А. С. Холево, М. Е. Широков, Об увеличении классической пропускной способности квантовых гауссовских каналов за счет использования сцепленности, *Матем. заметки*, 2015, том 97, выпуск 6, 951–954

Об увеличении классической пропускной способности квантовых гауссовских каналов за счет использования сцепленности

А. С. Холево, М. Е. Широков

Квантовые каналы – линейные сохраняющие след вполне положительные отображения банаховых пространств ядерных операторов (классов Шаттена порядка 1) являются некоммутативными аналогами марковских операторов в классической теории вероятностей. Они также играют роль динамических отображений в квантовой теории [1; гл. 6].

К числу основных характеристик, определяющих информационные свойства квантового канала, относятся его классические пропускные способности с использованием и без использования сцепленности. Классическая пропускная способность (без использования сцепленности) $C(\Phi)$ определяет предельную скорость передачи классической информации по каналу Φ при произвольном блочном кодировании на входе и соответствующем измерении на выходе, а классическая пропускная способность с использованием сцепленности $C_{\mathrm{ea}}(\Phi)$ предполагает дополнительное использование сцепленного состояния между входом и выходом канала Φ (подробное описание протоколов передачи см. в [1; гл. 8]). Поскольку использование сцеленности является дополнительным ресурсом, то $C_{\mathrm{ea}}(\Phi) \geqslant C(\Phi)$ для любого канала Φ.

Пусть $\mathcal{H}$ – сепарабельное гильбертово пространство, $\mathfrak{T}(\mathcal{H})$ – банахово пространство всех ядерных операторов в $\mathcal{H}$, а $\mathfrak{S}(\mathcal{H})$ – подмножество в $\mathfrak{T}(\mathcal{H})$, состоящее из положительных операторов с единичным следом, которые мы будем называть *квантовыми состояниями* и обозначать греческими буквами $\rho, \sigma, \dots$. Набор квантовых состояний $\{\rho_i\}$ с соответствующим распределением вероятностей $\{\pi_i\}$ будем обозначать $\{\pi_i, \rho_i\}$ и называть *ансамблем состояний*, а состояние $\overline{\rho} = \sum_i \pi_i \rho_i$ – *средним состоянием* ансамбля $\{\pi_i, \rho_i\}$.

Квантовым каналом называется линейное сохраняющее след вполне положительное отображение $\Phi\colon \mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}(\mathcal{H}_B)$ [1; гл. 6]. Пусть $H(\rho)$ – энтропия фон Неймана состояния ρ, а $H(\rho\|\sigma)$ – квантовая относительная энтропия состояний ρ и σ. Для заданного канала Φ и любого ансамбля $\{\pi_i, \rho_i\}$ входных квантовых состояний выходная χ-величина определяется выражением

$$\chi_\Phi(\{\pi_i, \rho_i\}) \doteq \sum_i \pi_i H(\Phi(\rho_i)\|\Phi(\overline{\rho})) = H(\Phi(\overline{\rho})) - \sum_i \pi_i H(\Phi(\rho_i)),$$

в котором вторая формула справедлива при условии $H(\Phi(\overline{\rho})) < +\infty$.

Если канал Φ конечномерен ($\dim \mathcal{H}_A, \dim \mathcal{H}_B < +\infty$), то теорема Холево–Шумахера–Вестморленда (HSW-теорема) показывает, что

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

где C_χ – χ-пропускная способность канала, определяемая выражением

$$C_\chi(\Phi) = \sup_{\{\pi_i, \rho_i\}} \chi_\Phi(\{\pi_i, \rho_i\}),$$

в котором супремум берется по всем ансаблям квантовых состояний.

Теорема Беннета–Шора–Смолина–Таплияла (BSST-теорема, [2]) дает следующее выражение для классической пропускной способности с использованием сцепленности конечномерного канала:

$$C_{\mathrm{ea}}(\Phi) = \sup_\rho I(\Phi, \rho),$$

Исследование выполнено за счет гранта Российского научного фонда (проект № 14-21-00162).
DOI: 10.4213/mzm10663

где $I(\Phi,\rho)=H(\rho)+H(\Phi(\rho))-H(\Phi,\rho)$ – квантовая взаимная информация канала Φ в состоянии $\rho\in\mathfrak{S}(\mathcal{H}_A)$ (здесь $H(\Phi,\rho)$ – обменная энтропия канала Φ в состоянии ρ).

При определении пропускных способностей бесконечномерного квантового канала необходимо накладывать ограничения на состояния, используемые в качестве кодов, например, ограничение на среднюю энергию этих состояний. Зафиксируем положительный самосопряженный оператор F в $\mathcal{H}_A$ и зададим линейные ограничения на входные состояния $\rho^{(n)}$ канала $\Phi^{\otimes n}$ вида[1]

$$\operatorname{Tr}\rho^{(n)}F^{(n)}\leqslant nE, \tag{1}$$

где

$$F^{(n)}=F\otimes\dots\otimes I+\dots+I\otimes\dots\otimes F. \tag{2}$$

Другая особенность бесконечномерного случая состоит в необходимости использовать обобщенные ансамбли квантовых состояний. Такой ансамбль можно определить как вероятностную борелевскую меру μ на множестве квантовых состояний $\mathfrak{S}(\mathcal{H}_A)$, его средним состоянием является барицентр $\overline{\rho}(\mu)$ меры μ. Выходная χ-величина обобщенного ансамбля μ для канала Φ определяется выражением

$$\chi_\Phi(\mu)\doteq\int H(\Phi(\rho)\|\Phi(\overline{\rho}(\mu)))\,\mu(d\rho)=H(\Phi(\overline{\rho}(\mu)))-\int H(\Phi(\rho))\,\mu(d\rho),$$

в котором вторая формула справедлива при условии $H(\Phi(\overline{\rho}(\mu)))<+\infty$ [1; гл. 10].

Операциональное определение классических пропускных способностей с использованием и без использования сцепленности квантового канала с линейным ограничением приведено в [3], где также доказаны соответствующие обобщения HSW и BSST теорем при определенных условиях на вид ограничения. Максимально полное обобщение BSST-теоремы для бесконечномерного канала с линейным ограничением дано в [4].

В силу HSW-теоремы для канала с линейными ограничениями [3; предложение 3] классическая пропускная способность канала Φ с ограничением (1) дается следующим регуляризованным выражением:

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

в котором оператор $F^{(n)}$ определен соотношением (2), а

$$C_\chi(\Phi,F,E)=\sup_{\mu:\operatorname{Tr}\overline{\rho}(\mu)F\leqslant E}\chi_\Phi(\mu). \tag{3}$$

В силу BSST-теоремы для канала с линейными ограничениями [4; теорема 1] классическая пропускная способность канала Φ с ограничением (1) дается следующим выражением:

$$C_{\mathrm{ea}}(\Phi,F,E)=\sup_{\rho:\operatorname{Tr}\rho F\leqslant E}I(\rho,\Phi),$$

где $I(\rho,\Phi)$ – квантовая взаимная информация (должным образом обобщенная на бесконечномерный случай).

Для любого квантового канала Φ имеет место неравенство

$$C_{\mathrm{ea}}(\Phi,F,E)\geqslant C(\Phi,F,E), \tag{4}$$

которое прямо следует из операциональных определений данных пропускных способностей. Строгое неравенство в (4) означает, что использование сцепленного состояния между входом и выходом увеличивает предельную скорость передачи информации по каналу Φ и дает экспоненциально растущий при $n\to\infty$ выигрыш в размере оптимального кода. Естественно возникает вопрос об условиях равенства (строгого неравенства) в (4). Для

[1] Величина $\operatorname{Tr}\rho^{(n)}F^{(n)}$ (конечная или бесконечная) определяется как $\sup_t\operatorname{Tr}\rho^{(n)}P_tF^{(n)}P_t$, где P_t – спектральный проектор оператора $F^{(n)}$, соответствующий отрезку $[0,t]$.

конечномерного канала без ограничений в [5] получен критерий равенства $C_{\mathrm{ea}}(\Phi) = C_\chi(\Phi)$, которое формально сильнее равенства $C_{\mathrm{ea}}(\Phi) = C(\Phi)$ (эти равенства равносильны, если для канала Φ имеет место аддитивность χ-пропускной способности).

В данной заметке будут получены достаточные условия строгого неравенства в (4) для бозонных гауссовских каналов, которые занимают центральное место в теории квантовых информационных систем с непрерывными переменными.

Пусть $\mathcal{H}_X$ $(X = A, B, \dots)$ – пространство неприводимого представления *канонических коммутационных соотношений*

$$W_X(z)W_X(z') = \exp\biggl[-\frac{i}{2}\Delta_X(z,z')\biggr]W_X(z'+z),$$

где (Z_X, Δ_X) – симплектическое пространство, а $W_X(z)$ – операторы Вейля [1; гл. 11]. Пусть s_X – число мод системы X, т.е. $2s_X = \dim Z_X$.

Бозонный гауссовский канал $\Phi\colon \mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}(\mathcal{H}_B)$ определяется действием сопряженного отображения $\Phi^*\colon \mathfrak{B}(\mathcal{H}_B) \to \mathfrak{B}(\mathcal{H}_A)$ на операторы Вейля:

$$\Phi^*(W_B(z)) = W_A(Kz)\exp\biggl[ilz - \frac{1}{2}z^\top \alpha z\biggr], \qquad z \in Z_B,$$

где K – линейный оператор $Z_B \to Z_A$, вектор l – $(2s_B)$-мерная вещественная строка, а α – $((2s_B)\times(2s_B))$-мерная вещественная симметрическая матрица, удовлетворяющая неравенству

$$\alpha \geqslant \pm\frac{i}{2}\Bigl[\Delta_B - K^\top \Delta_A K\Bigr].$$

В течение долгого времени одним из основных открытых вопросов квантовой теории информации была гипотеза о *гауссовских минимизаторах*, утверждающая, что выходная энтропия гауссовского канала Φ, т.е. функция $\rho \mapsto H(\Phi(\rho))$ достигает минимума в чистом гауссовском состоянии.

Недавно гипотеза о гауссовских минимизаторах была доказана для широкого класса гауссовских каналов, обладающих свойством калибровочной ковариантности или контравариантности [6]. Среди многочисленных следствий отметим следующий результат.

Теорема 1. *Пусть Φ – гауссовский нетривиальный $(K \neq 0)$ калибровочно-ковариантный или калибровочно-контравариантный канал, а $F = \sum_{ij}\epsilon_{ij}a_i^\dagger a_j$ – калибровочно-инвариантный осцилляторный оператор энергии (здесь $[\epsilon_{ij}]$ – положительно-определенная матрица). Тогда*

$$C_{\mathrm{ea}}(\Phi, F, E) > C(\Phi, F, E). \tag{5}$$

Доказательство. Как показано в [6], [7], из выполнимости гипотезы о гауссовских минимизаторах для канала Φ следует, что

1) $C(\Phi, F, E) = C_\chi(\Phi, F, E)$;
2) существует оптимальный ансабль-мера μ, на которой достигается суперемум в (3), а барицентр этой меры является невырожденным гауссовским состоянием.

Комбинируя эти утверждения и замечая, что для оператора F указанного вида из конечности $\operatorname{Tr} F\rho$ следует конечность энтропии $H(\rho)$, из теоремы 2 в [4] получаем, что равенство $C_{\mathrm{ea}}(\Phi, F, E) = C(\Phi, F, E)$ возможно, только если Φ – классически-квантовый канал дискретного типа. В силу предложения 5 в [4] это означает, что $K = 0$, т.е. что Φ – вполне деполяризующий канал, для которого $C_{\mathrm{ea}}(\Phi, F, E) = C(\Phi, F, E) = 0$.

Замечание 1. Утверждение теоремы 1 имеет место для любого квадратичного оператора энергии F, если условие (18) в [8] выполнено в виде строгого операторного неравенства, поскольку это обеспечивает выполнимость приведенных выше утверждений 1), 2).[2]

---

[2]Если $\operatorname{Ran} K = Z_A$, то в силу предложения 5 в [4] требование невырожденности барицентра в утверждении 2) необязательно для доказательства теоремы 1, а значит, достаточно требовать выполнения условия (18) в [8] в обычном виде.

Замечание 2. Условия теоремы 1, обеспечивающие выполнимость строгого неравенства (5), существенны: существуют нетривиальные гауссовские каналы с линейными ограничениями, для которых

$$C_{\mathrm{ea}}(\Phi, F, E) = C(\Phi, F, E) = C_\chi(\Phi, F, E) > 0.$$

Простейший одномодовый ($s = 1$) пример такого канала Φ и оператора F приведен в [9]. Существенная особенность этого примера – некомпактность множества решений неравенства $\operatorname{Tr} F\rho \leqslant E$, что влечет отсутствие оптимальной меры для канала Φ с ограничением (1).

Замечание 3. В условиях теоремы 1 имеет место следующая оценка снизу для выигрыша от использования сцепленности:

$$C_{\mathrm{ea}}(\Phi, F, E) - C(\Phi, F, E) \geqslant H(\overline{\rho}(\mu_{\mathrm{opt}})) + H(\Phi(\rho_0)) - H(\Phi, \overline{\rho}(\mu_{\mathrm{opt}})),$$

в которой $\overline{\rho}(\mu_{\mathrm{opt}})$ – среднее состояние оптимального ансамбля (определяемое с помощью оптимизационной процедуры, описанной в [7]), а ρ_0 – чистое вакуумное состояние.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

[1] А. С. Холево, *Квантовые системы, каналы, информация*, МЦНМО, М., 2010. **[2]** C. H. Bennett, P. W. Shor, J. A. Smolin, A. V. Thapliyal, *IEEE Trans. Inform. Theory*, **48**:10 (2002), 2637–2655. **[3]** А. С. Холево, *ТВП*, **48**:2 (2003), 359–374. **[4]** А. С. Холево, М. Е. Широков, *Пробл. передачи информ.*, **49**:1 (2013), 19–36. **[5]** М. Е. Широков, *Пробл. передачи информ.*, **48**:2 (2012), 3–20. **[6]** V. Giovannetti, A. S. Holevo, R. García-Patrón, *Commun. Math. Phys.*, **334**:3 (2015), 1553–1571. **[7]** А. С. Холево, *УМН*, **70**:2 (2015). **[8]** A. S. Holevo, *On the Constrained Classical Capacity of Infinite-Dimensional Covariant Channels*, arXiv: 1409.8085. **[9]** А. С. Холево, *Пробл. передачи информ.*, **50**:1 (2014), 3–17.

А. С. Холево
Математический институт им. В. А. Стеклова РАН
E-mail: holevo@mi.ras.ru

Поступило
30.12.2014

М. Е. Широков
Математический институт им. В. А. Стеклова РАН
E-mail: msh@mi.ras.ru