.

Логические противоречия, возникающие при попытках классической интерпретации несовместимых наборов квантовых событий, приводят к известным парадоксам и необычным свойствам квантовой теории. Например, внутренняя *квантовая неопределенность* состояния квантовой системы связана с нарушением классического закона исключенного третьего, когда не одно, а сразу множество элементарных событий имеет ненулевую вероятность, что в рамках классической логики невозможно. Другое необычное свойство квантовых состояний, играющее ключевую

роль в квантовых вычислениях —*квантовый параллелизм* — вытекает из квантовой неопределенности и состоит в том, что унитарное преобразование над квантовой системой затрагивает сразу все ее состояния: набор квантовых битов параллельно описывает сразу все состояния аналогичного набора классических битов. При этом классическая статистическая неопределенность состояния классического регистра битов переводится во внутреннюю квантовую неопределенность квантового регистра и обрабатывается квантовым компьютером когерентным образом.

1.2 Классическая взаимная информация

Основой для введения количественной меры квантовой совместимой информации является понятие шенноновского количества информации как количества информации о случайной переменной x системы X, содержащейся в случайной переменной y системы Y и определяемой в виде разности безусловной и условной энтропии [49]:

$$I_{XY} \equiv S[P(x)] - S[P(x|y)]. \tag{1.9}$$

Безусловная энтропия $S[P(x)]$ отражает априорную неопределенность состояний системы X, а условная энтропия $S[P(x|y)]$ отражает неопределенность имеющейся информации об X в состояниях системы Y; вычитая из априорной энтропии меру неопределённости полученной информации, мы и получаем величину “достоверной” информации I_{XY}, полученной системой Y об X.

Для дискретной случайной величины x с распределением вероятностей $P(x)$ энтропия $S[P(x)] \equiv S_X$ определяется как

$$S_X \equiv -\sum_X P(x) \log_2 P(x). \tag{1.10}$$

Основание логарифма определяет единицы измерения энтропии и, соответственно, информации: логарифму по основанию 2 соответствует *бит*. Максимальная величина энтропии равна $\log_2 N$, где N — число различных значений x и достигается в случае равномерного распределения x. Интуитивно понятно, что максимальная неопределенность состояния системы X достигается именно в случае, когда все элементарные события равновероятны. Минимальная величина энтропии равна нулю и достигается в случае, когда только одно из значений x имеет единичную вероятность, а вероятности остальных значений x равны нулю, т.е. фактически когда состояние системы X всегда одно и то же.

Энтропия непрерывной случайной величины x определяется как

$$S_X \equiv -\int_X p(x) \log_2 \frac{p(x)}{\nu_0(x)} dx, \tag{1.11}$$

где $p(x)$ — плотность распределения случайной величины x, а $\nu_0(x)$ — асимптотическая плотность распределения дискретизированного количества различимых (с учетом конечной точности измерений) событий на непрерывном множестве значений x [61]. Например, в статистической физике внутренняя квантовая неопределенность приводит к конечности элемента физически различимого фазового объема для квазиклассической системы из N материальных точек и соответствующей плотности

различимых событий $\nu_0(X) = \dfrac{dN}{dX} = \dfrac{1}{(2\pi\hbar)^{3N}}$ в пространстве фазовых координат $X = (\vec{r}_1, \ldots, \vec{r}_N, \vec{p}_1, \ldots, \vec{p}_N)$. В случае классического описания квантовой двухуровневой системы общее число классически различимых событий равно двум, т.е. $\oint \nu_0(x)dx = 2$, где x в данном случае соответствует элементу поверхности сферы Блоха, а $\nu_0(x) = \dfrac{1}{2\pi}$.

Из определения величины взаимной информации в виде разности безусловной и условной энтропии (1.9) видно, что минимальная величина взаимной информации равна нулю, т.к. условная энтропия по величине не превосходит безусловную. Максимальная величина взаимной информации определяется максимальной величиной безусловной энтропии, которая достигается в случае равномерного распределения вероятностей. Для дискретной системы с M равновероятными событиями она равна $S_{\max}(M) = \log_2 M$.

Используя соотношение для условной энтропии $S[P(x|y)] = S[P(x,y)] - S[P(y)]$, можем записать шенноновскую информацию в виде

$$I_{XY} = S_X + S_Y - S_{XY}, \tag{1.12}$$

где S_{XY} — энтропия совместного распределения $P(x,y)$, а S_X и S_Y — энтропия парциальных распределений $P(x) = \sum\limits_Y P(x,y)$ и $P(y) = \sum\limits_X P(x,y)$. Из формулы (1.12) видна симметричность I_{XY} относительно перестановки X и Y местами, что дает возможность интерпретировать меру информации Шеннона как меру взаимной скоррелированности систем X и Y посредством случайных величин x и y, что и обуславливает термин “взаимная информация”.

Рассмотрим применение понятия шенноновского количества взаимной информации в следующем примере: рассчитаем количество извлекаемой информации при угадывании игроком выпадения монеты на одну из двух сторон.

Пусть имеется система A в виде двусторонней монеты, выпадающей с вероятностью p на одну сторону и с вероятностью $1-p$ — на другую, и система B в виде игрока, угадывающего выпавшую сторону монеты с вероятностью q (независимо от конкретной выпавшей стороны): возможным выпадениям монеты на "орла" или "решку" сопоставляются аналогичные ответы игрока. В данном примере и монета, и игрок — это системы с минимальным количеством элементарных событий: по два элементарных события в каждой из систем (в случае одного элементарного события энтропия была бы равна нулю и информационная связь была бы невозможна).

Итак, при условном распределении вероятностей ответов игрока

$$P_{B|A}(1,1) = P_{B|A}(2,2) = q, \quad P_{B|A}(1,2) = P_{B|A}(2,1) = 1-q \qquad (1.13)$$

получаем совместное распределение вероятностей $P_{AB}(i,j) = P_{B|A}(i,j)P_A(j)$ выпадения монеты на сторону i и ответа игрока j и парциальные распределения $P_A(i)$ и $P_B(j)$:

$$P_{AB} = \begin{pmatrix} pq & p(1-q) \\ (1-p)(1-q) & (1-p)q \end{pmatrix},$$

$$P_A = (p, 1-p), \quad P_B = (pq + (1-p)(1-q), p(1-q) + (1-p)q). \qquad (1.14)$$

Количество информации связи ответов игрока и выпадения монеты, рассчитанное по формуле (1.12), графически представлено на рис. 1.1.

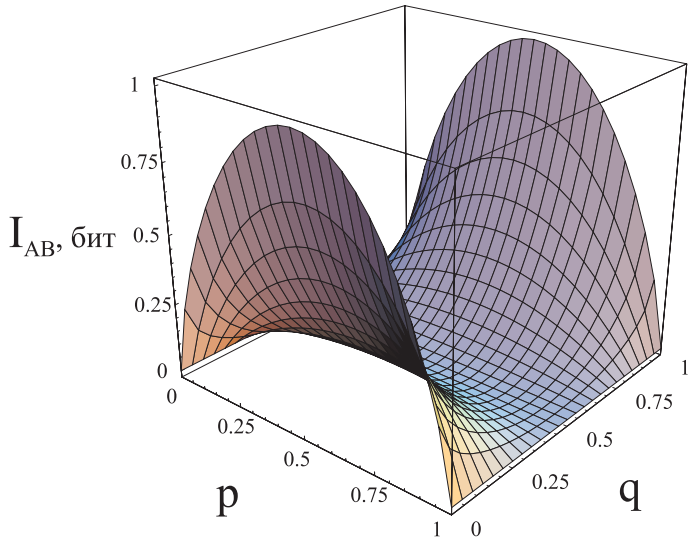


Рис. 1.1: Зависимость количества информации I_{AB} связи ответов игрока и выпадений монеты от вероятности угадывания q и вероятности выпадения монеты на одну из сторон p.

Если игрок угадывает выпадение монеты с вероятностью $q = 1/2$, то его показания статистически не связаны с выпадением монеты, т.е. системы A и B становятся статистически независимыми, что приводит к нулевой информации связи ($I_{AB}(p, 1/2) = 0$).

В случае симметричной монеты ($p = 1/2$) при $q = 0$ и $q = 1$ получаем $I_{AB}(1/2, 0) = I_{AB}(1/2, 1) = 1$ бит. Этот факт имеет простой наглядный смысл: если игрок всегда угадывает выпадение монеты ($q = 1$) или никогда не угадывает ($q = 0$) (т.е. фактически угадывает противоположный выпавшему вариант), то система B полностью (на 100%) скоррелирована

с системой A, т.е. извлекает из нее максимально возможную информацию, равную одному биту.

В случае асимметричной монеты ($p \neq 1/2$) максимально возможный объем информации меньше одного бита и определяется энтропией выпадений монеты.

1.3 Небайесовское количество взаимной информации

Существенным моментом при расчете взаимной информации является знание априорного распределения вероятностей элементарных событий. Однако существуют ситуации, в которых это распределение вероятностей заранее неизвестно. Например, в рассмотренном выше примере с угадыванием выпадений монеты игрок может заранее не знать, с какой именно вероятностью монета выпадает на ту или иную сторону. В такой ситуации формула (1.9) неприменима, т.к. априорное распределение вероятностей не задано и поэтому нельзя по формуле Байеса рассчитать апостериорное распределение вероятностей. Для расчета количества информации, получаемой игроком при угадывании такой монеты, необходимо знать энтропию такой неопределенной системы, о которой известно лишь количество элементарных событий в ней, а их вероятности неизвестны.

Энтропия классической системы с набором N элементарных событий в ней, имеющих заданные вероятности $p_1, p_2, \ldots, p_N$, согласно определе-

нию (1.10), есть

$$S_N(p_1, p_2, \ldots, p_N) = -\sum_{i=1}^{N} p_i \log_2 p_i. \tag{1.15}$$

Минимальное значение этой величины равно нулю и достигается в случае, когда только одно элементарное событие имеет единичную вероятность, а вероятности остальных элементарных событий равны нулю. Максимальное значение этой энтропии равно $\log_2 N$ и достигается в случае, когда все элементарные события имеют равные вероятности $p_i = 1/N$.

Для нахождения энтропии системы с неизвестным априорным распределением вероятностей усредним энтропию (1.15) по всем наборам вероятностей $\mathcal{P} = \{p_1, p_2, \ldots, p_N\}$ ее элементарных событий с мерой $\nu(d\mathcal{P})$:

$$\overline{S}_N = \frac{\int S[\mathcal{P}]\nu(d\mathcal{P})}{\int \nu(d\mathcal{P})}. \tag{1.16}$$

Если о вероятностях элементарных событий ничего заранее не известно, то нет причин считать один набор вероятностей более предпочтительным другому, т.е. все наборы можно считать равно представленными. Условие равновероятности всех наборов элементарных событий означает выбор меры интегрирования $\nu(d\mathcal{P}) = d\mathcal{P} = dp_1 dp_2 \ldots dp_N$, откуда получаем $\int \nu(d\mathcal{P}) = 1$ и

$$\overline{S}_N = \int\limits_{\sum\limits_{i=1}^{N} p_i = 1} S_N(p_1, p_2, \ldots, p_N) dp_1 dp_2 \ldots dp_N. \tag{1.17}$$

В случае $N = 2$ такая энтропия соответствует энтропии двусторонней монеты у которой вероятности выпадения ее на ту или иную сторо-

ны априори неизвестны. Прямым вычислением усредненной энтропии по всем вероятностям выпадения монеты на ту или иную сторону имеем:

$$\overline{S}_2 = \int\limits_{p+q=1} S(p,q)dpdq = \int\limits_0^1 S(p,1-p)dp = 1/\ln 4 \simeq 0,721. \qquad (1.18)$$

Аналитический расчет интеграла (1.17) для случая $N > 2$ напрямую невозможен из-за ограничений на переменные интегрирования в виде неотрицательности вероятностей всех элементарных событий и нормировки их суммы на единицу

$$\begin{cases} \forall\, i \quad p_i \geq 0 \\ \sum\limits_{i=1}^{N} p_i = 1. \end{cases} \qquad (1.19)$$

Если рассмотреть геометрическое представление области интегрирования в интеграле (1.17) в N–мерном евклидовом пространстве, где точки задаются координатами $\mathcal{P} = \{p_1, p_2, \ldots, p_N\}$, то видно, что область интегрирования — это часть гиперплоскости, проходящей через точки $\{1,0,\ldots,0\}$, $\{0,1,0,\ldots,0\}$, $\ldots$, $\{0,0,\ldots,1,0\}$, $\{0,0,\ldots,0,1\}$, ограниченная условием $\forall\, i \quad p_i \geq 0$.

Заметим, что для обеспечения условий (1.19) удобно перейти к квадратам полярных координат по формулам:

$$\begin{cases} p_1 = r^2 \cos^2 \varphi_1 \\ p_1 = r^2 \sin^2 \varphi_1 \cos^2 \varphi_2 \\ \ldots \\ p_{N-1} = r^2 \sin^2 \varphi_1 \sin^2 \varphi_2 \ldots \sin^2 \varphi_{N-2} \cos^2 \varphi_{N-1} \\ p_N = r^2 \sin^2 \varphi_1 \sin^2 \varphi_2 \ldots \sin^2 \varphi_{N-2} \sin^2 \varphi_{N-1}. \end{cases} \qquad (1.20)$$

Несложно получить, что якобиан перехода равен

$$J = 2^N r^{2N-1} \prod_{i=1}^{N-1} \cos\varphi_i \sin^{2(N-1)-1}\varphi_i. \tag{1.21}$$

Для выполнения условия $\sum\limits_{i=1}^{N} p_i = 1$ необходимо положить $r = 1$, что преобразует плоскую область интегрирования в часть гиперсферы, ограниченной условием $\forall\, i \quad \varphi_i \in [0, \pi/2]$.

Выполняя в (1.17) замену переменных (1.20), имеем

$$\overline{S}_N = \frac{\int\limits_0^{\pi/2} \dots \int\limits_0^{\pi/2} S_N(p_1(\varphi_1), \dots, p_N(\varphi_1, \dots, \varphi_{N-1}))Jd\varphi_1 d\varphi_2 \dots d\varphi_{N-1}}{\int\limits_0^{\pi/2} \dots \int\limits_0^{\pi/2} Jd\varphi_1 \dots d\varphi_{N-1}} = \\ = \frac{1}{\ln 2} \sum_{i=2}^{N} \frac{1}{i}. \tag{1.22}$$

Полученная величина средней энтропии классической системы при неизвестном априорном распределении вероятностей лишь совсем немного отличается от максимально возможной величины энтропии $S_N^{max} = \log_2 N$, и количество информации $\overline{I}_N$, извлекаемой из такой системы, при увеличении числа элементарных событий ограничено:

$$\lim_{N\to\infty} \overline{I}_N = S_N^{max} - \overline{S}_N = \frac{1-\gamma}{\ln 2} \simeq 0,61, \tag{1.23}$$

где γ — постоянная Эйлера ($\gamma \simeq 0,577$).

Отметим, что средняя энтропия (1.22) совпадает с объемом энтропии квантового состояния в отсутствие какой-либо селекции [62], т.е. априорной энтропией квантового состояния, и это не случайно. Эквивалентность усредненной классической энтропии и априорной энтропии

квантового состояния фактически связана с борновской вероятностной интерпретацией волновой функции.

Действительно, произвольное квантовое состояние, записанное в суперпозиции классического базиса, задает вероятности этих классических событий. В статистическом смысле квантовая система эквивалентна классической: различные волновые функции аналогичны различным наборам вероятностей классических элементарных событий. Усреднению по набору волновых функций N-мерного гильбертова пространства соответствует усреднение по наборам вероятностей N элементарных классических событий. Проекции волновой функции в классическом базисе — это лишь одно из возможных представлений ансамбля элементарных классических событий.

Заметим также, что величина априорной энтропии квантового состояния связывалась ранее исключительно с внутренней квантовой неопределенностью [62]. Теперь же мы видим, что у нее есть аналог и в классической теории. В дальнейшем это будет играть важную роль в установлении соотношений между различными типами совместимой информации.

1.4 Квантовая совместимая информация

Пусть имеются две квантовые системы A и B и совместная матрица плотности $\hat{\rho}_{AB}$, заданная в гильбертовом пространстве $H_{AB} = H_A \otimes H_B$ состояний системы $A+B$. Рассмотрим шенноновское количество информации, связанной со взаимными корреляциями в системах A и B посред-

ством элементарных событий, заданных выбором ПОМ $\hat{E}_A\ \hat{E}_B$ в каждой из систем:

$$I_{AB} = S_A[P_A] + S_B[P_B] - S_{AB}[P_{AB}], \tag{1.24}$$

где

$$\begin{gathered} P_A = \mathrm{Tr}_A(\hat{E}_A\hat{\rho}_A), \quad P_B = \mathrm{Tr}_B(\hat{E}_B\hat{\rho}_B), \\ P_{AB} = \mathrm{Tr}_{AB}[(\hat{E}_A \otimes \hat{E}_B)\hat{\rho}_B]. \end{gathered} \tag{1.25}$$

Два крайних случая ПОМ (для простоты далее будем говорить о двумерных пространствах, хотя результаты легко обобщаются и на многомерный случай) — двухкомпонентное ортогональное разложение единичного оператора [63]:

$$\hat{1} = |\nu\rangle\langle\nu| + |\tilde{\nu}\rangle\langle\tilde{\nu}|, \tag{1.26}$$

где $|\nu\rangle$ и $|\tilde{\nu}\rangle$ — произвольная пара ортогональных волновых функций, и континуальное неортогональное разложение единичного оператора [64]:

$$\hat{1} = \oint |\nu\rangle\langle\nu|\, dV_\nu, \tag{1.27}$$

где в стандартных угловых координатах на сфере Блоха дифференциал объема двумерного гильбертова пространства $dV_\nu = \sin\theta d\theta d\varphi/(2\pi)$, (вспомогательная мера dV_ν выражается через дифференциал поверхности сферы Блоха dS соотношением $dV_\nu = \nu_0 dS$, где $\nu_0 = \frac{2}{S}$, $S = 4\pi, dS = \sin\theta d\theta d\varphi$) определяют два предельных типа совместимой информации — предельно *селектированную* и *неселектированную*.

Первый тип — селектированная информация — отражает информационную связь между двумя квантовыми системами A и B через выделенный набор ортогональных квантовых событий. Заметим, что в силу

внутренней квантовой неопределенности в процессе передачи информации в той или иной степени участвуют *все* квантовые состояния, дающие ненулевую проекцию на выделенный ортогональный набор. Сам выделенный ортогональный набор несет в себе лишь смысл базиса для измерений, результаты которых и определяют величину информационной связи.

Т.к. выбрать ортогональный базис можно разными способами, определяемыми унитарными двухпараметрическими преобразованиями $U_A(\alpha)$ и $U_B(\beta)$ в каждой из систем A и B, то селектированная информация зависит от соответствующего выбора:

$$\begin{aligned} I_{AB}(\alpha,\beta) &= S_A(\alpha) + S_B(\beta) - S_{AB}(\alpha,\beta) = \\ &= \sum_{k,l=1}^{2} P_{AB}^{\alpha\beta}(k,l) \log_2 \frac{P_{AB}^{\alpha\beta}(k,l)}{P_A^{\alpha}(k) P_B^{\beta}(l)}, \end{aligned} \tag{1.28}$$

где параметры $\alpha = (\theta_1, \varphi_1)$ и $\beta = (\theta_2, \varphi_2)$ задаются стандартными углами на сфере Блоха.

Совместное распределение вероятностей, заданное на ортогональных базисах $|k\rangle_A^{\alpha} = U_A(\alpha)\,|k\rangle_A$, $|l\rangle_B^{\beta} = U_B(\beta)\,|l\rangle_B$ входа и выхода квантового канала, пронумерованных двузначными индексами k, l, рассчитывается как

$$P_{AB}^{\alpha\beta}(k,l) = \mathrm{Tr}_{\mathrm{AB}}\Big[\Big(|k\rangle_A^{\alpha}\,\langle k|_A^{\alpha} \otimes |l\rangle_B^{\beta}\,\langle l|_B^{\beta}\Big)\,\hat{\rho}_{AB}\Big]. \tag{1.29}$$

Селектированную информацию $I_{AB}(\alpha,\beta)$ можно рассматривать как информацию связи систем A и B посредством двух классических индексов α и β квантовых состояний $|\alpha\rangle$ и $|\beta\rangle$, или как информацию о состоянии $|\alpha\rangle$ системы A, содержащуюся в состоянии $|\beta\rangle$ системы B.

Состояния $|\alpha\rangle$ и $|\beta\rangle$ далее будем по отдельности называть *информационными состояниями*, а их в совокупности — *информационным базисом*.

Таким образом, в квантовом случае мы имеем возможность рассчитать и проанализировать информационный обмен двух квантовых систем посредством произвольной пары информационных базисов, задавая для каждой системы своё информационное состояние, в данном случае $|\alpha\rangle$ для A и $|\beta\rangle$ для B, в отличие от классического случая, где классические информационные состояния $|1\rangle$ и $|2\rangle$ всегда одни и те же. В этом отношении классическая взаимная информация представляет собой частный случай селектированной информации с фиксированным информационным базисом.

Второй тип совместимой информации — неселектированная информация — отражает информационный обмен сразу через все равноправно задействованные квантовые состояния систем с учетом их внутренней квантовой неопределённости. В данном случае роль информационных состояний входа и выхода канала играют *все* волновые функции гильбертовых пространств каждой системы, и соответствующая мера неселектированной информации представляется выражением

$$I_{AB} = S_A + S_B - S_{AB} = \iint\limits_{\alpha\ \beta} P_{AB}(d\alpha, d\beta) \log_2 \frac{P_{AB}(d\alpha, d\beta)}{P_A(d\alpha) P_B(d\beta)}, \qquad (1.30)$$

где

$$\begin{gathered} P_{AB}(d\alpha, d\beta) = \mathrm{Tr}_{\mathrm{AB}}\big[\Big(\hat{E}_A(d\alpha) \otimes \hat{E}_B(d\beta)\Big)\, \hat{\rho}_{AB}\big], \\ \hat{E}_{A,B}(d\nu) = |\nu\rangle_{A,B}\, \langle\nu|_{A,B}\, dV_\nu. \end{gathered} \qquad (1.31)$$

Неселектированная информация в наиболее общем виде отражает

структуру информационной связи обмена информацией между входом и выходом квантового канала, где нет априори выделенных состояний, т.е. какая-либо селекция квантовых состояний отсутствует.

Отметим важное аналитическое соотношение между селектированной и неселектированной информацией, прямо вытекающее из классической аналогии между классическими и квантовыми ансамблями, полученной в разделе 1.3: неселектированная информация равна селектированной, усредненной по всем ориентациям её информационных базисов:

$$I_{AB} = \iint\limits_{\alpha\ \beta} I_{AB}(\alpha,\beta)\frac{dV_\alpha dV_\beta}{V^2}\,, \quad V = \int dV_\nu = 2. \tag{1.32}$$

Действительно, и усредненная селектированная информация, и неселектированная информация в качестве носителей информации используют в равной мере все квантовые состояния, и в смысле получения величины классических корреляций безразлично, когда именно проводить усреднение: на этапе одного измерения (неселектированная информация) или после серии измерений (усредненная селектированная информация).

Соотношение (1.32) указывает также способ расчета неселектированной информации: неселектированная информация получается как асимптотический результат усреднения селектированной информации по случайно выбранному набору информационных базисов.

Для расчета информационного обмена двух квантовых систем A и B посредством произвольных наборов квантовых состояний $\Omega_A = \{\nu_A\}$ и $\Omega_B = \{\nu_B\}$ (при условии полноты соответствующего множества информационных событий, т.е. при условии, что набор проекторов, построен-

ный на выбранном наборе квантовых состояний, образует разложение единичного оператора: $\hat{1}_{A,B} = \sum\limits_{\Omega_{A,B}} |\nu_{A,B}\rangle \langle\nu_{A,B}|$) следует рассчитать совместное распределение вероятностей, аналогичное (1.29) или (1.31):

$$P_{AB}(\nu_A, \nu_B) = \mathrm{Tr_{AB}}\left[\left(|\nu_A\rangle \langle\nu_A| \otimes |\nu_B\rangle \langle\nu_B|\right) \hat{\rho}_{AB}\right], \tag{1.33}$$

далее, аналогично (1.28) или (1.30) рассчитывается искомое количество совместимой информации:

$$\begin{aligned} I_{AB}(\Omega_A, \Omega_B) &= S_A(\Omega_A) + S_B(\Omega_B) - S_{AB}(\Omega_A, \Omega_B) = \\ &= \sum_{\Omega_A, \Omega_B} P_{AB}(\nu_A, \nu_B) \log_2 \frac{P_{AB}(\nu_A, \nu_B)}{P_A(\nu_A) P_B(\nu_B)}. \end{aligned} \tag{1.34}$$

При этом, как и в случае селектированной информации, следует отметить роль внутренней квантовой неопределенности: селекция конкретных состояний имеет смысл лишь для проведения измерения в выбранном базисе, на результаты которого в той или иной степени оказывают влияние *все* квантовые состояния, а не только выделенный набор.

1.5 Информационный анализ максимально перепутанных и сепарабельных двухкубитных каналов

Рассмотрим применение понятия совместимой информации к двухкубитному каналу, образованному системой из двух кубитов, находящейся в некоторых выделенных состояниях. Говоря о двухкубитной паре можно

иметь в виду, например, двухфотонную пару с кодированием информации в поляризационной степени свободы. Рассмотрим следующие важные двухкубитные состояния:

1) Чистые максимально перепутанные бэлловские состояния, которые соответствуют специфически квантовым корреляциям и реализуются, например, при параметрическом рассеянии света [65, 66]:

$$\Phi^{+}_{AB} = \left(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B\right)/\sqrt{2} \tag{1.35}$$

$$\Phi^{-}_{AB} = \left(|0\rangle_A |0\rangle_B - |1\rangle_A |1\rangle_B\right)/\sqrt{2} \tag{1.36}$$

$$\Psi^{+}_{AB} = \left(|0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B\right)/\sqrt{2} \tag{1.37}$$

$$\Psi^{-}_{AB} = \left(|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B\right)/\sqrt{2}. \tag{1.38}$$

2) Смешанные состояния, которые описывают корреляции, соответствующие состоянию классического бита:

$$\begin{aligned} \hat{\rho}^{mix\Phi}_{AB} &= (|0\rangle_A |0\rangle_B \langle 0|_B \langle 0|_A + |1\rangle_A |1\rangle_B \langle 1|_B \langle 1|_A)/2 \\ \hat{\rho}^{mix\Psi}_{AB} &= (|0\rangle_A |1\rangle_B \langle 1|_B \langle 0|_A + |1\rangle_A |0\rangle_B \langle 0|_B \langle 1|_A)/2. \end{aligned} \tag{1.39}$$

Матричные элементы $P(\alpha, \beta)$ для рассмотренных выше состояний (1.35—1.39), рассчитанные согласно (1.29), в произвольном информационном базисе $\{\alpha = (\theta_1, \varphi_1), \beta = (\theta_2, \varphi_2)\}$ выглядят следующим образом:

$$\begin{aligned} P^{\Phi^{\pm}}_{AB}(\alpha, \beta) &= \frac{1}{4}(1 + \cos\theta_1 \cos\theta_2 \pm \cos(\varphi_1 + \varphi_2) \sin\theta_1 \sin\theta_2) \\ P^{\Psi^{\pm}}_{AB}(\alpha, \beta) &= \frac{1}{4}(1 - \cos\theta_1 \cos\theta_2 \pm \cos(\varphi_1 - \varphi_2) \sin\theta_1 \sin\theta_2) \\ P^{mix\Phi,\, mix\Psi}_{AB}(\alpha, \beta) &= \frac{1}{4}(1 \pm \cos\theta_1 \cos\theta_2) \end{aligned} \tag{1.40}$$

Легко видеть, что для всех этих состояний $P(\alpha) = P(\beta) = 1/2$, что приводит к $S_A = S_B = 1$ при любом выборе α и β.

Сначала рассмотрим классические корреляции в этих системах, т.е. возьмем классический информационный базис $|\alpha\rangle = |\beta\rangle = |1\rangle$. При таком выборе системы коррелируют только посредством индексов ортогональных классических событий $|1\rangle$ и $|2\rangle$. Нетрудно видеть, что для всех рассматриваемых нами систем в данном информационном базисе $S_{AB} = 1$, $I_{AB} = 1 + 1 - 1 = 1$ бит, т.е. все эти системы в классическом понимании жестко скоррелированы, и знание о классическом состоянии одной системы дает достоверное знание о состоянии другой.

Далее рассмотрим произвольный информационный базис. В общем случае пространство состояний двух кубитов четырехмерно, что не позволяет показать зависимость $I_{AB}(\alpha, \beta)$ в удобном для восприятия виде. Поэтому следует сократить число степеней свободы $I_{AB}(\alpha, \beta)$ как минимум до двух. Это можно сделать несколькими способами.

Рассмотрим случай, когда информационные состояния для обеих систем равны и совпадают друг с другом: $\alpha = \beta = (\theta, \varphi)$. Двумерное пространство состояний одной системы, представленное вектором на сфере Блоха, позволяет визуально показать зависимость информации в данном случае от двух углов (θ и φ), задающих вектор общего информационного состояния. Зависимость селектированной совместимой информации $I_{AB}(\alpha = \beta)$ от этих углов для систем (1.35)—(1.39) показана на рис. 1.2.

Как частный случай здесь виден и результат предыдущего выбора информационных состояний: классический информационный базис $|\alpha\rangle = |\beta\rangle = |1\rangle$ соответствует точке $\theta = \varphi = 0$.

Среди четырех белловских состояний (1.35—1.38) сразу выделяется

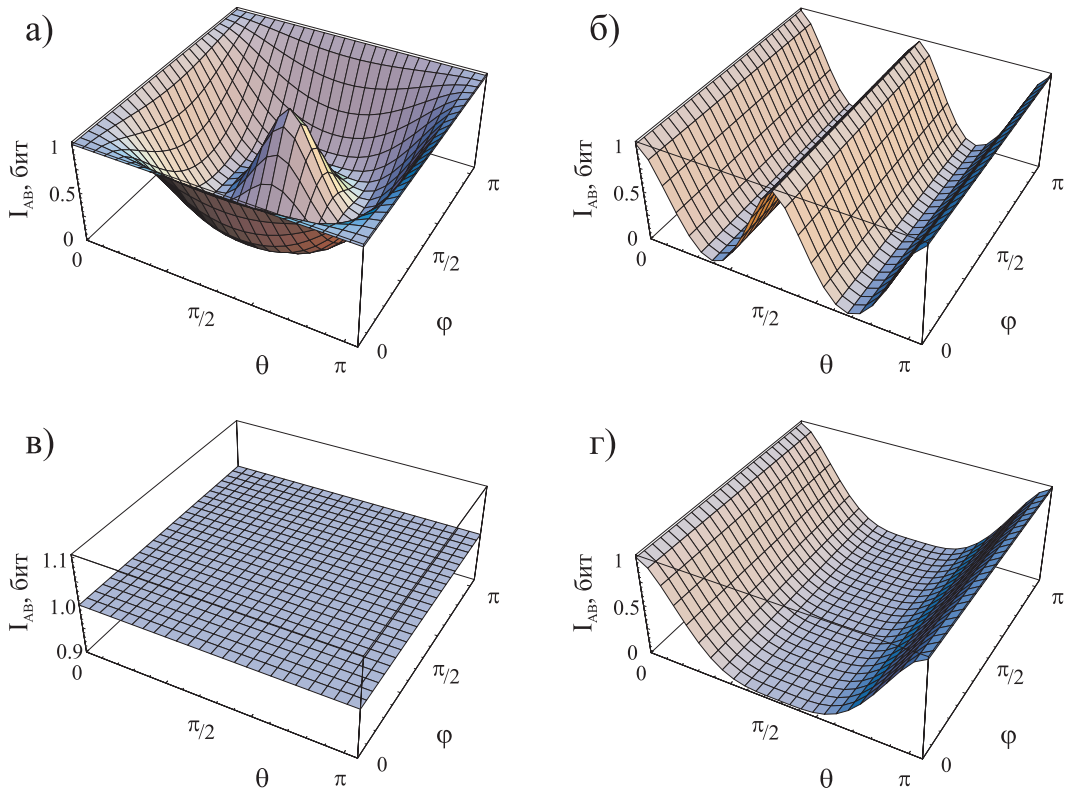


Рис. 1.2: Зависимость селектированной информации $I_{AB}(\alpha, \beta)$ в случае, когда общее информационное состояние $|\alpha\rangle = |\beta\rangle$ задано двумя углами θ и φ на сфере Блоха, для белловских состояний (три триплетных: а) $\Phi^{+}_{AB}, \Phi^{-}_{AB}$ (1.35)—(1.36), б) Ψ^{+}_{AB} (1.37) и одно синглетное в) Ψ^{-}_{AB} (1.38)) и классически коррелированного сепарабельного состояния г) $\hat{\rho}^{mix\Phi}_{AB}$ (1.39).

синглетное антисимметрическое состояние (1.38), которое инвариантно относительно вращений общего для двух систем A и B трехмерного пространства, отображаемого вращением информационного базиса $|\alpha\rangle$, $|\beta\rangle$ в пространстве состояний системы $A + B$. Эта инвариантность приводит к независимости количества информации от углов θ и φ. При любом выборе информационного состояния информация связи подсистем в антисимметрической системе равна 1, а при другом выборе информационного

базиса, когда информационные состояния систем не равны друг другу, количество информации для синглетного состояния будет зависеть только от разности углов между этими состояниями.

Для триплетных белловских состояний (1.35—1.37) информация в общем случае зависит от обоих углов θ и φ. Для триплетного состояния (1.37) зависимость $P(\alpha, \beta)$ включает в себя зависимость от углов φ_1 и φ_2 в виде $\varphi_1 - \varphi_2$, что и обуславливает отсутствие зависимости информации от азимутального угла, т.к. выбраны одинаковые информационные состояния для обеих систем, и $\varphi_1 - \varphi_2 = 0$.

Для смешанных состояний (1.39) зависимость от азимутального угла φ отсутствует уже на уровне совместной плотности распределения.

При $\theta{=}\pi/2$ информационный базис повернут так, что на сфере Блоха он перпендикулярен базису $|1\rangle, |2\rangle$. В результате для смешанных состояний (1.39) информация равна нулю, для состояний (1.37,1.38) равна 1, а для состояний (1.35,1.36) зависит от азимутального угла и периодически с периодом π по обоим углам меняется от 0 до 1.

Рассмотрим следующий тип информационного базиса, когда информационное состояние первой системы зафиксировано, например возьмем состояние $|\alpha\rangle_0 = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle)$, а второе будет произвольно меняться: $\alpha_0 = (\pi/2, \pi/2), \beta = (\theta, \varphi)$. В данном случае селектированная информация для сепарабельного состояния (1.39) равна нулю, а для всех максимально перепутанных состояний (1.35)—(1.38) зависимость селектированной информации I_{AB} от углов (θ, φ) одинакова и показана на рис. 1.3.

Отметим, что для максимально перепутанных состояний при произ-

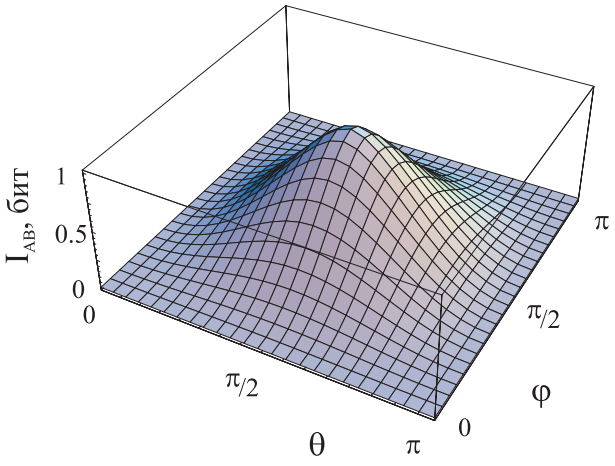


Рис. 1.3: Зависимость селектированной информации $I_{AB}(\alpha, \beta)$ от углов θ и ϕ для максимально перепутанных белловских состояний (1.35)—(1.38) в случае, когда одно информационное состояние фиксировано ($\alpha = (\pi/2, \pi/2)$), а второе произвольно меняется $\beta = (\theta, \varphi)$).

вольном выборе информационного состояния $|\alpha\rangle$ в одной системе всегда можно подобрать такое информационное состояние $|\beta\rangle$ в другой системе, что селектированная информация будет равна одному биту. Для сепарабельных состояний это не так. Здесь мы видим, что максимально перепутанные состояния более “информативны”, чем классические сепарабельные состояния, в том смысле, что они обеспечивают бóльшую скоррелированность систем, проявляющуюся в бóльшей величине селектированной информации.

Особенностью селектированной информации, как уже отмечалось выше, является ее зависимость от конкретного выбора информационных состояний для обеих подсистем A и B. В общем случае, при рассмотрении произвольных квантовых систем, это является недостатком, т.к.

такая информация учитывает скоррелированность только по некоторым выделенным состояниям, а в квантовом случае, если нет априорно выделенных состояний, все состояния должны быть равноправно представлены. Такому требованию отвечает неселектированная информация (1.30). Исследуем ее свойства на примере состояний (1.35—1.39).

Рассчитаем неселектированную информацию через соотношение (1.32) как усредненную селектированную информацию. Для смешанного состояния (1.39) после упрощений имеем:

$$I_{AB}(\theta_1,\theta_2)=\frac{1}{\ln 4}\sum_{k=1}^{2}(1+(-1)^k\cos\theta_1\cos\theta_2)\ln(1+(-1)^k\cos\theta_1\cos\theta_2). \tag{1.41}$$

Зависимость $I_{AB}(\theta_1,\theta_2)$, симметричная относительно перестановки $\theta_1 \leftrightarrow \theta_2$, показана на рис. 1.4.

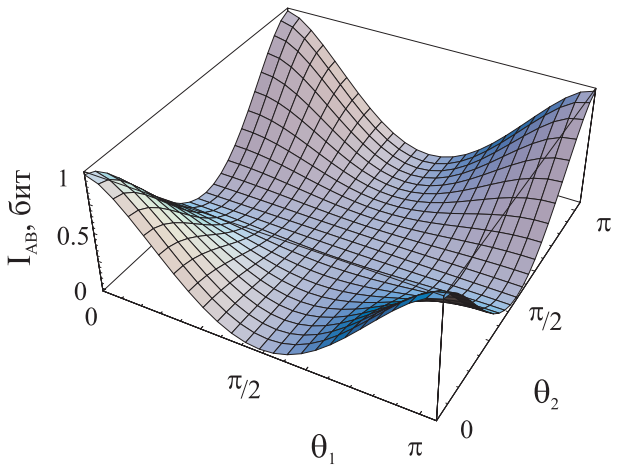


Рис. 1.4: Зависимость селектированной информации I_{AB} от полярных углов θ_1 и θ_2 для классически коррелированного состояния $\hat{\rho}_{AB}^{mix\Phi}$ (1.39).

Следует обратить внимание на то, что информация, в основном, скон-

центрирована в области малых углов θ_1 и θ_2. При $\theta_1 = \theta_2 = 0$ имеем $I_{AB} = 1$, что отражает 100% классическую корреляцию в данной системе. Усредняя селектированную информацию согласно (1.32) получаем[1]

$$I_{AB} = \int_0^{\pi} I(\theta_1, \theta_2) \frac{\sin\theta_1 \sin\theta_2}{4} d\theta_1 d\theta_2 = 1 - \frac{20 - \pi^2}{16 \ln 2} \simeq 0,087 \qquad (1.42)$$

Для состояний (1.35—1.38) неселектированная информация рассчитывается аналогично, однако выкладки несколько сложней ввиду громоздкости выражений для $I(\theta_1, \varphi_1, \theta_2, \varphi_2)$, поэтому далее приведем лишь итоговый результат:

$$I_{AB} = 1 - \frac{1}{\ln 4} \simeq 0,279, \qquad (1.43)$$

что равно максимальной величине *различимой* информации, содержащейся во всех состояниях входа при их неселективном учете [62].

Здесь мы видим существенную разницу между смешанными и перепутанными состояниями, которые при выборе классического информационного базиса $\{|0\rangle, |1\rangle\}$ дают одно и то же количество селектированной информации $I_{AB} = 1$ бит, т.е. классически эти состояния в информационном смысле неразличимы и одинаково жестко скоррелированы, но при расчете неселектированной информации дают величины 0,087 и 0,279 бит, отличающиеся в несколько раз.

Удивительный факт столь малого ($\simeq 0,087$ бит) количества неселектированной информации для системы, находящейся в смешанном состоянии и отражающей состояние классического бита, объясняется тем,

[1] Общая идея взятия подобных интегралов следующая: делаем замену переменной интегрирования ($-\sin\theta d\theta = d\cos\theta$) и все подынтегральные функции приводим к виду $F(\cos\theta)$.

что неселектированная информация равноправно учитывает информационный обмен через все квантовые состояния системы, и классические состояния $|1\rangle$ и $|2\rangle$, на которых, как видно из рис. 1.4, в основном и построена корреляция классического бита, — это всего лишь одни из них. При учете скоррелированности сразу всех состояний одной системы со всеми состояниями другой получаем однородно распределенную по всем квантовым состояниям псевдоклассическую информацию, которая равна столь малой величине. Для максимально перепутанных квантово-коррелированных систем (1.35—1.38) неселектированная информация в несколько раз больше ($\simeq 0,279$), чем для сепарабельных состояний, что обусловлено бóльшими корреляциями и было видно уже из анализа селектированной информации.

Отметим, что именно для максимально перепутанных состояний неселектированная информация достигает своей максимальной величины, т.е. именно максимально перепутанные состояния являются максимально информативными в случае отсутствия какой-либо селекции квантовых состояний. Это видно из аналогии между деквантованной волновой функций в N-мерном гильбертовом пространстве и набором вероятностей N элементарных классических событий, полученной в разделе 1.3. Неселектированная информация как усредненная селектированная соответствует усреднению по наборам информационных базисов, что в классической теории эквивалентно усреднению по наборам элементарных событий. Максимальная величина классической взаимной инфор-

мации для канала с усредненным входом равна

$$\overline{I}_N = \log_2 N - \overline{S}_N, \tag{1.44}$$

где $\overline{S}_N$ определяется соотношением (1.22). В частном случае $N = 2$, соответствующему двухкубитным каналам, из соотношения (1.18) имеем максимальную величину усредненной классической взаимной информации $\overline{I}_2 = 1 - 1/\ln 4 \simeq 0,279$, что и определяет максимально возможную величину неселектированной информации в двухкубитных каналах, примерно равную $0,279$ бит.

Для промежуточного класса состояний (от сепарабельных до максимально перепутанных) расчет неселектированной информации проведен в работах [53, 67]. Там было показано, в частности, что величина неселектированной информации монотонно растет с увеличением параметра перепутанности.

Основные результаты, представленные в этой главе, опубликованы в работе [87].

Глава 2

Информационный анализ двухкубитного канала в модели Дике

2.1 Математическое описание модели

В предыдущем разделе мы анализировали информационное содержание различных двухкубитных состояний в абстрактном виде, безотносительно природы их физической реализации. Реально же такие состояния могут возникать при взаимодействии произвольных физических квантовых систем. С информационной точки зрения физическое взаимодействие приобретает смысл обмена информацией между системами, одну из которых можно рассматривать как вход, другую как выход некоторого информационного канала связи.

Как простой, но не тривиальный, пример реализации квантового канала связи за счет взаимодействия двух физических систем рассмотрим динамику системы из двух идентичных двухуровневых атомов, находящихся на близком расстоянии друг от друга (порядка длины волны), на масштабах времени порядка обратной скорости радиационного распада одиночного атома и много больших времени межатомного запаздывания излучения. Для переходов в оптическом диапазоне это времена порядка 10^{-8} сек при расстоянии между атомами порядка 10^{-6} м.

Решение этой задачи представляется в терминах двух распадающихся со временем состояний Дике, которые являются максимально перепутанными: симметричного $||\, s \,\rangle\!\rangle = \big(|1\rangle\,|2\rangle + |2\rangle\,|1\rangle\big)/\sqrt{2}$ и антисимметричного $||\, a \,\rangle\!\rangle = \big(|1\rangle\,|2\rangle - |2\rangle\,|1\rangle\big)/\sqrt{2}$, двухфотонного верхнего состояния $||\, 2 \,\rangle\!\rangle = |2\rangle\,|2\rangle$ и стабильного вакуумного состояния $||\, v \,\rangle\!\rangle = |1\rangle\,|1\rangle$ [68, 80]. Для произвольного чистого начального состояния системы вида

$\Psi_{AB}(0) = \Psi_A \otimes \Psi_B$ имеем:

$$\Psi_{AB}(t) = c_s(t) \,||\, s \,\rangle\!\rangle + c_a(t) \,||\, a \,\rangle\!\rangle + c_2(t) \,||\, 2 \,\rangle\!\rangle + c_v(t) \,||\, v \,\rangle\!\rangle, \qquad (2.1)$$

где $c_s(t), c_a(t), c_2(t), c_v(t)$ — комплексные амплитуды соответствующих состояний:

$$\begin{aligned} c_s(t) &= c_s(0) e^{-(\gamma_s/2 + i\Lambda)t}, \\ c_a(t) &= c_a(0) e^{-(\gamma_a/2 - i\Lambda)t}, \\ c_2(t) &= c_2(0) e^{-2\gamma t}, \\ c_v(t) &= c_v(0) + \sqrt{c_s^2(0) + c_a^2(0) + c_2^2(0) - c_s^2(t) - c_a^2(t) - c_2^2(t)}\, e^{i\xi(t)}. \end{aligned} \qquad (2.2)$$

Комплексная амплитуда $c_v(t)$ вакуумной компоненты $||\, v \,\rangle\!\rangle$ включает некогерентную добавку $e^{i\xi(t)}$, обусловленную спонтанными радиационными переходами с возбужденных атомных состояний, где $\xi(t)$ — равномерно распределенная фаза атомных колебаний.

Ограничимся лишь случаем двух идентичных атомов с параллельными дипольными моментами, направленными перпендикулярно вектору, соединяющему рассматриваемые атомы. В этом случае существенны только два безразмерных параметра: время γt, где γ описывает скорость радиационного распада изолированного атома, и межатомное расстояние $\varphi = k_0 R$, где R — расстояние между атомами и k_0 — модуль волнового вектора, соответствующего частоте перехода изолированного атома. Безразмерные двухатомные скорости радиационного распада $\gamma_{s,a}$ и частотного сдвига Λ за счет короткодействующего диполь-дипольного взаимодействия описываются следующими соотношениями:

$$\frac{\gamma_{s,a}}{\gamma} = 1 \pm g, \quad \frac{\Lambda}{\gamma} = \frac{3}{4\varphi^3}, \quad g = \frac{3}{2}\Big(\frac{\sin\varphi}{\varphi} + \frac{\cos\varphi}{\varphi^2} - \frac{\sin\varphi}{\varphi^3}\Big). \qquad (2.3)$$

Из соотношений (2.3) следует, что на расстоянии, меньшем, чем длина волны, зависимость g от φ слабая и $g \approx 1$. При $\varphi \to 0$ получаем $\gamma_a \to 0$, что обеспечивает долгое время жизни антисимметричной компоненты Дике $||\, a \,\rangle\!\rangle$. Симметричная компонента $||\, s \,\rangle\!\rangle$ быстро распадается, поэтому в области малых φ при больших временах основную роль играет антисимметричная компонента $||\, a \,\rangle\!\rangle$.

Матрица плотности $\hat{\rho}_{AB}$ квантового канала связи, образуемого двумя атомами, получается усреднением по флуктуациям фазы чистого двухатомного состояния (2.1), представленным переменной $\xi(t)$. Начальные значения комплексных амплитуд $c_a(0)$, $c_s(0)$, $c_2(0)$, $c_v(0)$ определяются из начального состояния двухатомной системы. Если состояние системы изначально представляет собой некогерентную смесь, то следует также провести усреднение по когерентным составляющим этой смеси. В результате получаем решение задачи Дике в виде соответствующей матрицы плотности

$$\hat{\rho}_{AB} = \hat{\rho}_{AB}[\gamma t, \varphi, \hat{\rho}_A(t=0), \hat{\rho}_B(t=0)], \tag{2.4}$$

рассматриваемой в следующем разделе.

2.2 Анализ соотношения между информационными характеристиками и физическими наблюдаемыми величинами

Перейдем к анализу решения задачи Дике (2.4) с точки зрения обмена совместимой информацией между атомами. В данной задаче нет выделенных априори информационных переменных, поэтому наиболее адекватной информационной характеристикой является неселектированная информация. На основе формул (1.30) и (2.1) рассчитаем и проанализируем зависимости неселектированной информации I_{AB} от обезразмеренных времени γt и расстояния φ, а также от начальных условий $\hat{\rho}_A(t=0), \hat{\rho}_B(t=0)$.

Зависимости I_{AB} от γt и φ, полученные при различных начальных состояниях первого атома и основном начальном состоянии второго, идентичны на качественном уровне, но отличаются абсолютными величинами информации. Поэтому ограничимся рассмотрением зависимости лишь для случая чистого начального состояния $|2\rangle$ первого атома и состояния $|1\rangle$ для второго. В этом случае информация достигает максимально возможного значения $\simeq 0,279$ бит. Результаты расчетов представлены на рис. 2.1.

Видно, что зависимость I_{AB} от γt и φ носит осцилляционный характер, обусловленный короткодействующим диполь-дипольным взаимодействием. Характер изменения информации и ее максимальная и

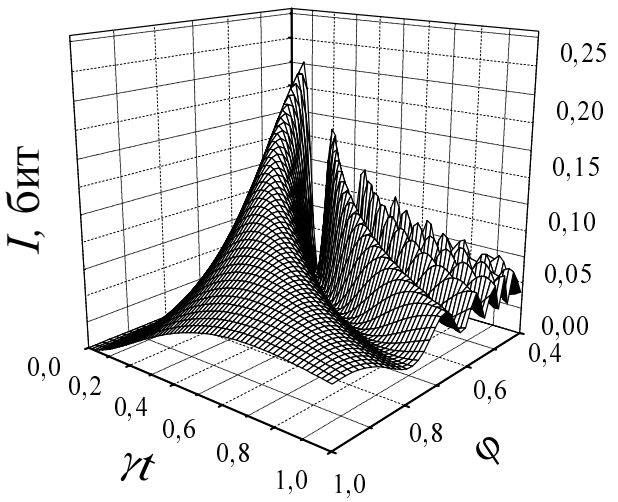


Рис. 2.1: Зависимость неселектированной информации I от безразмерных времени γt и расстояния φ. Первый атом в начальный момент времени находится полностью в верхнем состоянии $|2\rangle$, а второй — в нижнем $|1\rangle$.

минимальная величины проявляются в области изменения параметров $0 \leq \gamma t < 1,\ 0,4 < \varphi < 1$. При $\varphi \to 0$ наблюдается характерное увеличение частоты осцилляций. Для видимого диапазона энергии квантов нижняя граница R примерно соответствует масштабу 1 Å, до которого не имеет смысла учитывать обменное взаимодействие.

При $\gamma t = 0$ имеем $I_{AB} = 0$, так как атомы в начальный момент времени рассматриваются независимыми, т.е. $\hat{\rho}_{AB} = \hat{\rho}_A \otimes \hat{\rho}_B$. С течением времени информация возрастает до некоторого максимального значения, зависящего от начального состояния первого атома, а затем, осциллируя, стремится к нулю. Чем меньше расстояние между атомами, тем большее значение информации может быть достигнуто на первом периоде колебаний информации и тем дольше она будет убывать. Максимальное значе-

ние $\simeq 0,279$ бит асимптотически достигается в области малого времени и расстояния и соответствует величине неселектированной информации для полностью перепутанных подсистем (1.43), или величине *доступной* информации. На малых расстояниях информация очень долго остается ненулевой (при $\varphi \to 0$ и больших γt получаем $I_{AB} \to 0,053$ бит), что обусловлено долгоживущей компонентой Дике.

Такая зависимость отражает физическую картину процесса излучения одного атома в присутствии другого. При малых межатомных расстояниях для долгоживущей компоненты фотон долго не может уйти из атомной системы, переходя от одного атома к другому, создавая перепутанное состояние системы. Поэтому информация быстро достигает величины, близкой к максимально возможной ($\simeq 0,279$ бит), соответствующей максимально перепутанным состояниям. Понятно, что степень перепутанности будет зависеть от начальной разности населенностей одного атома. Чем больше населенность верхнего уровня первого атома в начальный момент времени, тем более "перепутанными" могут стать атомы и тем большая может получиться величина совместимой информации. Однако, со временем фотон все-таки излучается в вакуум, и атомы переходят в основное состояние, становясь при этом независимыми. Поэтому информация асимптотически стремится к нулю при $\gamma t \to \infty$. По отношению к этому пределу поведение совместимой и когерентной информации идентичны [68]. Однако, когерентная информация присутствует лишь на временах существования обеих компонент Дике (симметричной и антисимметричной), в то время как совместимая существует до

тех пор, пока существует долгоживущая антисимметричная компонента.

В дополнение к рассмотренной выше зависимости интересно рассмотреть также случай, когда начальное состояние первого атома выбрано в виде некогерентной смеси при той же разности населенностей, что и для чистого состояния. Зависимость информации I_{AB} от начальной разности населенностей $n = n_2 - n_1$ первого атома для случая смешанного и чистого его начального состояния при фиксированных значениях времени и расстояния $(\gamma t = 0,2, \varphi = 0,4)$ приведена на рис. 2.2. Видно, что в случае смешанного начального состояния информация немного меньше, чем в случае чистого при той же разности населенностей. Однако на характер зависимости I_{AB} от γt и φ эта разница не влияет.

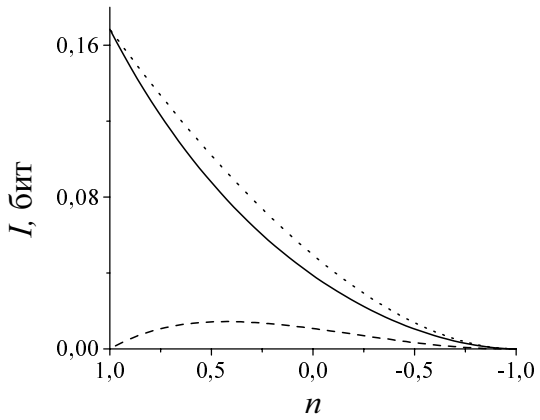


Рис. 2.2: Зависимость неселектированной информации I от разности населенностей n первого атома для $\gamma t = 0.2, \varphi = 0.4$. Сплошная линия — начальное состояние первого атома выбрано в виде равновероятной некогерентной смеси верхнего и нижнего уровней; пунктирная — в виде чистого равновероятного суперпозиционного состояния; штриховая — разность этих зависимостей.

При рассмотрении возбужденных начальных состояний обоих атомов основной интерес представляет зависимость информации от начального состояния атомов при фиксированном времени и расстоянии, так как характер пространственно-временной зависимости уже известен. Рассматривался случай начально независимых атомов, приготовленных в чистом состоянии $\Psi_{AB}(0) = \Psi_A \otimes \Psi_B$. Согласно (2.1), состояние системы $\Psi_{AB}(t)$ и соответствующая ему совместимая информация в этом случае зависят от двух параметров — разностей населенностей n_A и n_B индивидуальных состояний атомов. Результаты расчетов приведены на рис. 2.3.

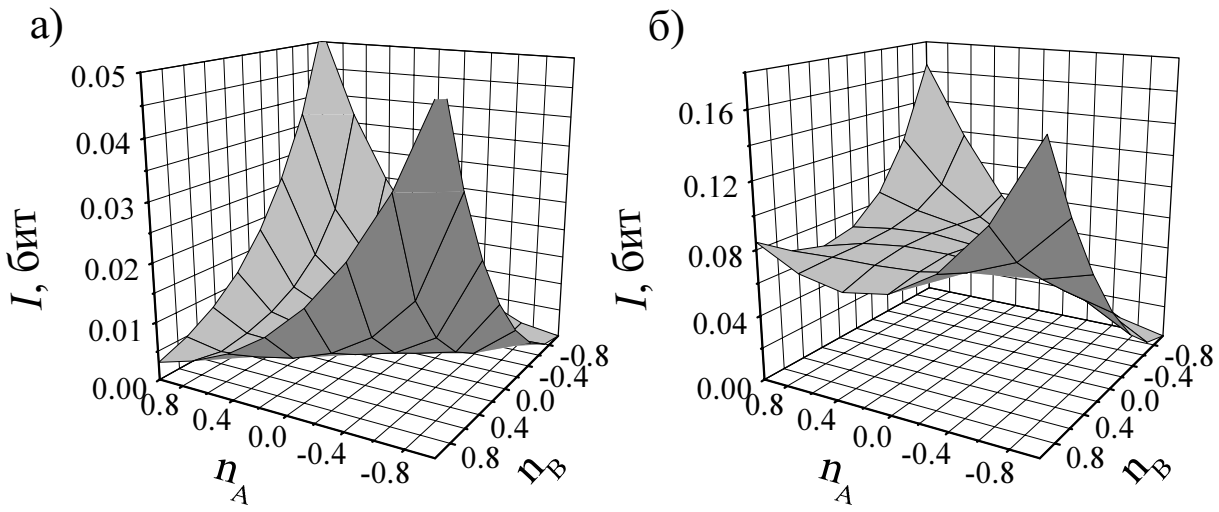


Рис. 2.3: Зависимость неселектированной информации I от разностей населенностей n_A и n_B двух атомов: $\varphi = 1$, $\gamma t = 1$ (а); $\varphi = 0.4$, $\gamma t = 0.2$ (б).

Зависимости неселектированной информации I_{AB} от разностей населенностей n_A и n_B обоих атомов при фиксированных γt и φ имеют максимальные значения в крайних точках осей графиков, когда один из

атомов полностью находится в нижнем состоянии, а другой полностью в верхнем. Эта зависимость симметрична относительно перестановки атомов местами, т.е. графики на рис. 2.3 имеют плоскость симметрии. Минимальное значение, равное нулю, информация имеет лишь для вакуумного состояния атомной системы. В центре графика зависимость в общем случае немонотонна.

На рис. 2.3,а время и расстояние выбраны достаточно большими: $\varphi = 1, \gamma t = 1$ для того, чтобы показать влияние антисимметричной компоненты Дике на величину совместимой информации. В плоскости симметрии графика антисимметричная компонента Дике отсутствует, а на краях она, наоборот, максимальна, что следует из самого определения антисимметричной компоненты. При выбранных параметрах ($\varphi = 1, \gamma t = 1$) короткоживущая симметричная компонента Дике быстро распадается и информация определяется в основном антисимметричной компонентой. В результате информация на краях и в центре графика отличается примерно на порядок.

На рис. 2.3,б ($\varphi = 0,4, \gamma t = 0,2$) видно, что зависимость совместимой информации от разности населенностей немонотонна. В частности, если атомы одинаково возбуждены, то информация по мере уменьшения разности населенностей сначала уменьшается, затем увеличивается, а затем снова уменьшается.

Для выявления характерных особенностей, незаметных на трехмерных графиках, следует рассмотреть срезы этих графиков в двух плоскостях — плоскости симметрии и перпендикулярной ей плоскости. Физи-

чески это соответствует одинаковой разности населенностей обоих атомов (срез по плоскости симметрии) и фиксированной сумме разностей населенностей (срезы в плоскостях, перпендикулярных плоскости симметрии). Результаты расчетов представлены на рис. 2.4

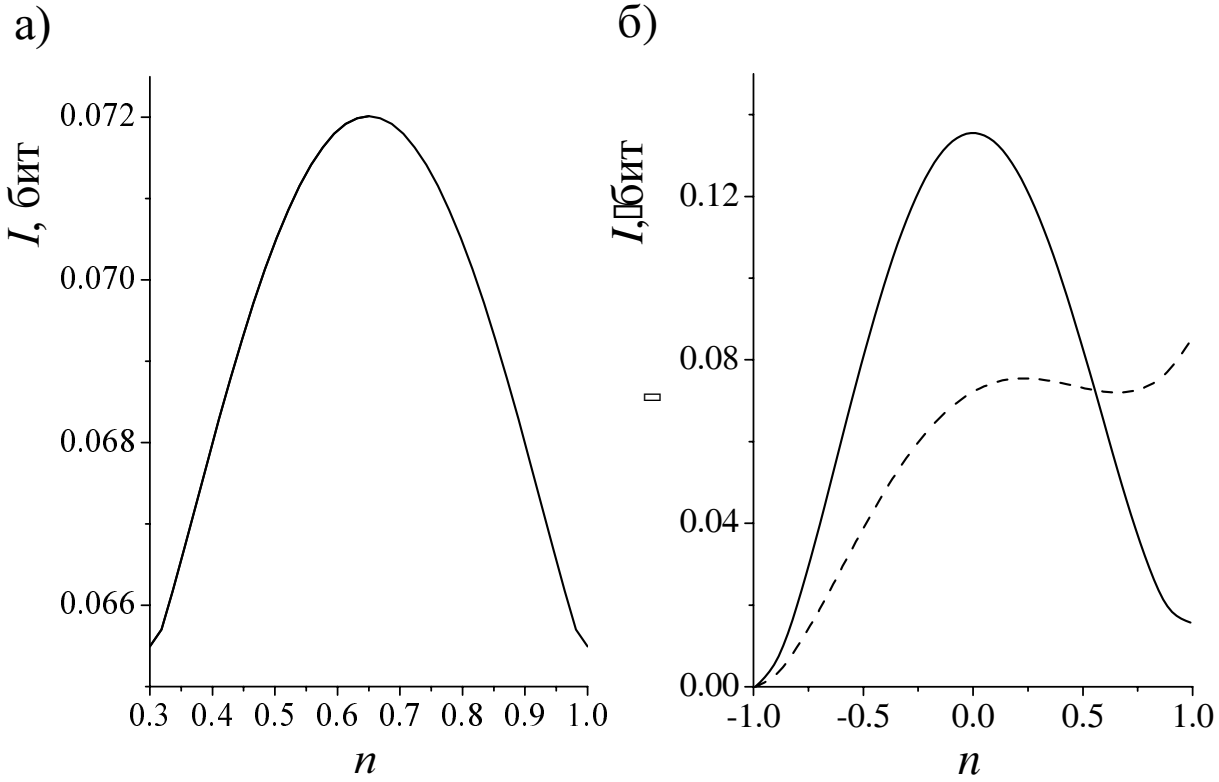


Рис. 2.4: Зависимость неселектированной информации I от разности населенностей n одного атома: суммарная разность населенностей двух атомов фиксирована: $n_A + n_B = 1.3$ при $\varphi = 0.4$, $\gamma t = 0.2$ (рис. 2.4,а) и разность населенностей n у обоих атомов одинакова при $\varphi = 0.25424$, $\gamma t = 0.01695$ (сплошная линия) и $\varphi = 0.4$, $\gamma t = 0.2$ (штриховая линия) (рис. 2.4,б).

Интересно отметить тот факт, что при максимально возбужденных атомах информация тем не менее не достигает экстремальных значе-

ний. Вообще, если атомы одинаково возбуждены и рассматривается одномерная зависимость от разности населенностей одного атома, то эта зависимость немонотонна (рис. 2.4,б). При различных параметрах φ и γt максимум достигается в разных точках, и характер зависимости также может быть различным: может существовать как один локальный максимум, так и два. Это объясняется интерференцией двух компонент, дающих ненулевой вклад в информацию, — симметричной компоненты Дике $||\, s \,\rangle\rangle$ и двухфотонного верхнего состояния $||\, 2 \,\rangle\rangle$.

Исследуя зависимость информации от разности населенностей одного атома при фиксированной суммарной разности населенностей обоих атомов (срез графика на рис. 2.3 в плоскости, перпендикулярной плоскости симметрии графика), отметим, что почти всегда информация растет с увеличением различия в разностях населенностей атомов. Этот факт объясняется тем, что, если атомы имеют одинаковую разность населенностей, то в состоянии такой симметричной системы отсутствует долгоживущая антисимметричная компонента Дике, дающая основной вклад в информацию на больших временах. Если же атомы сильно отличаются своими начальными условиями, то антисимметричная компонента, наоборот, ярко выражена, и информация может достичь своих максимальных значений. Однако это справедливо не всегда, например, график на рис. 2.4,а показывает, что информация в случае идентичных состояний атомов (центр графика) может быть немного больше, чем в случае различных разностей населенностей. Такой характер зависимости может существовать только в течение малого времени вследствие влияния ко-

роткоживущей симметричной компоненты Дике.

В заключение интересно сравнить полученную картину обмена совместимой информацией с картиной обмена когерентной информацией, рассчитанной в работах [68, 69]. Полученные зависимости позволяют выявить качественное различие физического содержания когерентной и совместимой информации. В данной системе из двух двухуровневых атомов оно оказывается существенно связанным с качественно различной ролью коллективных возбуждений системы — состояний Дике — в формировании двух данных типов квантовой информации. Ненулевая совместимая информация, как видно из полученных здесь расчетов, связана с наличием любого возбуждения в системе, в то время как когерентная информация не равна нулю, лишь если присутствуют обе компоненты Дике. С физической точки зрения это проявляется в разных временах жизни когерентной и совместимой информации: время жизни совместимой информации определяется долгоживущей антисимметричной компонентой, а время жизни когерентной информации — короткоживущей симметричной.

Результаты, представленные в этой главе, опубликованы в работах [80, 86, 87].

Глава 3

Информационный анализ квантовых каналов в задачах квантовой криптографии

3.1 Принцип некопируемости квантовой информации

С момента появления идеи квантовой криптографии (КК) [28] до настоящего времени было предложено несколько протоколов, реализующих ее [30–33]. Все они основаны на принципе неклонируемости произвольных квантовых состояний [26], благодаря которому невозможно создать наряду с оригиналом точную копию произвольного сообщения, передаваемого по квантовому каналу, если в качестве букв для него используются взаимно неортогональные состояния некоторого квантового носителя информации, например, фотона.

Под клонированием понимается такое действие некоторого устройства над неизвестным заранее состоянием, а, точнее, над физической системой A, находящейся в этом состоянии, после которого само состояние останется неизменным и дополнительно появится его *точная копия*[1] в форме независимого состояния другой физической системы B. Иными словами, клонирующее устройство создает информационный *клон* произвольного квантового состояния.

Можно показать, что такое клонирование, вообще говоря, невозможно. Действительно, рассмотрим клонирование двух произвольных квантовых состояний $|\Phi\rangle_A$ и $|\Psi\rangle_A$. Начальное состояние объекта, куда должно

[1] Если на выходе копирующего устройства будут два одинаковых состояния, не являющихся точными копиями исходного состояния, но наиболее близко отстоящих от него, то такое устройство называется оптимальной копирующей (или клонирующей) машиной [78].

быть клонировано неизвестное входное состояние, можно обозначить как $|0\rangle_B$, конечное — как $|\Psi\rangle_B$ и $|\Phi\rangle_B$. Преобразование клонирования

$$\begin{aligned} |\Phi\rangle_A |0\rangle_B &\to |\Phi\rangle_A |\Phi\rangle_B, \\ |\Psi\rangle_A |0\rangle_B &\to |\Psi\rangle_A |\Psi\rangle_B \end{aligned} \tag{3.1}$$

можно считать унитарным, т.к. если бы оно являлось неунитарным, то это соответствовало бы дополнительному усреднению по некоторым переменным, которые можно считать принадлежащими клонирующему устройству, и, с учетом преобразования этих переменных, клонирование было бы унитарным преобразованием.

Исходя из сохранения углов при унитарном преобразовании, можем записать:

$$\langle\Phi|\Psi\rangle_A = \langle\Phi|\Psi\rangle_A \langle\Phi|\Psi\rangle_B . \tag{3.2}$$

Это возможно лишь в двух ситуациях: либо при $\langle\Phi|\Psi\rangle_A = 0$ или $\langle\Phi|\Psi\rangle_A = 1$, что соответствует ортогональному, классическому набору входных состояний, либо при $\langle\Phi|\Psi\rangle_B = 1$, что соответствует независимости выходных переменных клонированной системы B от самого клонируемого состояния. Таким образом получаем, что клонирование произвольного квантового состояния из неортогонального набора невозможно.

В отношение копирования информации можно сделать и более сильное утверждение, чем запрет на клонирование произвольных квантовых состояний: можно показать, что точную информационную копию произвольного квантового состояния не только нельзя *создать*, но она вообще в принципе *не существует*.

Рассмотрим потенциально возможные корреляции двух квантовых систем A и B посредством некоторого ансамбля событий $\{|\alpha\rangle\}$, пронумерованных классическими индексами $\alpha \in \Omega$. Абстрагируясь от самой процедуры клонирования как создания нового квантового состояния, рассмотрим какие вообще ограничения существуют для взаимных корреляций двух квантовых систем.

Если мы говорим, что одна система A *точно копирует* другую систему B каким-либо набором событий $\{|\alpha\rangle\}$, то это означает полную эквивалентность систем во всех возможных результатах их измерения в данном наборе событий. Например в классическом случае, рассмотренном в разделе 1.2, в принципе можно рассматривать случай *точного* угадывания выпадения монетки, когда одна система точно копирует другую.

Точностью копирования можно считать среднее значение квадрата разности проекторов $|\alpha\rangle_A \langle\alpha|_A \otimes \hat{1}_B$ и $\hat{1}_A \otimes |\alpha\rangle_B \langle\alpha|_B$, как индикаторов события $|\alpha\rangle$ в первой и второй системах. Математически это можно записать с помощью оператора копирования

$$\hat{C}_{AB} = \sum_{\alpha\in\Omega} (|\alpha\rangle_A \langle\alpha|_A \otimes \hat{1}_B - \hat{1}_A \otimes |\alpha\rangle_B \langle\alpha|_B)^2. \tag{3.3}$$

Для классического совместимого набора событий, представленного ортогональным набором состояний $|\alpha\rangle = |k\rangle$, этот оператор равен нулю на пространстве скопированных состояний вида $|k\rangle_A |k\rangle_B$, что показывает возможность точного копирования в классических системах:

$$\hat{C}_{AB} |k\rangle_A |k\rangle_B = 0. \tag{3.4}$$

В случае, когда рассматривается копирование несовместимого набора

событий, оператор копирования уже не равен нулю ни для каких состояний системы $A + B$. Для случая, когда рассматривается копирование сразу всех состояний гильбертова пространства, оператор копирования принимает вид

$$\hat{C}_{AB} = \int (|\alpha\rangle_A \langle\alpha|_A \otimes \hat{1}_B - \hat{1}_A \otimes |\alpha\rangle_B \langle\alpha|_B)^2 d^2V_\alpha, \tag{3.5}$$

где dV_α — дифференциал объема гильбертова пространства. В этом случае для $\hat{C}_{AB}$ существует аналитическое представление в виде разложения по проекторам на перепутанные состояния (1.35—1.38) [64]:

$$\begin{aligned}\hat{C}_{AB} = 2\Bigg[\frac{1}{3}\left(\left|\left|\, \Psi^+ \right\rangle\right\rangle \left\langle\left\langle \Psi^+ \right|\right|\right. + \left|\left|\, \Phi^- \right\rangle\right\rangle \left\langle\left\langle \Phi^- \right|\right| + \left|\left|\, \Phi^+ \right\rangle\right\rangle \left\langle\left\langle \Phi^+ \right|\right|\right) + \\ + \left|\left|\, \Psi^- \right\rangle\right\rangle \left\langle\left\langle \Psi^- \right|\right|\Bigg],\end{aligned} \tag{3.6}$$

откуда следует, что минимальное значение его равно $2/3$, т.е. ни при каких состояниях системы AB одна ее часть не может копировать другую в том смысле, что *не существует* таких двухчастичных состояний $\hat{\rho}_{AB}$, что для любого измерения одной части двухчастичной системы результат такого же измерения второй ее части будет в точности таким же, как и первой.

Таким образом, можно говорить не только о неклонируемости квантовых состояний, как запрета на создание информационного клона, но и о некопируемости квантовой информации, как принципиального запрета на его существование.

Однако, при рассмотрении антикорреляций в системах A и B, т.е. одновременного осуществления события $|\alpha\rangle$ в системе A и ортогональ-

ного ему события $|\tilde{\alpha}\rangle$ в системе B, можно обнаружить возможность точного *антикопирования* в антисимметричном синглетном состоянии вида $||\,\Psi^-\,\rangle\!\rangle_{AB} = (|1\rangle_A|2\rangle_B - |2\rangle_A|1\rangle_B)/\sqrt{2}$, для которого антикорреляции равны нулю:

$$\hat{A}_{AB}\,||\,\Psi^-\,\rangle\!\rangle_{AB}\,\langle\!\langle\,\Psi^-\,||_{AB} = 0, \tag{3.7}$$

где оператор антикопирования определяется как

$$\hat{A}_{AB} = \int (|\alpha\rangle_A\langle\alpha|_A \otimes \hat{1}_B - \hat{1}_A \otimes |\tilde{\alpha}\rangle_B\langle\tilde{\alpha}|_B)^2 d^2V_\alpha. \tag{3.8}$$

Тем не менее, наличие такого антикопирования нельзя свести к обычному копированию в силу неунитарности преобразования $|\alpha\rangle \to |\tilde{\alpha}\rangle$, переводящего каждое квантовое состояние в соответствующее ему ортогональное. Кроме того, операция антиклонирования

$$|\Phi\rangle_A|0\rangle_B \to |\Phi\rangle_A|\tilde{\Phi}\rangle_B \tag{3.9}$$

также невозможна, что доказывается аналогично невозможности клонирования (3.1).

Физически ситуация антикопирования реализуется, например, при распаде частицы с нулевым спином на две частицы со спином $1/2$, когда образуется антисимметричное спиновое состояние. Получается, что спин одной частицы антикопирует спин другой в том смысле, что при измерении проекции спина одной частицы на какую-либо ось проекция спина другой частицы на эту же ось будет в точности противоположной.

На информационном языке наличие 100%-х корреляций, не только при копировании или при антикопировании, а при произвольном соот-

ветствии событий $|\alpha\rangle_A$ в одной системе событиям $|f(\alpha)\rangle_B$ в другой системе, означало бы равенство совместимой информации одному биту при соответствующем подборе информационного базиса: $I_{AB}(\alpha, f(\alpha)) = 1$. В разделе 1.5 мы видели, что для максимально перепутанных состояний всегда можно подобрать такой информационный базис, что совместимая информация равна одному биту. В этом смысле максимально перепутанные состояния хоть и не обеспечивают точное *копирование* квантовой информации, но, тем не менее, задают 100%-е корреляции при определенном взаимном отображении элементарных событий в двух квантовых системах.

3.2 Основные принципы квантовой криптографии

Напомним основные шаги стандартных протоколов КК, используя общепринятую терминологию [24, 36]: Алиса — передатчик информации, Боб — приемник и Ева — подслушиватель. Различные протоколы КК имеют похожие алгоритмы работы и фактически отличаются лишь своими алфавитами, т.е. наборами квантовых состояний, играющих роль букв, из которых строится сообщение.

Первый шаг состоит в выборе алфавита, т.е. в кодировании классической информации, которую Алиса хочет передать Бобу, квантовыми состояниями, при этом логической паре битов “0” и “1” сопоставляется набор из нескольких взаимно неортогональных друг другу, но внутренне

ортогональных, пар состояний. Так, например, в первом протоколе KK, названном по имени создателей BB84, алфавит состоит из четырех состояний: $\{|0\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. Здесь первые два состояния могут кодировать “0”, а вторые два — “1”:

$$\text{“0”} \rightarrow \left[\begin{array}{l} |0\rangle \\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \end{array} \right. , \qquad \text{“1”} \rightarrow \left[\begin{array}{l} |1\rangle \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array} \right. \tag{3.10}$$

Для кодирования конкретного бита в передаваемом сообщении конкретное состояние выбирается из этого набора случайно, например, строке классических битов

$$\text{“0,} \quad 0, \quad 0, \quad 1, \quad 1, \quad 1\text{”} \tag{3.11}$$

может соответствовать последовательность состояний

$$\text{“}|0\rangle, \quad \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |0\rangle, \quad \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \quad \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \quad |1\rangle\text{”}. \tag{3.12}$$

Закодированную случайным образом последовательность битов Алиса отправляет Бобу. Для извлечения классической информации Боб измеряет полученное состояние в базисе, случайно выбранном из общего с Алисой алфавита, и по результату измерения восстанавливает передаваемый классический бит. В случае, если он угадал “правильный” базис, т.е. измерил состояние в том базисе, в котором оно было закодировано, то он должен безошибочно восстановить классический бит. В случае же “неугадывания” вероятность правильного восстановления классического бита равна 1/2 (для рассматриваемого протокола BB84). Таким образом

на стороне Боба формируется так называемый “сырой ключ” (от англ. “raw key”) — последовательность классических битов, в котором неизбежно будут ошибки.

Далее выполняется процедура согласования базисов: сообщая по открытому классическому каналу, в каком именно базисе проводилось измерение (но не сообщая его результат), Алиса и Боб отберут только ту часть сообщений, для которой Боб “угадал” базис. В полученном “просеянном” ключе данные на стороне Алисы и Боба должны совпадать, т.к. наличие взаимно неортогональных состояний гарантирует невозможность незаметного подслушивания. Однако, реально всегда есть дополнительные ошибки, связанные с естественными шумами в канале передачи, с несовершенством оборудования и т.п. Поэтому, после получения просеянного ключа, Алиса и Боб выполняют дополнительные классические процедуры коррекции ошибок и усиления безопасности [36].

Общей чертой всех протоколов КК является наличие некоторого критического уровня ошибок, которые могут быть исправлены с помощью методов коррекции ошибок и усиления безопасности, и до которого протокол гарантирует возможность установления секретного сообщения. Наличие этого критического уровня ограничивает дальность секретной передачи данных из-за наличия естественных шумов в канале передачи. В настоящее время максимальная дальность секретной передачи данных по открытому воздуху составляет порядка 100 километров [70].

Одной из целей разработки новых протоколов КК является увеличение критического уровня ошибок, что делает протокол более помехоза-

щищенным и устойчивым как против потенциальных атак подслушивателя, так и против естественных шумов в экспериментальной установке и информационном канале, что позволит осуществить секретную передачу данных на большие расстояния. Увеличение критического уровня ошибок можно достичь варьированием как алфавита, так и размерности пространства состояний. Широко распространено мнение (хотя и не доказанное), что в двумерном случае наивысшим критическим уровнем ошибок обладает протокол с алфавитом из трех взаимно-несмещённых базисов — протокол six–state, или *шестибуквенный* протокол [32, 71, 72]. Дальнейшее увеличение критического уровня ошибок обычно связывается только с увеличением размерности пространства состояний [73–75].

Тем не менее, рассмотрим вопрос о возможностях увеличения критического уровня ошибок выше уровня шестибуквенного протокола только за счет варьирования алфавита в двумерном гильбертовом пространстве.

Заметив, что набор букв шестибуквенного протокола образует октаэдр на сфере Блоха[2], мы рассмотрим алфавиты, буквы которых образуют остальные правильные многогранники на сфере Блоха: тетраэдр, куб, икосаэдр и додекаэдр, имеющие 4,8,12 и 20 вершин соответственно, и, как предельный случай многогранника с бесконечным числом вершин, континуальный алфавит, равноправно включающий все квантовые состояния.

Протоколы, использующие такие алфавиты, повторяют все основные шаги стандартных протоколов КК, например протокола BB84 [28] (фор-

[2]В некоторых работах сфера Блоха называется также сферой Пуанкаре [76].

мирование сырого ключа, согласование базисов, усиление безопасности и т.д.). Некоторыми особенностями будут обладать только протокол с континуальным алфавитом (что будет обсуждено в разделе 3.3) и протокол с алфавитом в виде тетраэдра (раздел 3.4). В остальном информационный анализ этих протоколов можно выполнить по стандартной схеме, основанной на расчете совместимой информации в двухчастичных подсистемах трехчастичной системы Алиса–Ева–Боб [36].

3.3 Специфика протокола с континуальным алфавитом

С практической точки зрения основное отличие протокола с континуальным алфавитом от протоколов с дискретным алфавитом заключается в процедуре согласования базисов. Для дискретных алфавитов выполняется точное согласование базисов, т.е. Алиса и Боб отбирают только ту часть сообщений, для передачи и приема которой они использовали одинаковые базисы. Для континуального алфавита процедуру точного согласования базисов выполнить невозможно, т.к. количество информации о точке из континуума равно бесконечности. Поэтому для континуального алфавита мы предлагаем проводить *приблизительное* согласование базисов. Для этого разобьем все пространство состояний на несколько одинаковых, возможно даже частично перекрывающих друг друга областей с приблизительно одинаковыми состояниями, и при согласовании базисов будем передавать информацию о номере области, которой при-

надлежит базис. Будем считать базисы совпавшими, если они попали в одну и ту же область. В случае взаимного перекрытия областей возможна ситуация, когда базис принадлежит сразу нескольким областям. В такой ситуации конкретный номер области выбирается из них случайно.

Понятно, что в отобранных сообщениях после приблизительного согласования базисов будут дополнительные (по сравнению с точным согласованием базисов) ошибки, связанные с ненулевой проекцией вектора состояния, кодирующего сообщение "0" в одном базисе $\{|\nu\rangle, |\tilde{\nu}\rangle\}$, на вектор состояния, кодирующий сообщение "1" в другом базисе $\{|\mu\rangle, |\tilde{\mu}\rangle\}$, даже если эти базисы попали в одну и ту же область. Для уменьшения этих ошибок области согласования базисов должны включать в себя минимально отличающиеся друг от друга состояния. В случае равномерного заполнения сферы Блоха (с учетом неравномерности дифференциала объема) такому требованию отвечают круглые области.

Далее встает вопрос об оптимальном покрытии сферы одинаковыми круглыми областями, т.е. таком покрытии, при котором используется минимальное число кругов, или, возможно, каких-либо других правильных фигур, с минимальными взаимными перекрытиями. Сейчас мы не будем точно решать эту задачу, а будем для простоты рассматривать покрытие цилиндрической проекции сферы. Будем считать, что $4N^2$ кругами с угловым радиусом $\pi/2N$ заведомо можно покрыть всю сферу с единичным радиусом (рис. 3.1а), что соответствует $2N^2$ областей при согласовании базисов.

На рис. 3.1б приведен еще один вариант покрытия цилидрической

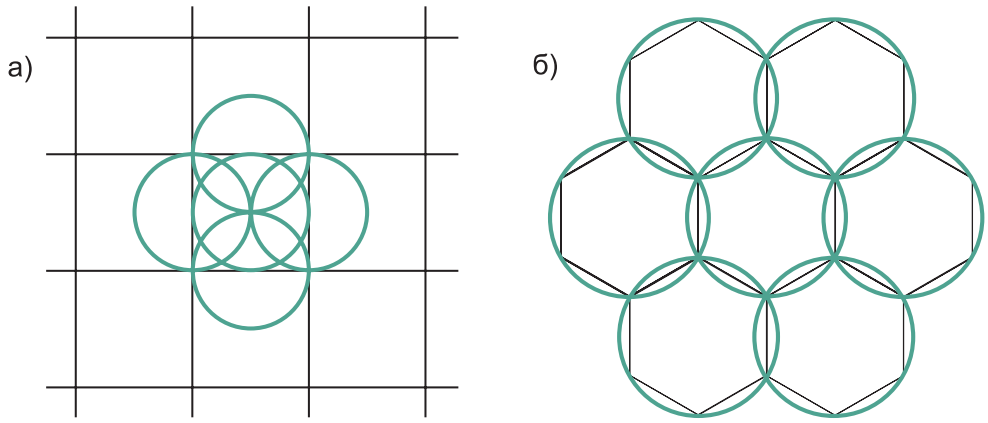


Рис. 3.1: Варианты покрытия плоскости круглыми областями.

проекции сферы, который несколько более оптимален, чем предыдущий. Оба варианта далеки от оптимальности при достаточно большом числе областей, т.к. в них присутствуют значительные взаимные перекрытия кругов вблизи полюсов сферы.

Тем не менее, при небольшом числе областей оптимальные варианты покрытия сферы несложно “угадать”. Например, случай $N = 1$ соответствует разделению сферы всего на две части — верхнюю и нижнюю, дает единственную область при согласовании базисов, т.е. фактически согласование базисов в данном случае не проводится.

Рассчитаем количество информации I в одном кубите при приблизительном согласовании базисов:

$$I = 1 + \int\limits_{\Omega} |\langle\mu|\nu\rangle|^2 \log_2 |\langle\mu|\nu\rangle|^2 dV_\nu dV_\mu / \int\limits_{\Omega} |\langle\mu|\nu\rangle|^2 dV_\nu dV_\mu, \qquad (3.13)$$

где интегрирование проводится по одной круглой области Ω согласования базисов, в которую попадают $|\nu\rangle$ и $|\mu\rangle$. Результаты расчета приведены в таблице 3.1.

Таблица 3.1: Количество информации I в одном кубите в зависимости от числа областей при приблизительном согласовании базисов.

Число областей	1	8	18	32	50	72	98
I, бит	0,469	0,801	0,906	0,946	0,965	0,976	0,982

С увеличением числа областей и, соответственно, уменьшением размера каждой области, информация в одном кубите увеличивается с $\simeq 0,47$ бита при одной области до 1 бита в пределе бесконечно большого числа областей. Заметим, что увеличение числа областей приводит к пропорциональному увеличению объема дополнительной информации о номере области при согласовании базисов, а также к пропорциональному уменьшению количества отобранных после согласования базисов сообщений.

Еще одной особенностью протокола с континуальным алфавитом является количественная мера оценки вмешательства подслушивателя. Одной из самых распространенных характеристик является уровень ошибок в квантовом бите — QBER (от англ. “quantum bit error rate”), равный

$$Q = 1 - \frac{N}{N_{\max}}, \tag{3.14}$$

где N — число правильно переданных букв и $N_{\max}$ — общее число переданных букв. Использование QBER как меры вмешательства подслушивателя неявно предполагает его равенство нулю при отсутствии подслушивания. Действительно, в идеальном квантовом канале после точ-

ного согласования базисов ошибок в переданном сообщении нет. Однако, в случае протокола с континуальным алфавитом точного согласования базисов осуществить не удастся, и QBER не равен нулю даже при отсутствии подслушивания, так что он, очевидно, не отражает реальный уровень вмешательства подслушивателя.

Для разрешения данного противоречия мы предлагаем считать точностью передачи не относительное число правильно переданных букв, а относительное количество правильно переданной информации. Тогда уровень ошибок может быть определен как

$$\tilde{Q} = 1 - \frac{I}{I_{\max}}, \tag{3.15}$$

где I описывает количество информации в одном кубите в присутствие подслушивания, а $I_{\max}$ — её максимально возможную величину при отсутствии подслушивания. По аналогии с QBER эту меру ошибок можно назвать уровнем ошибок во взаимной информации — MIER (от англ. “mutual information error rate”).

Из определения MIER видно, что он корректно отражает уровень вмешательства подслушивателя даже для протокола с континуальным алфавитом при приблизительном согласовании базисов. Независимо от наличия и природы внутренних, т.е. заложенных в самом протоколе, ошибок, они учитываются в том, что $I_{\max} \leq 1$ бит. Только внешние факторы (различные шумы в экспериментальной установке, в канале передачи данных, неточность создания и измерения состояний и т.п.) могут влиять на MIER, которые всегда целиком списываются на вмешатель-

ство подслушивателя.

Далее удобно использовать обе этих характеристики — QBER и MIER, по умолчанию подразумевая при использовании QBER предельный случай точного согласования базисов в протоколе с континуальным алфавитом.

3.4 Стратегия перехвата-пересылки

Самой простой стратегией подслушивания является измерение Евой передаваемого кубита в некотором базисе и последующая отправка результата измерения Бобу. Понятно, что в таком случае Ева точно знает, что получает Боб, и установление секретного сообщения между Алисой и Бобом невозможно. Следовательно, максимальный уровень ошибок, при котором секретная связь возможна, не превышает уровень ошибок, вызванных стратегией подслушивания типа перехвата-пересылки, т.е. расчет этих ошибок дает верхнюю границу эффективности протоколов КК.

Предположим, что Алиса передала Бобу некоторое состояние $|\alpha\rangle$, а Ева при его перехвате использовала базис $\{|\psi\rangle, |\psi_\perp\rangle\}$. Тогда Ева получила результат $|\psi\rangle$ с вероятностью $|\langle\psi|\alpha\rangle|^2$, либо $|\psi_\perp\rangle$ с вероятностью $|\langle\psi_\perp|\alpha\rangle|^2$, и отправила полученный результат Бобу. После измерения Бобом передаваемых состояний $|\psi\rangle$ и $|\psi_\perp\rangle$ в базисе $\{|\alpha\rangle, |\alpha_\perp\rangle\}$ он получит правильный результат — состояние $|\alpha\rangle$ — с вероятностями $|\langle\psi|\alpha\rangle|^2$ и $|\langle\psi_\perp|\alpha\rangle|^2$, и неправильный результат — состояние $|\alpha_\perp\rangle$ — с вероятностями $|\langle\psi|\alpha_\perp\rangle|^2$ и $|\langle\psi_\perp|\alpha_\perp\rangle|^2$. Общая вероятность получения правильного

результата Бобом равна $|\langle\psi|\alpha\rangle|^4+|\langle\psi_\perp|\alpha\rangle|^4$ и, соответственно, вероятность возникновения ошибки равна

$$Q_{\alpha\psi}=1-|\langle\psi|\alpha\rangle|^4+|\langle\psi_\perp|\alpha\rangle|^4. \tag{3.16}$$

Для расчета QBER необходимо усреднить $Q_{\alpha\psi}$ по всем базисам Алисы $\{\alpha\}$ и минимизировать результат усреднения по базисам Евы $\{\psi\}$:

$$Q=\sum_{\{\alpha\}}\sum_{\{\psi\}}\frac{Q_{\alpha\psi}}{N_\alpha N_\psi}, \tag{3.17}$$

где N_α и N_ψ — число базисов в алфавитах Алисы и Евы. Для протокола с континуальным алфавитом вместо суммирования выполняется соответствующее интегрирование. Результаты расчетов приведены в таблице 3.2.

Таблица 3.2: Уровень ошибок QBER, вызванный стратегией подслушивания типа перехвата–пересылки.

Число букв в алфавите	4	6	8	12	20	∞
Уровень ошибок, QBER	0,333	0,333	0,333	0,329	0,329	0,333

Максимально возможным критическим уровнем ошибок, равным $1/3$, обладают протоколы с алфавитами, включающими 4, 6 и 8 букв и протокол с континуальным алфавитом. Несколько меньшим уровнем ошибок обладают протоколы с 12 и 20 буквами, для которых он равен $74/225\simeq 0,329$.

Отметим одну особенность четырёхбуквенного протокола с алфавитом в виде тетраэдра. Т.к. у тетраэдра нет центральной симметрии, то

буквы в таком алфавите не образуют наборы ортогональных базисов и процедура согласования базисов в стандартном виде для такого протокола не выполняется. Тем не менее, для определения уровня ошибок Алиса и Боб могут вскрыть часть сообщений, т.е. открыто сравнить их, и на той части, для которой они использовали одинаковые состояния, определить уровень ошибок.

3.5 Стратегия оптимального подслушивания

Можно показать [77], что безопасное соединение между Алисой и Бобом возможно, если Боб получает от Алисы информации больше, чем Ева от Алисы или от Боба:

$$I_{AB} > \max\bigl(I_{AE}, I_{BE}\bigr). \tag{3.18}$$

Рассмотрим стратегию оптимального подслушивания, когда Ева извлекает из подслушиваемого сообщения максимум информации при заданном уровне вмешательства, вызывающем соответствующий уровень ошибок, что можно записать как

$$I_{AE,BE} = \max_{I_{AB}=\text{const}} I_{AE,BE}. \tag{3.19}$$

Заметим, что эта стратегия может отличаться от оптимального клонирования [78].

Без ограничения общности можно считать, что при оптимальном подслушивании Ева выполняет унитарное преобразование U_{BE} над переда-

ваемым от Алисы к Бобу состоянием $|\beta\rangle_B$ и присоединенным к информационному каналу пробным состоянием Евы $|0\rangle_E$ (если преобразование Евы является неунитарным, то оно соответствует некоторому унитарному преобразованию в расширенной системе с последующим усреднением по части переменных, что не добавляет ей какой-либо информации и не создаёт никаких дополнительных проблем для Алисы и Боба). Действие этого унитарного преобразования на базисные элементы выглядит следующим образом:

$$\left.\begin{aligned} |0\rangle_B |0\rangle_E &\xrightarrow{U_{BE}} |0\rangle_B |\Phi_{00}\rangle_E + |1\rangle_B |\Phi_{01}\rangle_E, \\ |1\rangle_B |0\rangle_E &\xrightarrow{U_{BE}} |0\rangle_B |\Phi_{10}\rangle_E + |1\rangle_B |\Phi_{11}\rangle_E . \end{aligned}\right\} \tag{3.20}$$

Унитарность предполагает наложение ограничений на набор $|\Phi_{ij}\rangle$, вытекающих из условий сохранения ортогональности

$$\langle\Phi_{00}|\Phi_{10}\rangle + \langle\Phi_{01}|\Phi_{11}\rangle = 0 \tag{3.21}$$

и нормировки

$$|\Phi_{00}|^2 + |\Phi_{01}|^2 = |\Phi_{10}|^2 + |\Phi_{11}|^2 = 1. \tag{3.22}$$

Учитывая эти ограничения, набор всех состояний $|\Phi_{ij}\rangle$ можно представить в форме суперпозиции всего двух базисных состояний:

$$\begin{pmatrix} |\Phi_{00}\rangle \\ |\Phi_{01}\rangle \\ |\Phi_{10}\rangle \\ |\Phi_{11}\rangle \end{pmatrix} = \begin{pmatrix} \gamma_{00} & \gamma_{01} \\ \gamma_{10} & \gamma_{11} \\ \gamma_{11} & \gamma_{10} \\ \gamma_{01} & \gamma_{00} \end{pmatrix} \begin{pmatrix} |0\rangle_E \\ |1\rangle_E \end{pmatrix}, \tag{3.23}$$

где все коэффициенты преобразования (3.23) определяются через два параметра θ и φ, контролируемых Евой:

$$\gamma_{mn} = (-1)^{mn} \cos(\theta - m\frac{\pi}{2}) \cos(\varphi - n\frac{\pi}{2}). \tag{3.24}$$

Начальная матрица плотности системы Боб—Ева $\hat{\rho}^{(1)}_{EB}(\alpha) = |0\rangle_E \langle 0|_E \otimes |\alpha\rangle_B \langle \alpha|_B$ после преобразования (3.20) переходит в конечную $\hat{\rho}^{(2)}_{EB}(\alpha)$, на основе которой получаем совместное трёхчастичное распределение вероятностей

$$P_{ABE}(\alpha, \beta, \varepsilon) = \mathrm{Tr}_{BE}(|\varepsilon\rangle_E \langle \varepsilon|_E \otimes |\beta\rangle_B \langle \beta|_B) \hat{\rho}^{(2)}_{EB}(\alpha) dV_E dV_B. \tag{3.25}$$

Естественной характеристикой для расчета количества информации в системах Алиса—Боб, Алиса—Ева и Ева—Боб является количество совместимой информации, определяемого стандартным информационным функционалом Шеннона (1.34). Отметим, что все рассматриваемые здесь квантовые алфавиты образуют полный набор событий, т.е. проекторы, построенные на состояниях из рассматриваемых алфавитов, образуют разложение единичного оператора, что гарантирует нормировку (3.25) на единицу.

Усредняя (3.25) по третьей системе получаем двухчастичные распределения вероятностей P_{AB}, P_{AE}, P_{BE} и, на основе (1.34), в зависимости от конкретного типа алфавита — соответствующие зависимости информации I_{AB}, I_{AE} и I_{BE} в системах Алиса—Боб, Алиса—Ева и Боб—Ева от параметров θ и φ.

Сравнивая описанные зависимости, получаем, что при любых значениях этих параметров выполняется условие $I_{AE} \geq I_{BE}$. Поэтому далее

зависимость информации I_{BE} рассматривать нет необходимости и условие безопасности (3.18) преобразуется в соотношение $I_{AB} > I_{AE}$.

Анализируя условие оптимальности подслушивания (3.19), получаем, что оно выполняется в области значений параметров $\theta = \pi/4 - \varphi$. С учётом того, что зависимость I_{AE} симметрична I_{AB} относительно $\theta = \varphi$, на рис.3.2 представлены лишь однопараметрические зависимости $I_{AB}(\theta)$ при выполнении условия оптимального подслушивания (3.19).

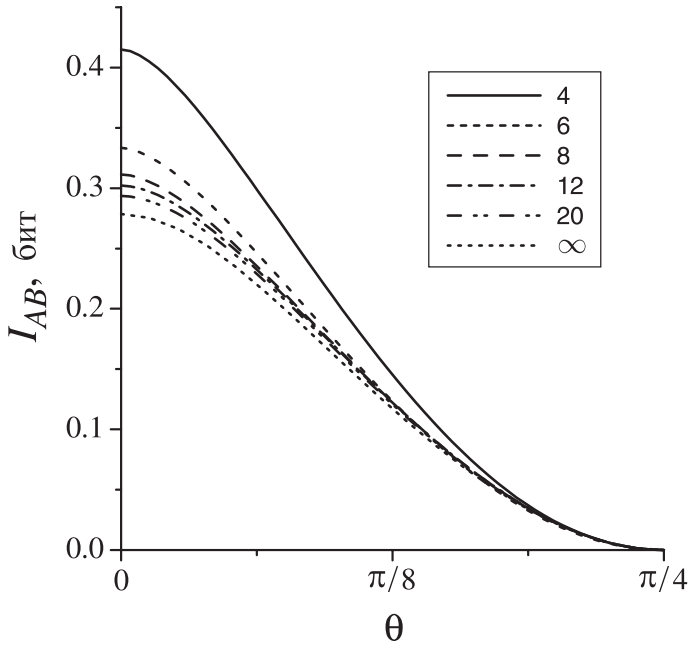


Рис. 3.2: Зависимость количества информации I_{AB} в системе Алиса–Боб от параметра θ для протоколов, использующих 4,6,8,12,20 букв и протокола с континуальным алфавитом (бесконечное число букв).

Условие безопасности работы протокола $I_{AB} > I_{AE}$ в силу симметрии $I_{AB}(\theta, \varphi) = I_{AE}(\varphi, \theta)$ выполняется вплоть до критического значения $\theta_0 = \pi/8$, при котором информация, перехваченная Евой, равна инфор-

мации, полученной Бобом. Критические величины ошибок $\tilde{Q}_0$ для рассматриваемых протоколов представлены в таблице 3.3.

Таблица 3.3: Критический уровень ошибок $\tilde{Q}_0$ до согласования базисов.

Число букв в алфавите	4	6	8	12	20	∞
Крит. уровень ошибок, MIER	0,650	0,630	0,607	0,597	0,589	0,600

Из таблицы 3.3 видно, что без согласования базисов наивысшим критическим уровнем ошибок обладает протокол с алфавитом в виде тетраэдра.

Заметим, что расчет количества информации напрямую не связан с *кодированием* информации. Наиболее часто используется двоичное кодирование, когда одному состоянию из ортогональной пары сопоставляется “0”, другому — “1”, что связано с процедурой согласования базисов. Кодирование в континуальном алфавите аналогично стандартным протоколам KK, т.к. для любой буквы из континуального алфавита существует ортогональная ей буква. Способ разделения сферы Блоха на ортогональные пары произволен, надо лишь учитывать разделение на области при приблизительном согласовании базисов. Можно, например, разделить ее на верхнюю часть, кодирующую “0”, и нижнюю, кодирующую “1”.

Буквы тетраэдрального алфавита ортогональных пар не образуют, поэтому для них следует использовать другое кодирование, где двум произвольным буквам сопоставляется “0”, а двум оставшимся — “1”.

Рассмотрим теперь роль согласования базисов. Будем предполагать, что Алиса и Боб выполняют *безопасное* согласование базисов, т.е. при согласовании базисов Ева не влияет на отбор данных, не вносит ложных сообщений в открытый канал связи и не использует дополнительных преобразований над своим пробным состоянием после согласования базисов, т.е. ее информация после согласования базисов не увеличивается. Отметим, что данное предположение сделано по нескольким причинам.

Во-первых, с учетом реальных возможностей современных технологий такое предположение вполне оправдано по физическим соображениям. Для извлечения дополнительной информации из процедуры согласования базисов Еве необходимо иметь неограниченное количество идеальной квантовой памяти, способной хранить перехваченную информацию в квантовом виде неограниченно долго. На данном этапе развития технологий это представляется невозможным. Любые же неидеальности в устройстве хранения информации неизбежно приводят к декогеренции, и, как следствие, к потере информации. Если легитимные участники (Алиса и Боб) между передачей квантовых данных и согласованием базисов сделают паузу, превосходящую характерное время декогеренции квантовой памяти, то согласование базисов не даст никакой дополнительной информации подслушивающей стороне.

Во-вторых, предположение о том, что подслушивающая сторона не получает информации из процедуры согласования базисов, хотя и безусловно является ограничением, но оно сделано в равной степени при анализе всех алфавитов. Полученные критические уровни ошибок, уже

не будут являться абсолютными критериями безопасности, но т.к. нашей целью стоит только сравнение различных протоколов, то предположение о безопасном согласовании базисов вполне разумно.

Информация I_{AB}, получаемая Бобом от Алисы после безопасного согласования базисов, пропорционально увеличивается по сравнению со случаем без согласования базисов так, что достигает максимального значения 1 бит на одно сообщение (подразумевается точное согласование базисов для протокола с континуальным алфавитом). Условие безопасности $I_{AB} > I_{AE}$ теперь выполняется вплоть до других (по сравнению со случаем отсутствия согласования базисов) значений θ_0, зависящих от конкретного протокола. Критический уровень ошибок при этом также увеличивается и приведен в таблице 3.4.

Таблица 3.4: Критический уровень ошибок $\tilde{Q}_0$ после согласования базисов.

Число букв в алфавите	6	8	12	20	∞
Крит. уровень ошибок, MIER	0,806	0,805	0,804	0,805	0,811

После согласования базисов наивысшим критическим уровнем ошибок обладает протокол с континуальным алфавитом, что справедливо в предельном случае точного согласования базисов. Для алфавита в виде тетраэдра процедура согласования базисов в стандартном виде не выполняется, поэтому в таблице нет соответствующего результата.

3.6 Многомерные протоколы квантовой криптографии

Проанализируем потенциальные возможности использования многомерных пространств, которые представляются наиболее обещающими для протокола с континуальным алфавитом. Для верхней оценки эффективности протоколов рассчитаем ошибки, вызываемые стратегией перехвата–пересылки в многомерном случае.

Рассмотрим произвольный симметричный многомерный алфавит, буквы в котором образуют взаимно-несмещенные базисы, т.е. такой алфавит, где все неортогональные буквы дают одинаковые проекции друг на друга. Рассчитаем, с какой точностью будет передана произвольная буква после подслушивания Евой с использованием стратегии перехвата-пересылки. Пусть D–мерный алфавит состоит из L_D взаимно-несмещённых базисов. Алиса передает Бобу некоторую букву из случайно выбранного базиса. Если Ева при перехвате “угадает” этот базис, то буква пройдет без искажений — такой вариант случается с вероятностью $1/L_D$. Если же Ева “не угадает” базис (а это происходит с вероятностью $1 - 1/L_D$), то, в силу предположения о симметрии алфавита, передаваемая буква равновероятно изменится при перехвате Евой на некоторую другую. При ее приеме Бобом с вероятностью $1/D$ получится правильный результат (буква, передаваемая Алисой), а во всех остальных случаях — неправильный.

Итоговая, совокупная по двум случаям (Ева “угадывает” или “не

угадывает" базис) вероятность не исказить передаваемую букву равна $F_D = 1/L_D + (1 - 1/L_D)/D$, а соответствующая вероятность ошибки —

$$Q_D = 1 - F_D = 1 - \frac{1}{L_D}\left(1 + \frac{L_D - 1}{D}\right). \tag{3.26}$$

Проверяя эту формулу для протоколов BB84 ($L_D = 2, D = 2$) и B98 ($L_D = 3, D = 2$) получаем уже найденные ранее величины $1/4$ и $1/3$.

Переходя к пределу $D \to \infty$ получаем

$$Q_\infty = \lim_{D\to\infty} Q_D = 1 - \frac{1}{L_D}$$

Из этого соотношения видно, что чем больше букв в алфавите, тем выше потенциально возможный критический уровень ошибок. Для максимального числа взаимно-несмещённых базисов в D-мерном гильбертовом пространстве [79] $L_D^{\max} = D + 1$ получаем $Q_\infty^{\max} = 100$ %:

$$Q_\infty^{\max} = \lim_{L_D = D+1, D\to\infty} Q_D = 1 - \frac{1}{D+1}\left(1 + \frac{D}{D}\right) = 1. \tag{3.27}$$

Отметим, что максимально возможный уровень ошибок в многомерном случае составляет 100%, а не 50%, как для двумерного случая. Это обусловлено тем, что в двумерном случае "не угадывание" буквы означает "угадывание" противоположной буквы, и если уровень ошибок $Q_2^{(1)} > 0,5$, то Боб может просто заменить все нули на единицу и наоборот, получив при этом $Q_2^{(2)} = 1 - Q_2^{(1)} < 0,5$. В многомерном же случае такой трюк не проходит, и чем больше размерность пространства, тем выше максимально возможный уровень ошибок.

Исходя из результата (3.27), можно сделать вывод о том, что принципиальных запретов на увеличение эффективности протоколов с ростом

размерности пространства нет, т.к. нет верхнего порога, устанавливаемого стратегией перехвата–пересылки.

Помня о такой особенности многомерных алфавитов, рассмотрим обобщение протокола с континуальным алфавитом на многомерный случай. Заметим, что в многомерном случае максимально возможная селектированная информация связи двух систем $I^D_{\max} = \log_2 D$ неограниченно возрастает при $D \to \infty$. Максимально же возможная неселектированная информация ограничена: она равна объему доступной информации [62]

$$I^D_{\text{accessible}} = \log_2 D - \frac{1}{\ln 2} \sum_{k=2}^{D} \frac{1}{k},$$

которая в пределе $D \to \infty$ стремится к удивительно малой величине $I^\infty_{\text{accessible}} \simeq 0,61$ бит.

Рассматривая случай безопасного согласования базисов, обсужденного в разделе 3.5, и абстрагируясь от конкретной стратегии подслушивания, можно оценить сверху максимальную величину неселектированной информации, получаемой Евой, величиной доступной информации. Реально информация, получаемая Евой, будет, конечно, меньше.

Т.к. после безопасного согласования базисов количество информации в системе Алиса—Боб задается максимально возможной селектированной информацией, а в системе Алисы—Ева — неселектированной, то критический уровень ошибок MIER (3.15) в пределе $D \to \infty$ равен единице:

$$\tilde{Q}^\infty_0 = \lim_{D\to\infty} \tilde{Q}^D_0 = 1 - \lim_{D\to\infty} \frac{I^D_{accessible}}{I^D_{max}} = 1 - \lim_{D\to\infty} \frac{0,61}{\log_2 D} = 1. \qquad (3.28)$$

Этот результат выражает качественно новую особенность протокола

с многомерным континуальным алфавитом по сравнению с двумерными протоколами, состоящую в том, что он может работать в принципе при практически любых помехах, и у него появляется новое свойство — отсутствие порога работы по ошибкам. Это означает, что, увеличивая размерность пространства состояний входа и выхода квантового канала, можно добиться того, чтобы критический уровень ошибок превышал любую наперед заданную величину. Конкретная зависимость критического уровня ошибок $\tilde{Q}_0$ от размерности пространства приведена на рис. 3.3

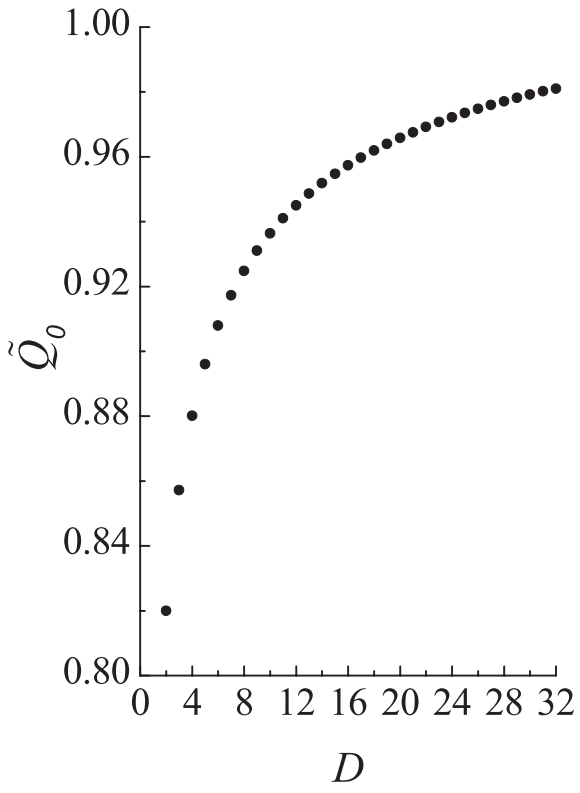


Рис. 3.3: Зависимость критического уровня $\tilde{Q}_0$ ошибок в совместимой информации от размерности пространства D.

Такая качественная особенность не зависит от конкретной структу-

ры подслушивания Евы и может быть объяснена следующим образом. Когда Алиса посылает сообщение, то и Ева и Боб априори имеют о нем минимальную информацию, они как бы максимально запутаны во всем многомерном пространстве. После согласования базисов Алиса и Боб могут отобрать только сильно коррелированные сообщения, для которых они выбрали примерно одинаковые базисы. В результате их информация связи в расчете на одно сообщение существенно возрастет. Ева же не может влиять на отбор сообщений, и ее информация остается прежней. Следовательно, с увеличением размерности пространства положение Евы и Боба становится все более неравноправным, что в конечном счете и приводит к полученной качественной особенности. Единственным предположением о стратегии подслушивания Евы является безопасность согласования базисов.

3.7 Экспериментальная схема реализации протоколов квантовой криптографии с произвольными алфавитами

На рис. 3.4 приведена предлагаемая нами экспериментальная схема реализации рассмотренных выше двумерных протоколов КК, где буквы кодируются поляризацией фотонов.

На стороне Алисы генерируются фотоны с произвольным квантовым поляризационным состоянием. Это можно реализовать с помощью источ-

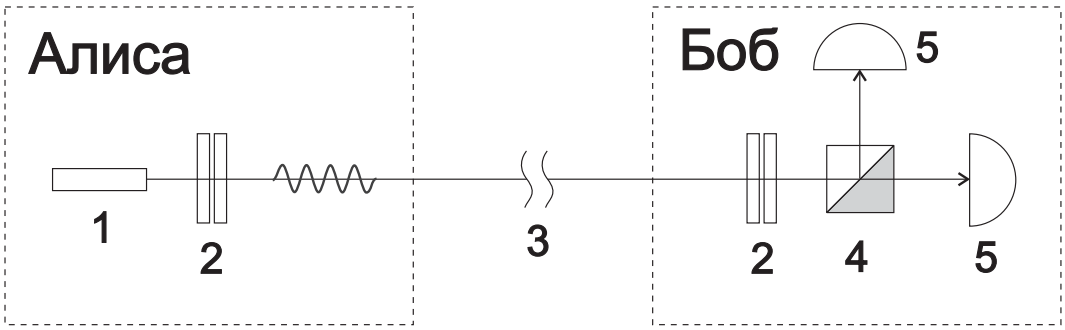


Рис. 3.4: Экспериментальная схема для реализации протоколов квантовой криптографии.

ника единичных фотонов с фиксированной поляризацией (1), например лазера, работающего в режиме генерации единичных фотонов. Набор букв, составляющих алфавит реализуемого протокола, задается набором точек на сфере Блоха и определяется набором углов поворота поляризационного базиса, например с помощью двух ячеек Поккельса (2), где первая ячейка поворачивает вертикальную составляющую поляризации, а вторая — горизонтальную. Вместо ячеек Поккельса также можно использовать четвертьволновые поляризационные пластинки, поворачивая их на углы, соответствующие выбранному алфавиту. Алфавитам с конечным дискретным набором букв будет соответствовать конечный дискретный набор углов поворота поляризации, а континуальному алфавиту — непрерывное множество углов поворота поляризации.

Полученный фотон с произвольным поляризационным состоянием далее передается Бобу по квантовому каналу (3), сохраняющему поляризацию, например, по открытому пространству. На стороне Боба поляризация каждого фотона преобразуется согласно заданному алфавиту

аналогично тому, как это делается на стороне Алисы, но в обратном порядке, так, чтобы после преобразования фотон находился в фиксированном поляризационном базисе, в котором он измеряется при помощи поляризационного делителя (4) и счетчиков фотонов (5).

В описанную схему, предназначенную для передачи квантовых букв, следует ещё добавить классический несекретный канал связи, с помощью которого Алиса и Боб обмениваются несекретной информацией для реализации открытых этапов передачи квантового ключа, например, для вычисления уровня ошибок, согласования базисов, проверки условия безопасности и т.д.

Выбор конкретного квантового алфавита должен определяться исходя из имеющегося уровня ошибок и требований к передаче данных. Континуальный алфавит обеспечивает несколько больший критический уровень ошибок, чем остальные алфавиты, но для достаточно точного согласования базисов требует гораздо большего числа переданных сообщений, чем дискретные алфавиты. Если процедуру согласования базисов по каким либо причинам лучше не выполнять, то наивысшим уровнем помехозащищенности будет обладать тетраэдральный алфавит.

Результаты, представленные в этой главе, опубликованы в работах [81–85, 88–97].

Заключение

В заключение просуммируем основные результаты, полученные в настоящей диссертационной работе.

В ней рассмотрен важный тип квантовой информации — совместимая информация. Изучены ее свойства на примере информационного анализа как абстрактных двухкубитных квантовых каналов, так и каналов, образованных в реальных системах — двухатомной задаче Дике и в системе Алиса–Ева–Боб в задачах квантовой криптографии. В результате можно сделать вывод об эффективности использования информационного анализа, основанного на расчете совместимой информации, для решения целого ряда задач.

По результатам анализа общих свойств совместимой информации, проведенного в главе 1, в первую очередь можно сделать вывод о практической ценности информационного подхода в квантовой теории. Обсуждение основных объектов квантовой теории в информационных терминах дает не только новую физическую картину, что уже само по себе интересно, но и помогает глубже осознать основы теории. Так, например, в параграфе 1.3 при рассмотрении, казалось бы, достаточно отвлеченной

задачи из классической теории информации, довольно неожиданно проявляется вероятностная интерпретация волновой функции.

При обсуждении различных двухчастичных состояний как потенциальных информационных каналов для передачи классической информации становится очевидной роль максимально перепутанных двухчастичных состояний. Именно такие состояния обеспечивают максимальную информационную связанность. Как показано в параграфе 1.5, величина неселектированной информации для квантовокоррелированных максимально перепутанных состояний в несколько раз больше величины неселектированной информации для квазиклассических сепарабельных состояний. Это следует учитывать при использовании информационной специфики распределенных перепутанных систем. Например, в схемах квантовой телепортации центральное место всегда занимает именно распределенная перепутанная пара. С учетом возможного применения телепортации как процедуры в алгоритмах квантовых вычислений результаты приведенного в параграфе 1.5 анализа представляются достаточно актуальными.

Результаты главы 2 позволяют сделать вывод о том, что наиболее естественным объектом анализа в терминах совместимой информации являются кинематически независимые системы, например, два различных взаимодействующих объекта. Анализ в терминах совместимой информации по сравнению с анализом в терминах избранных динамических переменных дает, с одной стороны, более абстрактную картину, с другой — наилучшим образом описывает именно информационные

аспекты взаимодействия. Так, например, результаты информационного анализа двухатомного взаимодействия представляют интерес для физического обсуждения фундаментальных процессов передачи информации на уровне отдельных атомов. Если представить отдельные атомы как минимальные носители информации, то становится понятной актуальность подобного анализа в будущем.

Важным приложением, где ценность информационного подхода наиболее очевидна, является квантовая криптография. Благодаря тому, что в конечном счете квантовая криптография связана с передачей чисто классических данных, совместимая информация в наилучшей форме отражает сущность происходящих там процессов. Нельзя сказать, что подход, основанный на расчете функционала взаимной информации Шеннона в задачах квантовой криптографии является новым. Но, если раннее он применялся во многом интуитивно (хотя и давал правильные результаты), то именно на основе систематического подхода с использованием совместимой информации как мощного инструмента информационного анализа появляется возможность получения новых результатов, которые вне рамок данного подхода получить было бы затруднительно. В итоге практически ценным выходом работы, проведенной в главе 3, является открытие новых протоколов квантовой криптографии с улучшенными по сравнению с предыдущими протоколами характеристиками. Также простым (в свете общих свойств совместимой информации), но практически важным и интересным результатом стало обнаружение возможности беспороговой по шумам передачи секретного сообщения.

По результатам работы можно сформулировать следующие **защищаемые положения**:

1. На ряде практически важных квантовых информационных каналов продемонстрирована эффективность использования понятия совместимой информации как адекватной информационной меры.

2. Показано, что максимально перепутанные двухчастичные состояния обеспечивают бóльшую информативность чем любые другие двухчастичные состояния. Выявлено соответствие между энтропией чистого квантового состояния в N–мерном гильбертовом пространстве и энтропией классической системы с N элементарными событиями. Выявлена качественная специфика описания динамики физических систем на языке совместимой и когерентной информации.

3. Выявлено соответствие между неклонируемостью квантовых состояний и некопируемостью квантовой информации. Предложены и проанализированы несколько протоколов квантовой криптографии, алфавиты которых образуют правильные многогранники на сфере Блоха. Показано, что они могут обеспечивать больший уровень помехозащищенности, чем существовавшие раннее протоколы с двумерными алфавитами. Рассчитана верхняя оценка помехозащищенности для протоколов квантовой криптографии с многомерными алфавитами. Показана принципиальная возможность создания секретного сообщения при произвольном уровне помех в кван-

товом канале связи.

Основные результаты диссертации доложены на научных семинарах и международных конференциях в России и за рубежом в 2002—2004 годах и опубликованы в работах [80–97].

В заключение выражаю искреннюю благодарность моим научным руководителям — Виктору Николаевичу Задкову за постоянное внимание к работе и Борису Андреевичу Гришанину за постановку задач и неоценимую помощь в освоении методов их решения. Я также глубоко благодарен своей семье за понимание и поддержку в процессе всей работы над диссертацией.

Приложения

Приложение А. Представление состояния кубита вектором на сфере Блоха

Рассмотрим простейшую двухуровневую квантовую систему A, или *кубит*, являющуюся квантовым аналогом классической системы с двумя элементарными событиями. Для обозначения волновых функций системы будем применять обозначения Дирака в виде бра– и кет–векторов. Ортогональные базисные состояния определяются как $|1\rangle = (1,0)$ и $|2\rangle = (0,1)$. Согласно принципу суперпозиции произвольное состояние $|\alpha\rangle$ кубита может быть представлено суммой этих двух базисных состояний, что может быть записано как поворот U одного из базисных состояний в пространстве состояний кубита:

$$|\alpha\rangle = U\,|1\rangle = (\cos\frac{\theta}{2}, e^{-i\varphi}\sin\frac{\theta}{2}), \tag{3.29}$$

где матрица поворота

$$U = \begin{pmatrix} \cos(\theta/2) & e^{-i\varphi}\sin(\theta/2) \\ -e^{i\varphi}\sin(\theta/2) & \cos(\theta/2) \end{pmatrix} \tag{3.30}$$

Полярный $\theta \in (0, \pi)$ и азимутальный $\varphi \in (0, 2\pi)$ углы позволяют наглядно представить вектор состояния системы как вектор на сфере Блоха (рис. 3.5).

Ортогональный вектору $|\alpha\rangle$ вектор $|\tilde{\alpha}\rangle$ есть $|\tilde{\alpha}\rangle = U|2\rangle = (-e^{i\varphi}\sin\frac{\theta}{2}, \cos\frac{\theta}{2})$, $\langle\alpha|\tilde{\alpha}\rangle = 0$. На сфере Блоха вектора $|\alpha\rangle$ и $|\tilde{\alpha}\rangle$ представляются центрально–симметричной парой векторов. Действительно, $|\tilde{\alpha}\rangle = (-e^{i\varphi}\sin\frac{\theta}{2}, \cos\frac{\theta}{2}) = -e^{i\varphi}(\cos\frac{\pi-\theta}{2}, e^{-i(\varphi+\pi)}\sin\frac{\pi-\theta}{2})$, что с точностью до фазового множителя $e^{-i\varphi}$ совпадает с $|\alpha\rangle$ с измененными углами $\theta \to \pi - \theta$, $\varphi \to \pi + \varphi$, и соответствует отражению вектора $|\alpha\rangle$ относительно центра сферы Блоха.

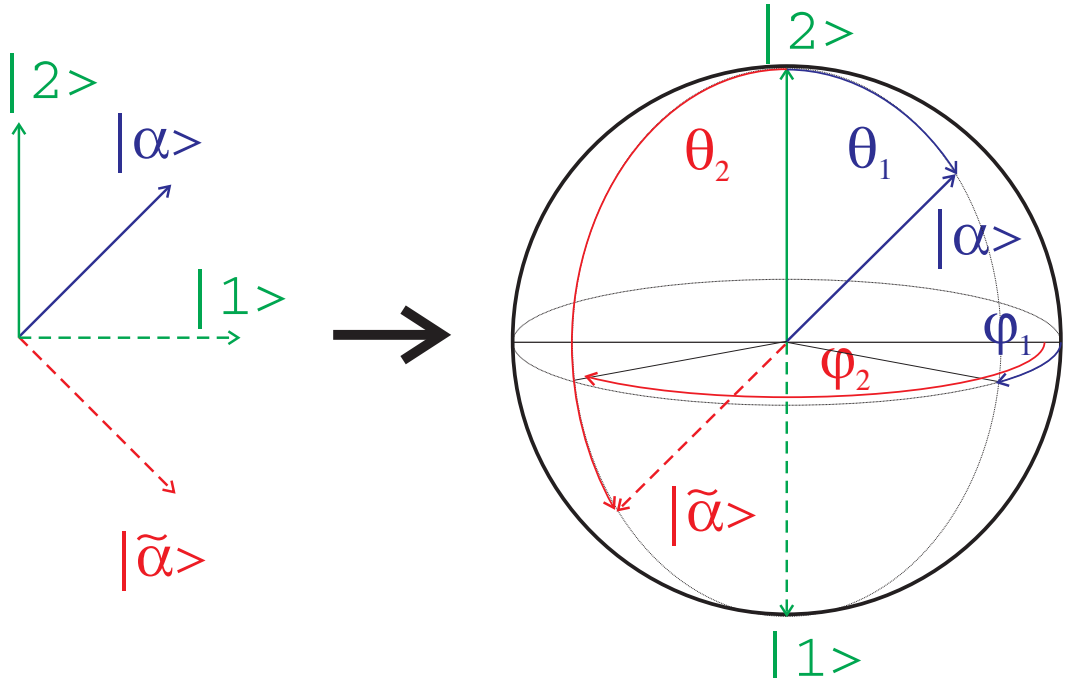


Рис. 3.5: Представление волновых функций двухуровневой квантовой системы векторами на сфере Блоха. Ортогональные волновые функции представляются центрально–симметричной парой векторов $|\alpha\rangle$ и $|\tilde{\alpha}\rangle$.

Приложение Б. Программа на языке Mathematica для вычисления некоторых полученных в работе величин

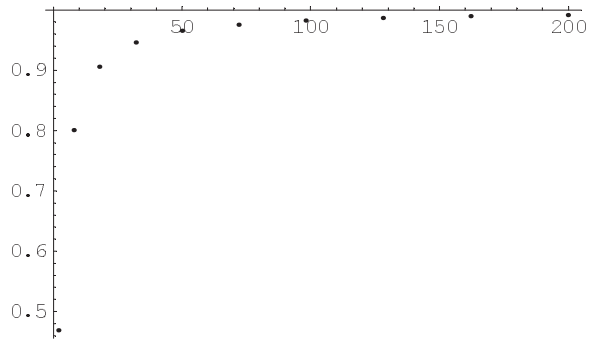
```
(*defenitions*)
φ1 =.; φ2 =.; Θ1 =.; Θ2 =.;
δ = 10^-8; ν = Sin[Θ]/(2 π);
α = {Θ → Θ1, φ → φ1}; β = {Θ → Θ2, φ → φ2};
ψ = ψn = ψD2 = {Cos[Θ/2], Sin[Θ/2] e^(i φ)};
CC[z_] := ComplexExpand[Conjugate[z]];
KetBra[t1_, t2_] :=
  Simplify[Table[t1[[i]] CC[t2[[j]]], {i, Length[t1]}, {j, Length[t1]}]];
BraKet[t1_, t2_] := Simplify[Sum[t1[[i]] CC[t2[[i]]], {i, Length[t1]}]];
```

```
(*unselected compatible information*)
ρ = 1/2 {{0, 0, 0, 0}, {0, 1, -1, 0}, {0, -1, 1, 0}, {0, 0, 0, 0}}; (*this is an example - antisymmetric state*)
pαβ = Simplify[Sum[ρ[[(2 i) + j + 1, (2 k) + l + 1]] (ψn[[i + 1]] /. α) (ψn[[j + 1]] /. β)
    CC[(ψn[[k + 1]] /. α) (ψn[[l + 1]] /. β)], {i, 0, 1}, {j, 0, 1}, {k, 0, 1}, {l, 0, 1}]];
pα = Chop[Integrate[Integrate[pαβ (ν /. β), {Θ2, 0, π}], {φ2, 0, 2 π}]];
pβ = Chop[Integrate[Integrate[pαβ (ν /. α), {Θ1, 0, π}], {φ1, 0, 2 π}]];
Iαβ = NIntegrate[Evaluate[pαβ Log[2, (pαβ + δ)/(pα pβ + δ)] (ν /. β) (ν /. α)],
   {φ2, 0, 2 π}, {Θ2, 0, π}, {φ1, 0, 2 π}, {Θ1, 0, π},
   Method → QuasiMonteCarlo, AccuracyGoal -> 2, PrecisionGoal → 2];
unity = NIntegrate[Evaluate[pαβ (ν /. β) (ν /. α)], {φ2, 0, 2 π},
   {Θ2, 0, π}, {φ1, 0, 2 π}, {Θ1, 0, π}, Method → QuasiMonteCarlo,
   AccuracyGoal -> 2, PrecisionGoal → 3];
Print["Iαβ= ", Iαβ, " ", "; Normalization= ", unity];
```

```
(*Alice-Bob,Bob-Eve and Alice-Eve states*)
kα = Table[(-1)^(m n) Cos[Θ - m π / 2] Cos[Φ - n π / 2], {m, 0, 1}, {n, 0, 1}];
EF = {{kα[[1,1]], kα[[1,2]]}, {kα[[2,1]], kα[[2,2]]}, {kα[[2,2]], kα[[2,1]]}, {kα[[1,2]], kα[[1,1]]}};
ψ1 = {1, 0}; ψ2 = 1/Sqrt[2] {0, 1, -1, 0}; ψ30 = ψ3 = Table[0, {i, 8}];
Do[ψ3[[4 i + 2 j + k + 1]] = ψ2[[2 i + j + 1]] ψ1[[k + 1]], {i, 0, 1}, {j, 0, 1}, {k, 0, 1}];

ρABE = Table[0, {i, 8}, {j, 8}];
Do[ρABE[[i, j]] = ψ3[[i]] CC[ψ3[[j]]], {i, 1, Length[ψ3]}, {j, 1, Length[ψ3]}];

Uni = ( EF[[1, 1]]  0  EF[[3, 1]]  0      0      0      0      0
        EF[[1, 2]]  0  EF[[3, 2]]  0      0      0      0      0
        EF[[2, 1]]  0  EF[[4, 1]]  0      0      0      0      0
        EF[[2, 2]]  0  EF[[4, 2]]  0      0      0      0      0
           0        0     0       0  EF[[1, 1]]  0  EF[[3, 1]]  0
           0        0     0       0  EF[[1, 2]]  0  EF[[3, 2]]  0
           0        0     0       0  EF[[2, 1]]  0  EF[[4, 1]]  0
           0        0     0       0  EF[[2, 2]]  0  EF[[4, 2]]  0 );

ψ30 = Uni.ψ3;
Do[ρABE[[i, j]] = ψ30[[i]] CC[ψ30[[j]]], {i, 1, Length[ψ3]}, {j, 1, Length[ψ3]}];
ρ2ae = ρ2be = ρ2ab = ρ2 = Table[0, {i, 4}, {j, 4}];
ρ3 = ρABE;
Do[ρ2[[(2 i) + j + 1, (2 k) + l + 1]] =
    Sum[ρ3[[(4 m) + (2 i) + j + 1, (4 m) + (2 k) + l + 1]], {m, 0, 1}],
  {i, 0, 1}, {j, 0, 1}, {k, 0, 1}, {l, 0, 1}];
ρ2be = ρ2;
Do[ρ2[[(2 i) + j + 1, (2 k) + l + 1]] =
    Sum[ρ3[[(4 i) + (2 m) + j + 1, (4 k) + (2 m) + l + 1]], {m, 0, 1}],
  {i, 0, 1}, {j, 0, 1}, {k, 0, 1}, {l, 0, 1}];
ρ2ae = ρ2;
Do[ρ2[[(2 i) + j + 1, (2 k) + l + 1]] =
  Sum[ρ3[[(4 i) + (2 j) + m + 1, (4 k) + (2 l) + m + 1]], {m, 0, 1}],
 {i, 0, 1}, {j, 0, 1}, {k, 0, 1}, {l, 0, 1}]
ρ2ab = ρ2;
```

```
(*approximate basis reconciliation*)
dθ = .; dφ = 2 π; dx = .; dy = .;
Pa = Abs[BraKet[ψD2 /. {θ → x, φ → y}, ψD2]]^2;
norm :=
 NIntegrate[Pa ν (ν /. {θ → x, φ → y}), {θ, 0, dθ}, {φ, 0, dφ}, {x, 0, dθ}, {y, 0, dφ}]
Sa := 1 + NIntegrate[Pa ν (ν /. {θ → x, φ → y}) Log[2, Pa],
    {θ, 0, dθ}, {φ, 0, dφ}, {x, 0, dθ}, {y, 0, dφ}] / norm
(*Timing[Sa/.{dθ→π/2}]*)
Table[{2 N^2, Sa /. {dθ → π / (2 N)}}, {N, 1, 10}]
ListPlot[%];
```

```
{{2, 0.468766}, {8, 0.800982}, {18, 0.905699}, {32, 0.945821}, {50, 0.964992},
 {72, 0.975563}, {98, 0.981991}, {128, 0.986184}, {162, 0.989069}, {200, 0.991137}}
```



Литература

[1] Einstein A., Podolsky B, and Rosen N. Can quantum–mechanical description of physical reality be considered complete? // Phys. Rev. — 1935. — 47. — p.777 — 780.

[2] Bohr N. H. D. Can quantum–mechanical description of physical reality be considered complete? // Phys. Rev. — 1935. — 48. — p.696 — 702.

[3] Proceedings of the Conference "Quantum Theory: Reconsideration of Foundations", Växjö: Växjö University Press, 2001.

[4] Shannon C. E. A mathematical theory of communication // Bell Syst. Tech. Journal. — 1948. — 27. — p. 379 — 423 and 623 — 656.

[5] Курикша А. А. Квантовая оптика и оптическая локация // М: Советское радио, 1973.

[6] Gordon J. P. Quantum effects in communication systems // Proc. IRE. — 1962. — 50. — 9. — с. 1898 — 1908.

[7] Лебедев Д. С., Левитин Л. Б. Максимальное количество информа-

ции, переносимое электромагнитным полем // Докл. АН СССР. — 1963. — 169. — 6. — с. 1299 — 1302.

[8] Лебедев Д. С., Левитин Л. Б. Перенос информации электромагнитным полем // сборник “Теория передачи информации”, М: Наука, 1964, с. 5 — 20.

[9] Стратонович Р. Л. Количество информации, передаваемое квантовым каналом связи I, II // Изв. высш. учебн. завед. Радиофизика. — 1965. — 8. — 1. — с. 116 — 141.

[10] Стратонович Р. Л. Скорость передачи информации в некоторых квантовых каналах связи // Проблемы передачи информации. — 1966. — 2. — 1. — с. 45 — 57.

[11] Хелстром К. Квантовая теория проверки гипотез и оценивания // М: Мир, 1979.

[12] Вальд А. Статистические решающие функции // сборник “Позиционные игры”, М: Наука, 1967.

[13] Гришанин Б. А. Некоторые методы и результаты квантовой теории решений // Труды V конф. по теории кодирования и передачи информации. — 1972. —- Горький. — с. 103.

[14] Гришанин Б. А. Некоторые методы решения квантовых задач обнаружения и измерения // Изв. АН СССР. Техническая кибернети-

ка. — 1973. — 11. — 5. — с. 127 — 137. См. также перевод на англ. — quant-ph/0301159.

[15] А. С. Холево, *Пробл. передачи информ.* **9**, 31 (1973).

[16] Hausladen P., Jozsa R. // Phys. Rev. A. — 1996. — 54. — p. 1869.

[17] Holevo A. S. // IEEE Trans. Inf. Theory. — 1998. — IT—44. — p. 269.

[18] Холево А. С. Вероятностные и статистические аспекты квантовой теории // М: Наука, 1980.

[19] Холево А. С. Введение в квантовую теорию информации// М: МУНМО, 2002.

[20] Feynman R. P. Simulating physics with computers // Int. J. Theor. Phys. — 1982. — 21. — p. 467 — 488.

[21] Shor P. W. Algorithms for quantum computation: Discrete logarithms and factoring // Proc. of the 35th Ann. Symp. of the Foundations of Computer Science. (Ed. S. Goldwasser). — Los Alamitos, CA: IEEE Computer Society, 1994. — p. 124 — 134.

[22] Grover L. K. Quantum mechanics helps in searching for a needle in a haystack // Phys. Rev. Lett. — 1997. — 79. — p. 4709.

[23] Steane A. Quantum computing // Rep. Prog. Phys. — 1998. — 61. — 2. — p. 117 — 173.

[24] Боумейстер Д., Экерт А., Цайлингер А. Физика квантовой информации // М.: Постмаркет, 2002.

[25] Clauser J. F., Shimony A. Bell's theorem: Experimental tests and implications // Rep. Prog. Phys. — 1978. — 41. — p. 1881 — 1927.

[26] Wootters W.K. and Zurek W.H. A single quantum cannot be cloned // Nature. — 1982. — 299. — p. 802 — 803.

[27] Dieks D. Communication by EPR devices // Phys. Lett. A. — 1982. — 92. — p. 271 — 272.

[28] Bennett Ch.H. and Brassard G. Quantum key distribution and coin tossing // Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing (Bangalore, India). — 1984. — p. 175 — 179. E, New York, 1984, p. 175).

[29] Bennett Ch.H. and Brassard G. The dawn of a new era for quantum cryptography: The experimental prototype is working! // Special Interest Group on Automata and Computability Theory News. — 1989. — 20. — p. 78 — 82.

[30] Ekert A. K. Quantum cryptography based on Bell's theorem // Phys. Rev. Lett. — 1991. — 67. — 6. — p. 661 — 663.

[31] Bennett Ch. H. Quantum cryptography using any two nonorthogonal states // Phys. Rev. Lett. — 1992. — 68. — 21. — p. 3121 — 3124.

[32] Bruss D. Optimal eavesdropping in quantum cryptography with six states // Phys. Rev. Lett. — 1998. — 81. — 14. — p. 3018 — 3021.

[33] Grosshans F. and Grangier P. Continuous variable quantum cryptography using coherent states // Phys. Rev. Lett. — 2002. — 88. — 5. — 057902.

[34] http://www.magiq.com/

[35] http://www.idquantique.com/

[36] Gisin N., Ribordy G., Tittel W., and Zbinden H. Quantum cryptography // Rev. Mod. Phys. — 2002. — 74. — p. 145 — 195.

[37] Whitaker M. A. B. Theory and experiment in the foundations of quantum theory // Prog. Quantum Electron. — 2000. — 24. — p. 1 — 106.

[38] Кадомцев Б. Б. Динамика и информация // УФН. — 1994. — 164. — 5. — с. 449 — 530.

[39] Клышко Д. Н. Основные понятия квантовой физики с операциональной точки зрения Аннотация // УФН. — 1998. — 168. — 9. — с. 975 — 1015.

[40] Килин С. Я. Квантовая информация // УФН. — 1999. — 169. — 5. — с. 507 — 527.

[41] Менский М. Б. Квантовая механика: новые эксперименты, новые

приложения и новые формулировки старых вопосов // УФН. — 2000. — 170. — с. 631 — 647.

[42] Баргатин И. В., Гришанин Б. А., Задков В. Н. Запутанные квантовые состояния атомных систем // УФН. — 2001. — 171. — с. 625 — 647.

[43] Валиев К. А., Кокин А. А. Квантовые компьютеры: надежды и реальность // Ижевск: НИЦ Регулярная и хаотическая динамика, 2001.

[44] Белокуров В. В., Тимофеевская О. Д., Хрусталев О. А. Квантовая телепортация — обыкновенное чудо // Ижевск: НИЦ Регулярная и хаотическая динамика, 2000.

[45] Кадомцев Б. Б. Динамика и информация // М.: Редакция журнала УФН, 2000.

[46] Менский М. Б. Квантовые измерения и декогеренция // М.: Физматлит, 2001.

[47] Rudolph T. Quantum Information is physical too! // quant-ph/9904037.

[48] Grishanin B. A. and Zadkov V. N. Coherent and compatible information: A basis to information analysis of quantum systems // Proc. 17-th Int. Conf. on Coherent and Nonlinear Optics. — 2001. — Minsk, Belarus.

[49] Галлагер Р. Теория информации и надежная связь // М.: Сов. Радио, 1974.

[50] Hall M. J. W. Quantum information and correlation bounds // Phys. Rev. A. — 1997. — 55. — 1. — p. 100 — 113.

[51] Schumacher B. and Nielsen M. A. Quantum data processing and error correction // Phys. Rev. A. — 1996. — 54. — 2629.

[52] Lloyd S. Capacity of the noisy quantum channel // Phys. Rev. A. — 1997. — 55. — 3. — p. 1613 — 1622.

[53] Гришанин Б. А. Совместимая информация как естественная информационная мера квантового канала // Проблемы передачи информации. — 2002. — 38. — 1.

[54] Born M. Zur Quantenmechanik der Stossvorgänge // Zeitschrift für Physik. — 1926. — 37. — p. 863 — 867.

[55] Колмогоров А. Н. Основные понятия теории вероятностей // ОНТИ, 1936.

[56] Гришанин Б. А. Квантовые случайные процессы // http://comsim1.phys.msu.ru/ publications/papers/bagbook.ps.gz

[57] Jauch J. M. and Piron C. Generalized localizability // Helv. Phys. Acta. — 1967. — 40. — p. 559 — 570.

[58] Davies E. B. and Lewis J. T. An operational approach to quantum probability // Comm. Math. Phys. — 1970. — 17. — p. 239 — 260.

[59] Peres A. Quantum Theory: Concepts and Methods // Dordrecht: Kluwert, 1993.

[60] Preskill J. Lecture notes on Physics 229: Quantum information and computation // http://www.theory.caltech.edu/people/preskill/ph229/

[61] Стратонович Р. Л. Теория информации // М.: Сов. Радио, 1975.

[62] Caves C. M. and Fuchs C. A. Quantum information: How much information in a state vector? // quant-ph/9601025.

[63] von Neumann J. Mathematical Foundations of Quantum Mechanics // Princeton: Princ. Univ. Press, 1955.

[64] Гришанин Б. А. и Задков В. Н. Количественное измерение и физическое содержание квантовой информации // Радиотехника и электроника. — 2002. — 47. — 9. — с. 1029 — 1046.

[65] Klyshko D. N. Coherent Photon Decay in a Nonlinear Medium, Sov.Phys.JETP Lett. — 1967. — 6. — 23.

[66] Кривицкий Л. А., Кулик С. П., Пенин А. Н., Чехова М. В. Бифотоны как трехуровневые системы: преобразование и измерение // ЖЭТФ. — 2003. — 124. — 4(10). — с. 943.

[67] Сыч Д.В. Исследование общих свойств совместимой квантовой информации и её приложение к анализу проблемы Дике // Дипломная работа. — Москва. — Физический факультет МГУ. — 2001 г.

[68] Гришанин Б. А. и Задков В. Н. Простые квантовые системы как источник когерентной информации // ЖЭТФ. — 2000. — 118. — 5. — с. 1048 — 1065.

[69] Grishanin B. A. and Zadkov V. N. Coherent—information analysis of quantum channels in simple quantum systems // Phys. Rev. A. — 2000. — 62. — 032303.

[70] Stucki D., Gisin N., Guinnard O., Ribordy G., and Zbinden H. Quantum key distribution over 67 km with a plug&play system // New Jouranl of Physics. — 2002. — 4. — p. 41.1 — 41.8.

[71] Bechmann-Pasquinucci H. and Gisin N. Incoherent and coherent eavesdropping in the six–state protocol of quantum cryptography // Phys. Rev. A. — 1999. — 59. — 6. — p. 4238 — 4248.

[72] Gottesman D. and Lo H.-K. Proof of security of quantum key distribution with two-way classical communications // IEEE Trans. Inf. Theory. — 2002. — 49. — 457.

[73] Bechmann-Pasquinucci H. and Tittel W. Quantum cryptography using larger alphabets // Phys. Rev. A. — 2000. — 61. — 6. — 062308.

[74] Bourennane M., Karlsson A., and Bjork G. Quantum key distribution using multilevel encoding // Phys. Rev. A. — 2001. — 64. — 1. — 012306.

[75] Cerf N. J., Bourennane M., Karlsson A., and Gisin N. Security of

Quantum Key Distribution Using d-Level Systems // Phys. Rev. Lett. — 2002. — 88. — 12. — 127902.

[76] Борн М., Вольф Э. Основы оптики // М.: Наука, 1973, с. 50.

[77] Bennett C. H., Brassard G. and Robert J. M. Privacy amplification by public discussion // Soc. Ind. Appl. Math. J. Comp. — 1988. — 17. — 2. — 210 — 229.

[78] Fuchs C. A., Gisin N., Griffiths R. B., Niu C.-S., and Peres A. Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy // Phys. Rev. A. — 1997. — 56. — 2. — p. 1163 — 1172.

[79] Wootters W. K. and Fields B. D. Optimal state—determination by mutually unbiased measurements // Ann. Phys. — 1989. — 191. — 2. — p. 363 — 381.

[80] Гришанин Б. А., Сыч Д. В. Совместимая квантовая информация в задаче Дике // Вестник Московского Университета. Серия 3. Физика. Астрономия. — 2002. — 4. — с. 37 — 42.

[81] Sych D. V., Grishanin B. A., Zadkov V. N. Quantum key distribution with continuous alphabet // Laser Physics. — 2004. — 14. — 10. — p. 1314.

[82] Grishanin B. A., Sych D. V., Zadkov V. N. Unselected information as

an effective tool for quantum cryptography // SPIE Proc. 5161. Eds: Ronald E. Meyers and Yanhua Shih. 2004. — p. 341 — 351.

[83] Grishanin B. A., Sych D. V., Zadkov V. N. Noise-resistant quantum key distribution protocol // Proc. SPIE 5401 Eds: Kamil A. Valiev, Alexander A. Orlikovsky. — 2004. — p. 714 — 724.

[84] Sych D. V., Grishanin B. A., Zadkov V. N. Critical error rate of QKD protocols versus the size and dimensionality of the quantum alphabet // Phys. Rev. A. — 2004. — 70. — 052331.

[85] Сыч Д. В., Гришанин Б. А., Задков В. Н. Анализ предельно возможных информационных характеристик протоколов квантовой криптографии // Квантовая Электроника. — 2005. — 35. — 1. — с. 80 — 84.

[86] Denis V. Sych, Boris A. Grishanin, Victor N. Zadkov Compatible Information: Properties and application to physical problems // тезисы международной конференции “International Quantum Electronics Conference”. — 22 — 27 июня 2002. — Москва, Россия.

[87] Sych D. V., Grishanin B. A., Zadkov V. N. Some applications of compatible information to physical problems // тезисы международной конференции “Quantum Informatics — 2002”. — 1 — 4 октября 2002. — Звенигород, Россия.

[88] Сыч Д. В., Гришанин Б. А., Задков В. Н. Квантовая криптография с неселектированной информацией // тезисы международной

научной конференции студентов, аспирантов и молодых ученых "Ломоносов — 2003". — 15 — 18 апреля 2003. — Москва, Россия.

[89] Grishanin B. A., Sych D. V., Zadkov V. N. Unselected quantum information as an effective tool for quantum cryptography // тезисы международной конференции "International Symposium on Optical Science and Technology, SPIE's 48th Annual Meeting". — 3 — 8 августа 2003. — San Diego, USA.

[90] Sych D., Grishanin B., Zadkov V., Chirkin A. Noise-threshold-free quantum cryptography // тезисы международной конференции "8th International Conference on Squeezed States and Uncertainty Relations". — 9 — 13 июня 2003. — Puebla, Mexico.

[91] Sych D. V., Grishanin B. A., Zadkov V. N. Noise-resistant quantum key distribution protocol // тезисы международной конференции "Micro– and nanoelectronics — 2003". — 6 — 10 октября 2003. — Звенигород, Россия.

[92] Sych D. V., Grishanin B. A., Zadkov V. N. Information analysis of the quantum key distribution protocols // тезисы международной конференции "304. WE–Heraeus–Seminar: Elementary Quantum Processors". — 13 — 15 октября 2003. — Physikzentrum Bad Honnef, Germany.

[93] Denis Sych Quantum Cryptography with unselected information // те-

зисы международной конференции “2nd Asia–Pacific Workshop on Quantum Information Science”. — 15 — 19 декабря 2003. — Singapore.

[94] Сыч Д. В., Гришанин Б. А., Задков В. Н. Исследование зависимости эффективности протоколов квантовой криптографии от параметров квантового алфавита // тезисы международной научной конференции студентов, аспирантов и молодых ученых “Ломоносов — 2004”. — 12 — 15 апреля 2004. — Москва, Россия.

[95] Sych D. V., Grishanin B. A., Zadkov V. N. Comparative characteristics of quantum key distribution protocols with alphabets corresponding to the regular polyhedrons on the Bloch sphere // тезисы международной конференции “X International Conference on Quantum Optics — 2004”. — 30 мая — 3 июня, 2004. — Минск, Беларусь.

[96] Sych D. V., Grishanin B. A., Zadkov V. N. Six–state protocol critical error rate can be exceeded // тезисы международной конференции “IV International Symposium on Modern Problems of Laser Physics”. — 22 — 27 августа, 2004. — Новосибирск, Россия.

[97] Sych D. V., Grishanin B. A., Zadkov V. N. Optimal alphabets for noise–resistant quantum cryptography // тезисы международной конференции “Quantum informatics — 2004”. — 4 — 8 октября 2004. — Москва, Россия.