Пропускные способности квантовых каналов

А.С.Холево

Дан краткий обобщенный обзор теории пропускных способностей квантовых каналов связи, являющейся развитием классической шенноновской теории. В отличие от классического канала связи, квантовый канал характеризуется целым набором различных пропускных способностей, зависящих от вида передаваемой информации (классической или квантовой), а также от дополнительных ресурсов, используемых при передаче. Рассмотрены основные характеристики квантового канала: классическая пропускная способность, классическая пропускная способность с использованием сцепленности (между входом и выходом канала), квантовая пропускная способность, секретная классическая пропускная способность. Подчеркнута уникальная роль квантового свойства сцепленности, которое находит проявление, в частности, в неклассическом феномене супераддитивности пропускных способностей.

Ключевые слова: *квантовая теория информации, квантовый канал связи, теорема кодирования, пропускная способность, сцепленность, супераддитивность.*

1. Введение

Квантовая теория информации – научная дисциплина, изучающая закономерности передачи и преобразования информации в системах, подчиняющихся законам квантовой механики. В настоящем обзоре затронута лишь одна, но весьма важная тема – теорема кодирования для квантовых каналов связи, и подчеркнута та особая роль, которую играет квантовое свойство сцепленности*. Понятие пропускной способности канала – центральное в классической теории Шеннона. В квантовом случае это понятие разветвляется, порождая целый спектр информационных характеристик квантового канала.

Квантовая теория информации является источником целого ряда математических задач, мотивированных физически, зачастую формулируемых достаточно элементарно, но трудно решаемых (или до сих пор нерешенных). Ее основной математический аппарат – линейная алгебра, теория операторов в гильбертовом пространстве, как правило, конечномерном. Подробное, более углубленное изложение рассматриваемых здесь вопросов, включающее многочисленные примеры, можно найти в книгах [1, 2], а также в курсе лекций [3]. Следует, однако, отметить, что со времени написания этих книг в решении некоторых открытых вопросов достигнут прогресс, получивший отражение в настоящей работе.

2. Рандомизация, сцепленность и информация

Для того чтобы понять, в чем проявляется различие между классическими и квантовыми системами с информационной точки зрения, рассмотрим следующее утверждение:

Принцип (C). Введение дополнительного независимого шума в наблюдения не может увеличить количество информации о наблюдаемой системе. Этот принцип представляется правдоподобным, и он в самом деле верен, если речь идет о классических системах. Уточним его, дав математическую формулировку. Пусть наблюдаемая классическая система описывается случайной величиной Y. Неопределенность состояния этой системы задается другой случайной величиной X, коррелированной с Y. Мерой неопределенности может служить энтропия распределения $\{p_x\}$ случайной величины X:

$$H(X) = -\sum_x p_x \log_2 p_x. \tag{1}$$

Количество информации о состоянии системы, содержащееся в наблюдении Y, выражается формулой Шеннона

$$I(X;Y) = H(X) + H(Y) - H(XY), \tag{2}$$

$$I(X;Y) = H(Y) - H(Y|X), \tag{3}$$

где $H(XY)$ – энтропия совместного распределения случайных величин X, Y; $H(Y|X) = H(XY) - H(Y)$ – условная энтропия. Допустим, что помимо Y наблюдается независимый шум Y_0, тогда количество информации о состоянии системы, содержащееся в наблюдении YY_0, есть $I(X;YY_0)$. Простой расчет с использованием формул (1), (2) показывает, что

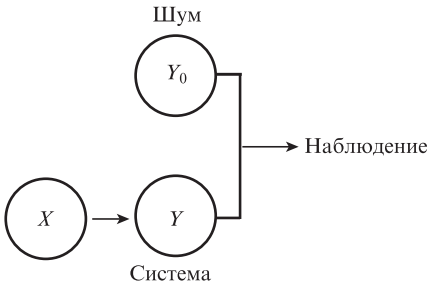
$$I(X;YY_0) = I(X;Y). \tag{4}$$

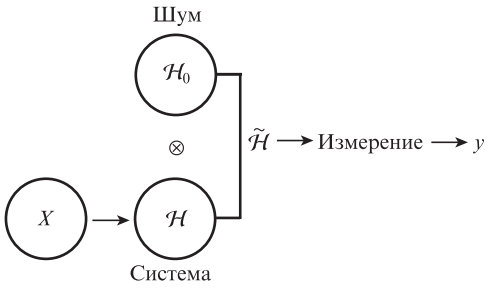
Это и есть количественное выражение сформулированного выше принципа (C) для классических систем. Введение дополнительного независимого шума в принимаемое решение называется рандомизацией. Отметим, что в классической статистике существуют другие ситуации (игрового характера, когда неизвестное состояние выбирается наихудшим для наблюдателя образом), в которых веро-

*Перевод английского термина «entanglement». В отечественной литературе используются термины «запутанность», «перепутанность».

А.С.Холево. Математический институт им. В.А.Стеклова РАН, Россия, 119991 Москва, ул.Губкина, 8; e-mail: holevo@mi-ras.ru

Поступила в редакцию 11 февраля 2020 г.





ятностный выбор решения оказывается в среднем выгодным. В рассмотренной ситуации простого наблюдения этот принцип представляется очевидным, если не сказать тривиальным. Однако он перестает быть справедливым, если речь идет о квантовых системах.

Утверждение (Q). Введение дополнительного независимого квантового шума в наблюдения (квантовая рандомизация) может увеличить количество информации о наблюдаемой квантовой системе. Для того чтобы дать точную формулировку, напомним основные элементы математического описания квантовых систем. В квантовой теории:

– системе сопоставляется гильбертово пространство $\mathcal{H}$;

– состояния системы описываются единичными векторами $\psi \in \mathcal{H}$;

– измерению (идеальному) с исходами y сопоставляется ортонормированный базис $\{e_y\} = E$ в $\mathcal{H}$;

– вероятность исхода y при измерении E в состоянии ψ

$$\mathcal{P} = (y|\psi) = |\langle \psi|e_y \rangle|^2. \tag{5}$$

Рассмотрим теперь квантовый аналог ситуации простого наблюдения. Наблюдаемая квантовая система описывается гильбертовым пространством $\mathcal{H}$; неопределенность ее состояния выражается заданием семейства единичных векторов $\{\psi_x\} \subset \mathcal{H}$, где x – значения случайной величины X. Таким образом, эта неопределенность имеет классический характер. Если над системой $\mathcal{H}$ произвести измерение $\{e_y\} = E$, то условная вероятность исхода y при условии, что состоянием системы является ψ_x, согласно статистическому постулату, примет вид

$$\mathcal{P}(y|x) = |\langle \psi_x|e_y \rangle|^2. \tag{6}$$

Вместе с распределением X эта условная вероятность вполне определяет совместное распределение значений x, y, что позволяет найти по формуле (2) количество информации о состоянии системы, доставляемое данным измерением, которое мы обозначим $I(X,E)$.

Квантовый шум представляет собой другую систему, которая описывается гильбертовым пространством $\mathcal{H}_0$ с фиксированным вектором состояния $\psi_0 \in \mathcal{H}_0$. Чтобы описать совокупность наблюдаемой системы и шума, необходимо привлечь следующий постулат квантовой теории.

Составная система $\mathcal{H}, \mathcal{H}_0$ описывается тензорным произведением гильбертовых пространств $\tilde{\mathcal{H}} = \mathcal{H} \otimes \mathcal{H}_0$; вектор $\psi \otimes \psi_0$ описывает состояние, в котором подсистемы независимы, причем первая находится в состоянии ψ, а вторая – ψ_0.

Рассмотрим измерения над составной системой, включающей дополнительный независимый квантовый шум, которые описываются ортонормированными базисами $\tilde{E}$ в пространстве $\tilde{\mathcal{H}}$, и соответствующее им количество информации $I(X,\tilde{E})$. Точная формулировка утверждения (Q) состоит в том, что возможно строгое неравенство

$$\max_{E \subset \mathcal{H}} I(X,E) < \max_{\tilde{E} \subset \tilde{\mathcal{H}}} I(X,\tilde{E}). \tag{7}$$

Простейший пример, в котором такое неравенство действительно имеет место, дает двухуровневая квантовая система с семейством из трех равновероятных состояний с равноугольными векторами $\{\psi_0, \psi_1, \psi_2\}$ (рис.1). Подразумевается, что векторы лежат в вещественном подпространстве; например, это могут быть векторы поляризации когерентного монохроматического лазерного излучения. В работе [4] показано, что для такой системы

$$\max_{E \subset \mathcal{H}} I(X,E) = \log_2\left(\sqrt{3}/\sqrt[3]{2}\right) \approx 0.459,$$

тогда как

$$\max_{\tilde{E} \subset \tilde{\mathcal{H}}} I(X,\tilde{E}) = \log_2(3/2) \approx 0.585.$$

Обе максимизационные задачи математически нетривиальны, и мы приводим здесь лишь результаты. Первый максимум достигается на базисе E из двух векторов, расположенных симметрично по отношению к любой паре из векторов $\{\psi_0, \psi_1, \psi_2\}$. Для описания решения второй задачи заметим, что она может быть переформулирована как задача максимизации по всевозможным переполненным системам в пространстве наблюдаемой системы $\mathcal{H}$. Переполненной системой называется семейство векторов $\{\varphi_y\} \subset \mathcal{H}$, удовлетворяющее условию

$$\sum_y |\langle \psi|\varphi_y \rangle|^2 = \|\psi\|^2; \quad \psi \in \mathcal{H}. \tag{8}$$

Это условие аналогично условию полноты базиса, однако система $\{\varphi_y\}$ не обязана быть ортонормированной и даже линейно независимой. Соответственно, всякий вектор разлагается по компонентам ортонормированной системы, но разложение может не быть однозначным. Можно доказать, что всякая переполненная система получается проецированием P на $\mathcal{H}$ ортонормированного базиса $\{\tilde{e}_y\} = \tilde{E}$ в некотором расширении $\tilde{\mathcal{H}}$ исходного гильбер-

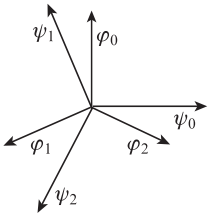


Рис.1. Информационный оптимум для трех равноугольных векторов состояний.

това пространства $\mathcal{H}$: $\varphi_y = P\tilde{e}_y$; это утверждение является частным случаем классической теоремы М.А.Наймарка (1940 г.) о продолжении обобщенной спектральной меры. Более того, расширение всегда можно выбрать так, что $\tilde{\mathcal{H}} = \mathcal{H} \otimes \mathcal{H}_0$, причем $\mathcal{H}$ отождествляется с подпространством $\mathcal{H} \otimes \psi_0$ (см. [1]). Тогда условная вероятность исхода y при измерении $\tilde{E}$ записывается как $\mathcal{P} = (y|\psi) = |\langle \psi|\varphi_y \rangle|^2$, и различие между левой и правой частями (7) заключается в том, что в первом случае максимум берется по всем ортонормированным базисам, тогда как во втором – по всем переполненным системам в $\mathcal{H}$. Оптимальная переполненная система состоит из трех равноугольных векторов $\{\varphi_0, \varphi_1, \varphi_2\}$ длины $\sqrt{2/3}$, ортогональных соответствующим векторам состояний (см. рис.1). В работе [5] экспериментально продемонстрирована реализация оптимального измерения $\tilde{E}$ для трех состояний плоскополяризованного фотона, использующая в качестве вспомогательной системы $\mathcal{H}_0$ поляризацию опорного излучения.

Таким образом, феномен (Q) действительно имеет место для квантовых систем. В его основе лежат необычные с классической точки зрения свойства составных квантовых систем, которые описываются тензорным произведением подсистем. Тензорное произведение гильбертовых пространств наряду с векторами вида $\psi \otimes \psi_0$ содержит и всевозможные их линейные комбинации (суперпозиции) $\sum_j \psi_j \otimes \psi_j^0$. Состояния составной системы, задаваемые векторами первого вида, называются несцепленными, а все, не сводящиеся к таковым, – сцепленными. Сцепленность представляет собой чисто квантовое свойство, отчасти родственное классической коррелированности, но к ней не сводящееся. Именно наличие сцепленных состояний позволяет не только теоретически, но и экспериментально опровергнуть гипотезу о скрытых параметрах, т.е. о возможности классического вероятностного описания квантовых систем, удовлетворяющего физически мотивированному условию локальности. Большой раздел современной квантовой теории информации составляет количественная теория сцепленности состояний, своеобразная комбинаторная геометрия тензорных произведений конечномерных гильбертовых пространств (см., напр., [6]).

Двойственным образом в составных квантовых системах существуют измерения, описываемые базисами, состоящими из сцепленных векторов. Только благодаря таким измерениям и возможно неравенство информаций (7) в ситуации, когда состояние наблюдаемой системы и шума является несцепленным. Более общо, рассмотрим две квантовые системы $\mathcal{H}_1$ и $\mathcal{H}_2$, находящиеся в неопределенном несцепленном состоянии. Пусть I_1, I_2, I_{12} – максимальные количества информации о состоянии, получаемые, соответственно, из измерений над системами 1, 2 и составной системой 12. Тогда в общем случае $I_{12} > I_1 + I_2$. Этот феномен строгой супераддитивности информации обнаруживается и играет важную роль в теории пропускной способности квантового канала связи.

3. Теорема Шеннона

Прежде чем перейти к квантовым каналам, напомним понятие пропускной способности в классической теории информации. В ней центральную роль играют теоремы кодирования, устанавливающие возможность асимптотически безошибочной передачи информации через канал с шумом при скоростях передачи, не превышающих некоторую пороговую величину, которая и называется пропускной способностью [7].

Математически канал с шумом задается условной вероятностью $p(y|x)$ получения сигнала (буквы) y на выходе при условии сигнала x на входе. Если передается длинное сообщение $x^{(n)} = (x_1, \ldots, x_n)$, причем каждая буква передается независимо (канал без памяти), то вероятность сообщения на выходе $p(y^{(n)}|x^{(n)}) = p(y_1|x_1), \ldots, p(y_n|x_n)$. Передачу информации можно отобразить следующей схемой:

$$X^{(n)} = \begin{Bmatrix} X_1 & \to & Y_1 \\ X_2 & \to & Y_2 \\ \vdots & & \vdots \\ X_n & \to & Y_n \end{Bmatrix} = Y^{(n)},$$

где X_i обозначают случайные величины на входе канала, а Y_i – на выходе ($i = 1, \ldots, n$). Пропускная способность такого канала дается формулой Шеннона

$$C = \max_X I(X; Y), \tag{9}$$

где максимум берется по всевозможным распределениям входного сигнала. Определяя аналогичную величину $C^{(n)} = \max_{X^{(n)}} I(X^{(n)}; Y^{(n)})$ для сообщений длины n, имеем $C^{(n)} = nC$. Это свойство аддитивности пропускной способности отражает отсутствие памяти, или корреляций между последовательными использованиями канала.

Кодирование сообщений на входе предполагает специальный выбор передаваемых сообщений, при котором сообщения на выходе, отвечающие различным сообщениям на входе, являются максимально различимыми. Теорема кодирования утверждает, что количество сообщений длины n, которое может быть передано асимптотически (при $n \to \infty$) безошибочно, $N \sim 2^{nC}$. Другими словами, nC есть количество двоичных символов (бит), необходимое и достаточное для асимптотически безошибочной передачи, при оптимальном выборе сообщений на входе и оптимальном их различении на выходе.

4. Квантовая теорема кодирования

Квантовые состояния, которые описываются единичными векторами гильбертова пространства, – чистые состояния. Чистому состоянию удобно сопоставить ортогональный проектор P_ψ на соответствующий вектор ψ. В квантовой статистике рассматриваются также смешанные состояния. Такое состояние есть статистическая смесь нескольких чистых состояний P_{ψ_i}, взятых с вероятностями p_i, и представляется оператором плотности $\rho = \sum_i p_i P_{\psi_i}$. Оператор плотности характеризуется двумя свойствами: 1) ρ – эрмитов положительный оператор; 2) ρ имеет единичный след, $\mathrm{Tr}\rho = 1$. Таким образом, собственные числа оператора плотности образуют распределение вероятностей. Энтропия этого распределения называется энтропией состояния ρ, или (в операторной форме)

$$H(\rho) = -\sum_j s_j \log_2 s_j = -\mathrm{Tr}\rho \log_2 \rho .$$

Простейший квантовый канал связи задается семейством квантовых состояний $\{\rho_x\}$, где x – входной сигнал. Такой канал называется классически-квантовым (вход – классический, выход – квантовый). Отображение $x \to \rho_x$ в сжатой форме содержит описание процесса, порождаю-

щего состояние ρ_x. Например, пусть $x = 0.1$, причем ρ_1 – когерентное состояние лазерного излучения, а ρ_0 – вакуумное состояние; тогда мы имеем классически-квантовый канал с двумя чистыми неортогональными состояниями. На выходе канала выполняется квантовое измерение, описываемое, вообще говоря, переполненной системой $\{\varphi_y\} = E$, так что условная вероятность исхода y при условии входного сигнала x имеет вид $\mathcal{P}(y|x) = \langle \varphi_y | \rho_x | \varphi_y \rangle = \mathrm{Tr}\rho_x P_{\varphi_y}$.

Если буквы сообщения длины n передаются независимо, то передача описывается диаграммой

$$X^{(n)} = \left.\begin{pmatrix} x_1 \\ \vdots \\ \vdots \\ \vdots \\ x_n \end{pmatrix} \begin{matrix} \to \rho_{x_1} \\ \otimes \\ \vdots \\ \otimes \\ \to \rho_{x_n} \end{matrix}\right\} \tilde{E}^{(n)} \to Y^{(n)},$$

где $\rho_{x_1} \otimes \cdots \otimes \rho_{x_n}$ – выходной оператор плотности в тензорном произведении пространств $\mathcal{H}^{\otimes n} = \mathcal{H} \otimes \cdots \otimes \mathcal{H}$, отвечающий сообщению $(x_1, \ldots, x_n)$. Пусть сообщения на входе имеют некоторое распределение, отвечающее случайной величине $X^{(n)}$. На выходе выполняется измерение $\tilde{E}^{(n)}$, порождающее случайный исход $Y^{(n)}$. Обозначив количество информации, отвечающее измерению $\tilde{E}^{(n)}$, как $I(X^{(n)}, \tilde{E}^{(n)}) \equiv I(X^{(n)}; Y^{(n)})$, определим

$$\max_{X^{(n)}, \tilde{E}^{(n)}} I(X^{(n)}, \tilde{E}^{(n)}) = C^{(n)}.$$

В отличие от классического канала, возможно строгое неравенство

$$C^{(n)} > nC^{(1)}, \tag{10}$$

т. е. для квантовых каналов без памяти передаваемая классическая информация может быть строго супераддитивна, что, конечно, обусловлено существованием сцепленных измерений на выходе канала. По этой причине мы не можем утверждать, что пропускная способность равна $C^{(1)}$, как в классическом случае, и должны определить ее как

$$C = \lim_{n \to \infty} C^{(n)}/n.$$

Замечательно, однако, что для определенной таким образом величины имеется явное выражение

$$C = \max_{p_x} \chi(\{p_x\}, \{\rho_x\}),$$

где

$$\chi(\{p_x\}, \{\rho_x\}) = H\left(\sum_x p_x \rho_x\right) - \sum_x p_x H(\rho_x). \tag{11}$$

Это утверждение составляет содержание квантовой теоремы кодирования. Неравенство «$\leqslant$» следует из энтропийной границы, существование которой доказано в 1973 г. [8]. Достижимость этой границы была установлена в 1996 г. (подробнее об истории доказательства теоремы кодирования см. в работе [1]). Отметим, что величину χ можно рассматривать как квантовый аналог выражения $H(Y) - H(Y|X)$ для информации Шеннона.

Вычисляя величины $C^{(1)}, C$ для некоторых конкретных каналов, можно убедиться, что $C^{(1)} < C$ и, следовательно, неравенство (10) действительно имеет место для достаточно больших n. Например, для канала с двумя чистыми состояниями ψ_0, ψ_1

$$C = h\left(\frac{1-\varepsilon}{2}\right),$$

$$C^{(1)} = 1 - h\left(\frac{1+\sqrt{1-\varepsilon^2}}{2}\right),$$

где $\varepsilon = |\langle \psi_0 | \psi_1 \rangle|$, а

$$h(p) = -p\log_2 p - (1-p)\log_2(1-p) \tag{12}$$

– двоичная энтропия. Действительно, $C^{(1)} < C$ при $0 < \varepsilon < 1$; в частности, $\lim_{\varepsilon \to 1} C/C^{(1)} = \infty$.

Как в случае C, так и в случае $C^{(1)}$ максимизирующее распределение приписывает равные вероятности 1/2 сигнальным состояниям, причем информационно-оптимальное измерение в случае $C^{(1)}$ дается базисом $\{e_0, e_1\}$, расположенным симметрично по отношению к этим состояниям.

Для канала с тремя чистыми симметричными состояниями (см. рис.1) $C = 1$, т. е. такой канал асимптотически является идеальным! Конечно, как и в классической теории информации, теорема кодирования указывает лишь на существование оптимального кодирования и декодирования, позволяющих достичь максимальной пропускной способности, но не дает конструктивного способа их построения. Для такого канала $C^{(1)} = 0.645$, причем максимум информации достигается, когда с вероятностями 1/2 выбираются два из трех состояний, а измерение является информационно-оптимальным для этих двух состояний [9]. Поскольку речь идет о передаче классической информации, величина C называется классической пропускной способностью квантового канала.

5. Проблема аддитивности

Рассмотрим теперь вопрос о классической пропускной способности канала, у которого как выход, так и вход являются квантовыми. Такой канал задается линейным вполне положительным отображением Φ, переводящим состояния на входе в состояния на выходе, $\rho \xrightarrow{\Phi} \rho'$. Свойство полной положительности означает, что тривиальное расширение канала посредством идеального канала (задаваемого тождественным отображением Id) любой конечной размерности остается положительным отображением и, следовательно, также является каналом,

$$\rho \left\{ \begin{matrix} \xrightarrow{\Phi} \\ \otimes \\ \xrightarrow[\mathrm{Id}]{} \end{matrix} \right\} \rho'.$$

Определение и подробное обсуждение этого свойства можно найти в [1]. Оно гарантирует сохранение положительности для тензорного произведения любых каналов. Передача классической информации через канал $\Phi^{\oplus n} = \Phi \otimes \overset{n}{\cdots} \otimes \Phi$ отобразится тогда следующей схемой:

$$X^{(n)} \to \rho^{(n)} \left\{ \begin{matrix} \xrightarrow{\Phi} \\ \otimes \\ \vdots \\ \otimes \\ \xrightarrow{\Phi} \end{matrix} \right\} \tilde{E}^{(n)} \to Y^{(n)},$$

где кодирование означает выбор некоторых квантовых состояний $\rho_x^{(n)}$ на входе канала $\Phi^{\otimes n}$ с вероятностями p_x, а $\tilde{E}^{(n)}$ – некоторое измерение на выходе. Заметим, что для фиксированных входных состояний мы получаем (блочный) канал с классическим входом, рассмотренный в разд.4. Применяя квантовую теорему кодирования, имеем следующее выражение для классической пропускной способности канала Φ:

$$C(\Phi) = \lim_{n\to\infty} \frac{1}{n} \bar{C}(\Phi^{\otimes n}), \tag{13}$$

где

$$\bar{C}(\Phi) = \max_{\pi_i, \rho_i} \left\{ H\left(\sum_i p_i \Phi[\rho_i] \right) - \sum_i p_i H(\Phi[\rho_i]) \right\}. \tag{14}$$

Возникает следующая фундаментальная гипотеза аддитивности: верно ли, что для произвольных квантовых каналов Φ_1, Φ_2 выполняется равенство

$$\bar{C}(\Phi_1 \otimes \Phi_2) \stackrel{?}{=} \bar{C}(\Phi_1) + \bar{C}(\Phi_2) \tag{15}$$

(заметим, что справедливость (15) со знаком «$\geqslant$» очевидна). Если бы эта гипотеза была верна, то это означало бы, что использование сцепленных состояний на входе, в отличие от сцепленных измерений на выходе, не позволяет увеличить количество передаваемой классической информации: $C(\Phi) = \bar{C}(\Phi)$. Этот вопрос оставался открытым до 2008 г., когда Хастингс [10], опираясь на свойство асимптотической концентрации меры [11] и предшествующие результаты Винтера и Хайдена, показал, что при очень высоких размерностях существуют случайные унитарные каналы, с высокой вероятностью проявляющие строгую супераддитивность. Практическое значение этого результата, однако, остается неясным, поскольку до сих пор не удалось предъявить ни одного конструктивного примера.

В то же время свойство аддитивности было установлено для ряда важных классов квантовых каналов [12–14]. Существенным достижением явилось решение давно стоявшей проблемы о гауссовых оптимизаторах и об аддитивности пропускной способности для бозонных гауссовых каналов связи [15, 16]. Такие каналы представляют собой (необратимые) преобразования систем с «непрерывными переменными», типа набора квантовых осцилляторов, приближенно описывающего электромагнитное излучение. Для широкого класса «фазонечувствительных» бозонных гауссовых каналов, включающего аттенюаторы, усилители и каналы с классическим шумом, доказана оптимальность когерентных входных состояний и аддитивность минимальной выходной энтропии. Это позволило установить, что классическая пропускная способность таких каналов также аддитивна и достигается при гауссовом кодировании, в результате чего приведены явные выражения фундаментальных пределов скорости передачи информации для наиболее используемых в квантовой оптике классов квантовых каналов (см., напр., [17, 18]).

6. Использование сцепленности между входом и выходом

Предположим, что имеются две пространственно удаленные друг от друга квантовые системы A и B, описываемые сцепленным состоянием ρ_{AB}. Такие состояния могут быть приготовлены экспериментально и представляют большой интерес в связи с прямой проверкой квантовой теории: предсказываемые ею корреляции между A и B не укладываются в рамки какой-либо приемлемой классической модели. Известно, что наличие одной сцепленности не дает возможности передавать информацию от A к B. Однако если A и B дополнительно связаны квантовым каналом Φ, то присутствие сцепленности позволяет повысить его классическую пропускную способность. Если $\Phi = \mathrm{Id}$ – идеальный канал, то выигрыш в пропускной способности, доставляемый так называемым сверхплотным кодированием, двукратен [2]. Это достигается использованием для кодирования максимально сцепленных состояний ортонормированного базиса в системе AB, которые B может получить благодаря наличию квантового канала Φ.

Чем сильнее канал отличается от идеального, тем выигрыш больше, и в пределе для каналов с очень большим шумом он может стремиться к бесконечности. Обобщая протокол сверхплотного кодирования, нетрудно дать математическое определение классической пропускной способности с использованием сцепленного состояния (entanglement-assisted classical capacity), для которой имеется замечательная формула, полученная в работе Беннета, Шора, Смолина и Таплияла [19]*

$$C_{\mathrm{ea}}(\Phi) = \max_{\rho} I(\rho, \Phi), \tag{16}$$

где $I(\rho, \Phi)$ – квантовая взаимная информация между A и B, задаваемая формулой

$$I(\rho, \Phi) = H(\rho) + H(\Phi[\rho]) - H(\rho; \Phi). \tag{17}$$

Здесь $H(\rho)$ и $H(\Phi[\rho])$ – энтропии соответственно входного и выходного состояния, а $H(\rho; \Phi)$ – так называемая обменная энтропия. Для определения последней нам потребуется понятие очищения квантового состояния. А именно, для любого оператора плотности ρ_A в гильбертовом пространстве $\mathcal{H}_A$ найдется чистое состояние, т.е. одномерный проектор P_ρ в пространстве $\mathcal{H}_A \otimes \mathcal{H}_R$, где $\mathcal{H}_R$ – пространство эталонной системы, такое, что частичный след P_ρ по пространству $\mathcal{H}_R$ совпадает с ρ_A. Более того, частичный след P_ρ по пространству $\mathcal{H}_A$, т.е. состояние эталонной системы, имеет ту же энтропию, что и ρ_A. Обменная энтропия определяется как

$$H(\rho; \Phi) = \Phi((\Phi \otimes \mathrm{Id})[P_\rho]) \tag{18}$$

и может быть интерпретирована как некий аналог совместной энтропии A и B. Тогда формула (17) является аналогом выражения $I(X; Y) = H(X) + H(Y) - H(XY)$ для информации Шеннона. Квантовая взаимная информация обладает рядом естественных свойств, аналогичных свойствам информации Шеннона; в частности, она субаддитивна относительно тензорного произведения каналов. Отсюда следует, что пропускная способность $C_{\mathrm{ea}}(\Phi)$ аддитивна.

Практическая реализация описанного выше протокола предполагает пространственное распределение сцепленности, что в настоящее время является инженерным вызовом. Возможные подходы к решению этой проблемы обсуждены в работе [20].

* Упрощенное доказательство формулы (16) см. в [1].

7. Квантовая пропускная способность

При передаче классической информации по квантовому каналу она записывается в квантовом состоянии, которое, таким образом, представляет собой информационный ресурс. Своеобразие этого ресурса в том, что вся полнота его информационного содержания (называемая иногда квантовой информацией) не может быть сведена к классическому сообщению. Это связано с тем, что квантовое состояние содержит в себе информацию о статистике всевозможных, в том числе и взаимоисключающих (дополнительных) измерений над системой. Простое рассуждение, основанное на линейности уравнений квантовой эволюции, показывает, что, в отличие от информации классической, не существует «квантового ксерокса», т.е. физического устройства, позволяющего копировать квантовую информацию.

Таким образом, преобразование квантового состояния $\rho \to \Phi[\rho]$ можно рассматривать как передачу квантовой информации. Естественно поставить вопрос об асимптотически (при $n \to \infty$) безошибочной передаче каналом $\Phi^{\otimes n}$:

$$\rho^{(n)} \left\{ \begin{array}{c} \Phi \\ \longrightarrow \\ \otimes \\ \vdots \\ \otimes \\ \Phi \\ \longrightarrow \end{array} \right\} \rho^{(n)'} \approx \rho^{(n)}.$$

Квантовая пропускная способность $Q(\Phi)$ определяется максимальной размерностью подпространства векторов входного пространства ($\sim 2^{nQ(\Phi)}$), для которых отвечающие им состояния передаются асимптотически безошибочно, т.е. почти обратимо. Для $Q(\Phi)$ имеется выражение с использованием когерентной информации

$$I_c(\rho, \Phi) = \max\{H(\Phi[\rho]) - H(\rho; \Phi), 0\},$$

а именно

$$Q(\Phi) = \lim_{n\to\infty} \frac{1}{n} \max_{\rho^{(n)}} I_c(\rho^{(n)}, \Phi^{\otimes n}). \tag{19}$$

Понятие о квантовой пропускной способности и ее связь с когерентной информацией на эвристическом уровне обсуждались в работе Ллойда [21], где была предложена формула

$$Q(\Phi) = \max_{\rho} I_c(\rho, \Phi), \tag{20}$$

основанная на предположении аддитивности когерентной информации, которое, однако, вскоре было опровергнуто. Точное определение квантовой пропускной способности дано в работе Барнума, Нильсена и Шумахера [22], где также было доказано неравенство со знаком «$\leqslant$» в (19). Вопрос о равенстве оставался открытым до 2003 г., когда Шор дал набросок доказательства, уточняющий аргументы Ллойда, а Деветак [23] представил совершенно иное доказательство, основанное на параллели между квантовым каналом и классическим каналом с перехватом [7], причем в квантовом случае роль перехватчика информации играет окружение рассматриваемой открытой системы.

Тем не менее квантовая пропускная способность остается наименее изученной из всего многообразия пропускных способностей квантового канала связи. Формула (19) из-за своего асимптотического характера мало пригодна для вычисления, однако известно, что для так называемых деградируемых каналов [24] она упрощается до выражения (20).

Смит и Ярд [25] построили пример замечательного явления суперактивации, когда для двух квантовых каналов Φ_1, Φ_2 с нулевой квантовой пропускной способностью выполняется неравенство $Q(\Phi_1 \otimes \Phi_2) > 0$. Широков [26] показал, что аналогичный феномен может иметь место для квантовой пропускной способности с нулевой ошибкой. Это можно рассматривать как экстремальное проявление супераддитивности пропускной способности, в основе которого лежат необычные геометрические свойства тензорного произведения каналов, улучшающие «обратимость» некоторых передаваемых состояний.

8. Секретная классическая пропускная способность

Рассмотрим передачу классической информации, в которой имеются три участника: отправитель A, получатель B и перехватчик E. Квантовый канал с перехватом Φ_{BE} задается изометрическим отображением пространства A в пространство BE. Предположим, что A выбирает состояния $\{\rho_A^x\}$ с вероятностями $\{p_x\}$; тогда участники B и E получают соответственно состояния $\{\rho_B^x\}$ и $\{\rho_E^x\}$, верхними границами шенноновской информации для B и E являются величины $\chi(\{p_x\}, \{\rho_B^x\})$ и $\chi(\{p_x\}, \{\rho_E^x\})$, где χ определено формулой (11). По аналогии с классическим каналом с перехватом [7], «секретность» передачи может быть охарактеризована величиной

$$\chi(\{p_x\}, \{\rho_B^x\}) - \chi(\{p_x\}, \{\rho_E^x\}).$$

Полагая, что входные состояния ρ_A^x являются чистыми, и обозначая среднее состояние входного ансамбля как $\bar{\rho}_A = \sum_x p_x \rho_A^x$, получаем ключевое соотношение

$$I_c(\bar{\rho}_A, \Phi_B) = \chi(\{p_x\}, \{\rho_B^x\}) - \chi(\{p_x\}, \{\rho_E^x\}), \tag{21}$$

которое раскрывает важную связь между когерентной информацией и секретной классической пропускной способностью (определена ниже); соотношение также указывает путь доказательства прямой теоремы кодирования для квантовой пропускной способности через рассмотрение канала с перехватом.

Точная верхняя грань множества достижимых скоростей передачи при условии, что взаимная информация между A и E асимптотически исчезает, называется секретной классической пропускной способностью $C_p(\Phi_{BE})$ канала с перехватом. Для нее имеет место выражение

$$C_p(\Phi_{BE}) = \lim_{n\to\infty} \frac{1}{n} \max_{p^{(n)}, \sum^{(n)}} \big[\chi(\{p_i^{(n)}\}, \{\rho_{B^{(n)}}^i\}) - \chi(\{p_i^{(n)}\}, \{\rho_{E^{(n)}}^i\})\big], \tag{22}$$

где максимум берется по всем конечным наборам состояний $\sum^{(n)} = \{\rho_{A^{(n)}}^i\}$ в $\mathcal{H}_A^{\oplus n}$ и распределениям вероятностей $p^{(n)} = \{p_i^{(n)}\}$ (мы используем обозначения $\rho_{B^{(n)}}^i = \Phi_B^{\otimes n}[\rho_{A^{(n)}}^i]$, $\rho_{E^{(n)}}^i = \Phi_E^{\otimes n}[\rho_{A^{(n)}}^i]$).

Из соотношений (19), (21) и (22) вытекает важное неравенство между квантовой и классической секретной пропускными способностями:

$$Q(\Phi_B) \leqslant C_p(\Phi_{BE}).$$

Это неравенство следует из того, что при вычислении $C_p(\Phi_{BE})$ учитываются все ансамбли состояний, а при вычислении $Q(\Phi_B)$ – только ансамбли чистых состояний для A. В общем случае возможно строгое неравенство, поэтому особый интерес представляет следующее утверждение: если канал Φ_B деградируемый [24], то

$$C_p(\Phi_{BE}) = Q(\Phi_B) = \max_{\rho} I_c(\rho, \Phi). \tag{23}$$

Это позволяет в ряде интересных случаев явно вычислить пропускные способности C_p и Q (подробнее см. в [1]).

В завершение краткого обсуждения каналов с перехватом упомянем обширную область квантовой криптографии, которая представляет собой самостоятельный и глубоко разработанный раздел квантовой информатики (см., напр., обзоры [27, 28]).

9. Заключение

В работе рассмотрены основные пропускные способности квантовых каналов связи. Дальнейшее развитие теории приводит к изучению квантовых каналов с многими пользователями («квантовый интернет») [29]. Большой раздел квантовой информатики посвящен исследованию систем с «непрерывными переменными», основанных на принципах квантовой оптики, а также гибридных оптико-атомарных систем. Многие эксперименты и протоколы квантовой теории информации, проводящиеся в лабораториях ряда развитых стран, реализуются именно на таких системах.

1. Холево А.С. *Квантовые системы, каналы, информация*, (М: МЦНМО, 2010); https://www.mccme.ru/free-books/holevo-quantum.pdf.
2. Nielsen M.A., Chuang I. *Quantum Computation and Quantum Information* (Cambridge: University Press, 2011).
3. Холево А.С. *Математические основы квантовой информатики, Лекц. курсы НОЦ МИАН*, **30**, 3 (2018); http://www.mathnet.ru/links/9ba278c4c4d205a233c7a937b95724fc/lkn30.pdf.
4. Холево А.С. *Проблемы передачи информации*, **9** (2), 31 (1973).
5. Sasaki M., Barnett S.M., Jozsa R., Osaki M., Hirota O. *Phys. Rev. A,* **59**, 3325 (1999); arXiv:quant-ph/9812062, 1998.
6. Walter M., Gross D., Eisert J. arXiv:1612.02437 (2016).
7. Чисар И., Кёрнер Я. *Теория информации* (М.: Мир, 1985).
8. Холево А.С. *Проблемы передачи информации*, **9** (3), 3 (1973).
9. Shor P.W. arXiv:quant-ph/0206058, 2002.
10. Hastings M.B. *Nature Phys*., **5**, 255 (2009); arXiv:quant-ph/0809.3972.
11. Aubrun G. Szarek S. *Mathematical Surveys and Monographs*, **223**, 414 (2017).
12. Амосов Г.Г., Холево А.С., Вернер Р.Ф. *Проблемы передачи информации*, **36** (4), 25 (2000); LANL e-print quant-ph/0003002.
13. King C. *J. Math. Phys*., **43**, 4641 (2002).
14. Shor P.W. *J. Math. Phys*., **43**, 4334 (2002).
15. Giovannetti V., Holevo A.S. Garcia-Patron R. *Commun. Math. Phys*., **334** (3), 1553 (2015).
16. Джованнетти В., Холево А.С., Мари А. *ТМФ*, **182** (2), 338 (2015).
17. Giovannetti V., Garcia-Patron R., Cerf N.J., Holevo A.S. *Nature Photon*., **8** (10), 216 (2014).
18. Papen G.C., Blahut R.E. *Lightwave Communication* (Cambridge University Press, 2019).
19. Bennett C.H., Shor P.W., Smolin J.A. *Phys. Rev. Lett*., **83** 3081 (1999); arXiv:quant-ph/9904023.
20. Guha S., Zhuang Q., Bash B. arXiv:2001.03934 (2000).
21. Lloyd S. *Phys. Rev. A,* **55**, 1613 (1997).
22. Barnum H., Nielsen M.A., Schumacher B. *Phys. Rev. A*, **57**, 4153 (1998).
23. Devetak I. arXiv:quant-ph/0304127 (2003).
24. Devetak I., Shor P. arXiv:quant-ph/0311131.
25. Smith G. Yard J. *Science*, **321**, 1812 (2010).
26. Shirokov M.E. *Quantum Inf. Process*, **14** (8), 3057 (2015).
27. Gisin N., Ribordy G., Tittel W. Zbinden H. *Rev. Mod. Phys*., **74**, 145 (2002).
28. Килин С.Я., Хорошко Д.Б., Низовцев А.П. *Квантовая криптография: идеи и практика* (Минск: Беларуская навука, 2007).
29. Kimble H.J. *Nature*, **453**, 1023 (2008).