

УДК 621.391.1 : 519.72

© 2013 г. А.С. Холево, М.Е. Широков

О КЛАССИЧЕСКИХ ПРОПУСКНЫХ СПОСОБНОСТЯХ БЕСКОНЕЧНОМЕРНЫХ КВАНТОВЫХ КАНАЛОВ¹

Получено обобщение теоремы кодирования для классической пропускной способности с использованием сцепленности на случай произвольных бесконечномерных квантовых каналов с любыми ограничениями линейного типа. Установлены соотношения между классической пропускной способностью с использованием сцепленности и χ -пропускной способностью, а также условия их совпадения. Получены достаточные условия непрерывности классической пропускной способности с использованием сцепленности как функции канала. Рассмотрены приложения полученных результатов к бозонным квантовым гауссовским каналам. Получена общая форма фундаментального соотношения между когерентной информацией и мерой секретности передачи классической информации для бесконечномерных квантовых каналов.

§ 1. Введение

Центральную роль в квантовой теории информации играет понятие квантового канала – некоммутативного аналога матрицы переходных вероятностей в классической теории. Информационные свойства квантовых каналов характеризуются различными пропускными способностями, определяемыми типом передаваемой информации, дополнительными ресурсами, используемыми при передаче, требованиями секретности и т.п. (см., например, [1]). Одной из наиболее важных характеристик является классическая пропускная способность с использованием сцепленности, которая определяет предельную скорость передачи классической информации при использовании сцепленного состояния между входом и выходом. В силу определения эта пропускная способность не меньше, чем обычная классическая пропускная способность канала. Теорема Беннетта–Шора – Смолина – Таплияла (BSST-теорема) [2] дает явное выражение для пропускной способности с использованием сцепленности конечномерного канала без ограничений в виде максимума квантовой взаимной информации.

При передаче информации по *бесконечномерному* каналу налагаются определенные ограничения на входные состояния. Типичное физически мотивированное ограничение на среднюю энергию состояний, используемых для кодирования, определяется линейным неравенством

$$\text{Tr } \rho F \leq E, \quad E > 0, \quad (1)$$

где F (положительный самосопряженный оператор) – гамильтониан входной квантовой системы. Операциональное определение классической пропускной способности

¹ Работа выполнена при частичной финансовой поддержке научной программы “Математическая теория управления и динамических систем” РАН и Российского фонда фундаментальных исследований (номера проектов 12-01-00319-а, 13-01-00295-а).

с использованием сцепленности бесконечномерного квантового канала с линейным ограничением (1) дано в [3], где получено обобщение BSSТ-теоремы при определенных предположениях относительно канала и оператора F . Недавние результаты относительно энтропийных характеристик бесконечномерных квантовых каналов (в частности, по поводу квантовой условной энтропии см. [4]) дают возможность получить обобщение BSSТ-теоремы для каналов с линейными ограничениями без каких-либо упрощающих предположений. Доказательство этого результата составляет первую часть статьи.

Вторая часть посвящена исследованию соотношений между классическими пропускными способностями с использованием и без использования сцепленности для бесконечномерных каналов с ограничениями, а также условий их (не)совпадения. При определенных условиях показано, что совпадение этих пропускных способностей возможно только для каналов, которые являются в существенном классически-квантовыми (см. определение в [1]).

Мы также рассматриваем вопрос о непрерывности классической пропускной способности с использованием сцепленности как функции канала. Физическая мотивация этого вопроса связана с тем, что квантовый канал в реальном эксперименте подвержен возмущениям. В конечномерном случае непрерывность классической пропускной способности с использованием сцепленности доказана в [5]. В бесконечномерном случае эта пропускная способность является лишь полунепрерывной снизу, и нами установлены достаточные условия ее непрерывности, а также рассмотрены некоторые их приложения.

В § 6 получено бесконечномерное обобщение соотношения, предложенного Шумахером и Вестморлендом [6], которое отражает фундаментальную связь между квантовой пропускной способностью и мерой секретности передачи классической информации по квантовому каналу.

В Приложении рассмотрены некоторые вспомогательные результаты о бозонных гауссовских каналах.

§ 2. Предварительные сведения

Всюду далее \mathcal{H} – сепарабельное гильбертово пространство, $\mathfrak{B}(\mathcal{H})$ – алгебра всех ограниченных операторов в \mathcal{H} и $\mathfrak{B}_+(\mathcal{H})$ – положительный конус в $\mathfrak{B}(\mathcal{H})$. Пусть $\mathfrak{T}(\mathcal{H})$ – банахово пространство всех ядерных операторов в \mathcal{H} , а $\mathfrak{S}(\mathcal{H})$ – замкнутое выпуклое подмножество пространства $\mathfrak{T}(\mathcal{H})$, состоящее из положительных операторов с единичным следом, называемых *состояниями* [1, 7]. Обозначим через $I_{\mathcal{H}}$ единичный оператор в гильбертовом пространстве \mathcal{H} , а через $\text{Id}_{\mathcal{H}}$ – тождественное преобразование банахова пространства $\mathfrak{T}(\mathcal{H})$.

Линейное вполне положительное сохраняющее след отображение $\Phi: \mathfrak{T}(\mathcal{H}_A) \rightarrow \mathfrak{T}(\mathcal{H}_B)$ называется *каналом* [1, 7]. В силу теоремы Стайнспринга полная положительность влечет существование гильбертова пространства \mathcal{H}_E и изометрии $V: \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_E$, таких что²

$$\Phi[\rho] = \text{Tr}_E V \rho V^*, \quad \rho \in \mathfrak{T}(\mathcal{H}_A). \quad (2)$$

Канал $\widehat{\Phi}: \mathfrak{T}(\mathcal{H}_A) \rightarrow \mathfrak{T}(\mathcal{H}_E)$, определяемый выражением

$$\widehat{\Phi}[\rho] = \text{Tr}_B V \rho V^*, \quad \rho \in \mathfrak{T}(\mathcal{H}_A), \quad (3)$$

называется *комплементарным* к каналу Φ [8]. Комплементарный канал определен однозначно в следующем смысле: если $\widehat{\Phi}': \mathfrak{T}(\mathcal{H}_A) \rightarrow \mathfrak{T}(\mathcal{H}_{E'})$ – канал, определенный

² Здесь и далее $\text{Tr}_{\mathcal{H}}(\cdot) = \text{Tr}_{\mathcal{H}_X}(\cdot)$.

выражением (3) посредством другой изометрии $V': \mathcal{H}_A \rightarrow \mathcal{H}_B \otimes \mathcal{H}_{E'}$, для которой выполняется (2), то существует частичная изометрия $W: \mathcal{H}_E \rightarrow \mathcal{H}_{E'}$, такая что

$$\widehat{\Phi}'[\rho] = W\widehat{\Phi}[\rho]W^*, \quad \widehat{\Phi}[\rho] = W^*\widehat{\Phi}'[\rho]W, \quad \rho \in \mathfrak{T}(\mathcal{H}_A).$$

Пусть $H(\rho)$ – энтропия фон Неймана состояния ρ , а $H(\rho \parallel \sigma)$ – квантовая относительная энтропия состояний ρ и σ [7, 9, 10]. Конечный набор состояний $\{\rho_i\}$ с соответствующим распределением вероятностей $\{\pi_i\}$ называется *ансамблем* и обозначается $\{\pi_i, \rho_i\}$. Состояние $\bar{\rho} = \sum_i \pi_i \rho_i$ называется *средним состоянием* ансамбля $\{\pi_i, \rho_i\}$.

χ -величина ансамбля $\{\pi_i, \rho_i\}$ определяется выражением

$$\chi(\{\pi_i, \rho_i\}) \doteq \sum_i \pi_i H(\rho_i \parallel \bar{\rho}) = H(\bar{\rho}) - \sum_i \pi_i H(\rho_i),$$

второе равенство в котором имеет место при условии $H(\bar{\rho}) < +\infty$. Будем использовать обозначение $\chi_\Phi(\{\pi_i, \rho_i\}) = \chi(\{\pi_i, \Phi[\rho_i]\})$. χ -величина является одним из квантовых аналогов шенноновской информации, она участвует в выражениях для классической пропускной способности квантового канала (см. ниже).

Пусть F – положительный самосопряженный оператор в \mathcal{H}_A . Для любого состояния $\rho \in \mathfrak{S}(\mathcal{H}_A)$ величина $\text{Tr } \rho F$ (конечная или бесконечная) определяется как $\sup_n \text{Tr } \rho P_n F P_n$, где P_n – спектральный проектор оператора F , соответствующий отрезку $[0, n]$.

Зададим линейные ограничения на входные состояния $\rho^{(n)}$ канала $\Phi^{\otimes n}$ вида

$$\text{Tr } \rho^{(n)} F^{(n)} \leq nE, \tag{4}$$

где

$$F^{(n)} = F \otimes \dots \otimes I + \dots + I \otimes \dots \otimes F. \tag{5}$$

Операциональное определение классической пропускной способности квантового канала с линейным ограничением приведено в [3]. Чтобы задать аналитическое выражение, введем χ -пропускную способность канала Φ с ограничением (4):

$$C_\chi(\Phi, F, E) = \sup_{\rho: \text{Tr } \rho F \leq E} C_\chi(\Phi, \rho),$$

где

$$C_\chi(\Phi, \rho) = \sup_{\sum_i \pi_i \rho_i = \rho} \chi_\Phi(\{\pi_i, \rho_i\}) \tag{6}$$

– так называемая χ -функция канала Φ (супремум берется по всем ансамблям со средним состоянием ρ). Если $H(\Phi[\rho]) < +\infty$, то

$$C_\chi(\Phi, \rho) = H(\Phi[\rho]) - \widehat{H}_\Phi(\rho), \tag{7}$$

где $\widehat{H}_\Phi(\rho) = \inf_{\sum_i \pi_i \rho_i = \rho} \sum_i \pi_i H(\Phi[\rho_i])$ – σ -выпуклая оболочка функции $\rho \mapsto H(\Phi[\rho])$.

В силу вогнутости этой функции инфимум можно брать только по ансамблям чистых состояний. В силу теоремы Холево – Шумахера – Вестморленда (HSW-теоремы) для каналов с линейными ограничениями (см. [3, предложение 3]) классическая пропускная способность канала Φ с ограничением (4) дается следующим регуляри-

зованным выражением:

$$C(\Phi, F, E) = \lim_{n \rightarrow +\infty} n^{-1} C_\chi(\Phi^{\otimes n}, F^{(n)}, nE),$$

в котором оператор $F^{(n)}$ определен соотношением (5).

Другим важным аналогом шенноновской информации, который возникает в связи с классической пропускной способностью с использованием сцепленности (см. § 3), является *квантовая взаимная информация*. В конечномерном случае для любого состояния $\rho \in \mathfrak{S}(\mathcal{H}_A)$ она определяется выражением (см. [11])

$$I(\rho, \Phi) = H(\rho) + H(\Phi[\rho]) - H((\Phi \otimes \text{Id}_R)[\hat{\rho}]), \quad (8)$$

в котором \mathcal{H}_R – гильбертово пространство эталонной системы, изоморфное пространству \mathcal{H}_A , а $\hat{\rho}$ – очищение состояния ρ в пространстве $\mathcal{H}_A \otimes \mathcal{H}_R$, так что $\rho = \text{Tr}_R \hat{\rho}$. С помощью комплементарного канала квантовую взаимную информацию можно выразить следующим образом:

$$I(\rho, \Phi) = H(\rho) + H(\Phi[\rho]) - H(\hat{\Phi}[\rho]). \quad (9)$$

В бесконечномерном случае выражения (8), (9) могут содержать неопределенность типа $\infty - \infty$; чтобы этого избежать, следует использовать определение

$$I(\rho, \Phi) = H((\Phi \otimes \text{Id}_R)[\hat{\rho}] \| (\Phi \otimes \text{Id}_R)[\rho \otimes \varrho]), \quad (10)$$

в котором $\varrho = \text{Tr}_A \hat{\rho}$ – состояние из $\mathfrak{S}(\mathcal{H}_R)$ с тем же ненулевым спектром, что и ρ . Аналитические свойства функции $(\rho, \Phi) \mapsto I(\rho, \Phi)$, определенной в (10), в бесконечномерном случае изучены в [12].

§ 3. Классическая пропускная способность с использованием сцепленности

Рассмотрим следующий протокол передачи классической информации по квантовому каналу $\Phi: \mathfrak{S}(\mathcal{H}_A) \rightarrow \mathfrak{S}(\mathcal{H}_{A'})$.³ Системы A и B находятся в сцепленном (чистом) состоянии ω_{AB} . Система A осуществляет кодирование $\lambda \rightarrow \mathcal{E}_\lambda$ классического сигнала λ из конечного алфавита Λ с вероятностями π_λ и посылает свою часть общего состояния по каналу Φ в B . Здесь \mathcal{E}_λ – кодирующие каналы, зависящие от сигнала λ . В результате B получает состояния $(\Phi \otimes \text{Id}_B)[\omega_\lambda]$, где $\omega_\lambda = (\mathcal{E}_\lambda \otimes \text{Id}_B)[\omega_{AB}]$, с вероятностями π_λ , и целью B является получение максимальной информации о λ , на основании измерений этих состояний. Для осуществления блочного кодирования эту процедуру следует применить к каналу $\Phi^{\otimes n}$. При этом сигнальные состояния $\omega_\lambda^{(n)}$, передаваемые по каналу $\Phi^{\otimes n} \otimes \text{Id}_B^{\otimes n}$, имеют вид

$$\omega_\lambda^{(n)} = (\mathcal{E}_\lambda^{(n)} \otimes \text{Id}_B^{\otimes n})[\omega_{AB}^{(n)}], \quad (11)$$

где $\omega_{AB}^{(n)}$ – чистое сцепленное состояние в n копиях системы AB , а $\lambda \rightarrow \mathcal{E}_\lambda^{(n)}$ – кодирующие каналы в n копиях системы A .

Ограничение (4) равносильно аналогичному ограничению на входные состояния канала $\Phi^{\otimes n} \otimes \text{Id}_B^{\otimes n}$ с оператором $F_{AB}^{(n)} = F^{(n)} \otimes I_B^{\otimes n}$. Пусть $\mathcal{P}_{AB}^{(n)}$ – множество всех ансамблей $\pi^{(n)} = \{\pi_\lambda^{(n)}, \omega_\lambda^{(n)}\}$, где $\omega_\lambda^{(n)}$ – состояния вида (11), удовлетворяющие неравенству

$$\sum_{\lambda \in \Lambda} \pi_\lambda^{(n)} \text{Tr} \omega_\lambda^{(n)} F_{AB}^{(n)} \leq nE.$$

³ В этом параграфе будет удобно обозначать выход квантового канала через A' вместо B .

Классическая пропускная способность данного протокола называется *классической пропускной способностью с использованием сцепленности* канала Φ с ограничением (4) и обозначается $C_{\text{ea}}(\Phi, F, E)$ (более подробное определение см. в [3]). Модифицируя доказательство предложения 2 в [3], получаем

$$C_{\text{ea}}(\Phi, F, E) = \lim_{n \rightarrow \infty} \frac{1}{n} C_{\text{ea}}^{(n)}(\Phi, F, E), \quad (12)$$

где

$$C_{\text{ea}}^{(n)}(\Phi, F, E) = \sup_{\pi^{(n)} \in \mathcal{P}_{AB}^{(n)}} \chi_{\Phi^{\otimes n} \otimes \text{Id}_B^{\otimes n}}(\{\pi_\lambda^{(n)}, \omega_\lambda^{(n)}\}). \quad (13)$$

Именно эти выражения будут использоваться в статье. Следующая теорема обобщает предложение 4 из [3] на случай произвольного канала Φ и произвольного оператора F , определяющего ограничение.

Теорема 1. Пусть $\Phi: \mathfrak{S}(\mathcal{H}_A) \rightarrow \mathfrak{S}(\mathcal{H}_{A'})$ – квантовый канал, а F – самосопряженный положительный оператор в пространстве \mathcal{H}_A . Пропускная способность с использованием сцепленности (конечная или бесконечная) канала Φ с ограничением (4) дается выражением

$$C_{\text{ea}}(\Phi, F, E) = \sup_{\rho: \text{Tr } \rho F \leq E} I(\rho, \Phi). \quad (14)$$

В силу теоремы 1 пропускная способность с использованием сцепленности канала Φ без ограничений равна

$$C_{\text{ea}}(\Phi) = \sup_{\rho \in \mathfrak{S}(\mathcal{H}_A)} I(\rho, \Phi).$$

Доказательство. Для доказательства неравенства \geq в (14) предположим сначала, что канал Φ имеет конечномерный выход (система A' имеет конечную размерность). В этом случае требуемое неравенство можно доказать, повторяя рассуждения из соответствующей части доказательства предложения 4 из [3], основанного на специальном кодирующем протоколе. Сделаем только несколько замечаний об обобщении этого рассуждения:

1. Из конечномерности системы A' следует конечность выходной энтропии канала Φ на всем пространстве входных состояний;
2. Из конечности величины $\text{Tr } \rho F$ следует принадлежность всех собственных векторов состояния ρ области определения оператора \sqrt{F} ;
3. В силу конечномерности системы A' для любого состояния ρ конечного ранга сужение канала $\Phi^{\otimes n}$ на носитель состояния $\rho^{\otimes n}$ можно считать конечномерным каналом при каждом n ;
4. Если состояний, удовлетворяющих неравенству $\text{Tr } \rho F < E$, не существует, но есть состояние ρ_0 бесконечного ранга, такое что $\text{Tr } \rho_0 F = E$, то найдется последовательность $\{\rho_n\}$ состояний конечного ранга, сходящаяся к ρ_0 , такая что $\text{Tr } \rho_n F = E$, для которой

$$\liminf_{n \rightarrow +\infty} I(\rho_n, \Phi) \geq I(\rho_0, \Phi)$$

в силу полунепрерывности снизу квантовой взаимной информации.

Пусть Φ – произвольный канал, а $\{P_n\}$ – последовательность проекторов в $\mathcal{H}_{A'}$ конечного ранга, сильно сходящаяся к единичному оператору $I_{A'}$. Канал Φ является пределом в топологии сильной сходимости (см. [13]) последовательности каналов $\Pi_n \circ \Phi$ с конечномерным выходом, где $\Pi_n(\rho) = P_n \rho P_n + [\text{Tr } \rho(I_{A'} - P_n)]\tau$, а τ – заданное

состояние в A' . Поскольку неравенство \geq в (14) доказано для каналов с конечно-мерным выходом, цепное правило для пропускной способности с использованием сцепленности показывает, что

$$C_{\text{ea}}(\Phi, F, E) \geq C_{\text{ea}}(\Pi_n \circ \Phi, F, E) \geq I(\rho, \Pi_n \circ \Phi)$$

для всех ρ , таких что $\text{Tr } \rho F \leq E$. Из полунепрерывности снизу функции $\Phi \mapsto I(\rho, \Phi)$ в топологии сильной сходимости и цепного правила для квантовой взаимной информации (см. [12, предложение 1]) следует, что

$$\lim_{n \rightarrow +\infty} I(\rho, \Pi_n \circ \Phi) = I(\rho, \Phi) \leq +\infty \quad \text{для всех } \rho.$$

Поэтому неравенство \geq в (14) для канала Φ следует из приведенного выше неравенства.

Докажем неравенство \leq в (14). В силу доказываемой ниже леммы величина $\chi_{\Phi \otimes n \otimes \text{Id}_B^{\otimes n}}(\dots)$ в правой части неравенства (13) ограничена сверху величиной $I\left(\sum_{\lambda} \pi_{\lambda}^{(n)}(\omega_{\lambda}^{(n)})_A, \Phi^{\otimes n}\right)$. Из (12) получаем

$$C_{\text{ea}}(\Phi, F, E) \leq \lim_{n \rightarrow \infty} \frac{1}{n} \sup_{\pi^{(n)} \in \mathcal{P}_{AB}^{(n)}} I\left(\sum_{\lambda} \pi_{\lambda}^{(n)}(\omega_{\lambda}^{(n)})_A, \Phi^{\otimes n}\right).$$

Правая часть не превосходит

$$\sup_{\rho^{(n)}: \text{Tr } \rho^{(n)} F^{(n)} \leq nE} I(\rho^{(n)}, \Phi^{\otimes n}) \equiv \bar{I}_n(\Phi).$$

Заметим, что последовательность $\bar{I}_n(\Phi)$ аддитивна. Для доказательства достаточно установить, что

$$\bar{I}_n(\Phi) \leq n\bar{I}_1(\Phi). \quad (15)$$

В силу субаддитивности квантовой взаимной информации

$$I(\rho^{(n)}, \Phi^{\otimes n}) \leq \sum_{j=1}^n I(\rho_j^{(n)}, \Phi),$$

где $\rho_j^{(n)}$ – частичные состояния, и в силу вогнутости

$$\sum_{j=1}^n I(\rho_j^{(n)}, \Phi) \leq nI\left(\frac{1}{n} \sum_{j=1}^n \rho_j^{(n)}, \Phi\right).$$

Неравенство $\text{Tr } \rho^{(n)} F^{(n)} \leq nE$ равносильно неравенству $\text{Tr}\left(\frac{1}{n} \sum_{j=1}^n \rho_j^{(n)}\right) F \leq E$, откуда следует (15). Поэтому

$$C_{\text{ea}}(\Phi, F, E) \leq \sup_{\rho: \text{Tr } \rho F \leq E} I(\rho, \Phi).$$

Лемма. Пусть $\Phi: \mathfrak{S}(\mathcal{H}_A) \rightarrow \mathfrak{S}(\mathcal{H}_{A'})$ – квантовый канал, а σ – произвольное состояние из $\mathfrak{S}(\mathcal{H}_B)$. Для любого ансамбля $\{\pi_i, \omega_i\}$ состояний из $\mathfrak{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$, таких что $(\omega_i)_B = \sigma \in \mathfrak{S}(\mathcal{H}_B)$ для всех i , имеет место неравенство

$$\chi_{\Phi \otimes \text{Id}_B}(\{\pi_i, \omega_i\}) \leq I(\omega_A, \Phi), \quad (16)$$

где $\omega = \sum_i \pi_i \omega_i$ – среднее состояние ансамбля $\{\pi_i, \omega_i\}$.

Для доказательства леммы потребуется бесконечномерное обобщение квантовой условной энтропии, предложенное в [4].

В конечномерном случае условная энтропия состояния ρ составной системы AB определяется выражением

$$H(A|B)_\rho \doteq H(\rho) - H(\rho_B). \quad (17)$$

Условная энтропия всегда конечна, но в отличие от классического случая может быть отрицательной.

Следуя работе [4], условную энтропию состояния ρ бесконечномерной составной системы AB определим выражением

$$H(A|B)_\rho \doteq H(\rho_A) - H(\rho \| \rho_A \otimes \rho_B) \quad (18)$$

при условии $H(\rho_A) < +\infty$. Нетрудно видеть, что правые части (17) и (18) совпадают в случае $H(\rho) < +\infty$ (конечность любых двух величин из тройки $H(\rho_A), H(\rho_B), H(\rho)$ гарантирует конечность третьей).

В [4] показано, что определенная таким образом условная энтропия является вогнутой функцией на выпуклом множестве всех состояний ρ системы AB , таких что $H(\rho_A) < +\infty$, и обладает следующими свойствами:

$$H(A|B)_{\rho_{AB}} \geq H(A|BC)_\rho \quad (19)$$

для любого состояния ρ системы ABC (монотонность);

$$H(A|B)_{\rho_{AB}} = -H(A|C)_{\rho_{AC}} \quad (20)$$

для любого чистого состояния ρ системы ABC в предположении, что $H(\rho_A) < +\infty$.

Доказательство леммы. Пусть $\{\pi_i, \omega_i\}$ – ансамбль состояний из множества $\mathfrak{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ со средним состоянием ω , такой что $(\omega_i)_B = \sigma \in \mathfrak{S}(\mathcal{H}_B)$ для всех i . Надо показать, что

$$\sum_i \pi_i H(\Phi \otimes \text{Id}_B[\omega_i] \| \Phi \otimes \text{Id}_B[\omega]) \leq I(\omega_A, \Phi). \quad (21)$$

Докажем сначала неравенство (21), предполагая, что $\dim \mathcal{H}_{A'} < +\infty$ и $\dim \mathcal{H}_B < +\infty$. В этом случае левую часть этого неравенства можно переписать в виде

$$L \doteq H(\Phi \otimes \text{Id}_B[\omega]) - \sum_i \pi_i H(\Phi \otimes \text{Id}_B[\omega_i]).$$

В силу субаддитивности энтропии фон Неймана имеем

$$L \leq H(\Phi[\rho]) + \sum_i \pi_i [H(\sigma) - H(\Phi \otimes \text{Id}_B[\omega_i])],$$

где $\rho = \omega_A$. Заметим, что $H(\Phi \otimes \text{Id}_B[\omega_i]) - H(\sigma)$ – условная энтропия $H(A'|B)$ в состоянии $\Phi \otimes \text{Id}_B[\omega_i]$. Пусть $\hat{\omega}_i$ – чистое состояние системы ABR_i , такое что $(\hat{\omega}_i)_{AB} = \omega_i$. В силу монотонности условной энтропии (свойство (19)) имеем

$$H(\Phi \otimes \text{Id}_B[\omega_i]) - H(\sigma) = H(A'|B)_{\Phi \otimes \text{Id}_B[\omega_i]} \geq H(A'|BR_i)_{\Phi \otimes \text{Id}_{BR_i}[\hat{\omega}_i]}, \quad (22)$$

где величина $H(A'|BR_i)$ определена в (18) (система R_i бесконечномерна, однако система A' предполагается конечномерной). Поскольку $\hat{\omega}_i$ – очищение состояния

$\rho_i \doteq (\omega_i)_A$, т.е. $(\widehat{\omega}_i)_A = \rho_i$, то в силу свойства (20) условной энтропии имеем

$$\begin{aligned} H(A' | BR_i)_{\Phi \otimes \text{Id}_{BR_i}[\widehat{\omega}_i]} &= H(A' | BR_i)_{\text{Tr}_E V \otimes I_{BR_i} \cdot \widehat{\omega}_i \cdot V^* \otimes I_{BR_i}} = \\ &= -H(A' | E)_{\text{Tr}_{BR_i} V \otimes I_{BR_i} \cdot \widehat{\omega}_i \cdot V^* \otimes I_{BR_i}} = -H(A' | E)_{V \rho_i V^*}, \end{aligned} \quad (23)$$

где E – система-окружение для канала Φ , а V – изометрия Стайнспринга (что означает $\Phi[\rho] = \text{Tr}_E V \rho V^*$).

Используя вогнутость условной энтропии (определенной формулой (18)) и свойство (20), получаем

$$\sum_i \pi_i H(A' | E)_{V \rho_i V^*} \leq H(A' | E)_{V \rho V^*} = -H(A' | R)_{\text{Tr}_E V \otimes I_R \cdot \widehat{\rho} \cdot V^* \otimes I_R},$$

где R – эталонная система для состояния ρ , а $\widehat{\rho}$ – чистое состояние системы AR , такое что $\widehat{\rho}_A = \rho$. Поэтому из (22) и (23) получаем

$$L \leq H(\Phi[\rho]) - H(A' | R)_{\Phi \otimes \text{Id}_R[\widehat{\rho}]} = H(\Phi \otimes \text{Id}_R[\widehat{\rho}] \| \Phi[\rho] \otimes \widehat{\rho}_R) = I(\rho, \Phi),$$

где были использованы определения (10) и (18).

Неравенство (21) доказано в предположении $\dim \mathcal{H}_{A'} < +\infty$, $\dim \mathcal{H}_B < +\infty$. Для его доказательства в общем случае воспользуемся методом аппроксимации.

Пусть $\{\pi_i, \omega_i\}$ – такой ансамбль, что $(\omega_i)_B = \sigma \in \mathfrak{S}(\mathcal{H}_B)$, а Q_n – спектральный проектор состояния σ , соответствующий его n наибольшим собственным значениям. Пусть $\lambda_n = \text{Tr} Q_n \sigma$ и $C_n = I_A \otimes Q_n$. При каждом натуральном n рассмотрим ансамбль $\{\pi_i, \omega_i^n\}$ со средним состоянием ω^n , где

$$\omega_i^n = \lambda_n^{-1} C_n \omega_i C_n, \quad \omega^n = \lambda_n^{-1} C_n \omega C_n.$$

Пусть $\{P_n\}$ – последовательность проекторов конечного ранга в пространстве $\mathcal{H}_{A'}$, сильно сходящаяся к единичному оператору $I_{A'}$, а τ – чистое состояние из $\mathfrak{S}(\mathcal{H}_{A'})$. Рассмотрим последовательность каналов $\Phi_n = \Pi_n \circ \Phi$, где

$$\Pi_n[\rho] = P_n \rho P_n + \tau \text{Tr}(I_{A'} - P_n) \rho, \quad \rho \in \mathfrak{S}(\mathcal{H}_{A'}).$$

Поскольку $(\omega_i^n)_B = \lambda_n^{-1} Q_n \sigma$ для всех i , из первой части доказательства следует, что

$$\sum_i \pi_i H(\Phi_n \otimes \text{Id}_B[\omega_i^n] \| \Phi_n \otimes \text{Id}_B[\omega^n]) \leq I(\omega_A^n, \Phi_n).$$

Поскольку $\lambda_n \omega_A^n \leq \omega_A$, из леммы 4 работы [12] вытекает, что $\lim_{n \rightarrow +\infty} I(\omega_A^n, \Phi_n) = I(\omega_A, \Phi)$. Поэтому из приведенного выше неравенства, в силу полунепрерывности снизу относительной энтропии, следует неравенство (21). Лемма, а значит, и теорема 1, полностью доказаны. \blacktriangle

§ 4. Соотношения между классическими пропускными способностями с использованием и без использования сцепленности

При исследовании бесконечномерных квантовых систем и каналов необходимо рассматривать *обобщенные ансамбли*, которые определяются как борелевские вероятностные меры μ на множестве всех квантовых состояний. При таком подходе обычным ансамблям соответствуют меры с конечным носителем. Обозначим через $\mathcal{P}(\mathfrak{S}(\mathcal{H}))$ множество всех обобщенных ансамблей состояний из $\mathfrak{S}(\mathcal{H})$.

χ -величина обобщенного ансамбля μ определяется выражением

$$\chi(\mu) = \int_{\mathfrak{S}(\mathcal{H})} H(\rho \parallel \bar{\rho}(\mu)) \mu(d\rho) = H(\bar{\rho}(\mu)) - \int_{\mathfrak{S}(\mathcal{H})} H(\rho) \mu(d\rho), \quad (24)$$

в котором $\bar{\rho}(\mu) = \int_{\mathfrak{S}(\mathcal{H})} \rho \mu(d\rho)$ – среднее состояние ансамбля μ (интеграл в смысле

Бохнера), а второе равенство справедливо при условии $H(\bar{\rho}(\mu)) < +\infty$ (см. [14]). Для произвольного обобщенного ансамбля $\mu \in \mathcal{P}(\mathfrak{S}(\mathcal{H}_A))$ и канала $\Phi: \mathfrak{S}(\mathcal{H}_A) \rightarrow \mathfrak{S}(\mathcal{H}_B)$ можно рассмотреть ансамбль $\mu \circ \Phi^{-1} \in \mathcal{P}(\mathfrak{S}(\mathcal{H}_A))$ – образ ансамбля μ при действии канала Φ , определяемый следующим образом:

$$\mu \circ \Phi^{-1}(B) = \mu(\{\rho \in \mathfrak{S}(\mathcal{H}_A) \mid \Phi[\rho] \in B\}).$$

χ -величину ансамбля $\mu \circ \Phi^{-1}$ будем обозначать через $\chi_\Phi(\mu)$. Она равна

$$\begin{aligned} \chi_\Phi(\mu) &= \int_{\mathfrak{S}(\mathcal{H}_A)} H(\Phi[\rho] \parallel \Phi[\bar{\rho}(\mu)]) \mu(d\rho) = \\ &= H(\Phi[\bar{\rho}(\mu)]) - \int_{\mathfrak{S}(\mathcal{H}_A)} H(\Phi[\rho]) \mu(d\rho), \end{aligned} \quad (25)$$

где второе равенство справедливо при условии $H(\Phi[\bar{\rho}(\mu)]) < +\infty$.

В [14] показано, что для χ -функции, определенной формулой (6), справедливо выражение

$$C_\chi(\Phi, \rho) = \sup_{\mu: \bar{\rho}(\mu)=\rho} \chi_\Phi(\mu) \quad (26)$$

(здесь супремум берется по множеству всех обобщенных ансамблей из $\mathcal{P}(\mathfrak{S}(\mathcal{H}_A))$ со средним состоянием ρ), а значит,

$$C_\chi(\Phi, F, E) = \sup_{\mu: \text{Tr } \bar{\rho}(\mu) F \leq E} \chi_\Phi(\mu). \quad (27)$$

В этом параграфе будут исследованы общие соотношения между пропускными способностями $C_\chi(\Phi, F, E)$, $C(\Phi, F, E)$ и $C_{\text{ea}}(\Phi, F, E)$, а также условия их совпадения в предположении⁴

$$H(\rho) < +\infty \quad \text{для всех } \rho, \text{ таких что } \text{Tr } \rho F \leq E, \quad (28)$$

которое гарантирует, в частности, конечность всех этих величин. Центральную роль в этом исследовании будет играть следующее выражение для квантовой взаимной информации:

$$I(\Phi, \rho) = H(\rho) + C_\chi(\Phi, \rho) - C_\chi(\widehat{\Phi}, \rho), \quad (29)$$

справедливое при условии $H(\rho) < +\infty$ (поскольку $C_\chi(\Phi, \rho) \leq H(\rho)$ для любого канала Φ , это условие гарантирует конечность всех слагаемых в правой части (29)).

Если $H(\Phi[\rho])$ и $H(\widehat{\Phi}[\rho])$ конечны, то выражение (29) прямо следует из (7), (9), поскольку $\widehat{H}_\Phi \equiv \widehat{H}_{\widehat{\Phi}}$ (это следует из совпадения $H(\Phi[\rho])$ и $H(\widehat{\Phi}[\rho])$ для чистого состояния ρ); в общем случае оно доказывается с помощью предложения 4 в § 6.

⁴ Можно показать, что это предположение равносильно тому, что $\text{Tr} \exp(-\lambda F) < +\infty$ при некотором $\lambda > 0$.

В силу субаддитивности квантовой взаимной информации из выражения (29) следует формальное доказательство неравенства

$$C(\Phi, F, E) \leq C_{\text{ea}}(\Phi, F, E), \quad (30)$$

которое представляется очевидным с точки зрения операционального понимания пропускных способностей. Это выражение также позволяет получить следующие неравенства.

Предложение 1. Пусть $\Phi: \mathfrak{S}(\mathcal{H}_A) \rightarrow \mathfrak{S}(\mathcal{H}_B)$ – квантовый канал, а F – положительный оператор, для которого выполнено условие (28). Имеют место неравенства

$$\begin{aligned} C_{\text{ea}}(\Phi, F, E) &\geq 2C_\chi(\Phi, F, E) - C_\chi(\widehat{\Phi}, F, E), \\ C_{\text{ea}}(\Phi, F, E) &\geq 2C(\Phi, F, E) - C(\widehat{\Phi}, F, E), \end{aligned} \quad (31)$$

в которых $\widehat{\Phi}: \mathfrak{S}(\mathcal{H}_A) \rightarrow \mathfrak{S}(\mathcal{H}_E)$ – комплементарный канал к Φ .

Заметим, что в отличие от (30) оба неравенства в (31) превращаются в равенства, если Φ – обратимый унитарный канал. Эти неравенства показывают, что равенство $C_{\text{ea}}(\Phi, F, E) = C_\chi(\Phi, F, E)$ (или аналогичное равенство для $C(\Phi, F, E)$) возможно только в случае $C_\chi(\Phi, F, E) \leq C_\chi(\widehat{\Phi}, F, E)$ (соответственно, $C(\Phi, F, E) \leq C(\widehat{\Phi}, F, E)$).

Доказательство. Для любого $\varepsilon > 0$ обозначим через ρ_ε состояние из $\mathfrak{S}(\mathcal{H}_A)$, такое что

$$C_\chi(\Phi, F, E) < C_\chi(\Phi, \rho_\varepsilon) + \varepsilon, \quad \text{Tr } \rho_\varepsilon F \leq E.$$

Поскольку $C_\chi(\Phi, \rho_\varepsilon) \leq H(\rho_\varepsilon) < +\infty$, теорема 1 и формула (29) показывают, что

$$\begin{aligned} C_{\text{ea}}(\Phi, F, E) &\geq I(\rho_\varepsilon, \Phi) \geq 2C_\chi(\Phi, \rho_\varepsilon) - C_\chi(\widehat{\Phi}, \rho_\varepsilon) \geq \\ &\geq 2C_\chi(\Phi, F, E) - C_\chi(\widehat{\Phi}, F, E) - 2\varepsilon, \end{aligned}$$

откуда следует первое неравенство в (31). Второе неравенство в (31) выводится из первого посредством регуляризации. \blacktriangle

Рассмотрим вопрос о совпадении пропускных способностей $C_{\text{ea}}(\Phi, F, E)$ и $C_\chi(\Phi, F, E)$.

Будем называть канал $\Phi: \mathfrak{S}(\mathcal{H}_A) \rightarrow \mathfrak{S}(\mathcal{H}_B)$ *классически-квантовым* (с-к каналом), если образ двойственного канала $\Phi^*: \mathfrak{B}(\mathcal{H}_B) \rightarrow \mathfrak{B}(\mathcal{H}_A)$ состоит из коммутирующих операторов. Если к тому же все эти операторы диагонализуются в некотором ортонормированном базисе $\{|k\rangle\}$ в \mathcal{H}_A , то будем называть этот канал с-к каналом *дискретного типа*. В этом случае он имеет следующее представление:

$$\Phi[\rho] = \sum_{k=1}^{\dim \mathcal{H}_A} \langle k|\rho|k\rangle \sigma_k, \quad (32)$$

в котором $\{\sigma_k\}$ – набор состояний из $\mathfrak{S}(\mathcal{H}_B)$. Конечномерный с-к канал всегда является каналом дискретного типа. Примером с-к канала недискретного типа является бозонный гауссовский с-к канал (см. Приложение).

В [15] показано, что $C_\chi(\Phi) = C_{\text{ea}}(\Phi)$ для любого конечномерного с-к канала Φ без ограничений; более того, из этого равенства следует, что сужение канала Φ на носитель среднего состояния любого оптимального ансамбля является с-к каналом (ансамбль называется оптимальным [16], если его χ -величина совпадает с $C_\chi(\Phi)$). Пример из [17] показывает, что при этом сам канал Φ может не быть с-к каналом.

Чтобы распространить это утверждение на бесконечномерный случай, необходимо использовать понятие обобщенного оптимального ансамбля для бесконечномерного канала с ограничением [14]. Обобщенный ансамбль μ_* является оптимальным для канала Φ с ограничением (4), если

$$\text{Tr } \bar{\rho}(\mu_*)F \leq E \quad \text{и} \quad C_\chi(\Phi, F, E) = \chi_\Phi(\mu_*),$$

т.е. если супремум в (27) достигается на мере μ_* .

Это определение – естественное обобщение понятия оптимального ансамбля для конечномерного канала. В отличие от конечномерного случая оптимальный обобщенный ансамбль для бесконечномерного канала с ограничением существует не всегда, однако имеет место следующее достаточное условие.

Предложение 2 [14]. *Если подмножество множества $\mathfrak{S}(\mathcal{H}_A)$, определяемое неравенством $\text{Tr } \rho F \leq E$, компактно⁵, а функция $\rho \mapsto H(\Phi[\rho])$ непрерывна на этом подмножестве, то существует обобщенный оптимальный ансамбль для канала Φ с ограничением (4).*

Это условие выполнено для произвольного бозонного гауссовского канала с ограничением на среднюю энергию, когда F – гамильтониан осцилляторного типа, задаваемый строго положительно определенной квадратичной формой от канонических наблюдаемых (см. [14, замечание после предложения 3]). Оно также выполнено для любого канала, имеющего представление Крауса с конечным числом слагаемых, если оператор F удовлетворяет условию $\text{Tr } \exp(-\lambda F) < +\infty$ при всех $\lambda > 0$ (это можно показать, используя предложение 6.6 из [10]).

Следующая теорема дает необходимое условие совпадения пропускных способностей $C_\chi(\Phi, F, E)$ и $C_{\text{ea}}(\Phi, F, E)$.

Теорема 2. *Предположим, что существует обобщенный оптимальный ансамбль μ_* для канала $\Phi: \mathfrak{S}(\mathcal{H}_A) \rightarrow \mathfrak{S}(\mathcal{H}_B)$ с ограничением (4) (например, выполнено условие предложения 2) и что выполнено условие (28). Пусть \mathcal{H}_* – носитель среднего состояния ансамбля μ_* , т.е. $\mathcal{H}_* = \text{supp } \bar{\rho}(\mu_*)$.*

Если $C_\chi(\Phi, F, E) = C_{\text{ea}}(\Phi, F, E)$, то сужение канала Φ на множество $\mathfrak{S}(\mathcal{H}_)$ является с-q каналом дискретного типа.*

Доказательство. Без ограничения общности можно считать, что оптимальный обобщенный ансамбль μ_* состоит из чистых состояний. Это следует из выпуклости функции $\sigma \mapsto H(\Phi[\sigma] \parallel \Phi[\rho])$, поскольку для произвольной меры $\mu \in \mathcal{P}(\mathfrak{S}(\mathcal{H}_A))$ существует мера $\hat{\mu} \in \mathcal{P}(\mathfrak{S}(\mathcal{H}_A))$ с носителем на множестве чистых состояний, такая что $\bar{\rho}(\hat{\mu}) = \bar{\rho}(\mu)$ и $\int f(\sigma)\hat{\mu}(d\sigma) \geq \int f(\sigma)\mu(d\sigma)$ для любой выпуклой полунепрерывной снизу неотрицательной функции f на $\mathfrak{S}(\mathcal{H}_A)$ (эту меру $\hat{\mu}$ можно построить, используя рассуждение из доказательства теоремы в [14]).

Из равенства $C_\chi(\Phi, F, E) = C_{\text{ea}}(\Phi, F, E)$ следует, что $C_\chi(\Phi, \bar{\rho}(\mu_*)) = I(\Phi, \bar{\rho}(\mu_*))$. В силу условия (28) и представления (29) это равносильно равенству $H(\bar{\rho}(\mu_*)) = C_\chi(\hat{\Phi}, \bar{\rho}(\mu_*)) < +\infty$. В силу замечания после предложения 4 в § 6 и условия (28) из равенства $C_\chi(\Phi, \bar{\rho}(\mu_*)) = \chi_\Phi(\mu_*)$ следует, что $C_\chi(\hat{\Phi}, \bar{\rho}(\mu_*)) = \chi_{\hat{\Phi}}(\mu_*)$. Поскольку $H(\bar{\rho}(\mu_*)) = \chi(\mu_*)$, равенство $H(\bar{\rho}(\mu_*)) = \chi_{\hat{\Phi}}(\mu_*)$ показывает, что канал $\hat{\Phi}$ сохраняет χ -величину ансамбля μ_* , т.е. $\chi_{\hat{\Phi}}(\mu_*) = \chi(\mu_*)$. В силу теоремы 5 из [18] сужение канала $\hat{\Phi} \cong \Phi$ на множество $\mathfrak{S}(\mathcal{H}_*)$ является с-q каналом дискретного типа. \blacktriangle

Замечание. В отличие от каналов без ограничений утверждение, обратное к утверждению теоремы 2, не имеет места даже в конечномерном случае: классическая пропускная способность с использованием сцепленности с-q канала дискретного

⁵ Это подмножество компактно тогда и только тогда, когда спектр оператора F состоит из собственных значений конечной кратности, стремящихся к бесконечности (см. лемму в [3] и лемму 3 в [14]).

типа с линейным ограничением может быть больше классической пропускной способности [15, пример 3]. Повторяя рассуждение из доказательства теоремы 2 в [15] и используя условие (28), можно показать, что $C_\chi(\Phi, F, E) = C_{\text{ea}}(\Phi, F, E)$ для любого s - q канала дискретного типа Φ с ограничением (4), если оператор F диагонализуем в базисе $\{|k\rangle\}$ из представления (32) канала Φ .

Для произвольного нетривиального подпространства $\mathcal{H}_0 \subset \mathcal{H}_A$ сужение канала $\Phi: \mathfrak{S}(\mathcal{H}_A) \rightarrow \mathfrak{S}(\mathcal{H}_B)$ на подмножество $\mathfrak{S}(\mathcal{H}_0)$ будем называть *подканалом* канала Φ , соответствующим подпространству \mathcal{H}_0 .

Теорема 2 дает следующее достаточное условие выполнения строгого неравенства $C_{\text{ea}}(\Phi, F, E) > C_\chi(\Phi, F, E)$.

Следствие. Если выполнены условия теоремы 2, то $C_{\text{ea}}(\Phi, F, E) > C_\chi(\Phi, F, E)$ в любом из следующих случаев:

1. Канал Φ не является s - q каналом дискретного типа, а оптимальная мера μ_* имеет невырожденное среднее состояние;
2. Канал Φ не имеет s - q подканалов дискретного типа.

Как было отмечено выше, условия теоремы 2 выполнены для произвольного гауссовского канала $\Phi_{K,l,\alpha}$, если F – гамильтониан осцилляторного типа (K, l, α – параметры канала, см. Приложение). В силу следствия и предложения 5 строгое неравенство $C_{\text{ea}}(\Phi_{K,l,\alpha}, F, E) > C_\chi(\Phi_{K,l,\alpha}, F, E)$ имеет место в каждом из следующих случаев:

1. $K \neq 0$, и оптимальная мера μ_* имеет невырожденное среднее состояние;
2. Ранг матрицы K совпадает с размерностью $2k$ входного симплектического пространства (k – число входных мод).

Условие 1 выполнено, если для канала $\Phi_{K,l,\alpha}$ справедлива гипотеза о гауссовских оптимизаторах (см. [1, глава 12]).

§ 5. О непрерывности пропускной способности с использованием сцепленности

Поскольку физический канал определяется с некоторой конечной точностью, возникает вопрос о непрерывности его пропускных способностей по отношению к малым возмущениям канала.

В этом параграфе рассмотрим свойства непрерывности пропускной способности с использованием сцепленности по отношению к топологии сильной сходимости на множестве всех каналов [13]. Сильная сходимость последовательности каналов $\Phi_n: \mathfrak{S}(\mathcal{H}_A) \rightarrow \mathfrak{S}(\mathcal{H}_B)$ к каналу $\Phi_0: \mathfrak{S}(\mathcal{H}_A) \rightarrow \mathfrak{S}(\mathcal{H}_B)$ означает, что $\lim_{n \rightarrow +\infty} \Phi_n[\rho] = \Phi_0[\rho]$ для любого состояния $\rho \in \mathfrak{S}(\mathcal{H}_A)$.

Из теоремы 1 и полунепрерывности снизу квантовой взаимной информации следует, что $\Phi \mapsto C_{\text{ea}}(\Phi, F, E)$ – полунепрерывная снизу функция в топологии сильной сходимости на множестве всех квантовых каналов, т.е.

$$\liminf_{n \rightarrow +\infty} C_{\text{ea}}(\Phi_n, F, E) \geq C_{\text{ea}}(\Phi_0, F, E) \quad (\leq +\infty)$$

для любой последовательности $\{\Phi_n\}$ каналов, сильно сходящейся к каналу Φ_0 .

Следующее предложение дает достаточные условия непрерывности.

Предложение 3. Пусть F – положительный оператор, такой что неравенство $\text{Tr} \exp(-\lambda F) < +\infty$ выполнено для всех $\lambda > 0$, а $\{\Phi_n\}$ – последовательность каналов, сильно сходящаяся к каналу Φ_0 . Соотношение

$$\lim_{n \rightarrow +\infty} C_{\text{ea}}(\Phi_n, F, E) = C_{\text{ea}}(\Phi_0, F, E) < +\infty \quad (33)$$

имеет место при выполнении одного из следующих условий:

1. $\lim_{n \rightarrow +\infty} H(\Phi_n[\rho_n]) = H(\Phi_0[\rho_0])$ для произвольной последовательности $\{\rho_n\}$, сходящейся к состоянию ρ_0 , такой что $\text{Tr } \rho_n F \leq E$ для всех $n = 0, 1, 2, \dots$;
2. Существует последовательность каналов $\{\widehat{\Phi}_n\}$, сильно сходящаяся к каналу $\widehat{\Phi}_0$, такая что $(\Phi_n, \widehat{\Phi}_n)$ – комплементарная пара при каждом $n = 0, 1, 2, \dots$

Условие 1 предложения 3 выполнено для любой сходящейся последовательности гауссовских каналов, если F – осцилляторный гамильтониан бозонной системы.

Условие 2 предложения 3 выполнено для последовательности каналов

$$\Phi_n[\rho] = \sum_{i=1}^{+\infty} V_i^n \rho (V_i^n)^*,$$

где $\{V_i^n\}_n$ – последовательность операторов из \mathcal{H}_A в \mathcal{H}_B , сильно сходящаяся к оператору V_i^0 при каждом i , таких что $\sum_{i=1}^{+\infty} (V_i^n)^* V_i^n = I_A$ для всех n . Действительно,

$$\widehat{\Phi}_n[\rho] = \sum_{i,j=1}^{+\infty} [\text{Tr } V_i^n \rho (V_j^n)^*] |i\rangle\langle j|,$$

где $\{|i\rangle\}_{i=1}^{+\infty}$ – ортонормированный базис в \mathcal{H}_E , и нетрудно видеть, что последовательности $\{\Phi_n\}$ и $\{\widehat{\Phi}_n\}$ сильно сходятся к каналам Φ_0 и $\widehat{\Phi}_0$ соответственно (которые определены аналогичными формулами при $n = 0$).

Доказательство. Прежде всего заметим, что множество

$$\mathcal{A} = \{\rho \in \mathfrak{S}(\mathcal{H}_A) \mid \text{Tr } \rho F \leq E\}$$

компактно (в силу леммы из [3]), а функция $\rho \mapsto H(\rho)$ непрерывна на этом множестве (в силу предложения 6.6 из [10]).

В силу предложения 4 из [12] функция $\rho \mapsto I(\rho, \Phi_n)$ непрерывна на компактном множестве \mathcal{A} при каждом n , и следовательно,

$$C_{\text{ea}}(\Phi_n, F, E) = \sup_{\rho \in \mathcal{A}} I(\rho, \Phi_n) = I(\rho_n, \Phi_n) < +\infty$$

для некоторого состояния ρ_n из \mathcal{A} .

Предположим, что существует

$$\lim_{n \rightarrow +\infty} C_{\text{ea}}(\Phi_n, F, E) > C_{\text{ea}}(\Phi_0, F, E). \quad (34)$$

В силу замечания перед предложением 3 для доказательства (33) достаточно установить, что (34) приводит к противоречию.

Поскольку множество \mathcal{A} компактно, можно считать (переходя к подпоследовательности), что последовательность $\{\rho_n\}$ сходится к некоторому состоянию $\rho_0 \in \mathcal{A}$. Поэтому для получения противоречия с (34) достаточно показать, что

$$\lim_{n \rightarrow +\infty} I(\rho_n, \Phi_n) = I(\rho_0, \Phi_0). \quad (35)$$

Условия 1 и 2 предложения 3 дают разные способы доказательства соотношения (35). Если выполнено условие 1, то

$$I(\rho_n, \Phi_n) = H(\rho_n) + H(\Phi_n[\rho_n]) - H(\Phi_n \otimes \text{Id}_R[|\varphi_n\rangle\langle\varphi_n|]),$$

где $|\varphi_n\rangle$ – любое очищение состояния ρ_n , $n = 0, 1, 2, \dots$

В силу полунепрерывности снизу функции $(\Phi, \rho) \mapsto I(\rho, \Phi)$, непрерывности энтропии на множестве \mathcal{A} и условия 1 для доказательства (35) достаточно установить, что

$$\liminf_{n \rightarrow +\infty} H(\Phi_n \otimes \text{Id}_R[|\varphi_n\rangle\langle\varphi_n|]) \geq H(\Phi_0 \otimes \text{Id}_R[|\varphi_0\rangle\langle\varphi_0|]).$$

Это соотношение следует из полунепрерывности снизу относительной энтропии, поскольку из сильной сходимости последовательности $\{\Phi_n\}$ к каналу Φ_0 следует сильная сходимость последовательности $\{\Phi_n \otimes \text{Id}_R\}$ к $\Phi_0 \otimes \text{Id}_R$, а последовательность $\{|\varphi_n\rangle\}$ можно выбрать сходящейся к вектору $|\varphi_0\rangle$ [12, лемма 2].

Если выполнено условие 2, то утверждение (35) непосредственно следует из предложения 5 в [12]. \blacktriangle

§ 6. Когерентная информация и мера секретности передачи классической информации

Пусть $\Phi: \mathfrak{S}(\mathcal{H}_A) \rightarrow \mathfrak{S}(\mathcal{H}_B)$ – квантовый канал, а $\widehat{\Phi}: \mathfrak{S}(\mathcal{H}_A) \rightarrow \mathfrak{S}(\mathcal{H}_E)$ – канал, комплементарный к Φ . В конечномерном случае *когерентная информация* канала Φ в любом состоянии ρ определяется как разность между $H(\Phi[\rho])$ и $H(\widehat{\Phi}[\rho])$. Когерентная информация – это еще один квантовый аналог шенноновской информации, имеющий отношение к квантовой пропускной способности канала [1, 6, 7]. В бесконечномерном случае величины $H(\Phi[\rho])$ и $H(\widehat{\Phi}[\rho])$ могут быть бесконечны даже для состояния ρ с конечной энтропией, поэтому когерентную информацию следует определить через квантовую взаимную информацию (как функцию со значениями в $(-\infty, +\infty]$) соотношением (см. [12])

$$I_c(\rho, \Phi) = I(\rho, \Phi) - H(\rho).$$

Пусть ρ – состояние из $\mathfrak{S}(\mathcal{H}_A)$ с конечной энтропией. В силу монотонности χ -величины значения $\chi_\Phi(\mu)$ и $\chi_{\widehat{\Phi}}(\mu)$ не превосходят $H(\rho) = \chi(\mu)$ для любой меры $\mu \in \mathcal{P}(\mathfrak{S}(\mathcal{H}_A))$ с носителем на множестве чистых состояний и барицентром ρ . Следующее предложение можно считать обобщением соотношения из работы [6], которое лежит в основе фундаментальной связи между квантовой пропускной способностью и мерой секретности передачи классической информации по квантовому каналу [6]. Эта мера определяется как разность $\chi_\Phi(\mu) - \chi_{\widehat{\Phi}}(\mu)$ между χ -величинами приемника и окружения (перехватчика).

Предложение 4. *Если μ – мера из $\mathcal{P}(\mathfrak{S}(\mathcal{H}_A))$ с носителем на множестве чистых состояний и барицентром ρ , то*

$$\chi_\Phi(\mu) - \chi_{\widehat{\Phi}}(\mu) = I(\rho, \Phi) - H(\rho) = I_c(\rho, \Phi). \quad (36)$$

Это предложение показывает, в частности, что разность $\chi_\Phi(\mu) - \chi_{\widehat{\Phi}}(\mu)$ не зависит от μ . Поэтому если супремум в выражении (26) для величины $C_\chi(\Phi, \rho)$ достигается на некоторой мере μ_* , то и в аналогичном выражении для величины $C_\chi(\widehat{\Phi}, \rho)$ супремум достигается на той же мере μ_* , и наоборот.

Доказательство. Если $H(\Phi[\rho]) < +\infty$, то $H(\widehat{\Phi}[\rho]) < +\infty$ в силу неравенства треугольника для энтропий (см. [7]), и соотношение (36) можно вывести из (9), используя второе выражение в (25) и совпадение функций $\rho \mapsto H(\Phi[\rho])$ и $\rho \mapsto H(\widehat{\Phi}[\rho])$ на множестве чистых состояний. В общем случае для доказательства (36) необходимо использовать метод аппроксимации. Для этого нам потребуются некоторые дополнительные понятия.

Пусть $\mathfrak{T}_1(\mathcal{H}) = \{A \in \mathfrak{T}(\mathcal{H}) \mid A \geq 0, \text{Tr } A \leq 1\}$. Будем использовать следующие продолжения энтропии фон Неймана на множество $\mathfrak{T}_1(\mathcal{H})$ (см. [9]):

$$S(A) = -\text{Tr } A \log A, \quad H(A) = S(A) + \text{Tr } A \log \text{Tr } A, \quad \forall A \in \mathfrak{T}_1(\mathcal{H}).$$

Из неотрицательности, вогнутости и полунепрерывности снизу энтропии фон Неймана следуют аналогичные свойства функций S и H на множестве $\mathfrak{T}_1(\mathcal{H})$.

Относительная энтропия операторов $A, B \in \mathfrak{T}_1(\mathcal{H})$ определяется следующим образом (подробнее см. в [9]):

$$H(A \parallel B) = \sum_i \langle i \mid (A \log A - A \log B + B - A) \mid i \rangle,$$

где $\{|i\rangle\}$ – ортонормированный базис из собственных векторов оператора A . С помощью этого расширения относительной энтропии χ -величину меры μ из $\mathcal{P}(\mathfrak{T}_1(\mathcal{H}))$ можно определить выражением (24).⁶

Линейное вполне положительное отображение $\Phi: \mathfrak{T}(\mathcal{H}_A) \rightarrow \mathfrak{T}(\mathcal{H}_B)$, не увеличивающее след, называется *квантовой операцией* [7]. Для любой квантовой операции Φ имеет место представление Стайнспринга (2), в котором V – сжимающий оператор. Комплементарная операция $\hat{\Phi}: \mathfrak{T}(\mathcal{H}_A) \rightarrow \mathfrak{T}(\mathcal{H}_E)$ определяется с помощью этого представления формулой (3).

Модифицируя рассуждения в доказательстве предложения 1 из [14], нетрудно показать, что функция $\mu \mapsto \chi(\mu)$ полунепрерывна снизу на множестве $\mathcal{P}(\mathfrak{T}_1(\mathcal{H}))$ и что для произвольной квантовой операции Φ и любой меры $\mu \in \mathcal{P}(\mathfrak{S}(\mathcal{H}_A))$, таких что $S(\Phi[\bar{\rho}(\mu)]) < +\infty$, χ -величину для меры $\mu \circ \Phi^{-1} \in \mathcal{P}(\mathfrak{T}_1(\mathcal{H}_B))$ можно выразить следующей формулой:

$$\chi_\Phi(\mu) = S(\Phi[\bar{\rho}(\mu)]) - \int_{\mathfrak{S}(\mathcal{H}_A)} S(\Phi[\rho]) \mu(d\rho). \quad (37)$$

Теперь можно доказать соотношение (36) в общем случае. Заметим, что для заданной меры $\mu \in \mathcal{P}(\mathfrak{S}(\mathcal{H}_A))$ функция $\mu \mapsto \chi_\Phi(\mu)$ полунепрерывна снизу на множестве всех квантовых операций, снабженном топологией сильной сходимости (для которой $\Phi_n \rightarrow \Phi$ означает, что $\Phi_n[\rho] \rightarrow \Phi[\rho]$ для всех ρ [13]). Это следует из полунепрерывности снизу функции $\mu \mapsto \chi(\mu)$ на множестве $\mathcal{P}(\mathfrak{T}_1(\mathcal{H}_B))$, поскольку для любой последовательности $\{\Phi_n\}$ квантовых операций, сильно сходящейся к квантовой операции Φ , последовательность $\{\mu \circ \Phi_n^{-1}\}$ слабо сходится к мере $\mu \circ \Phi^{-1}$ (это можно проверить непосредственно, используя определение слабой сходимости и заметив, что для последовательностей квантовых операций сильная сходимость равносильна равномерной сходимости на компактных подмножествах множества $\mathfrak{S}(\mathcal{H}_A)$, см. доказательство леммы 1 в [13]).

Пусть $\{P_n\}$ – возрастающая последовательность проекторов конечного ранга в $\mathfrak{B}(\mathcal{H}_B)$, сильно сходящаяся к I_B . Рассмотрим последовательность квантовых операций $\Phi_n = \Pi_n \circ \Phi$, где $\Pi_n[\sigma] = P_n \sigma P_n$. Тогда

$$\hat{\Phi}_n[\rho] = \text{Tr}_{\mathcal{H}_B} P_n \otimes I_{\mathcal{H}_E} V \rho V^*, \quad \rho \in \mathfrak{S}(\mathcal{H}_A), \quad (38)$$

где V – изометрия из представления Стайнспринга (2) канала Φ .

Последовательности $\{\Phi_n\}$ и $\{\hat{\Phi}_n\}$ сильно сходятся к каналам Φ и $\hat{\Phi}$ соответственно. Пусть $\rho = \sum_k \lambda_k |k\rangle\langle k|$ и $|\varphi_\rho\rangle = \sum_k \sqrt{\lambda_k} |k\rangle \otimes |k\rangle$. Поскольку $H(\rho) < +\infty$ и

⁶ $\mathcal{P}(\mathfrak{T}_1(\mathcal{H}))$ – множество всех вероятностных мер на $\mathfrak{T}_1(\mathcal{H})$, снабженное топологией слабой сходимости.

$S(\Phi_n[\rho]) < +\infty$, то и $S(\widehat{\Phi}_n[\rho]) < +\infty$ в силу неравенства треугольника для энтропий. Поэтому

$$\begin{aligned} I(\rho, \Phi_n) &= H(\Phi_n \otimes \text{Id}_R[|\varphi_\rho\rangle\langle\varphi_\rho|] \parallel \Phi_n[\rho] \otimes \varrho) = \\ &= -S(\widehat{\Phi}_n[\rho]) + S(\Phi_n[\rho]) + a_n = -\chi_{\widehat{\Phi}_n}(\mu) + \chi_{\Phi_n}(\mu) + a_n, \end{aligned} \quad (39)$$

где

$$a_n = -\sum_k \text{Tr}(\Phi_n[|k\rangle\langle k|]) \lambda_k \log \lambda_k, \quad (40)$$

а последнее равенство получено с помощью соотношения (37), где использовано совпадение функций $\rho \mapsto S(\Phi[\rho])$ и $\rho \mapsto S(\widehat{\Phi}[\rho])$ на множестве чистых состояний.

Поскольку функция $\Phi \mapsto I(\rho, \Phi)$ полунепрерывна снизу (в силу полунепрерывности снизу относительной энтропии) и $I(\rho, \Phi_n) \leq I(\rho, \Phi)$ для всех n в силу монотонности относительной энтропии при действии квантовой операции $\Pi_n \otimes \text{Id}_R$, имеем

$$\lim_{n \rightarrow +\infty} I(\rho, \Phi_n) = I(\rho, \Phi). \quad (41)$$

Покажем также, что

$$\lim_{n \rightarrow +\infty} \chi_{\Phi_n}(\mu) = \chi_\Phi(\mu) \quad \text{и} \quad \lim_{n \rightarrow +\infty} \chi_{\widehat{\Phi}_n}(\mu) = \chi_{\widehat{\Phi}}(\mu). \quad (42)$$

Первое соотношение в (42) следует из полунепрерывности снизу функции $\Phi \mapsto \chi_\Phi(\mu)$ (установленной ранее) и неравенства $\chi_{\Phi_n}(\mu) \leq \chi_\Phi(\mu)$, выполненного для всех n в силу монотонности χ -величины при действии квантовой операции Π_n .

Для доказательства второго соотношения в (42) заметим, что из (38) следует $\widehat{\Phi}_n[\rho] \leq \widehat{\Phi}[\rho]$ для любого состояния $\rho \in \mathfrak{S}(\mathcal{H}_A)$. Поэтому лемма 2 из [13] показывает, что

$$\chi_{\widehat{\Phi}_n}(\mu) \leq \chi_{\widehat{\Phi}}(\mu) + f(\text{Tr} \widehat{\Phi}_n[\rho]), \quad (43)$$

где $f(x) = -2x \log x - (1-x) \log(1-x)$, для любой меры $\mu \in \mathcal{P}(\mathfrak{S}(\mathcal{H}_A))$ с конечным носителем и барицентром ρ . Пусть μ – произвольная мера из $\mathcal{P}(\mathfrak{S}(\mathcal{H}_A))$, а $\{\mu_k\}$ – последовательность мер с конечным носителем и барицентром ρ , построенная в доказательстве леммы 1 из [14], которая слабо сходится к мере μ . Выполнимость неравенства (43) для меры μ выводится из того, что оно выполнено для всех мер μ_k . При этом используются полунепрерывность снизу функции $\mu \mapsto \chi_{\widehat{\Phi}_n}(\mu)$ и неравенство $\chi_{\widehat{\Phi}}(\mu_k) \leq \chi_{\widehat{\Phi}}(\mu)$, которое выполнено для всех k в силу конструкции последовательности $\{\mu_k\}$ и выпуклости относительной энтропии.

Из неравенства (43) и полунепрерывности снизу функции $\Phi \mapsto \chi_\Phi(\mu)$ следует второе соотношение в (42).

Поскольку последовательность $\{a_n\}$ (определенная в (40)), очевидно, сходится к $H(\rho)$, из соотношений (39), (41) и (42) следует (36). \blacktriangle

ПРИЛОЖЕНИЕ

Гауссовские классически-квантовые каналы. Основные приложения теории бесконечномерных квантовых систем и каналов связаны с бозонными системами, подробное описание которых можно найти, например, в [1, глава 11]. Пусть \mathcal{H}_A –

пространство неприводимого представления канонических коммутационных соотношений

$$W_A(z_A)W_A(z'_A) = \exp\left(-\frac{i}{2}z_A^\top \Delta_A z'_A\right) W_A(z'_A + z_A) \quad (44)$$

с координатным симплектическим пространством (Z_A, Δ_A) и семейством операторов Вейля $W_A(z_A) = \exp(iR_A \cdot z_A)$, $z_A \in Z_A$. Здесь R_A – вектор-строка канонических переменных в пространстве \mathcal{H}_A , а Δ_A – кососимметрическая коммутационная матрица компонент строки R_A . Гауссовский канал $\Phi: \mathfrak{T}(\mathcal{H}_A) \rightarrow \mathfrak{T}(\mathcal{H}_B)$ (где пространство \mathcal{H}_B определяется аналогично пространству \mathcal{H}_A) задается действием двойственного отображения Φ^* на операторы Вейля:

$$\Phi^*[W_B(z_B)] = W_A(Kz_B) \exp\left[il^\top z_B - \frac{1}{2}z_B^\top \alpha z_B\right], \quad (45)$$

где K – матрица линейного оператора $Z_B \rightarrow Z_A$, $l \in Z_B$, а α – вещественная симметрическая матрица, удовлетворяющая условию

$$\alpha \geq \pm \frac{i}{2} (\Delta_B - K^\top \Delta_A K).$$

Предложение 5. Пусть $\Phi_{K,l,\alpha}$ – гауссовский канал с параметрами K, l, α .

1) Канал $\Phi_{K,l,\alpha}$ является s - q каналом тогда и только тогда, когда

$$K^\top \Delta_A K = 0.$$

В этом случае он является s - q каналом дискретного типа тогда и только тогда, когда $K = 0$, т.е. когда он является вполне деполаризующим каналом.

2) Если $\text{rank } K = \dim Z_A$, то канал $\Phi_{K,l,\alpha}$ не имеет s - q подканалов дискретного типа.

Доказательство. 1) Поскольку семейство $\{W_B(z_B)\}_{z_B \in Z_B}$ порождает алгебру $\mathfrak{B}(\mathcal{H}_B)$, все операторы $\Phi_{K,l,\alpha}^*(A)$, $A \in \mathfrak{B}(\mathcal{H}_B)$, коммутируют тогда и только тогда, когда операторы (45), т.е. $W_A(Kz_B)$, коммутируют для всех z_B . В силу (44)

$$W_A(Kz_B)W_A(Kz'_B) = \exp(-iz_B^\top K^\top \Delta_A K z'_B) W_A(Kz'_B)W_A(Kz_B),$$

откуда следует первое утверждение. Из предположения о существовании дискретного представления (32) следует, что все операторы $W_A(Kz_B) = \exp(iR_A \cdot Kz_B)$ имеют чисто точечный спектр, что возможно, только если $Kz_B \equiv 0$, поскольку, как известно, канонические наблюдаемые R_A имеют непрерывный спектр.

2) Предположим, что существует подпространство $\mathcal{H}_0 \subset \mathcal{H}_A$, такое что

$$\Phi_{K,l,\alpha}[\rho] = \sum_k \langle k|\rho|k\rangle \sigma_k$$

для всех $\rho \in \mathfrak{S}(\mathcal{H}_0)$, где $\{|k\rangle\}$ – ортонормированный базис в \mathcal{H}_0 . Тогда

$$\begin{aligned} PW_A(Kz_B)P \exp\left[il^\top z_B - \frac{1}{2}z_B^\top \alpha z_B\right] &= P\Phi_{K,l,\alpha}^*[W_B(z_B)]P = \\ &= \sum_k [\text{Tr } W_B(z_B)\sigma_k] |k\rangle\langle k|, \end{aligned}$$

где $P = \sum_k |k\rangle\langle k|$ – проектор на \mathcal{H}_0 . Следовательно, $\langle k|W_A(Kz_B)|j\rangle = 0$ для всех $k \neq j$. Но это невозможно, поскольку $\{Kz_B \mid z_B \in Z_B\} = Z_A$, а значит, семейство $\{W_A(Kz_B)\}_{z_B \in Z_B}$ операторов Вейля действует неприводимо на \mathcal{H}_A . \blacktriangle

СПИСОК ЛИТЕРАТУРЫ

1. Халево А. С. Квантовые системы, каналы, информация. М.: МЦНМО, 2010.
2. Bennett C.H., Shor P.W., Smolin J.A., Thapliyal A.V. Entanglement-Assisted Classical Capacity of Noisy Quantum Channels // Phys. Rev. Lett. 1999. V.83. № 15. P. 3081–3084.
3. Халево А. С. Классические пропускные способности квантового канала с ограничением на входе // Теория вероятностей и ее применения. 2003. Т. 48. № 2. С. 359–374.
4. Кузнецова А. А. Условная энтропия для бесконечномерных квантовых систем // Теория вероятностей и ее применения. 2010. Т. 55. № 4. С. 782–790.
5. Leung D., Smith G. Continuity of Quantum Channel Capacities // Comm. Math. Phys. 2009. V. 292. № 1. P. 201–215.
6. Schumacher B., Westmoreland M.D. Quantum Privacy and Quantum Coherence // Phys. Rev. Lett. 1998. V. 80. № 25. P. 5695–5697.
7. Нильсен М. А., Чанг И. Квантовые вычисления и квантовая информация. М.: Мир, 2006.
8. Халево А. С. Комплементарные каналы и проблема аддитивности // Теория вероятностей и ее применения. 2006. Т. 51. № 1. С. 133–143.
9. Lindblad G. Expectations and Entropy Inequalities for Finite Quantum Systems // Commun. Math. Phys. 1974. V. 39. № 2. P. 111–119.
10. Ohya M., Petz D. Quantum Entropy and Its Use. Berlin: Springer, 2004.
11. Adami C., Cerf N.J. Von Neumann Capacity of Noisy Quantum Channels // Phys. Rev. A. 1997. V. 56. № 5. P. 3470–3483.
12. Халево А. С., Широков М. Е. Взаимная и когерентная информации для бесконечномерных квантовых каналов // Пробл. передачи информ. 2010. Т. 46. № 3. С. 3–21.
13. Халево А. С., Широков М. Е. Об аппроксимации бесконечномерных квантовых каналов // Пробл. передачи информ. 2008. Т. 44. № 2. С. 3–22.
14. Халево А. С., Широков М. Е. Непрерывные ансамбли и пропускная способность квантовых каналов бесконечной размерности // Теория вероятностей и ее применения. 2005. Т. 50. № 1. С. 98–114.
15. Широков М. Е. Условия совпадения классической пропускной способности и классической пропускной способности с использованием сцепленности квантового канала // Пробл. передачи информ. 2012. Т. 48. № 2. С. 3–20.
16. Schumacher B., Westmoreland M.D. Optimal Signal Ensembles // Phys. Rev. A. 2001. V. 63. № 2. P. 022308.
17. Bennett C.H., Shor P.W., Smolin J.A., Thapliyal A.V. Entanglement-Assisted Capacity of a Quantum Channel and the Reverse Shannon Theorem // IEEE Trans. Inform. Theory. 2002. V. 48. № 10. P. 2637–2655.
18. Широков М. Е. On Quantum Channels Reversible with Respect to a Given Family of Pure States // arXiv:1203.0262v1 [quant-ph], 2012.

Халево Александр Семенович
 Широков Максим Евгеньевич
 Математический институт им. В.А. Стеклова РАН
 holevo@mi.ras.ru
 msh@mi.ras.ru

Поступила в редакцию
 22.10.2012