Math-Net.Ru

Общероссийский математический портал

А. А. Кузнецова, А. С. Холево, Теоремы кодирования для гибридных каналов. II, *Теория вероятн. и ее примен.*, 2014, том 59, выпуск 1, 168–178

DOI: <https://doi.org/10.4213/tvp4556>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.224.187.69

26 апреля 2023 г., 17:10:08

3. Fournié E., Lasry J. M., Lebuchoux J., Lions P. L., Touzi N. Applications of Malliavin calculus to Monte Carlo methods in finance. — *Finance Stoch.*, 1999, v. 3, № 4, p. 391–412.
4. Montero M., Kohatsu-Higa A. Malliavin calculus applied to finance. — *Phys. A*, 2003, v. 320, № 1–4, p. 548–570.
5. Гусев С. А. Оценка производных по параметрам функционалов диффузионного процесса, движущегося в области с поглощающей границей. — *Сиб. журн. вычисл. матем.*, 2008, т. 11, № 4, с. 385–404.
6. Itô K. On a stochastic integral equation. — *Proc. Japan Acad.*, 1946, v. 22, № 1–4, p. 32–35.
7. Гихман И. И., Скороход А. В. Введение в теорию случайных процессов. М.: Наука, 1977, 567 с.
8. Ладыженская О. А., Солонников В. А., Уральцева Н. Н. Линейные и квазилинейные уравнения параболического типа. М.: Наука, 1967, 736 с.
9. Гихман И. И., Скороход А. В. Стохастические дифференциальные уравнения. Киев: Наукова думка, 1968, 354 с.
10. Lieberman G. E. Second Order Parabolic Differential Equations. World Scientific Publ. Co., 2005.

Поступила в редакцию
12.III.2012

Исправленный вариант
11.XII.2013

© 2014 г.

КУЗНЕЦОВА А. А.*, ХОЛЕВО А. С.**

ТЕОРЕМЫ КОДИРОВАНИЯ ДЛЯ ГИБРИДНЫХ КАНАЛОВ. II¹⁾

Настоящая работа продолжает исследование пропускных способностей измерительных (квантово-классических) каналов в наиболее общей постановке, начатое в [10]. В ней дается доказательство теорем кодирования для классической пропускной способности и классической пропускной способности с использованием сцепленности в случае измерительного канала с произвольным выходным алфавитом без предположения, что канал задается ограниченной операторной плотностью.

Ключевые слова и фразы: измерительный канал, гибридная вероятностная система, классическая пропускная способность, сцепленное состояние, теорема кодирования.

1. Введение. Настоящая работа продолжает исследование пропускных способностей измерительных каналов в наиболее общей постановке, начатое в [10]. В ней дается доказательство теорем кодирования для классической пропускной способности (теорема 1) и классической пропускной способности с использованием сцепленности (теорема 2) в случае измерительного канала с произвольным выходным алфавитом при минимальных предположениях регулярности. Утверждение теоремы 2 было ранее доказано в [10] при дополнительном предположении, что измерительный канал задается ограниченной операторной плотностью. В настоящей работе мы освобождаемся от этого ограничения, привлекая обобщение теоремы Радона–Никодима для

* МГТУ им. Н. Э. Баумана, Москва, Россия; e-mail: kuznetsova.a.a@bk.ru

** Математический институт им. В. А. Стеклова РАН, Москва, Россия; e-mail: holevo@mi.ras.ru

¹⁾ Работа выполнена при поддержке РФФИ (грант № 12-01-00319) и Российского Квантового Центра.

вероятностных операторнозначных мер [6]. Полученный результат иллюстрируется примером гомодинного измерения из квантовой оптики.

Отметим, что классическая пропускная способность с использованием сцепленности изучалась рядом авторов под названиями *purification capacity*, *measurement strength*, *forward classical communication cost*. В недавней работе [2], где можно найти дальнейшие ссылки, развита ее альтернативная интерпретация. Показано, что (конечномерный) измерительный канал асимптотически может быть смоделирован передачей классического сообщения, размером равного максимальной редукции энтропии, при наличии достаточной классической корреляции между входом и выходом канала. Этот результат может рассматриваться как квантовая инвертированная (reverse) теорема Шеннона, в которой использование сцепленности и квантового канала заменяется соответственно классической корреляцией и классическим каналом.

2. Предварительные сведения. Пусть $\mathcal{H}$ — сепарабельное гильбертово пространство. Мы будем использовать следующие обозначения: $\mathfrak{B}(\mathcal{H})$ — алгебра всех ограниченных операторов, $\mathfrak{T}(\mathcal{H})$ — пространство операторов со следом (ядерных операторов) в $\mathcal{H}$, $\mathfrak{S}(\mathcal{H})$ — выпуклое подмножество операторов плотности (т.е. положительных операторов с единичным следом), называемых также квантовыми состояниями.

Введем пространство с мерой $(\Omega, \mathcal{F}, \mu)$, где Ω — полное сепарабельное метрическое пространство, $\mathcal{F}$ — σ -алгебра его подмножеств, μ — σ -конечная мера на $\mathcal{F}$. Гибридная (классически-квантовая) система описывается алгеброй фон Неймана $\mathcal{L} = \mathcal{L}^\infty(\Omega, \mathcal{F}, \mu; \mathfrak{B}(\mathcal{H}))$, элементами которой являются слабо измеримые, существенно ограниченные функции $X(\omega)$, $\omega \in \Omega$, со значениями в $\mathfrak{B}(\mathcal{H})$. Рассмотрим сопряженное пространство $\mathcal{L}_* = \mathcal{L}_1(\Omega, \mathcal{F}, \mu; \mathfrak{T}(\mathcal{H}))$, элементами которого являются измеримые функции $S = \{S(\omega)\}$ со значениями в $\mathfrak{T}(\mathcal{H})$, интегрируемые по мере μ . Элемент $S = \{S(\omega)\} \in \mathcal{L}_*$ такой, что

$$S(\omega) \geq 0 \pmod{\mu}, \quad \int_{\Omega} \text{Tr } S(\omega) \mu(d\omega) = 1,$$

называется *состоянием* на алгебре $\mathcal{L}$. Для обозначения энтропийных характеристик гибридных систем будем использовать индекс “cq”, для классических и квантовых — индексы “c” и “q” соответственно.

Следуя [9], введем понятия энтропии и относительной энтропии cq-состояний. По поводу определений и свойств квантовых энтропий см., например, [8].

О п р е д е л е н и е 1. Энтропия cq-состояния S определяется соотношением

$$H_{cq}(S) = \int_{\Omega} H_q(S(\omega)) \mu(d\omega),$$

где $H_q(S) = -\text{Tr } S \log S$ — энтропия фон Неймана положительного оператора $S \in \mathfrak{T}(\mathcal{H})$.

Заметим, что

$$H_{cq}(S) = H_c(p) + \int_{\Omega} p(\omega) H_q(\hat{S}(\omega)) \mu(d\omega), \quad (1)$$

где $p(\omega) = \text{Tr } S(\omega)$, $\hat{S}(\omega) = (p(\omega))^{-1} S(\omega)$, $H_c(p)$ — дифференциальная энтропия распределения вероятностей с плотностью $p(\omega)$ относительно меры μ .

О п р е д е л е н и е 2. Относительная энтропия cq-состояний S_1, S_2 определяется соотношением

$$H_{cq}(S_1 \| S_2) = \int_{\Omega} H_q(S_1(\omega) \| S_2(\omega)) \mu(d\omega),$$

где

$$H_q(S_1(\omega) \| S_2(\omega)) = \text{Tr } S_1(\omega) (\log S_1(\omega) - \log S_2(\omega))$$

— квантовая относительная энтропия.

В дальнейшем для описания измерительных каналов нам потребуется следующее определение.

О п р е д е л е н и е 3. Вероятностной операторнозначной мерой (ВОЗМ) на Ω называется семейство $M = \{M(A), A \in \mathcal{F}\}$ ограниченных эрмитовых операторов в $\mathcal{H}$, удовлетворяющее следующим условиям:

- 1) $M(A) \geq 0, A \in \mathcal{F}$;
- 2) $M(\Omega) = I$, где I — единичный оператор в $\mathcal{H}$;
- 3) для любого счетного разбиения $A = \bigcup A_i$ ($A_i \cap A_j = \emptyset, i \neq j$) выполняется соотношение $M(A) = \sum_i M(A_i)$ в смысле слабой сходимости операторов.

ВОЗМ задает квантовую наблюдаемую со значениями в Ω . Распределение вероятностей наблюдаемой M в состоянии S дается формулой

$$P_S(A) = \text{Tr } SM(A), \quad A \in \mathcal{F}. \quad (2)$$

Для краткости будем иногда писать $P_S(d\omega) = \text{Tr } SM(d\omega)$.

Если ВОЗМ $M(d\omega)$ определяется плотностью $P(\omega)$ относительно скалярной σ -конечной меры μ , где $P(\omega)$ — равномерно ограниченная (по операторной норме) слабо измеримая операторнозначная функция, то распределение вероятностей имеет плотность $p_S(\omega) = \text{Tr } SP(\omega)$ относительно меры μ . Этот случай рассмотрен в [10].

В общем случае справедлива следующая лемма (обобщение теоремы Радона–Никодима для ВОЗМ [6]).

Лемма 1. Для произвольной ВОЗМ на полном сепарабельном метрическом пространстве Ω найдутся плотное подпространство $\mathcal{D} \in \mathcal{H}$, σ -конечная мера μ на Ω , счетное семейство борелевских функций $\omega \rightarrow a_k(\omega)$ такие, что $a_k(\omega)$ для почти всех ω являются линейными функционалами на $\mathcal{D}$, удовлетворяющими условиям

$$\int_{\Omega} \sum_k |\langle a_k(\omega) | \psi \rangle|^2 \mu(d\omega) = \|\psi\|^2, \quad \psi \in \mathcal{D}, \quad (3)$$

$$\langle \psi | M(A) \psi \rangle = \int_A \sum_k |\langle a_k(\omega) | \psi \rangle|^2 \mu(d\omega), \quad \psi \in \mathcal{D}. \quad (4)$$

В [6] показано, что в качестве $\mathcal{D}$ можно взять $\text{lin}\{\varphi_i\}$ — линейную оболочку фиксированного ортонормированного базиса $\{\varphi_i\}$.

Лемма 2. Для произвольной наблюдаемой $M(d\omega)$ с множеством значений в Ω и оператора плотности $S \in \mathfrak{S}(\mathcal{H})$ распределение вероятностей $P_S(d\omega) = \text{Tr } SM(d\omega)$ имеет плотность $p_S(\omega)$ относительно меры μ .

Д о к а з а т е л ь с т в о. Рассмотрим спектральное разложение состояния S :

$$S = \sum_{i=1}^{\infty} \lambda_i |\varphi_i\rangle \langle \varphi_i|. \quad (5)$$

Применим лемму 1, считая, что $\mathcal{D} = \text{lin}\{\varphi_i\}$. Для всех $A \in \mathcal{F}$ справедливо равенство

$$P_S(A) \equiv \text{Tr } SM(A) = \int_A p_S(\omega) \mu(d\omega), \quad (6)$$

где

$$p_S(\omega) = \sum_{i=1}^{\infty} \lambda_i \sum_k |\langle a_k(\omega) | \varphi_i \rangle|^2$$

— неотрицательная интегрируемая функция в силу условия (3) и спектрального разложения (5). Лемма доказана.

Зафиксируем ортонормированную систему $\{e_k\}$ в $\mathcal{H}$. В силу тех же условий (3) и (5), соотношение

$$\hat{S}(\omega) = (p_S(\omega))^{-1} \sum_{i=1}^{\infty} \lambda_i \sum_{j,k} |e_k\rangle \langle a_k(\omega) | \varphi_i \rangle \overline{\langle a_j(\omega) | \varphi_i \rangle} \langle e_j | \quad (7)$$

для P_S -почти всех ω задает оператор плотности в $\mathcal{H}$, который мы будем называть *апостериорным состоянием*. Смысл этого названия в том, что при определенных условиях $\hat{S}(\omega)$ описывает состояние квантовой системы после измерения наблюдаемой M , которое завершилось исходом ω [8].

Следуя [7], определим *редукцию энтропии* соотношением

$$\text{ER}(S, M) = H_q(S) - \int_{\Omega} p(\omega) H_q(\hat{S}(\omega)) \mu(d\omega), \quad (8)$$

которое корректно, если $H_q(S) < \infty$. Отметим следующее свойство аппроксимации. Рассмотрим последовательность состояний $S_n = \sum_{i=1}^n \tilde{\lambda}_i |\varphi_i\rangle \langle \varphi_i|$, где $\tilde{\lambda}_i = (\sum_{k=1}^n \lambda_k)^{-1} \lambda_i$. По лемме 4 работы [7] построенная выше последовательность S_n удовлетворяет условию

$$\lim_{n \rightarrow \infty} H_q(S_n) = H_q(S) < \infty. \quad (9)$$

Согласно теореме 2 из [7], это влечет равенство

$$\lim_{n \rightarrow \infty} \text{ER}(S_n, M) = \text{ER}(S, M) < \infty. \quad (10)$$

3. Классическая пропускная способность измерительного канала.

О п р е д е л е н и е 4. Пусть M некоторая ВОЗМ, P_S — ее распределение вероятностей в состоянии S , которое дается формулой (2). *Измерительным каналом* $\mathcal{M}$ называется аффинное отображение $S \rightarrow P_S(d\omega)$ выпуклого множества квантовых состояний $\mathfrak{S}(\mathcal{H})$ в множество распределений вероятностей на Ω .

Чтобы использовать методы блочного кодирования, необходимо определить n -ю степень $\mathcal{M}^{\otimes n}$ канала $\mathcal{M}$. Пусть $\mathcal{H}^{\otimes n}$ есть n -я тензорная степень гильбертова пространства $\mathcal{H}$ и $(\Omega^{\times n}, \mathcal{F}^{\times n})$ — произведение n экземпляров измеримого пространства $(\Omega, \mathcal{F})$. Канал $\mathcal{M}^{\otimes n}$ определяется наблюдаемой $M^{\otimes n}$ со значениями в $\Omega^{\times n}$ такой, что

$$M^{\otimes n}(A_1 \times \cdots \times A_n) = M(A_1) \otimes \cdots \otimes M(A_n).$$

Используя аналог теоремы о продолжении для ВОЗМ, можно показать, что это соотношение однозначно определяет значения $M^{\otimes n}(A^{(n)})$, $A^{(n)} \in \mathcal{F}^{\times n}$.

В случае бесконечномерного $\mathcal{H}$ обычно вводится ограничение на входные состояния канала (иначе пропускные способности, как правило, бесконечны). Пусть F — самосопряженный положительный (вообще говоря, неограниченный) оператор в пространстве $\mathcal{H}$, имеющий спектральное разложение $F = \int_0^\infty x dE(x)$, где $E(x)$ — спектральная функция. Введем подмножество состояний

$$\mathcal{A}_E = \{S \in \mathfrak{S}(\mathcal{H}) : \text{Tr } SF \leq E\}, \quad (11)$$

где E — некоторая положительная постоянная, причем след в (11) понимается как интеграл $\int_0^\infty x d(\text{Tr } SE(x))$ (более подробно см. [3]). Отметим, что если оператор F удовлетворяет условию

$$\text{Tr } \exp(-\beta F) < \infty \quad \text{для всех } \beta > 0, \quad (12)$$

то $H_q(S) < \infty$ для всех S таких, что $\text{Tr } SF \leq E$ (см. [3]). Для канала $\mathcal{M}^{\otimes n}$ соответствующее ограничение задается оператором

$$F^{(n)} = F \otimes I \otimes \cdots \otimes I + \cdots + I \otimes I \otimes \cdots \otimes F.$$

Обозначим

$$\mathcal{A}_E^{(n)} = \{S^{(n)} \in \mathfrak{S}(\mathcal{H}^{\otimes n}) : \text{Tr } S^{(n)} F^{(n)} \leq nE\}. \quad (13)$$

О п р е д е л е н и е 5. *Кодом* длины n и размера N называется пара $(\Sigma^{(n)}, \mathcal{V}^{(n)})$, где:

- 1) $\Sigma^{(n)} = \{S_i^{(n)}, i = 1, \dots, N\}$ — семейство состояний из $\mathcal{A}_E^{(n)}$;
- 2) $\mathcal{V}^{(n)} = \{V_j, j = 0, 1, \dots, N\}$ — разбиение пространства $\Omega^{\times n}$.

О п р е д е л е н и е 6. Средней вероятностью ошибки кода $(\Sigma^{(n)}, \mathcal{V}^{(n)})$ называется величина

$$\bar{u}(\Sigma^{(n)}, \mathcal{V}^{(n)}) = \frac{1}{N} \sum_{j=1}^N \left(1 - \text{Tr } S_j^{(n)} M^{\otimes n}(V_j)\right). \quad (14)$$

Точную нижнюю грань величины $\bar{u}(\Sigma^{(n)}, \mathcal{V}^{(n)})$ по всем кодам длины n и размера N будем обозначать $u(n, N)$.

О п р е д е л е н и е 7. Классической пропускной способностью $C(\mathcal{M}, \mathcal{A}_E)$ измерительного канала $\mathcal{M}$ с ограничением (13) называется супремум достижимых скоростей, т.е. значений $R > 0$, для которых выполняется условие

$$\lim_{n \rightarrow \infty} u(n, 2^{nR}) = 0. \quad (15)$$

Ансамблем состояний называется конечное распределение $\pi = \{\pi_x; S_x\}$ на множестве состояний $\mathfrak{S}(\mathcal{H})$, сопоставляющее вероятности π_x состояниям S_x . Среднее состояние ансамбля определяется следующим образом: $\bar{S}_\pi = \sum_x \pi_x S_x$. Обозначим $\mathcal{P}_E$ совокупность ансамблей π таких, что $\bar{S}_\pi \in \mathcal{A}_E$; аналогично, обозначим $\mathcal{P}_E^{(n)}$ совокупность ансамблей $\pi^{(n)}$ в $\mathfrak{S}(\mathcal{H}^{\otimes n})$, среднее состояние которых удовлетворяет условию (13).

Для данного измерительного канала $\mathcal{M}$ и ансамбля π определим величину

$$I(\pi, \mathcal{M}) = \sum_x \pi_x \int_{\Omega} p(\omega|x) \log \frac{p(\omega|x)}{\bar{p}(\omega)} \mu(d\omega). \quad (16)$$

Здесь $\bar{p}(\omega)$ и $p(\omega|x)$ — плотности распределения вероятностей $\bar{P}(d\omega) = \text{Tr } \bar{S}_\pi M(d\omega)$ и $P_x(d\omega) = \text{Tr } S_x M(d\omega)$ соответственно. Величина $I(\pi, \mathcal{M})$ является взаимной информацией Шеннона между дискретной случайной величиной X , имеющей распределение вероятностей $\{\pi_x\}$, и случайной величиной ω с условной плотностью $p(\omega|x)$, определенной с помощью леммы 2. Заметим, что имеет место представление величины $I(\pi, \mathcal{M})$ в виде супремума по разбиениям $\mathcal{V} = \{V_i\}$ выходного пространства Ω (ср. [5, соотношение (1.2.3)]):

$$I(\pi, \mathcal{M}) = \sup_{\mathcal{V}} \left(\sum_i \sum_x \pi_x P_x(V_i) \log \frac{P_x(V_i)}{\bar{P}(V_i)} \right). \quad (17)$$

Величина под знаком супремума равна $I(\pi, \mathcal{M}_{\mathcal{V}})$, где $\mathcal{M}_{\mathcal{V}}$ — измерительный канал, отвечающий дискретной наблюдаемой $\{M(V_i)\}$.

Теорема 1. Классическая пропускная способность измерительного канала $\mathcal{M}$ с ограничением (13) дается соотношением

$$C(\mathcal{M}, \mathcal{A}_E) = \sup_{\pi \in \mathcal{P}_E} I(\pi, \mathcal{M}). \quad (18)$$

Д о к а з а т е л ь с т в о. Обозначим

$$C_n = \sup_{\pi^{(n)} \in \mathcal{P}_E^{(n)}} I(\pi^{(n)}, \mathcal{M}^{\otimes n}).$$

Нам надо доказать, что

$$C(\mathcal{M}, \mathcal{A}_E) = C_1.$$

Установим сначала свойство аддитивности $C_n = nC_1$.

Для фиксированного разбиения $\mathcal{V} = \{V_i\}$ измерительный канал $\mathcal{M}_{\mathcal{V}}$ вкладывается в квантовый канал, разрушающий сцепленность (см., например, [4]), поэтому согласно [3] его пропускная способность дается выражением

$$C(\mathcal{M}_{\mathcal{V}}, \mathcal{A}_E) = \sup_{\pi \in \mathcal{P}_E} I(\pi, \mathcal{M}_{\mathcal{V}}), \quad (19)$$

причем имеет место аддитивность (см. [6])

$$C(\mathcal{M}_{\mathcal{V}}^{\otimes n}, \mathcal{A}_E^{(n)}) = nC(\mathcal{M}_{\mathcal{V}}, \mathcal{A}_E).$$

Отметим, что, аналогично (19), левая часть равна $\sup_{\pi^{(n)} \in \mathcal{P}_E^{(n)}} I(\pi^{(n)}, \mathcal{M}_{\mathcal{V}}^{\otimes n})$, так что

$$\sup_{\pi^{(n)} \in \mathcal{P}_E^{(n)}} I(\pi^{(n)}, \mathcal{M}_{\mathcal{V}}^{\otimes n}) = n \sup_{\pi \in \mathcal{P}_E} I(\pi, \mathcal{M}_{\mathcal{V}}). \quad (20)$$

Используя результат Р. Л. Добрушина (теорема 2.2 в [5]), имеем

$$I(\pi^{(n)}, \mathcal{M}^{\otimes n}) = \sup_{\mathcal{V}} I(\pi^{(n)}, \mathcal{M}_{\mathcal{V}}^{\otimes n}),$$

поскольку супремум в правой части равен супремуму информации по разбиениям пространства $\Omega^{\times n}$ специального вида, состоящим из произведений $V_1 \times \dots \times V_n$ множеств разбиения $\mathcal{V}$. Класс всех таких произведений обладает свойством направленности, которое требуется для выполнения теоремы 2.2 в [5]. Следовательно,

$$\begin{aligned} C_n &= \sup_{\pi^{(n)} \in \mathcal{P}_E^{(n)}} \sup_{\mathcal{V}} I(\pi^{(n)}, \mathcal{M}_{\mathcal{V}}^{\otimes n}) = \sup_{\mathcal{V}} \sup_{\pi^{(n)} \in \mathcal{P}_E^{(n)}} I(\pi^{(n)}, \mathcal{M}_{\mathcal{V}}^{\otimes n}) \\ &= n \sup_{\mathcal{V}} \sup_{\pi \in \mathcal{P}_E} I(\pi, \mathcal{M}_{\mathcal{V}}) = n \sup_{\pi \in \mathcal{P}_E} \sup_{\mathcal{V}} I(\pi, \mathcal{M}_{\mathcal{V}}) \\ &= n \sup_{\pi \in \mathcal{P}_E} I(\pi, \mathcal{M}) = nC_1, \end{aligned}$$

где в третьем равенстве было использовано (20).

Теперь докажем неравенство $C(\mathcal{M}, \mathcal{A}_E) \leq C_1$. Не ограничивая общности, можем считать, что $C_1 < \infty$. Пусть $R > C_1$. Применяя неравенство Фано, получаем аналогично соотношению (10.19) в [8]

$$u(n, 2^{nR}) \geq 1 - \frac{C_n}{nR} - \frac{1}{nR} = 1 - \frac{C_1}{R} - \frac{1}{nR},$$

где во втором соотношении использована аддитивность $C_n = nC_1$. Отсюда $\liminf_{n \rightarrow \infty} u(n, 2^{nR}) > 0$, следовательно, $C(\mathcal{M}, \mathcal{A}_E) \leq C_1$.

Для доказательства обратного неравенства заметим, что

$$C(\mathcal{M}, \mathcal{A}_E) \geq C(\mathcal{M}_{\mathcal{V}}, \mathcal{A}_E) = \sup_{\pi \in \mathcal{P}_E} I(\pi, \mathcal{M}_{\mathcal{V}})$$

для любого разбиения $\mathcal{V}$. Беря супремум по разбиениям $\mathcal{V}$, получаем $C(\mathcal{M}, \mathcal{A}_E) \geq \sup_{\pi \in \mathcal{P}_E} I(\pi, \mathcal{M}) = C_1$. Теорема 1 доказана.

4. Пропускная способность измерительного канала с использованием сцепленности. Рассмотрим следующий протокол передачи классической информации через измерительный канал $\mathcal{M}$. Передатчик A и приемник B находятся в чистом сцепленном состоянии $S_{AB} = |\psi\rangle\langle\psi|$, где $|\psi\rangle = \sum_j c_j |e_j\rangle \otimes |\tilde{e}_j\rangle$, причем выполняется условие $H_q(S_A) = H_q(S_B) < \infty$.

Пусть $\mathcal{X}$ — конечный алфавит и классический сигнал $x \in \mathcal{X}$ появляется с вероятностью π_x . Участник A осуществляет кодирование $x \rightarrow \mathcal{E}_x$ и пересылает через канал $\mathcal{M}$ свою часть общего состояния. Таким образом, в распоряжении участника B оказывается гибридная система ΩB , где Ω — классическая система на выходе измерительного канала. После измерения наблюдаемой $M(dw)$ состояние в гибридной системе описывается следующим образом:

$$\sigma_x(dw) = \sum_{j,k} c_j \bar{c}_k [\text{Tr } \mathcal{E}_x(|e_j\rangle\langle e_k|) M(dw)] |\tilde{e}_j\rangle\langle\tilde{e}_k|.$$

Предполагается, что участник B может производить измерения наблюдаемых в системе ΩB , извлекая, таким образом, информацию о сигнале x .

Возможно применение блочного кодирования, тогда кодированные состояния, передаваемые через канал $\mathcal{M}^{\otimes n} \otimes \text{Id}_B^{\otimes n}$, имеют вид

$$S_\alpha^{(n)} = (\mathcal{E}_\alpha^{(n)} \otimes \text{Id}_B^{\otimes n})[S_{AB}^{(n)}], \quad (21)$$

где $S_{AB}^{(n)}$ — чистое сцепленное состояние для n экземпляров системы AB , удовлетворяющее условию $H(S_B^{(n)}) < \infty$, α — классическое сообщение (например, слово в алфавите $\mathcal{X}$), $\alpha \rightarrow \mathcal{E}_\alpha^{(n)}$ — кодирования для n экземпляров системы A . На входные состояния канала $\mathcal{M}^{\otimes n}$ налагается ограничение (13), которое эквивалентно аналогичному ограничению для канала $\mathcal{M}^{\otimes n} \otimes \text{Id}_B^{\otimes n}$ с операторами $F^{(n)} \otimes I_B^{\otimes n}$.

Для канала $\mathcal{M}$ с ограничением (11) на входные состояния рассмотрим величину

$$C_{\text{ea}}^{(n)}(\mathcal{M}^{\otimes n}, \mathcal{A}_E^{(n)}) = \sup_{(\pi_\alpha^{(n)}, S_\alpha^{(n)})} \chi_{\text{cq}}\left(\{\pi_\alpha^{(n)}\}; \{(\mathcal{M}^{\otimes n} \otimes \text{Id}_B^{\otimes n})S_\alpha^{(n)}\}\right), \quad (22)$$

где

$$\chi_{\text{cq}}(\{\pi_x\}; \{S_x\}) = H_{\text{cq}}\left(\sum_x \pi_x S_x\right) - \sum_x \pi_x H_{\text{cq}}(S_x), \quad S_x \in \mathcal{L}_*,$$

а супремум берется по всевозможным ансамблям состояний вида (21), удовлетворяющим ограничению

$$\sum_\alpha \pi_\alpha^{(n)} \text{Tr} S_\alpha^{(n)} (F^{(n)} \otimes I_B^{\otimes n}) \leq nE.$$

Классическая пропускная способность с использованием сцепленного состояния для квантово-классического канала $\mathcal{M}$ при ограничении (11) определяется соотношением

$$C_{\text{ea}}(\mathcal{M}, \mathcal{A}_E) = \lim_{n \rightarrow \infty} \frac{1}{n} C_{\text{ea}}^{(n)}(\mathcal{M}^{\otimes n}, \mathcal{A}_E^{(n)}).$$

Теорема 2. Пусть $\mathcal{M}$ — произвольный измерительный канал с ограничением (13) на входные состояния. Предположим, что оператор F удовлетворяет условию (12), а канал $\mathcal{M}$ удовлетворяет условию

$$\sup_{S_A: \text{Tr } S_A F \leq E} H_c(p_{S_A}) < \infty, \quad (23)$$

где $H_c(p_{S_A})$ — классическая дифференциальная энтропия плотности выходного распределения вероятностей канала $\mathcal{M}$. Тогда пропускная способность с использованием сцепленного состояния дается выражением

$$C_{\text{ea}}(\mathcal{M}, \mathcal{A}_E) = \sup_{S_A: \text{Tr } S_A F \leq E} \text{ER}(S_A, M). \quad (24)$$

Доказательство. В доказательстве мы используем соответствующий результат для измерительных каналов, определяемых ограниченной операторной плотностью, полученный в [10].

Пусть S_{AB} — исходное сцепленное состояние системы AB . После применения кодирования $\mathcal{E}_A^x$ в системе A состояние составной системы описывается оператором

$$S_{AB}^x = (\mathcal{E}_A^x \otimes \text{Id}_B) S_{AB}$$

с частичными состояниями $S_A^x = \mathcal{E}_A^x(S_A)$ и $S_B^x = S_B$.

Чтобы установить неравенство $\leq$ в формуле (24), достаточно доказать (см. подробнее [10]), что

$$H_{\text{cq}}\left(\sum_x \pi_x (\mathcal{M} \otimes \text{Id}_B) S_{AB}^x\right) - \sum_x \pi_x H_{\text{cq}}(\mathcal{M} \otimes \text{Id}_B(S_{AB}^x)) \leq \text{ER}(\bar{S}_A, M). \quad (25)$$

Здесь $\bar{S}_A = \sum_x \pi_x S_A^x$, причем вследствие ограничения (13) выполняется условие

$$\text{Tr } \bar{S}_A F \leq E. \quad (26)$$

Из результата работы [10] вытекает, что (25) выполняется для состояний $\bar{S}_A$ конечного ранга, удовлетворяющих ограничению (26). Для доказательства в общем случае применим аппроксимацию состояниями конечного ранга.

Предположим сначала, что $\text{Tr } \bar{S}_A F \leq E' < E$ для некоторого положительного E' . Пусть $\bar{S}_A$ имеет спектральное разложение $\bar{S}_A = \sum_i \lambda_i |\varphi_i\rangle\langle\varphi_i|$. Рассмотрим возрастающую последовательность проекторов $P_n = \sum_{i=1}^n |\varphi_i\rangle\langle\varphi_i|$, сходящуюся к единичному оператору I_A , и последовательность состояний

$$S_{AB}^x(n) = P_n \otimes I_B S_{AB}^x P_n \otimes I_B + |\phi\rangle\langle\phi| \otimes (S_B - S_B^x(n)),$$

где $S_B^x(n) = \text{Tr}_A(P_n \otimes I_B S_{AB}^x P_n \otimes I_B)$, $|\phi\rangle$ — фиксированный единичный вектор из $\text{lin}\{\varphi_i\}$, принадлежащий области определения $\sqrt{F}$. Частичными состояниями $S_{AB}^x(n)$ являются

$$\text{Tr}_B S_{AB}^x(n) = S_A^x(n) = P_n S_A^x P_n + (1 - \text{Tr } P_n S_A^x) |\phi\rangle\langle\phi|, \quad \text{Tr}_A S_{AB}^x(n) = S_B.$$

Тогда среднее состояние в системе A равно

$$\bar{S}_A(n) = \sum_x \pi_x S_A^x(n) = P_n \bar{S}_A P_n + (1 - \text{Tr } P_n \bar{S}_A) |\phi\rangle\langle\phi|.$$

Имеем $\bar{S}_A(n) = \sum_{i=1}^n \lambda_i |\varphi_i\rangle\langle\varphi_i| + (1 - \text{Tr } P_n \bar{S}_A) |\phi\rangle\langle\phi|$, тогда $\|\bar{S}_A(n) - \bar{S}_A\|_1 \rightarrow 0$ при $n \rightarrow \infty$ и

$$\text{Tr } \bar{S}_A(n) F = \sum_{i=1}^n \lambda_i \|\sqrt{F} \varphi_i\|^2 + (1 - \text{Tr } P_n \bar{S}_A) \langle\phi| F |\phi\rangle \leq E' + \varepsilon_n,$$

где $\varepsilon_n \rightarrow 0$ при $n \rightarrow \infty$. Таким образом, начиная с некоторого n для оператора плотности $\bar{S}_A(n)$ выполняется входное ограничение (26).

Используя условие (23) и действуя аналогично доказательству теоремы кодирования для измерения наблюдаемой в [10], получаем неравенство (25) для ансамбля $\{\pi_x, S_{AB}^x(n)\}$, которое можно записать с использованием относительной энтропии следующим образом:

$$\sum_x \pi_x H_{\text{ср}} \left((\mathcal{M} \otimes \text{Id}_B)(S_{AB}^x(n)) \left\| \sum_x \pi_x (\mathcal{M} \otimes \text{Id}_B) S_{AB}^x(n) \right. \right) \leq \text{ER}(\text{Tr } \bar{S}_A(n), M). \quad (27)$$

Перейдем в (27) к пределу при $n \rightarrow \infty$. Заметив, что $\lim_{n \rightarrow \infty} H_q(\bar{S}_A(n)) = H_q(\bar{S}_A)$, и воспользовавшись в левой части теоремой 2 из [7] (т.е. равенством (10)), а в правой части полунепрерывностью снизу относительной энтропии, получаем (25) для ансамбля $\{\pi_x, S_{AB}^x\}$.

Теперь рассмотрим случай $\text{Tr } \bar{S}_A F = E$. Возьмем единичный вектор $|e\rangle \in \text{lin}\{\phi_i\}$, удовлетворяющий условию $\langle e| F |e\rangle < E$, и построим аппроксимацию $S_{AB}^x(\varepsilon) = (1 - \varepsilon) S_{AB}^x + \varepsilon |e\rangle\langle e| \otimes S_B$, $0 < \varepsilon < 1$. Тогда среднее состояние системы A равно $\bar{S}_A(\varepsilon) = (1 - \varepsilon) \bar{S}_A + \varepsilon |e\rangle\langle e|$ и выполняется условие

$$\text{Tr } \bar{S}_A(\varepsilon) F < E.$$

Повторим предыдущие рассуждения, приближая $S_{AB}^x(\varepsilon)$ состояниями вида

$$(1 - \varepsilon) P_n \otimes I_B S_{AB}^x P_n \otimes I_B + |e\rangle\langle e| (S_B - (1 - \varepsilon) \text{Tr}_A P_n \otimes I_B S_{AB}^x)$$

с частичными состояниями $(1 - \varepsilon) S_A^x + (1 - (1 - \varepsilon) \text{Tr } P_n S_A^x) |e\rangle\langle e|$ и S_B в системах A и B соответственно. Получаем, что неравенство (25) выполняется для $S_{AB}^x(\varepsilon)$, $\bar{S}_A(\varepsilon)$. Так как $\lim_{\varepsilon \rightarrow 0} H_q(\bar{S}_A(\varepsilon)) = H_q(\bar{S}_A)$, то, устремляя ε к нулю, получаем (25) для ансамблей, удовлетворяющих условию $\text{Tr } \bar{S}_A F = E$. Дальнейшее доказательство повторяет рассуждения для случая измерения наблюдаемой, имеющей плотность [10].

Для доказательства неравенства $\geq$ в формуле (24) рассмотрим произвольное состояние $S \in \mathfrak{S}(\mathcal{H})$, $S = \sum_{i=1}^{\infty} \lambda_i |\varphi_i\rangle\langle\varphi_i|$, удовлетворяющее входному ограничению.

Применим лемму 1, полагая $\mathcal{D} = \text{lin}\{\varphi_i\}$ и задавая апостериорные состояния $\hat{S}(\omega)$ соотношением (7). Далее рассуждения аналогичны доказательству предложения 4 из [3], а также теоремы 3 из [10]. Теорема 2 доказана.

Специальный интерес представляет случай *чистых* ВОЗМ, для которых существует представление (4) вида

$$\langle \psi | M(A) \psi \rangle = \int_A |\langle a(\omega) | \psi \rangle|^2 \mu(d\omega), \quad \psi \in \mathcal{D}. \quad (28)$$

В этом случае апостериорное состояние (7) оказывается чистым состоянием, не зависящим от x :

$$\hat{S}(\omega) = |e\rangle\langle e|, \quad (29)$$

где $e \in \mathcal{H}$ — единичный вектор. Таким образом, $H_q(\hat{S}(\omega)) = 0$ и редукция энтропии равна

$$\text{ER}(S, M) = H_q(S). \quad (30)$$

Формула (24) принимает вид

$$C_{\text{ea}}(\mathcal{M}, \mathcal{A}_E) = \sup_{S_A: \text{Tr } S_A F \leq E} H_q(S). \quad (31)$$

Хорошо известно, что этот супремум достигается на состоянии Гиббса

$$S_\beta = c(\beta)^{-1} \exp(-\beta F), \quad c(\beta) = \text{Tr} \exp(-\beta F), \quad (32)$$

где β находится из условия $\text{Tr } S_\beta F = E$, и равен $\beta E + c(\beta)$. Таким образом, из теоремы 2 вытекает следующее утверждение.

Следствие 1. Для любого измерительного канала, соответствующего чистой ВОЗМ,

$$C_{\text{ea}}(\mathcal{M}, \mathcal{A}_E) = \beta E + c(\beta),$$

где β находится из условия $\text{Tr } S_\beta F = E$.

Проиллюстрируем этот результат двумя примерами. Пусть $\mathcal{H} = L^2(\mathbf{R})$, Q — оператор умножения на x , $P = -id/dx$ с общей существенной областью определения $\mathcal{D} = \mathcal{S}(\mathbf{R})$ (пространство бесконечно дифференцируемых функций, быстро убывающих со всеми производными, см., например, [8]). Спектральная мера M самосопряженного оператора Q представляется в виде (28):

$$\langle \psi | M(A) \psi \rangle = \int_A |\langle x | \psi \rangle|^2 dx, \quad \psi \in \mathcal{S}(\mathbf{R}),$$

где $\langle x | \psi \rangle = \psi(x)$, $\psi \in \mathcal{S}(\mathbf{R})$, суть δ -функционалы Дирака. Таким образом, ВОЗМ M не имеет ограниченной плотности, результат работы [10] неприменим и следует использовать подход настоящей работы. Всякий оператор плотности S в $L^2(\mathbf{R})$ задается ядром, которое удобно записывать символически в виде $\langle x | S | y \rangle$ (для непрерывных ядер такую запись можно понимать буквально). Рассмотрим канал, соответствующий измерению наблюдаемой Q , который отображает оператор плотности S в плотность распределения $\langle x | S | x \rangle$ относительно меры Лебега на прямой. В квантовой оптике такой канал описывает статистику *гомодинного измерения* одной моды Q , P электромагнитного излучения [12]. В качестве оператора ограничения обычно фигурирует энергия осциллятора $F = (P^2 + Q^2)/2$. Отметим, что условие (23) выполнено, так как неравенство $\text{Tr } SF \leq E$ влечет

$$\int x^2 p_S(x) dx = \text{Tr } S Q^2 \leq 2 \text{Tr } S F \leq 2E,$$

а при таком ограничении максимальную дифференциальную энтропию (равную $(1/2) \log(2\pi e(2E))$) имеет гауссовская плотность. Подставляя значение супремума в

(31), равное энтропии гиббсовского состояния осциллятора со средней энергией E (см., например, [12], [8]), получаем

$$C_{\text{ea}}(\mathcal{M}, \mathcal{A}_E) = \left(E + \frac{1}{2}\right) \log \left(E + \frac{1}{2}\right) - \left(E - \frac{1}{2}\right) \log \left(E - \frac{1}{2}\right). \quad (33)$$

С другой стороны, классическая пропускная способность гомодинного канала, вычисленная в [12], [13], равна

$$C(\mathcal{M}_{\text{hom}}, \mathcal{A}_E) = \log(2E). \quad (34)$$

Рис. 1. Пропускные способности оптических измерительных каналов.

Согласно следствию 1, соотношение (33) имеет место для любого чистого измерительного канала, в том числе и для *гетеродинного канала*, который отображает оператор плотности S в плотность распределения $\langle x, y | S | x, y \rangle$ относительно меры Лебега на плоскости, где $|x, y\rangle$ — когерентные состояния квантового осциллятора [4]. Отметим, что в этом случае существует ограниченная плотность и применимы результаты работы [10]. Классическая пропускная способность гетеродинного канала, вычисленная в [13], [4], равна

$$C(\mathcal{M}_{\text{het}}, \mathcal{A}_E) = \log \left(E + \frac{1}{2}\right). \quad (35)$$

Для всех $E > 1/2$ имеют место неравенства

$$C(\mathcal{M}_{\text{het}}, \mathcal{A}_E) < C(\mathcal{M}_{\text{hom}}, \mathcal{A}_E) < C_{\text{ea}}(\mathcal{M}, \mathcal{A}_E).$$

Графики этих трех пропускных способностей приведены на рис. 1.

СПИСОК ЛИТЕРАТУРЫ

1. 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.
2. Berta M., Renes J. M., Wilde M. M. Identifying the information gain of a quantum measurement. arXiv:1301.1594.
3. Холево А. С. Классические пропускные способности квантового канала с ограничением на входе. — Теория вероятн. и ее примен., 2003, т. 48, в. 2, с. 359–374.
4. Холево А. С. Информационная емкость квантовой наблюдаемой. — Пробл. передачи информ., 2012, т. 48, № 1, с. 3–13.
5. Добрушин Р. Л. Общая формулировка теоремы Шеннона в теории информации. — Успехи матем. наук, 1959, т. 14, № 6, с. 3–104.

6. Холево А. С. Каналы, разрушающие сцепленность, в бесконечных размерностях. — Пробл. передачи информ., 2008, т. 44, № 3, с. 3–18.
7. Shirokov M. E. Entropy reduction of quantum measurement. — J. Math. Phys., 2011, v. 52, № 5, paper № 052202, 18 p.
8. Холево А. С. Квантовые системы, каналы, информация. М.: МЦНМО, 2010, 327 с.
9. Barchielli A., Lupieri G. Instruments and mutual entropies in quantum information. — Banach Center Publ., 2006, v. 73, p. 65–80.
10. Кузнецова А. А., Холево А. С. Теоремы кодирования для гибридных каналов. — Теория вероятн. и ее примен., 2013, т. 58, в. 2, с. 298–324.
11. Lindblad G. Expectations and entropy inequalities for finite quantum systems. — Comm. Math. Phys., 1974, v. 39, p. 111–119.
12. Caves C. M., Drummond P. B. Quantum limits of bosonic communication rates. — Rev. Modern Phys., 1994, v. 66, p. 481–538.
13. Hall M. J. W. Quantum information and correlation bounds. — Phys. Rev. A, 1997, v. 55, № 1, p. 100–113.

Поступила в редакцию
16.VII.2013

© 2014 г.

ЛОТОВ В. И.*

ОБ АСИМПТОТИКЕ ВЕРОЯТНОСТИ РАЗОРЕНИЯ¹⁾

Найдено асимптотическое представление вероятности разорения для случайного блуждания с отрицательным сносом при условии неограниченного роста верхней границы полосы. Результат выражается через распределения супремума траектории и величины перескока через отрицательный уровень. В последующих следствиях используются известные асимптотические формулы для распределения супремума, полученные при различных ограничениях на скорость убывания на бесконечности распределения скачков случайного блуждания.

Ключевые слова и фразы: случайное блуждание, вероятность разорения, асимптотический анализ.

Пусть $X_1, X_2, \dots$ — независимые случайные величины, имеющие одно и то же невырожденное распределение, и

$$S_0 = 0, \quad S_n = X_1 + \dots + X_n.$$

Везде в дальнейшем предполагается, что распределение X_1 не является арифметическим (т.е. не сосредоточено на решетке вида $\{kh, k = 0, \pm 1, \dots\}$), $\mathbf{P}(X_1 > 0) > 0$ и существует $\mathbf{E} X_1 < 0$. Для произвольных $a \geq 0$ и $b > 0$ введем случайную величину

$$N = N_{a,b} = \inf\{n \geq 1: S_n \notin (-a, b)\},$$

равную моменту первого выхода случайного блуждания из интервала $(-a, b)$, и пусть

$$\alpha(a, b) = \mathbf{P}(S_N \leq -a), \quad \beta(a, b) = \mathbf{P}(S_N \geq b).$$

Обе эти величины принято называть вероятностями разорения в связи с известными приложениями, здесь, очевидно, $\alpha(a, b) + \beta(a, b) = 1$. В работе изучается асимптотическое поведение вероятности $\beta(a, b)$ при условии, что $b \rightarrow \infty$. Число a в ряде случаев

* Институт математики им. С.Л. Соболева СО РАН, Новосибирский государственный университет, Новосибирск, Россия; e-mail: lotov@math.nsc.ru

¹⁾ Работа выполнена при поддержке РФФИ (грант № 13-01-00046).