# Квантовая теория информации. Каналы и пропускные способности[1]

А.С. Холево

**Аннотация.** Квантовая теория информации изучает общие закономерности хранения и преобразования информации в системах, подчиняющихся законам квантовой механики, используя математические модели преобразователей информации - каналов связи - для исследования потенциальных возможностей таких систем, а также разрабатывает принципы их рационального и помехоустойчивого синтеза. Понятие пропускной способности канала - центральное в классической теории информации. Оказывается, что в квантовом случае это понятие разветвляется, порождая целый спектр информационных характеристик квантового канала связи. В статье представлен обзор ряда основных концепций и результатов, приводятся формулировки «теорем кодирования," дающих аналитические выражения для пропускных способностей квантового канала связи в терминах его энтропийных характеристик, при этом подчеркнута особая роль, которую играет квантовое свойство сцепленности.

**Ключевые слова:** квантовый канал связи, энтропия, пропускные способности, квантовая сцепленность.

## Введение

Одним из магистральных направлений научно-технического прогресса является микроминиатюризация устройств обработки информации, вплоть до освоения молекулярных и атомных масштабов, что в конечном счете ведет к необходимости привлечения квантово-механических представлений. С другой стороны, разработка средств оптической связи, использующих когерентное лазерное излучение, привела к появлению квантовой оптики и квантовой электроники. Квантовая теория информации изучает общие закономерности хранения и преобразования информации в любых системах, подчиняющихся законам квантовой механики, используя математические модели преобразователей информации - каналов связи - для исследования потенциальных возможностей таких систем, а также разрабатывает принципы их рационального и помехоустойчивого синтеза.

Практически одновременно с изобретением транзистора, с которого началась современная микроэлектроника, появились идеи теории информации, послужившие основой для перехода на принципы цифрового представления и обработки данных. В 1948 г. была опубликована историческая работа К. Шеннона [13], а еще ранее в трудах В.А. Котельникова [6] были сформулированы принципы теории помехоустойчивой связи[2]. Квантовая теория информации сформировалась как самостоятельная дисциплина в 1990-е годы, однако ее зарождение относится к 1950-м гг. С появлением источников когерентного излучения и оптической связи встал вопрос о фундаментальных ограничениях на возможности передачи и обработки сообщений, накладываемых природой физического носителя информации [19, 20]. Современное развитие информационных технологий заставляет предположить, что в обозримой перспективе такие

[1] Доклад на научной сессии Отделения нанотехнологий и информационных технологий РАН "Квантовые компьютеры и квантовая информатика" 25 февраля 2010 г. Работа частично поддержана грантом РФФИ 09-01-07066 и программой РАН "Математическая теория управления".

[2] Примечательно, что В.А. Котельников сохранял интерес к квантовой механике в течение всей своей жизни [7].

ограничения станут основным препятствием для дальнейшей экстраполяции существующих принципов обработки информации. Систематическое изучение этих фундаментальных ограничений привело к построению в 1960-80 гг. квантовой теории статистических решений (т.е. оптимального обнаружения и оценивания квантовых сигналов) [9, 11]. Появление в 1980-90 гг. идей квантового компьютинга (Р. Фейнман, Ю. И. Манин, П. Шор), квантовой криптографии и новых коммуникационных протоколов (Ч. Беннет и др.) позволило говорить не только об ограничениях, но и новых возможностях, заключенных в использовании специфически квантовых ресурсов, таких как квантовый параллелизм, сцепленность (entanglement) и дополнительность между измерением и возмущением [8, 25]. К настоящему моменту квантовая теория информации является развитой научной дисциплиной, которая дает ключ к пониманию фундаментальных закономерностей, до недавних пор остававшихся вне поля зрения исследователей, а также стимулирует развитие экспериментальной физики, значительно расширяющее возможности целенаправленного манипулирования состояниями микросистем и потенциально важное для новых эффективных приложений. Работы в области квантовой информатики, включающей квантовую теорию информации, ее экспериментальные основы и технологические разработки, ведутся в научно-исследовательских центрах всех развитых стран.

## 1. Классическая и квантовая информация

Носителем информации является состояние квантовой системы, которое представляет собой информационный ресурс постольку, поскольку имеет статистическую неопределенность. При математическом рассмотрении *чистому состоянию* соответствует ортогональный проектор $|\psi\rangle\langle\psi|$ на вектор $|\psi\rangle$ из гильбертова пространства системы $\mathcal{H}$. В квантовой статистике рассматриваются также *смешанные состояния*, представляющие собой статистический ансамбль чистых состояний $|\psi_i\rangle\langle\psi_i|$ с вероятностями $p_i$. Такое состояние описывается оператором плотности $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$, который характеризуется свойствами: 1) $\rho$ - положительный оператор; 2) $\rho$ имеет единичный след, $\mathrm{Tr}\rho = 1$. Таким образом, собственные числа $\lambda_j$ оператора плотности образуют распределение вероятностей. Шенноновская энтропия этого распределения, совпадающая с энтропией фон Неймана оператора плотности,

$$H(\rho) = -\sum_j \lambda_j \log_2 \lambda_j = -\mathrm{Tr}\rho\log_2\rho,$$

является мерой неопределенности и, как объясняется ниже, информационного содержания состояния $\rho$.

При передаче классической информации (т.е. произвольного сообщения) по квантовому каналу она записывается в квантовом состоянии. Это означает, что передаваемый сигнал $x$ используется как один из параметров процедуры приготовления состояния, что в конечном счете выражается в зависимости приготовленного состояния $\rho_x$ от $x$.

Однако вся полнота информационного содержания квантового состояния не может быть сведена к классическому сообщению и поэтому заслуживает специального термина *квантовая информация*. Это связано с тем, что квантовое состояние содержит в себе информацию о статистике всевозможных, в том числе и взаимоисключающих (дополнительных), измерений над системой. Наиболее ярким отличием квантовой информации является *невозможность копирования* (no-cloning). Очевидно, что в принципе классическая информации может воспроизводиться в любом количестве. Но физический прибор, который бы выполнял аналогичную задачу для квантовой информации, противоречит принципам квантовой механики, так как преобразование

$$|\psi\rangle \to \underbrace{|\psi\rangle\otimes\cdots\otimes|\psi\rangle}_{n}$$

является нелинейным и не может быть осуществлено унитарным оператором. Конечно, это можно сделать каждый раз специальным прибором для данного конкретного состояния (и даже для фиксированного набора ортогональных состояний), но не существует универсального прибора, который бы размножал произвольное квантовое состояние.

Подобно тому, как количество классической информации может быть измерено минимальным числом двоичных символов (битов), необходимым для кодирования (сжатия) сообщения, количество квантовой информации может быть определено как минимальное число элементарных квантовых систем с двумя уровнями (q-*битов* или кубитов), необходимое для хранения или передачи данного ансамбля квантовых состояний при оптимальном кодировании. Показано (Шумахер-Джоза, [21]), что для асимптотически безошибочной передачи квантового сообщения длины $n \to \infty$, в котором состояния $|\psi_i\rangle\langle\psi_i|$ появляются с вероятностями $p_i$, необходимо $nH(\rho)$ q-бит, где $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. Это означает, что размерность квантовой системы, в которой осуществляется оптимальное сжатие квантовой информации, содержащейся в состоянии $\rho^{\otimes n}$, равна $\approx 2^{nH(\rho)}$. Это, в частности, позволяет оценить размер квантового регистра, в который можно "упаковать" данное квантовое сообщение.

Это утверждение, являющееся квантовым аналогом 1-й теоремы Шеннона о кодировании источника информации, показывает, что в квантовой теории информации логарифм размерности пространства векторов состояний является мерой максимального информационного содержания системы, и играет здесь ту же роль, что логарифм размера фазового пространства для классических систем.

## 2. Сцепленностъ квантовых состояний

Как и в классической теории информации, для передачи длинных сообщений используется принцип блочного кодирования. При этом постоянно приходится иметь дело с составными квантовыми системами, отвечающими повторному либо параллельному использованию каналов связи.

*Квантовая сцепленностъ* (Verschranktheit, entanglement, "запутанность", "перепутанность") отражает необычные свойства составных квантовых систем, которые описываются тензорным (а не декартовым, как в классической механике) произведением подсистем. Сцепленность возникает при квантовом взаимодействии подсистем. В силу принципа суперпозиции, пространство составной системы $AB$ наряду с векторами вида $|\psi_A\rangle\otimes|\psi_B\rangle$ содержит и всевозможные их линейные комбинации $\sum_j |\psi^j{}_A\rangle\otimes|\psi^j{}_B\rangle$. Состояния составной системы, задаваемые векторами-произведениями, называются *разделимыми* или несцепленными, а все не сводящиеся к таковым - *сцепленными*. Смешанное состояние называется разделимым, если оно является смесью состояний-произведений. Сцепленность представляет собой чисто квантовое свойство, лишь отчасти родственное классической коррелированное, однако к ней не сводящееся (в физике говорят о корреляциях Эйнштейна-Подольского-Розена, поскольку эти авторы впервые обратили внимание на необычные свойства таких корреляций). Именно, наличие сцепленных состояний противоречит гипотезе о локальной теории со скрытыми параметрами, т.е. классическому статистическому описанию квантовых систем, удовлетворяющему физическому требованию локальности [11].

Большой раздел квантовой теории информации посвящен количественной теории сцепленности, которая представляет собой своеобразную комбинаторную геометрию тензорных произведений гильбертовых пространств (например, [23]). В частности, показано, что мера сцепленности чистого состояния $\rho_{AB}$ составной системы $AB$ определяется однозначно как энтропия частичного следа $\mathrm{Tr}_B\rho_{AB}$, тогда как для смешанных состояний имеется целый ряд существенно различных характеристик, важнейшей из которых является *сцепленность формирования*

$$E_F(\rho_{AB}) = min\sum_i p_i H(\mathrm{Tr}_B P_{\psi i}),$$

где минимум берется по всевозможным ансамблям, представляющим состояние $\rho_{AB.}$ Показано, что эта характеристика связана с количеством максимально сцепленных пар q-битов (т. н. е-битов), которое необходимо для создания состояния $\rho_{AB}$ с использованием локальных операций (затрагивающих только $A$ либо $B$) и обмена классической информацией между $A$ и $B$.

Двойственным образом, в составных квантовых системах существуют сцепленные и несцепленные *наблюдаемые* (измерения). Если квантовые системы $A$ и $B$ находятся в несцепленном состоянии, то максимальные шенноновские количества информации о состоянии $I_A$, $I_B$, $I_{AB}$, получаемые, соответственно, из измерений над системами $A$, $B$ и составной системой $AB$ удовлетворяют в общем случае соотношению $I_{AB} > I_A + I_B$ . Этот неклассический феномен строгой *супераддитивности* информации обнаруживается и играет важную роль в теории пропускной способности квантового канала связи.

## 3. Передача классической информации по квантовому каналу

В дальнейшем мы сосредоточимся на одной из главных тем - квантовых каналах связи и их пропускных способностях, которая является развитием классической шенноновской теории. Подчеркнем, что при всей ее важности, эта тема далеко не исчерпывает содержание квантовой теории информации, некоторые разделы которой, такие как количественная теория сцепленности, вообще не имеют классического аналога. Другие направления будут кратко затронуты в заключении.

В теории информации центральную роль играет понятие канала связи и его пропускной способности, дающей предельную скорость безошибочной передачи. Математический подход придает этим понятиям универсальную значимость: например, память компьютера (классического или квантового) может рассматриваться как канал из прошлого в будущее, а пропускная способность дает количественное выражение для предельной емкости памяти при исправлении ошибок. Важность рассмотрения квантовых каналов связи обусловливается тем, что всякий физический канал в конечном счете является квантовым и такой подход позволяет учесть фундаментальные квантово-механические закономерности. Существенно, что в квантовом случае понятие пропускной способности разветвляется, порождая целый спектр информационных характеристик канала, зависящих от вида передаваемой информации (квантовой или классической), а также от дополнительных ресурсов, используемых при передаче [17, 12].

Теоремы кодирования дают явные выражения для пропускных способностей через энтропийные параметры канала. Одним из главных достижений квантовой теории информации является открытие целого набора важнейших энтропийных характеристик.

При передаче классической информации (т.е. сообщения $w = (x_1,..., x_n)$) по квантовому каналу связи она записывается в квантовом состоянии посредством задания значений параметров прибора, приготавливающего состояние $\rho_w$. Приемник производит квантовое измерение над состоянием на выходе канала связи, результатом которого являются значения $w' = (y_1,..., y_n)$. Процесс передачи классической информации описывается диаграммой

$$w \xrightarrow{\text{кодирование}} \rho_w \xrightarrow{\text{канал}} \rho_w{}' \xrightarrow{\text{декодирование}} w' \qquad (1)$$

Простейшая математическая модель канала задается семейством квантовых состояний $\{\rho_x\}$ в пространстве $\mathcal{H}$, где $x$ входной сигнал. Такой канал называется *классически-квантовым* (вход - классический, выход - квантовый). Отображение $x \to \rho_x$ в сжатой форме содержит описание процесса, порождающего состояние $\rho_x$. Например, если $x = 0,1$, причем $\rho_o$ когерентное состояние лазерного излучения с комплексной амплитудой $z$, а $\rho_1$ - с амплитудой - $z$, то имеется классически-квантовый канал с двумя чистыми неортогональными состояниями [12]. Если буквы сообщения $w = (x_1,..., x_n)$ передаются независимо (канал без памяти), то на выходе возникает несцепленное состояние $\rho_{x1} \otimes \cdots \otimes \rho_{xn}$. На выходе производится квантовое измерение $M^{(n)}$, результатом которого является некоторая оценка для $w$. *Классическая пропускная способность* рассматриваемого канала определяется как

$$C = \lim_{n\to\infty} C^{(n)} / n, \qquad (2)$$

где $C^{(n)}$ - максимальное шенноновское количество информации, которое может быть получено путем применения произвольных классических кодирований на входе и квантовых измерений на выходе. Оказывается, что в общем случае $C^{(n)} > nC^{(1)}$ т.е. для квантовых каналов без памяти передаваемая классическая информация может быть строго супераддитивна, что обусловлено существованием сцепленных измерений на выходе канала. Более того, в отличие от классического канала без памяти, возможно строгое неравенство $C > C^{(1)}$; при этом для величины $C$, определенной в (2), имеет место явное выражение

$$C = \max_{p_x} \left\{ H\left( \sum_x p_x \rho_x \right) - \sum_x p_x H(\rho_x) \right\}, \quad (3)$$

составляющее содержание *теоремы кодирования* [12]. Это утверждение, доказанное Холево [10, 24] (см. также Шумахер-Вестморленд [26]), можно рассматривать как "классически-квантовый" аналог 2-й теоремы Шеннона о кодировании для канала с шумом.

Очевидным, но важным следствием является неравенство

$$C \le \log \dim \mathcal{H}, \quad (4)$$

в котором равенство достигается для идеального канала с ортогональными состояниями. Таким образом, то обстоятельство, что $\mathcal{H}$ содержит бесконечное число различных векторов состояний, не позволяет увеличить пропускную способность выше предельного информационного ресурса квантовой системы: с неограниченным увеличением числа сигнальных векторов они становятся все более неразличимы при квантовом измерении. В примере канала с двумя когерентными состояниями

$$C = h_2\left( \frac{1+\varepsilon}{2} \right), \quad (5)$$

где $\varepsilon = \langle z | -z \rangle = \exp(-2|z|^2)$, тогда как

$$C_1 = \max_{\pi, \mathrm{M}} J(\pi, M) = 1 - h_2\left( \frac{1+\sqrt{1-\varepsilon^2}}{2} \right), \quad (6)$$

так что $C/C_1 > 1$, причем отношение стремится к $\infty$ при $\varepsilon \to 1$, т.е. $z \to 0$.

## 4. Пропускная способность квантового канала

В общем случае как выход, так и вход канала являются квантовыми; такой канал представляет собой открытую квантовую систему, взаимодействующую с окружением, которое привносит помехи в передаваемое состояние. Рассмотрим (вообще говоря, необратимую) эволюцию открытой системы, взаимодействующей с окружением. Обозначим $\mathcal{H}$ гильбертово пространство системы, $\mathcal{H}_E$ - пространство окружения, и пусть $\rho_E$ - начальное чистое состояние окружения. Предположим, что обратимая эволюция, описывающая взаимодействие системы с окружением, задается унитарным оператором $U$. Тогда эволюция системы дается формулой

$$\Phi[\rho] = \mathrm{Tr}_{\mathcal{H}_E} U(\rho \otimes \rho_E) U^*. \quad (7)$$

С точки зрения теории информации канал связи вполне определяется отображением $\rho \to \mathbf{\Phi}[\rho]$, переводящим состояния на входе в состояния на выходе. Отображение $\mathbf{\Phi}$ дает сжатое статистическое описание результата взаимодействия системы на входе с ее окружением (шумом). Например, *деполяризующий* канал (с вероятностью ошибки $p$) задается формулой

$$\Phi[\rho] = (1-p)\rho + p\frac{1}{d}\mathrm{Tr}\rho, \quad (8)$$

где $\dim \mathcal{H} = d$. Это соотношение описывает смесь идеального канала и полностью деполяризующего канала, который переводит любое состояние в хаотическое $\bar{\rho} = \frac{I}{d}$

Применение квантовой теоремы кодирования (3) дает следующее выражение для классической пропускной способности канала $\Phi$

$$C(\Phi) = \lim_{n\to\infty} \frac{1}{n} C_\chi(\Phi^{\otimes n}), \quad (9)$$

где

$$C_\chi(\Phi) = \max_{p_i, \rho_i} \left\{ H\left( \sum_i p_i \Phi[\rho_i] \right) - \sum_i p_i H(\Phi[\rho_i]) \right\}. \quad (10)$$

Если выполняется свойство *аддитивности*, $C_\chi(\Phi^{\otimes n}) = nC_\chi(\Phi)$, то $C(\Phi) = \overline{C}(\Phi)$; это означает, что использование сцепленных состояний на входе, в отличие от сцепленных измерений на выходе, не позволяет увеличить количество передаваемой классической информации. Справедливость этого свойства была установлена для ряда каналов [12, 23], в частности, для деполяризующего канала (8). Это позволяет найти его пропускную способность

$$C(\Phi) = C_\chi(\Phi) = \log d + $$
$$+\left(1 - p\frac{d-1}{d}\right)\log\left(1 - p\frac{d-1}{d}\right) + p\frac{d-1}{d}\log\frac{p}{d}. \quad (11)$$

Аддитивность величины $C_\chi(\Phi)$ означает, что использование сцепленных кодовых состояний не увеличивает классическую пропускную способность. Долгое время оставался открытым вопрос, существуют ли вообще каналы, не обладающие таким свойством аддитивности. Лишь недавно удалось показать [22], что такие каналы существуют, по крайней мере в очень высоких размерностях, хотя конструктивного примера до сих пор нет.

## 5. Квантовая сцепленность как информационный ресурс

Неклассический феномен супераддитивности информации в квантовом канале связи имеет в своей основе сцепленные кодирования и декодирования. Еще более впечатляющий выигрыш приносит введение сцепленности как дополнительного информационного ресурса. Классическая пропускная способность канала Ф может быть увеличена путем использования сцепленности между входом и выходом канала, при том, что наличие одной только сцепленности не позволяет передавать информацию. Здесь, как и в ряде других случаев, сцепленность играет роль "катализатора", выявляющего скрытые ресурсы квантовой системы. Если Ф - идеальный канал, т.е. канал без шума, то выигрыш в пропускной способности, доставляемый так называемым сверхплотным кодированием, двукратен. Чем более канал отличается от идеального, тем выигрыш больше, и в пределе для каналов с очень большим шумом может быть сколь угодно большим. Для *классической пропускной способности с использованием сцепленного состояния* имеется простая формула (Беннет-Шор-Смолин-Таплиял, [16])

$$C_{ea}(\Phi) = \max_\rho I(\rho,\Phi), \quad (12)$$

где $I(\rho,\Phi)$ - *квантовая взаимная информация* между передатчиком и приемником, задаваемая соотношением

$$I(\rho,\Phi) = \{H(\rho) + H(\Phi(\rho)) - H(\rho;\Phi)\}. \quad (13)$$

Здесь $H(\rho)$, $H(\Phi(\rho))$ - энтропии, соответственно, входного и выходного состояний, а $H(\rho;\Phi)$ - так называемая *обменная энтропия*, равная приращению энтропии окружения. Поскольку начальное состояние окружения $\rho_E$ предполагается чистым, то $H(\rho;\Phi) = H(\rho_E')$, где $\rho_E'$ - конечное состояние окружения

$$\rho_E' = \mathrm{Tr}_{\mathcal{H}} U(\rho\otimes\rho_E)U^*.$$

Например, для деполяризующего канала (8)

$$C_{ea}(\Phi) = \log d^2 + \left(1 - p\frac{d^2-1}{d^2}\right)\log\left(1 - p\frac{d^2-1}{d^2}\right) +$$
$$+p\frac{d^2-1}{d^2}\log\frac{p}{d^2}. \quad (14)$$

Сравнивая это с величиной $C(\Phi)$, которая дается формулой (11), мы видим, что выигрыш $\frac{C_{ea}(\Phi)}{C_\chi(\Phi)} > 1$, причем $\frac{C_{ea}(\Phi)}{C_\chi(\Phi)} \to d+1$ в пределе сильного шума $p \to 1$.

## 6. Квантовая пропускная способность

Преобразование квантового состояния $\rho \to \Phi[\rho]$ можно рассматривать как передачу квантовой информации. Теория предсказывает возможность нетривиального способа передачи, при котором носитель состояния физически не пересылается, а передается лишь некоторая классическая информация (так называемая *телепортация квантового состояния*) [17]. При этом необходимым дополнительным ресурсом также является сцепленность между входом и выходом канала связи. Свести передачу произвольного квантового состояния только к передаче классической информации, не используя дополнительного квантового ресурса, невозможно: поскольку классическая информация копируема, это означало бы возможность копирования и квантовой информации.

Открытие *квантовых кодов, исправляющих ошибки* [17, 8] поставило вопрос об асимптотически (при $n \to \infty$) безошибочной передаче квантовых сообщений каналом $\Phi^{\otimes n}$. При этом *квантовая пропускная способность* $Q(\Phi)$ определяется как максимальное количество передаваемой квантовой информации и связана с размерностью подпространства векторов входного пространства $\left(\approx 2^{nQ(\Phi)}\right)$, отвечающие которым состояния передаются асимптотически безошибочно. Для нее имеется выражение через *когерентную информацию* $I_c(\rho, \Phi) = H(\Phi(\rho)) - H(\rho; \Phi)$, а именно

$$Q(\Phi) = \lim_{n\to\infty} \frac{1}{n} \max_{\rho^{(n)}} I_c(\rho^{(n)}, \Phi^{\otimes n}) . \qquad (15)$$

Доказательство (Деветак, [18]) основано на глубокой аналогии между квантовым каналом и классическим каналом с перехватом, причем в квантовом случае роль перехватчика информации играет окружение рассматриваемой системы. Величина $Q(\Phi)$ тесно связана с криптографическими характеристиками канала, такими как пропускная способность для секретной передачи классической информации и скорость распределения случайного ключа.

Аналитическое выражение для квантовой пропускной способности деполяризующего канала до сих пор неизвестно, хотя имеются достаточно близкие нижние и верхние оценки.

## 7. Многообразие пропускных способностей

В классической теории информации хорошо известно, что обратная связь не увеличивает пропускную способность канала и шенноновская пропускная способность остается основной характеристикой. В квантовом случае аналогичный факт установлен для $C_{ea}(\Phi)$, а относительно $Q(\Phi)$ известно следующее: квантовая пропускная способность не может быть увеличена с помощью дополнительного классического канала от входа к выходу, сколь ни велика была бы его пропускная способность. Однако она может увеличиться, если есть возможность передачи классической информации в обратном направлении. Такая передача позволяет создать максимальную сцепленность между входом и выходом, которая может быть использована для телепортации квантового состояния. Даже канал с нулевой квантовой пропускной способностью, дополненный классической обратной связью, может быть использован для передачи квантовой информации [8].

Три пропускные способности (9), (12), (15) связаны соотношением $Q(\Phi) \le C(\Phi) \le C_{ea}(\Phi)$ и образуют основу для определения и изучения всего многообразия пропускных способностей квантового канала связи, которое возникает при применении дополнительных ресурсов, таких как обратная или прямая связь, коррелированность или сцепленность. Так, в квантовой теории информации изучаются классическая и квантовая пропускные способности с обратной связью (обозначаемые, соответственно, $C_{\leftarrow}, Q_{\leftarrow}$), а также классическая и квантовая пропускные способности с дополнительным независимым классическим двусторонним каналом (соответственно, $C_{\leftrightarrow}, Q_{\leftrightarrow}$). Для квантового канала имеет место следующая иерархия

$$\begin{array}{ccccccc} C_\chi & \le & C_{\leftarrow} & \le & C_{\leftrightarrow} & \le & C_{ea} \\ \text{VI} & & \text{VI} & & \text{VI} & & \text{VI} \; , \\ Q & \le & Q_{\leftarrow} & \le & Q_{\leftrightarrow} & \le & Q_{ea} \end{array}$$

где $\le$ следует понимать как "меньше или равно для всех каналов и строго меньше для некоторых [15]. Известно также, что $C_{ea} = 2Q_{ea}$ и для ряда остальных пар возможны неравенства как в ту, так и в другую стороны. Далее, оказывается возможным построить так называемый "материнский" протокол передачи через квантовый канал, который при использовании различных частных дополнительных ресурсов (таких, например, как обратная связь либо сцепленность) позволяет реализовать всевозможные способы передачи, включая упомянутые выше [14].

## 8. Другие направления

Дальнейшее развитие теории приводит к изучению *квантовых каналов с памятью и систем с многими пользователями*. Большой раздел квантовой теории информации посвящен исследованию систем с "непрерывными переменными", основанных на принципах квантовой оптики. Многие эксперименты по квантовой обработке информации реализованы именно в таких системах. Особенно важными здесь являются *гауссовские состояния*, включающие когерентные и сжатые состояния, реализуемые в лазерах и нелинейных квантовых оптических устройствах, и соответствующий класс преобразователей квантовой информации - *гауссовские каналы*. Для них получен ряд результатов, касающихся сцепленности состояний, пропускных способностей и других информационных характеристик [12].

В заключение перечислим ряд других направлений, некоторые из них были лишь вскользь упомянуты выше:

- квантовая теория оценивания состояний;
- количественные характеристики сцепленности;
- алгоритмы сжатия квантовой информации;
- квантовые коды, исправляющие ошибки; вычисления, устойчивые к ошибкам;
- быстрые квантовые алгоритмы; сложность квантовых вычислений;
- квантовая криптография.

Последние 15 лет характеризуются нарастающим потоком публикаций в этой области. Основным и наиболее оперативным источником научной информации является электронный архив Корнеллского университета (прежде - исследовательского центра в Лос-Аламосе): http://xxx.arxiv.org/quant-ph/. Появились специализированные журналы: Quantum Information Processing; International Journal of Quantum Information; Quantum Information and Computation, Квантовый компьютер и квантовые вычисления. Эта тематика представлена в таких известных журналах как Physical Reviews; Physical Reviews Letters; IEEE Transactions on Information Theory; Communications on Mathematical Physics; Journal of Mathematical Physics; Проблемы передачи информации, появилась и монографическая литература, представление о которой дает библиография к этой статье.

## Литература


1. Боумейстер Д., Экерт А., Цайлингер А., Физика квантовой информации, М., 2002.
2. К.А. Валиев, Исследования в области квантовых технологий в информатике и метрологии, Вестник РАН, 73 №5, (2003), 400-405.
3. К.А. Валиев, А.А. Кокин, Квантовые компьютеры: надежды и реальность, М.-Ижевск: РХД, 2001.
4. Б.Б. Кадомцев, Динамика и информация, М., УФН, 1999.
5. А.Ю. Китаев, А. Шень, М. Вялый, Классические и квантовые вычисления, М.: МЦНМО 1999.
6. Котельников В.А. Теория потенциальной помехоустойчивости. М.; Л., 1956.
7. Котельников В.А. Модельная нерелятивистская квантовая механика. Размышления. М.: Физматлит 2008.
8. Нильсен М.А., Чанг И., Квантовые вычисления и квантовая информация, М.: Мир, 2006.
9. Хелстром К., Квантовая теория проверки гипотез и оценивания, М.: Мир 1978.
10. Холево А.С, Некоторые оценки для количества информации, передаваемого квантовым каналом связи, Пробл. передачи информ. 9 №3, (1973), 3-11.
11. Холево А.С, Вероятностные и статистические аспекты квантовой теории, 2 изд., М.-Ижевск: ИКИ 2004.
12. Холево А.С, Квантовые системы, каналы, информация, М., МЦН-МО 2010.
13. Шеннон К. Математическая теория связи. В кн.: теория передачи электрических сигналов при наличии помех. М.: ИЛ 1953.
14. A. Abeyesinghe, I. Devetak, P. Hayden, A. Winter, The mother of all protocols: Restructuring quantum information's family tree, arXiv:quant-ph/0606225.
15. Bennett, I. Devetak, P. W. Shor, J. A. Smolin, Inequality and separation between assisted capacities of quantum channel, arXiv:quant-ph/0406086.
16. C. H. Bennett, P. W. Shor, J. A. Smolin, A. V. Thapliyal, Entanglement-assisted Capacity of a Quantum Channel and the Reverse Shannon Theorem, IEEE Transactions on Information Theory, 48, 2637 (2002).
17. Bennett C. H., Shor P. W., Quantum information theory, IEEE Trans. Inform. Theory, 1998, 44, 2724-2742.
18. I. Devetak, The private classical information capacity and quantum information capacity of a quantum channel, IEEE Transactions on Information Theory, 51(1), 44-55 (2005).
19. Gabor D., Communication theory and physics, Phil. Mag., 41, (1950), 1161-1187.
20. J.P. Gordon, Quantum effects in communication systems, Proc. IRE, Sep. 1962, 1898-1908.
21. R. Josza, B. Schumacher, A new proof of the quantum noiseless coding theorem, J. Modern Optics 41, pp. 2343-2349 1994.
22. M.B. Hastings, Superadditivity of communication capacity using entangled inputs, Nature Physics 5, 255 (2009); arXiv:0809.3972quant-ph..
23. Hayashi M., Quantum information: an introduction. Berlin-New York, Springer 2006.
24. A.S. Holevo, The capacity of quantum communication channel with general signal states, IEEE Trans. Inform. Theory 44, 269-272 1998; arXiv: quant-ph/9611023, 1996.
25. Knill E., Nielsen M. A., Quantum information processing, Encyclopaedia of Mathematics, Supplement III, 2002.
26. B. Schumacher, M. D. Westmoreland, Sending classical information via noisy quantum channel, Phys. Rev. A. 56, 131-138 1997.


**Холево Александр Семенович**. Ведущий научный сотрудник Математического института им. В.А. Стеклова РАН. Окончил МФТИ в 1966 году. Профессор, доктор физико-математических наук. Автор 170 научных работ (в их числе пяти монографий). Лауреат премии им. А.А. Маркова Российской академии наук за 1997г., международной премии "Quantum Communication Award" за 1996г. и премии А. фон Гумбольдта за 1999г. Специалист в областях теории вероятностей, математической статистики, теории информации, математической физики. Круг научных интересов: квантовая теория информации и статистических решений, некоммутативная теория вероятностей, математические основания квантовой теории. E-mail: holevo@mi.ras.ru.