Теоремы кодирования квантовой теории информации

Холево А. С.

Математический институт им. В. А. Стеклова

Российской академии наук

Аннотация

Квантовая теория информации – новая научная дисциплина, изучающая закономерности передачи и преобразования информации в системах, подчиняющихся законам квантовой механики. В настоящем обзоре мы затрагиваем одну, но весьма важную тему квантовой теории информации – теоремы кодирования для квантовых каналов связи, стараясь подчеркнуть ту особую роль, которую играет квантовое свойство сцепленности. Понятие о пропускной способности канала – центральное в классической теории информации. Оказывается, что в квантовом случае это понятие разветвляется, порождая целый спектр информационных характеристик квантового канала связи.

1 Введение

Хотя квантовая теория информации сформировалась как самостоятельная научная дисциплина в 1990-е годы, ее рождение относится к 1950-м, вслед за появлением основ теории информации и помехоустойчивой связи в трудах В. А. Котельникова и К. Шеннона. На начальном этапе, который охватывает период 1950-80 гг., основным вопросом было выяснение фундаментальных ограничений на возможности передачи и обработки информации, обусловленных квантовомеханической природой ее носителя. Развитие информационных технологий в направлении микроминиатюризации позволяет предположить, что через 10-15 лет такие ограничения станут основным препятствием для дальнейшей экстраполяции существующих технологий и принципов обработки информации. Однако помощь идет с неожиданной стороны: появление в 1980-х идей квантового компьютинга, криптографии и новых квантовых коммуникационных протоколов повернуло исследования в новое русло [1]. Речь идет уже не только об ограничениях, но и о новых возможностях, заключенных в использовании специфически квантовых информационных ресурсов, таких как сцепленность (перепутанность, англ. термин entanglement) квантовых состояний и измерений. В настоящее время теоретические и экспериментальные разработки в области квантовой теории информации и компьютинга ведутся в научно-исследовательских центрах ряда развитых стран. В Московском Государственном Университете работает большая группа ученых под общим руководством акад. В. А. Садовничего.

Имеется ряд превосходных обзоров и вводных статей, посвященных данному направлению, см. например [2], [3]. В настоящем обзоре мы затронем лишь одну, но весьма важную тему – теоремы кодирования для квантовых каналов связи, стараясь подчеркнуть ту особую роль, которую играет квантовое свойство сцепленности. Понятие о пропускной способности канала – центральное в классической теории Шеннона. Оказывается, что в квантовом случае это понятие разветвляется, порождая целый спектр информационных характеристик квантового канала.

Мы хотим здесь также подчеркнуть, что квантовая теория информации является источником целого ряда математических задач, мотивированных физически, формулируемых достаточно элементарно, но зачастую трудно решаемых (или до сих пор нерешенных). Ее основной математический аппарат – линейная алгебра, теория операторов в гильбертовом пространстве, как правило, конечномерном, причем интересные задачи есть уже в размерностях 2 и 3. Подробное изложение рассматриваемых здесь вопросов читатель найдет в книгах [4], [5]. Следует, однако, отметить, что со времени написания этих книг в решении некоторых открытых вопросов был достигнут прогресс, получивший отражение в настоящей статье.

2 Рандомизация и информация

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

(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, так что известна условная вероятность $p(y|x) = \mathsf{P}(Y = y|X = x)$. Мерой неопределенности может служить энтропия распределения $\{p_x\}$ случайной величины X,

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

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

$$\begin{aligned} I(X;Y) &= H(X) + H(Y) - H(XY) && (2)\\ &= H(Y) - H(Y|X), && (3) \end{aligned}$$

где $H(XY)$ – энтропия совместного распределения случайных величин X, Y, а $H(Y|X) = H(XY) - H(Y)$– условная энтропия. Допустим теперь, 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 подсчет 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.

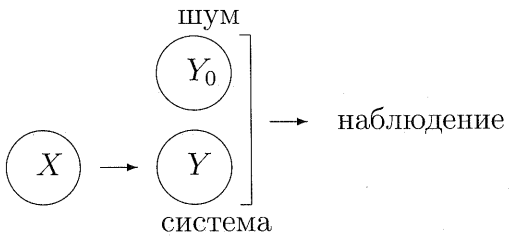

Рис. 1: *Рандомизованное наблюдение*

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 рандомизация оказывается выгодной. Однако в рассмотренной ситуации простого наблюдения ("Бог суров, но не злонамерен") этот принцип представляется очевидным, если не тривиальным.

Тем удивительнее, что он перестает быть справедливым, если речь идет о квантовых системах. Именно,

(Q) *Введение дополнительного независимого квантового шума в наблюдения (квантовая рандомизация) может увеличить количество информации о наблюдаемой квантовой системе.*

3 Квантовая рандомизация и переполненные системы

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 $\mathcal{H}$;

постулируется, что *вероятность исхода y при измерении E в состоянии ψ* равна

$$\mathsf{P}(y|\psi) = |(\psi, e_y)|^2. \tag{5}$$

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 теперь над системой $\mathcal{H}$ производится измерение $\{e_y\} = E$, то условная вероятность исхода y при условии, что состоянием системы является ψ_x, согласно статистическому постулату, равна

$$\mathsf{P}(y|x) = |(\psi_x, e_y)|^2. \tag{6}$$

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, нам придется привлечь следующий постулат квантовой теории:

• *совокупность систем* $\mathcal{H}$, $\mathcal{H}_0$ 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.

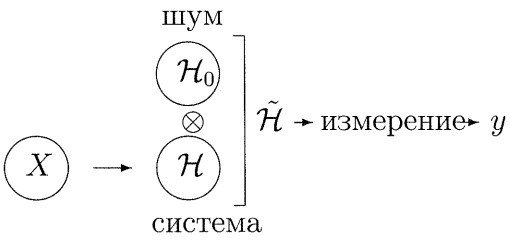

Рис. 2: *Квантовая рандомизация*

Теперь мы можем рассмотреть 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 в общем случае

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

Простейший пример, в котором это неравенство действительно имеет место, дает двухуровневая квантовая система, или *кубит* (т. е. система, описываемая двумерным гильбертовым пространством) с семейством из трех равновероятных состояний с равноугольными векторами $\{\psi_0, \psi_1, \psi_2\}$, как изображено на рис. 3 (подразумевается, что векторы лежат в вещественном подпространстве). Например, это могут быть векторы поляризации когерентного монохроматического излучения лазера. Для такой системы $\max_{E \subset \mathcal{H}} I(X, E) = \log\left(\sqrt{3}/\sqrt[3]{2}\right) \approx 0,459$, тогда как $\max_{\tilde{E} \subset \tilde{\mathcal{H}}} I(X, \tilde{E}) = \log(3/2) \approx 0,585$ [4].

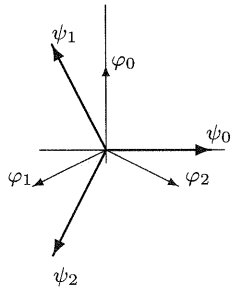

Рис. 3: *Информационный оптимум для трех векторов*

Обе максимизационные задачи совсем не тривиальны и мы приведем здесь лишь ответы. 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 сначала, что она может быть переформулирована как задача максимизации по всевозможным переполненным системам в пространстве наблюдаемой системы $\mathcal{H}$. *Переполненной системой* (или *жестким*

фреймом) называется семейство векторов $\{\varphi_y\} \subset \mathcal{H}$, удовлетворяющее условию

$$\sum_y |(\psi, \varphi_y)|^2 = \|\psi\|^2; \quad \psi \in \mathcal{H}. \tag{8}$$

Это условие аналогично условию полноты базиса, однако система $\{\varphi_y\}$ не обязана быть ортонормированной и даже линейно независимой. Соответственно, всякий вектор разлагается по компонентам переполненной 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 гильбертова пространства $\mathcal{H}$: $\varphi_y = P\tilde{e}_y$ (это является весьма частным случаем классической теоремы М. А. Наймарка (1940г.) 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. [4]. Тогда условная вероятность исхода y при измерении $\tilde{E}$ равна $\mathsf{P}(y|\psi) = |(\psi, \varphi_y)|^2$ и различие между левой и правой частями в (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. 3). В работе [6] была экспериментально продемонстрирована реализация оптимального измерения $\tilde{E}$ для трех состояний плоскополяризованного фотона, использующая в качестве вспомогательной системы $\mathcal{H}_0$ поляризацию опорного излучения (так называемого локального осциллятора).

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 (а не декартовым) 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, называются *сцепленными*. Сцепленность представляет собой чисто квантовое свойство, отчасти родственное классической коррелированности, но отнюдь к ней не сводящееся. Именно наличие сцепленных состояний позволяет опровергнуть гипотезу о скрытых параметрах, т. е. о возможности классического вероятностного описания квантовых систем. Большой и увлекательный раздел современной квантовой теории информации составляет количественная теория сцепленности состояний, своеобразная комбинаторная геометрия тензорных произведений конечномерных гильбертовых пространств (см. например [7]).

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, мы можем рассмотреть

две квантовые системы $\mathcal{H}_1$ и $\mathcal{H}_2$, находящиеся в неопределенном несцепленном состоянии. Обозначим 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, о которой пойдет речь ниже.

4 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 [8].

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 есть $p(y^{(n)}|x^{(n)}) = p(y_1|x_1) \cdot \ldots \cdot p(y_n|x_n)$. Передачу информации можно изобразить следующей схемой

$$X^{(n)} = \left\{ \begin{array}{ccc} X_1 & \longrightarrow & Y_1 \\ X_2 & \longrightarrow & Y_2 \\ \vdots & & \vdots \\ X_n & \longrightarrow & Y_n \end{array} \right\} = Y^{(n)},$$

где X обозначают случайные величины на входе канала, а Y – на выходе. 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 при оптимальном выборе сообщений на входе и оптимальном их различении на выходе, есть $N \sim 2^{nC}$, т. е. может быть задано количеством двоичных символов (бит) $\sim nC$.

Например, для двоичного симметричного канала с вероятностью ошибки p

$$C = 1 - h(p), \tag{10}$$

где

$$h(p) = -p\log p - (1-p)\log(1-p) \tag{11}$$

– двоичная энтропия.

5 Квантовая теорема кодирования

Квантовые состояния, которые описываются единичными векторами гильбертова пространства, суть *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 оно представляется оператором плотности $S = \sum_i p_i P_{\psi_i}$. *Оператор плотности* характеризуется двумя свойствами: 1) S эрмитов положительный оператор 2) S имеет единичный след, $\mathrm{Tr}S = 1$. Таким образом, собственные числа оператора плотности образуют распределение вероятностей. Энтропия этого распределения называется энтропией состояния S, или, в операторной форме,

$$H(S) = -\sum_j s_j \log s_j = -\mathrm{Tr}S\log S.$$

Простейший квантовый канал связи задается семейством квантовых состояний $\{S_x\}$, где x входной сигнал. Такой канал называется *классически-квантовым* (вход – классический, выход – квантовый). Отображение $x \to S_x$ в сжатой форме содержит описание процесса, порождающего состояние S_x. Например, пусть $x = 0, 1$, причем S_1 когерентное состояние излучения лазера, а S_0 – вакуумное состояние, тогда мы имеем классически-квантовый канал с двумя чистыми неортогональными состояниями, см. рис. 4. На выходе канала производится квантовое измерение, описываемое, вообще говоря, переполненной системой $\{\varphi_y\} = E$, так что условная вероятность исхода y при условии входного сигнала x есть $\mathsf{P}(y|x) = (\varphi_y, S_x\varphi_y) = \mathrm{Tr}S_x P_{\varphi_y}$.

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

$$X^{(n)} = \left\{ \begin{array}{ccc} x_1 & \longrightarrow & S_{x_1} \\ & & \otimes \\ \vdots & & \vdots \\ & & \otimes \\ x_n & \longrightarrow & S_{x_n} \end{array} \right\} \tilde{E}^{(n)} \to Y^{(n)},$$

где $S_{x_1}\otimes\cdots\otimes S_{x_n}$ 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 производится измерение $\tilde{E}^{(n)}$, порождающее случайный исход $Y^{(n)}$. Обозначая $I(X^{(n)}, \tilde{E}^{(n)}) \equiv I(X^{(n)}; Y^{(n)})$ количество информации, отвечающее измерению $\tilde{E}^{(n)}$, определим

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

Оказывается, что в общем случае

$$C^{(n)} > nC^{(1)}, \tag{12}$$

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

$$C = \max_{p_x} \left\{ H\left(\sum_x p_x S_x\right) - \sum_x p_x H(S_x) \right\}.$$

Это утверждение составляет содержание квантовой теоремы кодирования. Неравенство $\leq$ следует из энтропийной границы, доказанной автором в 1973 г. Достижимость этой границы была установлена в работах автора, и, независимо, Шумахера и Вестморленда в 1996 г. (подробнее об истории доказательства этой теоремы см. в [4]). Отметим, что величину в фигурных скобках 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, таким образом, (12) действительно имеет место для достаточно больших n. Например, для канала с двумя чистыми состояниями ψ_0, ψ_1

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

где $\varepsilon = |(\psi_0, \psi_1)|$, и действительно, $C^{(1)} < C$ при $0 < \varepsilon < 1$.

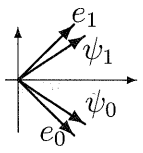

Рис. 4: *Канал с двумя чистыми состояниями*

Как в случае C, так и $C^{(1)}$, 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 (рис. 3) $C = 1$, т. е. такой канал асимптотически является идеальным! Конечно, как и в классической теории информации, теорема кодирования говорит лишь о существовании оптимального кодирования и декодирования, позволяющих достичь 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.

6 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, $S \xrightarrow{\Phi} S'$. Свойство полной положительности означает, что тривиальное расширение канала посредством идеального канала (задаваемого тождественным отображением Id) любой конечной размерности остается положительным отображением и, следовательно, также переводит состояния в состояния:

$$S \left\{ \begin{array}{c} \xrightarrow{\Phi} \\ \otimes \\ \xrightarrow{\mathrm{Id}} \end{array} \right\} S'.$$

Определение и подробное обсуждение этого свойства можно найти в [4]. Оно гарантирует сохранение положительности для тензорного произведения любых каналов. Передача классической информации через канал $\Phi^{\otimes n} = \Phi \otimes \overset{n}{\ldots} \otimes \Phi$ изобразится тогда следующей схемой:

$$X^{(n)} \longrightarrow S^{(n)} \left\{ \begin{array}{c} \xrightarrow{\Phi} \\ \otimes \\ \vdots \\ \otimes \\ \xrightarrow{\Phi} \end{array} \right\} \tilde{E}^{(n)} \longrightarrow Y^{(n)},$$

где кодирование означает выбор некоторых квантовых состояний $S_x^{(n)}$ 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 предыдущем разделе. 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

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

Здесь возникает следующая фундаментальная *гипотеза аддитивности*: верно ли, что для произвольных квантовых каналов Φ_1, Φ_2 выполняется

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

(заметим, что неравенство $\geq$ очевидно). Если эта гипотеза верна, то это означает, что использование сцепленных состояний на входе, в отличие от сцепленных измерений на выходе, не позволяет увеличить количество передаваемой классической информации; в частности,

$$C(\Phi) = \bar{C}(\Phi). \tag{16}$$

К настоящему времени справедливость этой гипотезы установлена для некоторых классов квантовых каналов [10], [11], [12], [13], но доказать ее во всей полноте, либо опровергнуть, пока не удается, несмотря на предпринятый интенсивный численный поиск. Если она верна, то в основе аддитивности величины $\bar{C}$, вероятно, лежит гипотетическое свойство мультипликативности норм вполне положительных отображений

$$\Phi : \ell_1(\mathcal{H}) \to \ell_p(\mathcal{H}); \quad p \geq 1,$$

где $\ell_p(\mathcal{H})$ – некоммутативный аналог пространства ℓ_p – так называемый класс Шаттена. А именно, гипотеза состоит в том, что для p, достаточно близких к единице,

$$\|\Phi_1 \otimes \Phi_2\|_p \stackrel{?}{=} \|\Phi_1\|_p \|\Phi_2\|_p, \tag{17}$$

где

$$\|\Phi\|_p = \sup_{X \neq 0} \frac{(\mathrm{Tr}|\Phi[X]|^p)^{\frac{1}{p}}}{\mathrm{Tr}|X|}.$$

Отсюда при $p \downarrow 1$ следует аддитивность минимальной выходной энтропии $\min_S H(\Phi[S])$, одно из целого ряда свойств, эквивалентных, как недавно показано [14], [15], гипотезе аддитивности.

Во всех случаях, в которых гипотеза аддитивности доказана, мультипликативность норм (для всех $p \geq 1$) также установлена, более того, в наиболее интересных случаях она и лежит в основе единственного способа доказательства. Мультипликативность норм имеет место для произвольных ограниченных отображений классических пространств ℓ_p, где ее доказательство достаточно просто и опирается на одно из неравенств Минковского. Тем более интригующим представляется пример квантового канала Φ, для которого (17) с $\Phi_1 = \Phi_2 = \Phi$ нарушается для достаточно больших p ($p \geq 4,7823$ если $\dim\mathcal{H} = 3$) [16].

7 Использование сцепленности между входом и выходом

Предположим, что имеются две пространственно удаленные друг от друга квантовые системы A и B, описываемые сцепленным состоянием S_{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. Чем более канал отличается от идеального,

тем выигрыш больше, и в пределе 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); замечательно, что для нее имеется простая формула

$$C_{ea}(\Phi) = \max_S I(S, \Phi), \tag{18}$$

где $I(S, \Phi)$ *квантовая взаимная информация* между A и B, задаваемая соотношением

$$I(S, \Phi) = \{H(S) + H(\Phi[S]) - H(S; \Phi)\}. \tag{19}$$

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

$$H(S; \Phi) = H((\Phi \otimes \mathrm{Id})[P_S]), \tag{20}$$

и может быть интерпретирована как некий аналог совместной энтропии A и B. Тогда формула (19) 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 $C_{ea}(\Phi)$ аддитивна.

Квантовая взаимная информация была введена в работе [17], где была высказана догадка о ее связи с пропускной способностью канала, использующего сцепленность. Доказательство формулы (18) было дано в работе Беннета, Шора, Смолина и Таплияла [18] и впоследствии упрощено, см. [4].

8 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 не существует "квантового ксерокса", т. е. физического устройства, позволяющего копировать квантовую информацию, в отличие от информации классической.

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

$$S^{(n)} \left\{ \begin{array}{c} \stackrel{\Phi}{\longrightarrow} \\ \otimes \\ \vdots \\ \otimes \\ \stackrel{\Phi}{\longrightarrow} \end{array} \right\} S^{(n)\prime} \approx S^{(n)}$$

Этот вопрос имеет отношение к очень важной проблеме *квантовых кодов, исправляющих ошибки.* Можно представить себе память квантового компьютера (квантовый регистр) как набор из n кубитов. Канал Φ может описывать распад состояния кубита (декогерентизацию) из-за неизбежного, хотя и нежелательного, взаимодействия с окружением (квантовым шумом). Возможность почти безошибочной передачи квантовой информации предполагает тогда специфический отбор состояний квантового регистра (кодирование), допускающих приближенное восстановление (декодирование) после воздействия шума[1].

Квантовая пропускная способность $Q(\Phi)$ определяется максимальной размерностью подпространства векторов входного пространства ($\approx 2^{nQ(\Phi)}$), отвечающие которым состояния передаются асимптотически безошибочно. Для нее имеется выражение через когерентную информацию

$$I_c(S, \Phi) = H(\Phi[S]) - H(S; \Phi),$$

а именно

$$Q(\Phi) = \lim_{n\to\infty} \frac{1}{n} \max_{S^{(n)}} I_c(S^{(n)}, \Phi^{\otimes n}). \tag{21}$$

Понятие о квантовой пропускной способности и ее связь с когерентной информацией на эвристическом уровне обсуждались в работе Ллойда [19], где была предложена формула $Q(\Phi) = \max_S I_c(S, \Phi)$, основанная на предположении аддитивности когерентной информации, которое однако вскоре было опровергнуто. Точное определение пропускной способности было дано в работе Барнума, Нильсена и Шумахера [20], где также было доказано неравенство $\leq$ в (21). Вопрос о равенстве оставался открытым до 2003 г., когда Шор дал набросок доказательства, уточняющий аргументы Ллойда, а Деветак

[1]На самом деле конструкция квантовых кодов, исправляющих ошибки [2], [5], использует другую модель шума, при которой ошибки происходят редко, например, только в одном из n кубитов, зато могут быть произвольными, а код должен обеспечивать *точное* воспроизведение квантовой информации. Однако модели декогерентизации могут быть различными, и любой метод борьбы с ней представляет интерес.

[21] дал совершенно иное доказательство, основанное на параллели между квантовым каналом и классическим каналом с перехватом [8], 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 (21) из-за своего асимптотического характера мало пригодна для вычисления, и явное выражение для квантовой пропускной способности известно лишь для самых простых каналов [2]. В классической теории информации хорошо известно, что обратная связь не увеличивает пропускную способность канала. 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. Дело в том, что такая передача позволяет создать максимальную сцепленность между входом и выходом, которая может быть использована для телепортации, т. е. безошибочной передачи квантового состояния. Даже канал с нулевой квантовой пропускной способностью, дополненный классической обратной связью, может быть использован для передачи квантовой информации, см. п. 12.5.2 в [5].

Список литературы

[1] К. А. Валиев, *Исследования в области квантовых технологий в информатике и метрологии* // Вестник РАН, **73** №5, (2003), 400-405.

[2] C. H. Bennett, P. W. Shor, *Quantum Information Theory* // IEEE Trans. Inform. Theory **44** (1998), 2724-2742.

[3] М. Нильсен, *Правила для сложного квантового мира* // В мире науки, №3,(2003), 50-59; перев. с англ. Scientific American, №10, (2002).

[4] А. С. Холево, *Введение в квантовую теорию информации* // МЦНМО, Москва, 2003.

[5] M. A. Nielsen, I. Chuang, *Quantum Computation and Quantum Information* // Cambridge University Press, 2000.

[6] M. Sasaki, S. M. Barnett, R. Jozsa, M. Osaki, O. Hirota, *Accessible information and optimal strategies for real symmetric quantum sources* // Phys. Rev. A **59**, (1999), 3325; LANL e-print quant-ph/9812062, 1998.

[7] M. Keyl, *Fundamentals of Quantum Information* // LANL e-print quant-ph/0202122, 2002.

[8] И. Чисар, Я. Кёрнер, *Теория информации* // Мир, Москва, 1985.

[9] P. W. Shor, *The adaptive classical capacity of a quantum channel, or information capacity of 3 symmetric pure states in three dimensions* // LANL Report quant-ph/0206058, 2002.

[10] Г. Г. Амосов, А. С. Холево, Р. Ф. Вернер, *О проблеме аддитивности в квантовой теории информации* // Пробл. передачи информ., **36** №4, (2000), 25-34. LANL e-print quant-ph/0003002.

[11] C. King, M. B. Ruskai, *Minimal entropy of states emerging from noisy quantum channels* // LANL e-print quant-ph/9911079, 1999.

[12] C. King, *Additivity for a class of unital qubit channels*, LANL e-print quant-ph/0103156, 2001; *The capacity of quantum depolarizing channel* // LANL e-print quant-ph/0204172, 2002.

[13] P. W. Shor, *Additivity of the classical capacity of entanglement-breaking quantum channels* // LANL e-print quant-ph/0201149, 2002.

[14] P. W. Shor, *Equivalence of additivity questions in quantum information theory* // LANL e-print quant-ph/0305035, 2003.

[15] A. S. Holevo, M. E. Shirokov, *On Shor's channel extension and constrained channels* // LANL e-print quant-ph/0306196, 2003.

[16] A. S. Holevo, R. F. Werner, *Counterexample to an additivity conjecture for output purity of quantum channels* // J. Math. Phys., **43** №9, (2002), 4353-4357; LANL e-print quant-ph/0203003, 2002.

[17] C. Adami, N. J. Cerf, *Capacity of noisy quantum channels* // Phys. Rev. A **56**, (1997), 3470-3485.

[18] C. H. Bennett, P. W. Shor, J. A. Smolin, A. V. Thapliyal, *Entanglement-assisted classical capacity of noisy quantum channel* // LANL e-print quant-ph/9904023, 1999.

[19] S. Lloyd, *Capacity of noisy quantum channel* // Phys. Rev. **A 55** , (1997), 1613-1622.

[20] H. Barnum, M. A. Nielsen, B. Schumacher, *Information transmission through a noisy quantum channel* // Phys. Rev. A, **57**, (1998), 4153-4175.

[21] I. Devetak, *The private classical information capacity and quantum information capacity of a quantum channel* // LANL e-print quant-ph/0304127, 2003.