

Краткое сообщение, представленное А.М. Бикчентаевым

Г.Г. АМОСОВ

О МАЖОРИЗАЦИИ КВАНТОВЫХ КАНАЛОВ РАСПРЕДЕЛЕНИЯМИ ВЕРОЯТНОСТЕЙ

Аннотация. На основе понятия мажоризации для распределения вероятностей введено определение мажоризации квантового канала распределением вероятностей. Показано, что предложенный подход позволяет решать задачу о взятии экстремумов выпуклых функций от выходных собственных значений смешанных унитарных каналов в случае, когда суммирование в определении канала ведется по группе Гейзенберга–Вейля.

Ключевые слова: информационные характеристики каналов, квантовый канал, представление унитарной группы.

УДК: 517.98: 519.724

DOI: 10.26907/0021-3446-2025-1-93-98

ВВЕДЕНИЕ

Пусть $\lambda = (\lambda_j, 1 \leq j \leq n)$ — конечное распределение вероятностей. Всегда можно перенумеровать его составляющие в порядке убывания

$$\lambda_1^\downarrow \geq \lambda_2^\downarrow \geq \dots \geq \lambda_n^\downarrow.$$

В работе [1] для двух распределений вероятностей $\lambda = (\lambda_j, 1 \leq j \leq n)$ и $\mu = (\mu_j, 1 \leq j \leq n)$ было введено понятие мажоризации. Говорят, что μ мажоризирует λ (записывается $\lambda \prec \mu$), если

$$\sum_{j=1}^k \lambda_j^\downarrow \leq \sum_{j=1}^k \mu_j^\downarrow, \quad 1 \leq k \leq n.$$

Там же было показано, что выполнение условия мажоризации эквивалентно тому, что

$$\sum_{j=1}^n F(\lambda_j) \leq \sum_{j=1}^n F(\mu_j)$$

для любой выпуклой функции $F(x)$. Современное изложение теории мажоризации можно найти в монографии [2].

На конечное распределение вероятностей можно смотреть как на набор собственных чисел некоторого положительного оператора с единичным следом. При этом можно считать,

Поступила в редакцию 24.10.2024, после доработки 24.10.2024. Принята к публикации 18.12.2024.

Благодарности. Исследование выполнено за счет гранта Российского научного фонда № 24-11-00145, <https://rscf.ru/project/24-11-00145/>.

что число n равно рангу оператора. Можно предположить, что оператор действует в любом пространстве большей размерности, но число его собственных значений, отличных от нуля, равно n . На этих соображениях основывается наше определение свойства мажоризации для квантовых каналов.

В последние годы возрос интерес к исследованию применимости теории мажоризации к исследованию пропускной способности квантовых каналов в конечномерных пространствах [3], [4]. В указанных работах удалось получить интересные оценки сверху для пропускной способности каналов. В бесконечномерном случае, применение метода мажоризации позволило найти пропускную способность целого класса гауссовских каналов с энергетическими ограничениями [5], [6].

В разделе 1 работы мы вводим понятие мажоризации для квантовых каналов. Раздел 2 посвящен смешанным унитарным каналам, для которых можно найти примеры каналов, мажоризирующихся распределениями вероятностей. Раздел 3 посвящен вопросу достижимости оценки, вытекающей из условия мажоризации. Тут же помещен основной результат статьи, позволяющий вычислять экстремумы выпуклых функций от выходных состояний квантовых каналов.

1. МАЖОРИЗАЦИЯ КВАНТОВЫХ КАНАЛОВ

В данной работе рассматриваются, как правило, конечномерные гильбертовы пространства H , для которых тождественный оператор $I = I_H$ конечномерен. Тем не менее, конструкция представляет интерес и для произвольного сепарабельного гильбертова пространства. Пусть $\Phi : B(H) \rightarrow B(H)$ — линейное отображение на алгебре ограниченных операторов $B(H)$ в сепарабельном гильбертовом пространстве H . Отображение Φ называется *квантовым каналом* [7], если оно вполне положительно, т. е. положительно любое отображение, заданное на матрицах размера $k \times k$ по формуле

$$[x_{jm}] \rightarrow [\Phi(x_{jm})], \quad 1 \leq j, m \leq k, \quad x_{jm} \in B(H), \quad k \geq 1, \quad (1)$$

и сохраняет след

$$Tr(\Phi(x)) = Tr(x)$$

на ядерных операторах $x \in \mathfrak{T}(H)$ в H . Из определения квантового канала следует, что корректно определено сужение Φ на выпуклое множество $\mathfrak{S}(H)$ всех положительных операторов с единичным следом (квантовых состояний) в H . Данное сужение $\Phi : \mathfrak{S}(H) \rightarrow \mathfrak{S}(H)$ также будем называть квантовым каналом.

Определение 1. Говорят, что распределение вероятностей $\lambda = (\lambda_j, 1 \leq j \leq n)$ мажоризирует квантовый канал Φ (записывается $\Phi \prec \lambda$), если для любого выбора единичных попарно ортогональных векторов $e_j \in H$, $1 \leq j \leq n$, выполнено неравенство

$$\sum_{j=1}^k (\Phi(\rho) e_j, e_j) \leq \sum_{j=1}^k \lambda_j^\downarrow, \quad 1 \leq k \leq n, \quad \rho \in \mathfrak{S}(H).$$

Замечание 1. Размерность пространства H не обязана совпадать с числом n . Она может быть больше, чем n , что существенно для дальнейшего рассмотрения. Конечно, если $\dim H > n$ векторов в равенстве слева может быть и больше, чем n , поскольку при $k = n$ справа получаем единицу, а сумма слева не может превысить след ρ , равный единице.

Для канала $\Phi : \mathfrak{S}(H) \rightarrow \mathfrak{S}(H)$ возьмем его тензорное произведение на тождественный канал $\Phi \otimes Id_k$, действующий в пространстве квадратных матриц $M_k(\mathbb{C})$. В результате $\Phi \otimes Id_k$ действует по формуле (1).

Предложение 1. *Предположим, что $\Phi \prec \lambda$. Тогда*

$$\Phi \otimes Id_k \prec \lambda$$

для любого $k \geq 1$.

Схема доказательства. Согласно известной теореме Стайнспринга [7] любой квантовый канал $\Phi : \mathfrak{S}(H) \rightarrow \mathfrak{S}(H)$ может быть представлен в виде

$$\Phi(\rho) = Tr_E(U_\Phi(\rho \otimes R)U_\Phi^*), \quad \rho \in \mathfrak{S}(H), \quad (2)$$

где $U_\Phi : H \otimes E \rightarrow H \otimes E$ — унитарный оператор и R — одномерный проектор в гильбертовом пространстве E . Здесь через Tr_E обозначен частичный след по пространству E . Для канала $\Phi \otimes Id_K$, получившегося после взятия тензорного произведения, можно использовать представление (2). Тогда

$$(\Phi \otimes Id_k)(\rho) = Tr_E((U_\Phi \otimes I_k)(\rho \otimes R)(U_\Phi^* \otimes I_k)). \quad (3)$$

Отметим, что для схемы доказательства предложения 1 достаточно использовать только чистые состояния (одномерные проекторы) $\rho = P \in \mathfrak{S}(H \otimes \mathbb{C}^k)$. В этом случае, при замене в (3) частичного следа по E на частичный след по $H \otimes \mathbb{C}^k$ получится положительный оператор с тем же спектром. Более того,

$$Tr_{H \otimes \mathbb{C}^k}((U_\Phi \otimes I_k)(P \otimes R)(U_\Phi^* \otimes I_k)) = Tr_H(U_\Phi \tilde{\rho} U_\Phi^*), \quad (4)$$

где $\tilde{\rho} = Tr_E P$. При взятии супремума по состояниям $\tilde{\rho}$ от любой выпуклой функции от собственных значений оператора (4), максимум будет достигаться на операторах $\tilde{\rho}$, являющихся одномерными проекторами, т. е. при условии $P = \tilde{\rho} \otimes \tilde{\rho}$. Применяя теорему Караматы, получаем, что на таких состояниях условие мажоризации выполнено.

2. ПРИМЕР КАНАЛОВ, КОТОРЫЕ МАЖОРИЗИРУЮТСЯ РАСПРЕДЕЛЕНИЕМ ВЕРОЯТНОСТЕЙ

Рассмотрим смешанный унитарный канал вида

$$\Phi(\rho) = \sum_{U \in \mathcal{U}} \pi_U U \rho U^*, \quad \rho \in \mathfrak{S}(H), \quad (5)$$

где суммирование ведется по элементам конечной группы унитарных операторов $\mathcal{U}$, действующей в гильбертовом пространстве H , и (π_U) — распределение вероятностей на группе $\mathcal{U}$.

Мы уже обращались к исследованию каналов вида (5) в работах [8]–[10] и показали, что в ряде случаев методом мажоризации информационные характеристики таких каналов достигают своих супремумов на состояниях, факторизующихся относительно структуры тензорного произведения, что позволяет, в частности, найти классическую пропускную способность таких каналов. Следует отметить, что контрпример к указанному свойству также находится в таком классе каналов [11].

Предположим, что у группы $\mathcal{U}$ существует абелева подгруппа $\mathcal{T}$. В своих предыдущих работах [8]–[10] мы требовали, чтобы $\mathcal{T}$ была нормальна. На самом деле, это требование представляется излишним, и без его выполнения можно определить смежные классы $[U] = \{UT, T \in \mathcal{U}\}$. Условие нормальности появилось для того, чтобы получаемая нами оценка достигалась. В любом случае, если $\mathcal{T}$ — группа, можно определить маргинальное распределение P на множестве смежных классов по формуле

$$p[U] = \sum_{T \in \mathcal{T}} \pi_{UT}.$$

Поскольку смежные классы группы не пересекаются, можно выделить такой набор операторов $U_j \in \mathcal{U}$, где индекс j пробегает значения от единицы до общего числа смежных классов n , что числа $p_j = p_{[U_j]} \in P$ обладают свойством

$$p_1 \geq p_2 \geq \dots \geq p_n.$$

Нашей целью будет установить, при каких условиях распределение вероятностей P мажоризирует квантовый канал (5).

Обозначим через $\Pi_j = \{\pi_U, U \in [U_j]\}$ подмножества распределения вероятностей π , отвечающие j -му смежному классу.

Определение 2. Будем говорить, что для распределения π выполнено условие порядка по отношению к маргинальному распределению P , если

$$p_j \geq p_k \Rightarrow \pi_j \geq \pi_k \text{ для любого выбора } \pi_j \in \Pi_j, \pi_k \in \Pi_k.$$

Обозначим $\mathcal{U}' = \{x \in B(H), xU = Ux, U \in \mathcal{U}\}$.

Предложение 2. *Предположим, что для распределения π выполнено условие порядка по отношению к маргинальному распределению P , $n \leq \dim H$, $|\mathcal{U}| \leq \dim H |\mathcal{T}|$ и $\mathcal{U}' = \{\mathbb{C}I\}$. Тогда для квантового канала (5) выполнено*

$$\Phi \prec P.$$

Замечание 2. Оценка, полученная в предложении 2, может быть не достижима в том смысле, что в неравенстве

$$\sum_{j=1}^k (\Phi(\rho)e_j, e_j) \leq \sum_{j=1}^k p_j$$

сумма в левой части не равна правой ни для какого $\rho \in \mathfrak{S}(H)$.

Схема доказательства. Возьмем k попарно ортогональных единичных векторов $e_j \in H$, $1 \leq j \leq k$. Тогда

$$\begin{aligned} (\Phi(\rho)e_j, e_j) &= \sum_{U \in \mathcal{U}} \pi_U(\rho U^* e_j, U^* e_j), \\ \sum_{j=1}^k (\rho U^* e_j, U^* e_j) &\leq \text{Tr}(\rho) = 1, \quad 1 \leq k \leq n. \end{aligned}$$

Отметим, что

$$\Theta(x) = \frac{1}{|\mathcal{U}|} \sum_{U \in \mathcal{U}} UxU^*,$$

$x \in B(H)$ — проектор на алгебру неподвижных точек относительно действий $x \rightarrow UxU^*$, $U \in \mathcal{U}$. Из предложения 2 вытекает

$$\Theta(\rho) = \frac{1}{\dim H} I, \quad \rho \in \mathfrak{S}(H).$$

Следовательно,

$$\begin{aligned} \sum_{U \in \mathcal{U}} (U\rho U^* e_j, e_j) &= |\mathcal{U}| \frac{1}{\dim H} \leq |\mathcal{T}|, \\ \sum_{j=1}^k (\Phi(\rho)e_j, e_j) &\leq \sum_{j=1}^k p_j, \quad 1 \leq k \leq n, \end{aligned}$$

в силу выполнения условия порядка.

3. Достижимость оценки в условии мажоризации

Как было отмечено в замечании 2, оценка, следующая из условия мажоризации может быть не достижима. Нам интересно привести пример, когда достижимость имеет место. Обозначим через $\mathbb{Z}_n$ кольцо вычетов по модулю n , $2 \leq n < +\infty$. Множество верхнетреугольных матриц

$$\begin{pmatrix} 1 & k & l \\ 0 & 1 & m \\ 0 & 0 & 1 \end{pmatrix}, \quad k, l, m \in \mathbb{Z}_n,$$

снабженное операцией матричного умножения, называется группой Гейзенберга $\mathbb{H}_3(\mathbb{Z}_n)$.

Расширим определение группы из примера канала, определенного в работах [8], [9], на произвольную конечную размерность. Пусть e_j , $1 \leq j \leq n$, — ортонормированный базис в пространстве H , $\dim H = n$. Введем два унитарных оператора U и S по формуле

$$Ue_j = e^{i\frac{2\pi(j-1)}{n}} e_j, \quad 1 \leq j \leq n,$$

$$Se_j = e_{j+1}, \quad 1 \leq j \leq n-1, \quad Se_n = e_1.$$

Отображение

$$(j, k, l) \rightarrow e^{i\frac{2\pi j}{n}} U^k S^l$$

задает унитарное представление $\mathbb{H}_3(\mathbb{Z}_n)$ в гильбертовом пространстве H , $\dim H = n$, и $\mathcal{U} = \{e^{i\frac{2\pi j}{n}} U^k S^l, 0 \leq j, k, l \leq n-1\}$ называется группой Гейзенберга–Вейля. Абелева подгруппа $\mathcal{T} = \{e^{i\frac{2\pi j}{n}} U^k, 0 \leq j, k \leq n-1\}$ является нормальной в $\mathcal{U}$. Отметим, что для группы $\mathcal{U}$ выполнены условия предложения 2, поскольку $\dim H = n$, $|\mathcal{U}| = n^3$ и $|\mathcal{T}| = n^2$. Следовательно, условие мажоризации выполнено при условии сохранения порядка. Мы докажем нечто большее.

Теорема. Пусть для распределения вероятностей π и маргинального распределения P , полученного относительно абелевой подгруппы $\mathcal{T}$ группы Гейзенберга–Вейля $\mathcal{U}$, выполнено условие сохранения порядка. Тогда для любой выпуклой функции F выполняется

$$\sup_{\rho \in \mathfrak{S}(H)} \sum_{j=1}^n F(\lambda_j(\Phi(\rho))) = \sum_{j=1}^n F(p_j).$$

Здесь через $(\lambda_j(\Phi(\rho)))$ обозначили собственные числа оператора $\Phi(\rho)$, где Φ — смешанный унитарный канал (5), построенный по распределению вероятностей π на группе $\mathcal{U}$.

Схема доказательства. Из предложения 2 следует, что $\Phi \prec P$. Следовательно, по теореме Караматы получаем

$$\sum_{j=1}^n F(\lambda_j(\Phi(\rho))) \leq \sum_{j=1}^n F(p_j). \quad (6)$$

Равенство в (6) достигается на любом одномерном проекторе $\rho = P$ из алгебры, порожденной абелевой группой $\mathcal{T}$.

Автор признателен А.С. Холево за содержательное обсуждение текста и полезные замечания, позволившие существенно улучшить изложение.

ЛИТЕРАТУРА

- [1] Karamata J. *Sur une inegalite relative aux fonctions convexes*, Publ. Math. Univ. Belgrade **1**, 145–148 (1932).
- [2] Bhatia R. *Matrix analysis* (Springer, 1996).
- [3] Ur Rehman J., Jeong Y., Kim J.S., Shin H. *Holevo capacity of discrete Weyl channels*, Scientific Reports **8**, 17457 (2018).
- [4] Siudzińska K. *Classical capacity of generalized Pauli channels*, J. Phys. A: Math. Theor. **53** (44), 445301 (2020).
- [5] Mari A., Giovannetti V., Holevo A.S. *Quantum state majorization at the output of bosonic Gaussian channels*, Nature Commun. **5**, 3826 (2014).
- [6] Holevo A.S. *On the proof of the majorization theorem for quantum Gaussian channels*, Russ. Math. Surv. **71** (3), 585–587 (2016).
- [7] Holevo A.S. *Quantum Systems, Channels, Information. A mathematical introduction.*, 2nd ed., extended and complemented (De Gruyter, Berlin–Boston, 2019).
- [8] Amosov G.G. *On classical capacity of Weyl channels*, Quant. Inform. Process. **19**, 401–411 (2020).
- [9] Amosov G.G. *On capacity of quantum channels generated by irreducible projective unitary representations of finite groups*, Quant. Inform. Process. **21** (2), 81 (2022).
- [10] Amosov G.G. *On characteristics of mixed unitary channels being additive or multiplicative with respect to taking tensor products*, arXiv:2401.05104 (2024).
- [11] Hastings M.B. *A counterexample to additivity of minimum output entropy*, Nature Phys. **5**, 255–257 (2009).

Григорий Геннадьевич Амосов

Математический институт им. В.А. Стеклова Российской академии наук,
ул. Губкина, д. 8, г. Москва, 199911, Россия,

e-mail: gramos@mi-ras.ru

G.G. Amosov

On majorization of quantum channels by probability distributions

Abstract. Based on the concept of majorization for the probability distribution, a definition of the majorization of a quantum channel by a probability distribution is introduced. It is shown that the proposed approach makes it possible to solve the problem of taking the extremes of convex functions from the output eigenvalues of mixed unitary channels in the case when summation in the definition of the channel is carried out according to the Heisenberg–Weyl group.

Keywords: information characteristics of channels, quantum channel, representation of unitary group.

Grigori Gennadievich Amosov

Steklov Mathematical Institute of Russian Academy of Sciences,
8 Gubkina str., Moscow, 199911 Russia,

e-mail: gramos@mi-ras.ru