ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 52 2016 Вып. 3

УДК 621.391.1 : 519.7

© 2016 г. **Ф. Бушеми**

ДЕГРАДИРУЕМЫЕ КАНАЛЫ, КАНАЛЫ С МЕНЬШИМ ШУМОМ И КВАНТОВЫЕ СТАТИСТИЧЕСКИЕ МОРФИЗМЫ: ОТНОШЕНИЕ ЭКВИВАЛЕНТНОСТИ[1]

Два отношения частичного порядка между каналами связи, а именно “быть деградируемым в” и “иметь меньший шум, чем” рассматриваются в свете недавних результатов о статистических сравнениях квантовых каналов. Хотя полученные результаты покрывают как классические, так и квантовые каналы, случай классических каналов с шумом разобран отдельно и показано, что в этом случае можно получить альтернативное независимое доказательство, обладающее определенными преимуществами по сравнению с общим результатом.

§ 1. Введение

Для двух заданных каналов естественно спросить, какой из них “лучше”. Как легко понять, упорядочение каналов по их пропускной способности излишне ограничивает возможности, поскольку могут быть и другие меры “качества” канала, более подходящие для той или иной рассматриваемой задачи. Это тем более справедливо для *квантовых* каналов, для которых существует много неэквивалентных определений пропускной способности [1]. На самом деле нетрудно понять, что есть бесконечно много таких “критериев сравнения”, и каждый из них задает лишь *частичное*, а не *полное* отношение порядка на каналах. В этом нет ничего удивительного: каналы – это объекты больших размерностей, и любой полный порядок на них весьма груб – как правило, слишком груб, чтобы иметь какую-либо практическую пользу. Как бы то ни было, некоторые из этих критериев сравнения более естественны, более убедительны, или даже математически более просты, чем другие, и поэтому лучше изучены в литературе. В настоящей статье фактически рассматриваются два таких хорошо изученных критерия сравнения, а именно отношения частичного порядка “быть деградируемым в” и “иметь меньший шум, чем”, задаваемые определениями 1, 2 (большой список разнообразных мер сравнения для дискретных каналов с шумом см. в [2]).

Цель настоящей статьи – установить взаимосвязь между деградируемыми каналами и каналами с меньшим шумом помимо очевидного “деградируемость влечет меньший шум”. Более точно, мы показываем, что формального (но не значительного) изменения определения канала с меньшим шумом достаточно, чтобы сделать эти два упорядочивания эквивалентными. Результат доказан в общей постановке, где каналы моделируются как вполне положительные сохраняющие след отображения операторных алгебр, включая тем самым квантовые каналы, классические каналы (в которых вход и выход являются коммутативными алгебрами), а также гибридные классически-квантовые и квантово-классические каналы.

[1] Работа выполнена при финансовой поддержке фонда JSPS KAKENHI (номер гранта 26247016).

Ключевым для нашего подхода является понятие *квантовых статистических морфизмов*, т.е. линейных отображений операторных алгебр, обобщающих в статистическом смысле идею “постобработки” или “укрупнения зерна” (см. определение 5). Использование статистических морфизмов позволяет доказывать результаты при весьма слабых предположениях, так что квантовый и классический случай получаются как частные случаи единого универсального подхода. Такой подход от большего к меньшему помимо математической простоты обладает тем достоинством, что статистика очевидным образом отделена от физики: его можно непосредственно применять к общим вероятностным теориям, поскольку он не опирается ни на какое конкретное свойство квантовой теории, такое как, например, полная положительность.

Статья имеет следующую структуру. В § 2 вводятся обозначения и некоторые основные понятия. В § 3 вводится понятие статистических морфизмов и доказывается основное отношение эквивалентности. В § 4 рассматривается частный случай полуклассических каналов. Случай дискретных классических каналов с шумом разбирается отдельно в п. 4.1, причем способом, не использующим знание квантового случая и позволяющим изучить аппроксимативный случай, рассматриваемый в Приложении. В § 5 рассматривается случай полностью квантовых каналов. В заключение в § 6 даются некоторые комментарии и возможные направления дальнейшего развития.

§ 2. Обозначения и определения

Всюду далее все множества конечны, а гильбертовы пространства конечномерны.

- Множества обозначаются буквами $\mathcal{X} = \{x : x \in \mathcal{X}\}$, $\mathcal{Y} = \{y : y \in \mathcal{Y}\}$ и т.д.
- Распределение вероятностей на $\mathcal{X}$ – функция $p\colon \mathcal{X} \to [0,1]$, такая что $\sum_x p(x) = 1$.
- *Множество всех распределений вероятностей* на $\mathcal{X}$ обозначается через $\mathrm{P}(\mathcal{X})$.
- Случайные величины обозначаются заглавными буквами X, Y и т.д. и принимают значения на множествах $\mathcal{X} = \{x\}$, $\mathcal{Y} = \{y\}$ и т.д.
- Дискретные каналы с шумом отождествляются с соответствующими условными распределениями вероятностей.
- Квантовые системы обозначаются заглавными буквами Q, R и т.д., ассоциированные гильбертовы пространства обозначаются через $\mathcal{H}_Q$, $\mathcal{H}_R$ и т.д., а их размерности – через $d_Q \stackrel{\text{def}}{=} \dim \mathcal{H}_Q$ и т.д.
- *Множество линейных операторов*, действующих на гильбертовом пространстве $\mathcal{H}$, обозначается через $\mathrm{L}(\mathcal{H})$. *Тождественный оператор* обозначается через $\mathbb{1}$.
- Состояния системы Q представляются *операторами плотности*, т.е. операторами $\rho \in \mathrm{L}(\mathcal{H})$, такими что $\rho \geqslant 0$ и $\mathrm{Tr}[\rho] = 1$.
- *Множество операторов плотности*, действующих на гильбертовом пространстве $\mathcal{H}$, обозначается через $\mathrm{S}(\mathcal{H})$.
- Положительная операторнозначная мера (*ПОЗМ*) – это функция $P\colon \mathcal{X} \to \mathrm{L}(\mathcal{H})$, такая что $P(x) \geqslant 0$ и $\sum_x P(x) = \mathbb{1}$. Для удобства чтения мы зачастую указываем аргумент x в виде верхнего индекса, т.е. пишем P^x вместо $P(x)$.
- *Множество ПОЗМ* из $\mathcal{X}$ в $\mathrm{L}(\mathcal{H})$ обозначается через $\mathrm{M}(\mathcal{X}, \mathcal{H})$.
- *Квантовые каналы* – это вполне положительные сохраняющие след линейные отображения $\mathcal{N}\colon \mathrm{L}(\mathcal{H}_Q) \to \mathrm{L}(\mathcal{H}_R)$. *Область значений* канала $\mathcal{N}$ определяется как образ множества $\mathrm{L}(\mathcal{H}_Q)$ под действием $\mathcal{N}$, т.е. множество $\{\mathcal{N}(X) : X \in \mathrm{L}(\mathcal{H}_Q)\}$. *Тождественное отображение* обозначается через id.
- *Множество квантовых каналов* из $\mathrm{L}(\mathcal{H}_Q)$ в $\mathrm{L}(\mathcal{H}_R)$ будем обозначать через $\mathrm{C}(\mathcal{H}_Q, \mathcal{H}_R)$.

- Для линейного отображения $\mathcal{L}\colon \mathrm{L}(\mathcal{H}_Q) \to \mathrm{L}(\mathcal{H}_R)$ его *двойственное относительно следа* отображение $\mathcal{L}^*\colon \mathrm{L}(\mathcal{H}_R) \to \mathrm{L}(\mathcal{H}_Q)$ – это линейное отображение, задаваемое соотношением

  $$\mathrm{Tr}[\mathcal{L}^*(X_R)\, Y_Q] \stackrel{\mathrm{def}}{=} \mathrm{Tr}[X_R\, \mathcal{L}(Y_Q)]$$

  для всех $Y_Q \in \mathrm{L}(\mathcal{H}_Q)$ и всех $X_R \in \mathrm{L}(\mathcal{H}_R)$. При этом $\mathcal{N}$ сохраняет след тогда и только тогда, когда $\mathcal{N}^*$ *сохраняет единицу*, т.е. $\mathcal{N}^*(\mathbb{1}_R) = \mathbb{1}_Q$. Кроме того, линейное отображение $\mathcal{L}$ *эрмитово* тогда и только тогда, когда для любых $X = X^\dagger$ выполнено $\mathcal{L}(X) = \mathcal{L}(X)^\dagger$.
- *Классически-квантовый канал* (*cq-канал*) – это функция $\mathcal{E}\colon \mathcal{X} \to \mathrm{S}(\mathcal{H})$. Как правило, будем обозначать операторы плотности $\mathcal{E}(x)$ через ρ^x, σ^x и т.д. Эквивалентным образом cq-канал $\mathcal{E}$ можно описывать как семейство операторов плотности $\mathcal{E} = \{\rho^x : x \in \mathcal{X}\}$.
- *Классически-квантовое состояние* (*cq-состояние*) – это двухчастичный оператор плотности, описывающий квантовую систему Q, коррелированную со случайной величиной X. Поскольку случайные величины можно рассматривать как коммутирующие операторы плотности, будем представлять cq-состояния в виде, например, $\rho_{XQ} = \sum\limits_{x\in\mathcal{X}} p(x)|x\rangle\langle x|_X \otimes \rho_Q^x$, где $\{|x\rangle : x \in \mathcal{X}\}$ – единичные ортогональные векторы.
- Для заданного двухчастичного оператора плотности $\rho_{RQ} \in \mathrm{S}(\mathcal{H}_R\otimes\mathcal{H}_Q)$ его *условная* min-*энтропия* $H_{\min}(R\,|\,Q)_\rho$ определяется как

  $$H_{\min}(R\,|\,Q)_\rho \stackrel{\mathrm{def}}{=} -\inf_{\sigma_Q\in\mathrm{S}(\mathcal{H}_Q)} \inf\bigl\{\lambda \in \mathbb{R} :\ \rho_{RQ} \leqslant 2^\lambda \mathbb{1}_R \otimes \sigma_Q\bigr\}.$$

  В частности, будем использовать тот факт [3], что

  $$2^{-H_{\min}(R|Q)_\rho} = d_R \max_{\mathcal{N}\in\mathrm{C}(\mathcal{H}_Q,\mathcal{H}_{R'})} F^2\bigl((\mathrm{id}_R \otimes \mathcal{N})\rho_{RQ}, \Phi^+_{RR'}\bigr),$$

  где $\mathcal{H}_{R'} \cong \mathcal{H}_R$, $F^2(\rho,\sigma) \stackrel{\mathrm{def}}{=} \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$ и $\Phi^+_{RR'} \stackrel{\mathrm{def}}{=} d_R^{-1} \sum\limits_{i,j=1}^{d_R} |i_R\rangle|i_{R'}\rangle\langle j_R|\langle j_{R'}|$ для некоторого ортогонального базиса $\{|i\rangle\}$ пространства $\mathcal{H}_R$. В случае cq-состояния $\rho_{XQ} = \sum\limits_{x\in\mathcal{X}} p(x)|x\rangle\langle x|_X \otimes \rho_Q^x$ эта формула принимает вид

  $$2^{-H_{\min}(X\,|\,Q)_\rho} = \max_{P\in\mathrm{M}(\mathcal{X},\mathcal{H}_Q)} \sum_{x\in\mathcal{X}} p(x)\,\mathrm{Tr}\bigl[\rho_Q^x\, P_Q^x\bigr] \stackrel{\mathrm{def}}{=} P_{\mathrm{guess}}(X\,|\,Q)_\rho$$

  – ожидаемая *вероятность угадывания*, т.е. вероятность правильно угадать значение X, имея доступ только к квантовой системе Q.

2.1. "Деградируемые" каналы и каналы "с меньшим шумом". Для классического случая следующие определения содержатся в [4–7].

Определение 1 (деградируемые каналы). Для дискретных каналов $p(y\,|\,x)$ и $p'(z\,|\,x)$ говорят, что p *деградируем* в p', если существует дискретный канал $q(z\,|\,y)$, такой что

$$p'(z\,|\,x) = \sum_{y\in\mathcal{Y}} q(z\,|\,y)p(y\,|\,x).$$

Определение 2 (каналы с меньшим шумом). Для дискретных каналов $p(y\,|\,x)$ и $p'(z\,|\,x)$ говорят, что p – канал *с меньшим шумом*, чем p', если для любой дискретной случайной величины U, любого распределения вероятностей $q(u)$ и любого канала $q(x\,|\,u)$ совместные распределения вероятностей входа-выхода $q(u)q(x\,|\,u)p(y\,|\,x)$

и $q(u)q(x\,|\,u)p'(z\,|\,x)$ удовлетворяют условию

$$H(U\,|\,Y) \leqslant H(U\,|\,Z).$$

Если p_1 деградируем в p_2, то p_1 – канал с меньшим шумом, чем p_2: доказательство является простым следствием леммы об обработке данных. К обратному утверждению имеются контрпримеры [5], т.е. один канал может быть каналом с меньшим шумом, чем другой, не будучи при этом деградируемым. Следствием результатов настоящей статьи является то, что в определении 2 достаточно заменить H на $H_{\min}$, чтобы частичный порядок "с меньшим шумом" (теперь определенный через $H_{\min}$) стал эквивалентным частичному порядку "быть деградируемым". Этот факт формально представлен в следствии 3. (Читатель, интересующийся только классическим случаем, может сразу обратиться к п. 4.1: в нем следствие 3 доказано независимым образом, не используя идеи, развитые для общего некоммутативного случая. Более того, это доказательство позволяет исследовать аппроксимативный случай, рассматриваемый в Приложении.)

На самом деле наш анализ не ограничится случаем классических каналов с шумом, а будет включать некоторые результаты, справедливые и для квантовых каналов. Поэтому обобщим определения 1, 2 на квантовый случай следующим образом (впрочем, ср. с [8]).

Определение 3 (деградируемые квантовые каналы). Для вполне положительных сохраняющих след отображений $\mathcal{N}\colon \mathrm{L}(\mathcal{H}_Q) \to \mathrm{L}(\mathcal{H}_R)$ и $\mathcal{N}'\colon \mathrm{L}(\mathcal{H}_Q) \to \mathrm{L}(\mathcal{H}_S)$ говорят, что $\mathcal{N}$ *деградируемо* в $\mathcal{N}'$, если существует вполне положительное сохраняющее след отображение $\mathcal{T}\colon \mathrm{L}(\mathcal{H}_R) \to \mathrm{L}(\mathcal{H}_S)$, такое что

$$\mathcal{N}' = \mathcal{T} \circ \mathcal{N}.$$

Определение 4 (квантовые каналы с меньшим шумом). Для вполне положительных сохраняющих след отображений $\mathcal{N}\colon \mathrm{L}(\mathcal{H}_Q) \to \mathrm{L}(\mathcal{H}_R)$ и $\mathcal{N}'\colon \mathrm{L}(\mathcal{H}_Q) \to \mathrm{L}(\mathcal{H}_S)$ говорят, что $\mathcal{N}$ – канал с *меньшим шумом*, чем $\mathcal{N}'$, если для любой дискретной случайной величины U, любого распределения вероятностей $q(u)$ и любого cq-канала $\mathcal{E} = \{\rho_Q^u : u \in \mathcal{U}\}$ соответствующие cq-состояния входа-выхода

$$\sigma_{UR} \stackrel{\text{def}}{=} \sum_u q(u)|u\rangle\langle u|_U \otimes \mathcal{N}_Q(\rho_Q^u) \quad \text{и} \quad \tau_{US} \stackrel{\text{def}}{=} \sum_u q(u)|u\rangle\langle u|_U \otimes \mathcal{N}'_Q(\rho_Q^u)$$

удовлетворяют условию

$$H(U\,|\,R)_\sigma \leqslant H(U\,|\,S)_\tau.$$

В статье изучается взаимосвязь между понятиями деградируемых каналов и каналов с меньшим шумом как в классической, так и в квантовой теории информации. Далее будет показано, в частности, как можно формально модифицировать определения 2, 4, чтобы эти два частичных порядка стали эквивалентными. Представленные результаты основаны на недавно полученных вариантах теоремы Блэквелла – Шермана – Стейна [9–11] для квантовых систем [12–17].

§ 3. Статистические морфизмы и основное соотношение эквивалентности

Начнем с обобщения определения, данного в [15].

Определение 5 (квантовые статистические морфизмы). Для вполне положительного сохраняющего след отображения $\mathcal{N}\colon \mathrm{L}(\mathcal{H}_Q) \to \mathrm{L}(\mathcal{H}_R)$ его *статистический морфизм* – это линейное отображение $\mathcal{L}\colon \mathrm{L}(\mathcal{H}_R) \to \mathrm{L}(\mathcal{H}_S)$, такое что для любого конечного множества исходов $\mathcal{X}$ и любой ПОЗМ $\{\bar{P}_S^x : x \in \mathcal{X}\}$ существует другая ПОЗМ $\{P_R^x : x \in \mathcal{X}\}$, такая что

$$\mathrm{Tr}[(\mathcal{L}\circ\mathcal{N})(\rho_Q)\,\bar{P}_S^x] = \mathrm{Tr}[\mathcal{N}(\rho_Q)\,P_R^x], \quad \forall x \in \mathcal{X}, \forall \rho_Q \in \mathrm{S}(\mathcal{H}_Q). \tag{1}$$

Замечание 1. Ясно, что положительное сохраняющее след линейное отображение всегда задает статистический морфизм *для любого* канала. Однако отображение может быть статистическим морфизмом *для некоторого канала*, не будучи положительным и сохраняющим след, – на самом деле статистические морфизмы, вообще говоря, даже *не могут быть продолжены* до положительных сохраняющих след отображений, как показано в [18] с помощью явного контрпримера[2]. Можно лишь утверждать, что если $\mathcal{L}$ – статистический морфизм отображения $\mathcal{N}$, то $\mathcal{L}$ – положительное сохраняющее след (ПСС) отображение на области значений $\mathcal{N}$, т.е. $\mathrm{Tr}[(\mathcal{L}\circ\mathcal{N})(X_Q)] = \mathrm{Tr}[\mathcal{N}(X_Q)]$ для всех $X_Q \in \mathrm{L}(\mathcal{H}_Q)$, и если $\mathcal{N}(X_Q) \geqslant 0$, то $\mathrm{Tr}[(\mathcal{L}\circ\mathcal{N})(X_Q)\,\bar{P}_S] \geqslant 0$ для всех $\bar{P}_S \geqslant 0$. Возникает следующий вопрос: всякое ли линейное отображение $\mathcal{L}$, положительное и сохраняющее след на области значений отображения $\mathcal{N}$, является статистическим морфизмом $\mathcal{N}$? Ответ на этот вопрос снова отрицательный, поскольку чтобы гарантировать, что $\mathcal{L}$ положительно и сохраняет след на области значений $\mathcal{N}$, достаточно, чтобы (1) выполнялось только для двоичных ПОЗМ (т.е. *воздействий*) $\{\bar{P}, \mathbb{1}-\bar{P}\}$, однако известно, что такое условие строго слабее, чем условие, требуемое в определении 5, которое должно выполняться для любого конечного $\mathcal{X}$ [20]. Таким образом, обобщая, получаем следующее:

$$\text{ПСС всюду} \underset{\not\Leftarrow}{\Longrightarrow} \text{статистический морфизм } \mathcal{N} \underset{\not\Leftarrow}{\Longrightarrow} \text{ПСС на области значений } \mathcal{N}.$$

Замечание 2. В дальнейшем, говоря “сохраняющий след статистический морфизм”, мы подразумеваем сохраняющее след (всюду) линейное отображение, которое, в частности, является статистическим морфизмом (для некоторого канала).

Теперь мы готовы сформулировать основное соотношение эквивалентности.

Предложение 1. *Для вполне положительных сохраняющих след отображений $\mathcal{N}\colon \mathrm{L}(\mathcal{H}_Q) \to \mathrm{L}(\mathcal{H}_R)$ и $\mathcal{N}'\colon \mathrm{L}(\mathcal{H}_Q) \to \mathrm{L}(\mathcal{H}_S)$ следующие утверждения эквивалентны:*

(i) *Для любой дискретной случайной величины U, любого распределения вероятностей $q(u)$ и любого cq-канала $\mathcal{E} = \{\rho_Q^u : u \in \mathcal{U}\}$ соответствующие cq-состояния входа-выхода*

$$\sigma_{UR} = \sum_{u\in\mathcal{U}} q(u)|u\rangle\langle u|_U \otimes \mathcal{N}(\rho_Q^u) \quad \text{и} \quad \tau_{US} = \sum_{u\in\mathcal{U}} q(u)|u\rangle\langle u|_U \otimes \mathcal{N}'(\rho_Q^u)$$

удовлетворят неравенству

$$H_{\min}(U\,|\,R)_\sigma \leqslant H_{\min}(U\,|\,S)_\tau,$$

т.е. $P_{\mathrm{guess}}(U\,|\,R)_\sigma \geqslant P_{\mathrm{guess}}(U\,|\,S)_\tau$;

(ii) *Существует эрмитов сохраняющий след статистический морфизм $\mathcal{L}\colon \mathrm{L}(\mathcal{H}_R) \to \mathrm{L}(\mathcal{H}_S)$ отображения $\mathcal{N}$, такой что*

$$\mathcal{N}' = \mathcal{L}\circ\mathcal{N}.$$

Отметим, что утверждение (i) предложения 1 выглядит в точности, как определение каналов с меньшим шумом (определение 4), с той лишь разницей, что вместо H используется $H_{\min}$.

[2] Об этой задаче см. также [19].

Доказательство. Если справедливо утверждение (ii), то

$$
\begin{aligned}
&P_{\mathrm{guess}}(U\,|\,S)_\tau = \max_{\bar{P}\in \mathrm{M}(\mathcal{U},\mathcal{H}_S)} \sum_{u\in\mathcal{U}} q(u)\,\mathrm{Tr}[\mathcal{N}'(\rho_Q^u)\,\bar{P}_S^u] = \\
&= \max_{\bar{P}\in \mathrm{M}(\mathcal{U},\mathcal{H}_S)} \sum_{u\in\mathcal{U}} p(u)\,\mathrm{Tr}[(\mathcal{L}\circ\mathcal{N})(\rho_Q^u)\,\bar{P}_S^u] \leqslant \max_{P\in \mathrm{M}(\mathcal{U},\mathcal{H}_R)} \sum_{u\in\mathcal{U}} p(u)\,\mathrm{Tr}[\mathcal{N}(\rho_Q^u)\,P_R^u] = \\
&= P_{\mathrm{guess}}(U\,|\,R)_\sigma,
\end{aligned}
$$

где неравенство следует из определения 5.

Наоборот, пусть выполнено утверждение (i). Как показано в [15–17], отсюда следует, что для любой ПОЗМ $\{\bar{P}_S^x : s \in \mathcal{X}\}$ на $\mathcal{H}_S$ существует ПОЗМ $\{P_R^x : s \in \mathcal{X}\}$ на $\mathcal{H}_R$, такая что

$$
\mathrm{Tr}[\mathcal{N}'(\rho_Q)\,\bar{P}_S^x] = \mathrm{Tr}[\mathcal{N}(\rho_Q)\,P_R^x] \tag{2}
$$

для всех $x \in \mathcal{X}$ и всех $\rho_Q \in \mathrm{S}(\mathcal{H}_Q)$. В качестве $\{\bar{P}_S^x : s \in \mathcal{X}\} \in \mathrm{M}(\mathcal{X},\mathcal{H}_S)$ выберем информационно полную ПОЗМ, т.е. такую, что $\mathrm{span}\{\bar{P}_S^x : x \in \mathcal{X}\} = \mathrm{L}(\mathcal{H}_S)$. Пусть $\{P_R^x : s \in \mathcal{X}\} \in \mathrm{M}(\mathcal{X},\mathcal{H}_R)$ – соответствующая ПОЗМ, удовлетворяющая условию (2), и зададим линейное отображение $\mathcal{L}^*\colon \mathrm{L}(\mathcal{H}_S) \to \mathrm{L}(\mathcal{H}_R)$ как

$$
\mathcal{L}^*(\bar{P}_S^x) \stackrel{\mathrm{def}}{=} P_R^x, \quad x \in \mathcal{X}.
$$

Такое отображение определено однозначно, поскольку $\{\bar{P}_S^x : x \in \mathcal{X}\}$ является базисом в $\mathrm{L}(\mathcal{H}_S)$, и сохраняет единицу по построению, откуда следует, что его двойственное относительно следа отображение $\mathcal{L}\colon \mathrm{L}(\mathcal{H}_R) \to \mathrm{L}(\mathcal{H}_S)$ сохраняет след. Чтобы доказать, что отображение $\mathcal{L}$ эрмитово, рассмотрим множество $\{\Theta_S^x : x \in \mathcal{X}\}$ эрмитовых операторов в $\mathrm{L}(\mathcal{H}_S)$, таких что

$$
X_S = \sum_{x\in\mathcal{X}} \mathrm{Tr}[X_S\,\bar{P}_S^x]\Theta_S^x
$$

для всех $X_S \in \mathrm{L}(\mathcal{H}_S)$. Отсюда следует, что для любого $Y_R = Y_R^\dagger$ из $\mathrm{L}(\mathcal{H}_R)$ выполнено

$$
\begin{aligned}
&\mathcal{L}(Y_R) = \sum_{x\in\mathcal{X}} \mathrm{Tr}[\mathcal{L}(Y_R)\,\bar{P}_S^x]\Theta_S^x = \sum_{x\in\mathcal{X}} \mathrm{Tr}[Y_R\,\mathcal{L}^*(\bar{P}_S^x)]\Theta_S^x = \sum_{x\in\mathcal{X}} \mathrm{Tr}[Y_R\,P_R^x]\Theta_S^x = \\
&= \sum_{x\in\mathcal{X}} \lambda_x \Theta_S^x,
\end{aligned}
$$

где $\lambda_x \in \mathbb{R}$, т.е. оператор $\mathcal{L}(Y_R)$ также эрмитов. Следовательно, определенное таким образом линейное отображение $\mathcal{L}$ эрмитово и сохраняет след. Остается только показать, что $\mathcal{N}' = \mathcal{L}\circ\mathcal{N}$ и что $\mathcal{L}$ – корректно определенный статистический морфизм отображения $\mathcal{N}$.

Чтобы показать, что $\mathcal{N}' = \mathcal{L}\circ\mathcal{N}$, заметим, что условие (2) можно переформулировать следующим образом: для любого $\rho_Q \in \mathrm{S}(\mathcal{H}_Q)$ и любого $x \in \mathcal{X}$ выполнено

$$
\mathrm{Tr}[\mathcal{N}'(\rho_Q)\,\bar{P}_S^x] = \mathrm{Tr}[\mathcal{N}(\rho_Q)\,P_R^x] = \mathrm{Tr}[\mathcal{N}(\rho_Q)\,\mathcal{L}^*(\bar{P}_S^x)] = \mathrm{Tr}[(\mathcal{L}\circ\mathcal{N})(\rho_Q)\,\bar{P}_S^x].
$$

Так как мера $\{\bar{P}_S^x : x \in \mathcal{X}\}$ в этом выражении информационно полная, то $\mathcal{N}'(\rho_Q) = (\mathcal{L}\circ\mathcal{N})(\rho_Q)$ для всех ρ_Q, т.е. $\mathcal{N}' = \mathcal{L}\circ\mathcal{N}$. Таким образом мы также установили, что из условия (2) автоматически следует, что $\mathcal{L}$ – корректно определенный статистический морфизм. ▲

Другими словами, предложение 1 утверждает, что замены H на $H_{\min}$ в определении 4 достаточно для установления *деградируемости в слабой форме* в том смысле, что деградирующее отображение – не квантовый канал, а эрмитов сохраняющий след статистический морфизм. В дальнейшим мы увидим, в каком случае можно утверждать, что деградирующее отображение действительно является вполне положительным и сохраняющим след.

Однако прежде чем приступить к этому, уточним предложение 1 для случая cq-каналов, которые всегда можно рассматривать как вполне положительные сохраняющие след отображения на коммутирующих входных подалгебрах. Начнем со следующего упрощения определения статистического морфизма (это первоначальное определение, данное в [15]).

Определение 6. Для cq-канала $\mathcal{E}\colon \mathcal{X} \to \mathrm{S}(\mathcal{H}_R)$, где $\mathcal{E} = \{\sigma_R^x : x \in \mathcal{X}\}$, *статистическим морфизмом* $\mathcal{E}$ называется линейное отображение $\mathcal{L}\colon \mathrm{L}(\mathcal{H}_R) \to \mathrm{L}(\mathcal{H}_S)$, такое что для любого $\mathcal{Y}$ и любой ПОЗМ $\{\bar{P}_S^y : y \in \mathcal{Y}\}$ существует соответствующая ПОЗМ $\{P_R^y : y \in \mathcal{Y}\}$, такая что $\mathrm{Tr}[\mathcal{L}(\sigma_R^x)\,\bar{P}_S^y] = \mathrm{Tr}[\sigma_R^x\, P_R^y]$.

Замечание 3. Отметим, что для того чтобы $\mathcal{L}$ было корректно определенным статистическим морфизмом $\mathcal{E}$, недостаточно того, что $\mathcal{L}(\sigma_R^x) \in \mathrm{S}(\mathcal{H}_S)$ для всех $x \in \mathcal{X}$. В частности, такое отображение не является, вообще говоря, положительным на всем $\mathrm{span}\{\sigma_R^x : x \in \mathcal{X}\}$. Подробнее см. также в замечании 1.

Предложение 2. *Для cq-каналов* $\mathcal{E}\colon \mathcal{X} \to \mathrm{S}(\mathcal{H}_R)$ *и* $\mathcal{E}'\colon \mathcal{X} \to \mathrm{S}(\mathcal{H}_S)$, *где* $\mathcal{E} = \{\sigma_R^x : x \in \mathcal{X}\}$ *и* $\mathcal{E}' = \{\tau_S^x : x \in \mathcal{X}\}$, *следующие утверждения эквивалентны*:

(i) *Для любой дискретной случайной величины* U, *любого распределения вероятностей* $q(u)$ *и любого классического канала* $q(x\,|\,u)$ *соответствующие cq-состояния входа-выхода*

$$\sigma_{UR} = \sum_{x\in\mathcal{X}}\sum_{u\in\mathcal{U}} q(u)q(x\,|\,u)|u\rangle\langle u|_U \otimes \sigma_R^x \quad и \quad \tau_{US} = \sum_{x\in\mathcal{X}}\sum_{u\in\mathcal{U}} q(u)q(x\,|\,u)|u\rangle\langle u|_U \otimes \tau_S^x$$

удовлетворяют неравенству

$$H_{\min}(U\,|\,R)_\sigma \leqslant H_{\min}(U\,|\,S)_\tau,$$

т.е. $P_{\mathrm{guess}}(U\,|\,R)_\sigma \geqslant P_{\mathrm{guess}}(U\,|\,S)_\tau$;

(ii) *Существует эрмитов сохраняющий след статистический морфизм канала* $\mathcal{E}$, *обозначаемый* $\mathcal{L}\colon \mathrm{L}(\mathcal{H}_R) \to \mathrm{L}(\mathcal{H}_S)$, *такой что*

$$\tau_S^x = \mathcal{L}(\sigma_R^x), \quad x \in \mathcal{X}.$$

§ 4. Первый результат о продолжении: полуклассический и классический случаи

Одним из достаточных условий того, что статистический морфизм можно продолжить до вполне положительного сохраняющего след отображения, состоит в том, что композиция отображений $\mathcal{L} \circ \mathcal{N}$ имеет коммутирующий выход.

Лемма 1. *Пусть* $\mathcal{L}\colon \mathrm{L}(\mathcal{H}_R) \to \mathrm{L}(\mathcal{H}_S)$ – *статистический морфизм данного канала* $\mathcal{N} \in \mathrm{C}(\mathcal{H}_Q, \mathcal{H}_R)$. *Если*

$$\big[(\mathcal{L}\circ\mathcal{N})(\rho)\,(\mathcal{L}\circ\mathcal{N})(\sigma)\big] = 0$$

для всех $\rho, \sigma \in \mathrm{S}(\mathcal{H}_Q)$, *то существует вполне положительное сохраняющее след отображение* $\mathcal{T}\colon \mathrm{L}(\mathcal{H}_R) \to \mathrm{L}(\mathcal{H}_S)$, *такое что*

$$\mathcal{T}\circ\mathcal{N} = \mathcal{L}\circ\mathcal{N}.$$

Доказательство. Так как $\mathcal{L}$ – статистический морфизм $\mathcal{N}$, то согласно определению 5 для любой ПОЗМ $\{\bar{P}_S^x : x \in \mathcal{X}\}$ на $\mathcal{H}_S$ существует ПОЗМ $\{P_R^x : x \in \mathcal{X}\}$ на $\mathcal{H}_R$, такая что

$$\mathrm{Tr}[(\mathcal{L}\circ\mathcal{N})(\rho_Q)\,\bar{P}_S^x] = \mathrm{Tr}[\mathcal{N}(\rho_Q)\,\mathcal{L}^*(\bar{P}_S^x)] = \mathrm{Tr}[\mathcal{N}(\rho_Q)\,P_R^x]$$

для всех $\rho_Q \in \mathrm{S}(\mathcal{H}_Q)$. Для $\mathcal{X} = [1, d_S]$ обозначим через $\{|x\rangle : x \in \mathcal{X}\}$ ортонормированный базис в $\mathcal{H}_S$, одновременно диагонализирующий любой выход композиции $\mathcal{L} \circ \mathcal{N}$. (Такой базис существует, поскольку $[(\mathcal{L} \circ \mathcal{N})(\rho), (\mathcal{L} \circ \mathcal{N})(\sigma)] = 0$.) Выберем в последнем соотношении $\bar{P}_S^x = |x\rangle\langle x|_S$ и зададим линейное отображение $\mathcal{T} \colon \mathrm{L}(\mathcal{H}_R) \to \mathrm{L}(\mathcal{H}_S)$ равенством

$$\mathcal{T}(Z_R) \overset{\mathrm{def}}{=} \sum_{x \in \mathcal{X}} |x\rangle\langle x|_S \operatorname{Tr}[Z_R\, P_R^x]$$

для любого $Z_R \in \mathrm{L}(\mathcal{H}_R)$. По построению $\mathcal{T}$ – вполне положительное сохраняющее след отображение (действительно, это квантовый канал, разрушающий сцепленность). Более того, для всех $\rho_Q \in \mathrm{S}(\mathcal{H}_Q)$ справедливо

$$(\mathcal{T} \circ \mathcal{N})(\rho_Q) = \sum_{x \in \mathcal{X}} |x\rangle\langle x|_S \operatorname{Tr}[\mathcal{N}(\rho_Q)\, P_R^x] = \sum_{x \in \mathcal{X}} |x\rangle\langle x|_S \operatorname{Tr}[\mathcal{N}(\rho_Q)\, \mathcal{L}^*(|x\rangle\langle x|_S)] =$$

$$= \sum_{x \in \mathcal{X}} |x\rangle\langle x|_S \operatorname{Tr}[(\mathcal{L} \circ \mathcal{N})(\rho_Q)\, |x\rangle\langle x|_S] = (\mathcal{L} \circ \mathcal{N})(\rho_Q),$$

где последнее равенство следует из того, что все $\mathcal{N}'(\rho_Q)$ диагональны в базисе $\{|x\rangle\}$. ▲

Из леммы 1 и предложения 1 немедленно вытекает

Следствие 1. *Пусть $\mathcal{N} \in \mathrm{C}(\mathcal{H}_Q, \mathcal{H}_R)$ и $\mathcal{N}' \in \mathrm{C}(\mathcal{H}_Q, \mathcal{H}_S)$ – вполне положительные сохраняющие след отображения. Пусть, кроме того, $\mathcal{N}'$ – такое, что $[\mathcal{N}'(\rho), \mathcal{N}'(\sigma)] = 0$ для всех $\rho, \sigma \in \mathrm{S}(\mathcal{H}_Q)$. Тогда следующие утверждения эквивалентны*:

(i) *Для любой дискретной случайной величины U, любого распределения вероятностей $q(u)$ и любого cq-канала $\mathcal{E} = \{\rho_Q^u : u \in \mathcal{U}\}$ соответствующие cq-состояния входа-выхода*

$$\sigma_{UR} = \sum_{u \in \mathcal{U}} q(u) |u\rangle\langle u|_U \otimes \mathcal{N}_Q(\rho_Q^u) \quad \text{и} \quad \tau_{US} = \sum_{u \in \mathcal{U}} q(u) |u\rangle\langle u|_U \otimes \mathcal{N}'_Q(\rho_Q^u)$$

удовлетворяют неравенству

$$H_{\min}(U \,|\, R)_\sigma \leqslant H_{\min}(U \,|\, S)_\tau,$$

т.е. $P_{\text{guess}}(U \,|\, R)_\sigma \geqslant P_{\text{guess}}(U \,|\, S)_\tau$;

(ii) *$\mathcal{N}$ деградируемо в $\mathcal{N}'$, т.е. существует вполне положительное сохраняющее след отображение $\mathcal{T} \colon \mathrm{L}(\mathcal{H}_R) \to \mathrm{L}(\mathcal{H}_S)$, такое что*

$$\mathcal{N}' = \mathcal{T} \circ \mathcal{N}.$$

Вариант этого следствия для cq-каналов выглядит следующим образом.

Следствие 2. *Рассмотрим cq-каналы $\mathcal{E} \colon \mathcal{X} \to \mathrm{S}(\mathcal{H}_R)$ и $\mathcal{E}' \colon \mathcal{X} \to \mathrm{S}(\mathcal{H}_S)$, где $\mathcal{E} = \{\sigma_R^x : x \in \mathcal{X}\}$ и $\mathcal{E}' = \{\tau_S^x : x \in \mathcal{X}\}$. Пусть при этом $[\tau_S^x, \tau_S^{x'}] = 0$ для всех $x, x' \in \mathcal{X}$. Тогда следующие утверждения эквивалентны*:

(i) *Для любой дискретной случайной величины U, любого распределения вероятностей $q(u)$ и любого классического канала $q(x \,|\, u)$ соответствующие cq-состояния входа-выхода*

$$\sigma_{UR} = \sum_{x \in \mathcal{X}} \sum_{u \in \mathcal{U}} q(u) q(x \,|\, u) |u\rangle\langle u|_U \otimes \sigma_R^x \quad \text{и} \quad \tau_{US} = \sum_{x \in \mathcal{X}} \sum_{u \in \mathcal{U}} q(u) q(x \,|\, u) |u\rangle\langle u|_U \otimes \tau_S^x$$

удовлетворяют неравенству

$$H_{\min}(U \,|\, R)_\sigma \leqslant H_{\min}(U \,|\, S)_\tau,$$

т.е. $P_{\mathrm{guess}}(U\,|\,R)_\sigma \geqslant P_{\mathrm{guess}}(U\,|\,S)_\tau$;

(ii) *Канал* $\mathcal{E}$ *деградируем в* $\mathcal{E}'$, *т.е. существует вполне положительное сохраняющее след отображение* $\mathcal{T}\colon \mathrm{L}(\mathcal{H}_R) \to \mathrm{L}(\mathcal{H}_S)$, *такое что*

$$\tau_S^x = \mathcal{T}(\sigma_R^x), \quad x \in \mathcal{X}.$$

4.1. Классический случай. Если оба cq-канала имеют коммутирующий выход, результат можно сформулировать в чисто классических терминах следующим образом.

Следствие 3. *Для классических каналов с шумом* $p(y\,|\,x)$ *и* $p'(z\,|\,x)$ *следующие утверждения эквивалентны*:

(i) *Канал* p *деградируем в* p';

(ii) *Для любой дискретной случайной величины* U, *любого распределения вероятностей* $q(u)$ *и любого канала* $q(x\,|\,u)$ *совместные распределения вероятностей* $q(u)q(x\,|\,u)p(y\,|\,x)$ *и* $q(u)q(x\,|\,u)p'(z\,|\,x)$ *удовлетворяют неравенству*

$$H_{\min}(U\,|\,Y) \leqslant H_{\min}(U\,|\,Z).$$

Иными словами, заменяя H на $H_{\min}$ в определении 2, получаем, что соответствующее понятие “с меньшим шумом, чем” эквивалентно понятию “деградируемый в”. С другой стороны, напомним, что существуют каналы с меньшим шумом, не являющиеся деградируемыми [5]. Для удобства читателя дадим независимое доказательство следствия 3, не опирающиеся на вышеприведенный результат о статистических морфизмах квантовых каналов.

Доказательство следствия 3. Очевидно, что из утверждения (i) следует (ii). Пуст, наоборот, выполнено (ii). Это означает, что для любого совместного распределения вероятностей $q(x,u)$ верно

$$\max_d \sum_{x,y,u} q(x,u)p(y\,|\,x)d(u\,|\,y) \geqslant \max_{d'} \sum_{x,z,u} q(x,u)p'(z\,|\,x)d'(u\,|\,z),$$

где $d(u\,|\,y)$ и $d'(u\,|\,z)$ – стратегии угадывания, т.е. дискретные каналы с шумом $d\colon Y \to \widehat{U}$ и $d'\colon Z \to \widehat{U}$, которые приемник может оптимизировать для максимизации вероятности правильного угадывания $\Pr\{U = \widehat{U}\}$.

Теперь выберем случайную величину U с $\mathcal{U} = \mathcal{Z}$, будем обозначать ее состояния через z'. Также зафиксируем стратегию $d'(z'\,|\,z) = \delta_{z',z}$. Тогда для любого $q(x,z')$ существует канал $d(z'\,|\,y)$, такой что

$$\sum_{x,z'} q(x,z')\biggl(\sum_z p'(z\,|\,x)d'(z\,|\,z') - \sum_y p(y\,|\,x)d(z'\,|\,y)\biggr) =$$
$$= \sum_{x,z'} q(x,z')\biggl(p'(z'\,|\,x) - \sum_y p(y\,|\,x)d(z'\,|\,y)\biggr) \leqslant 0,$$

что равносильно

$$\max_q \min_d \biggl\{\sum_{x,z'} q(x,z')\biggl(p'(z'\,|\,x) - \sum_y p(y\,|\,x)d(z'\,|\,y)\biggr)\biggr\} \leqslant 0.$$

По теореме о минимаксе (в нашем случае см. [11, лемма 4.13]) можно изменить порядок оптимизации:

$$\min_d \max_q \biggl\{\sum_{x,z'} q(x,z')\biggl(p'(z'\,|\,x) - \sum_y p(y\,|\,x)d(z'\,|\,y)\biggr)\biggr\} \leqslant 0.$$

Обозначим через $\Delta(x,z')$ разность $p'(z'\,|\,x)-\sum\limits_y p(y\,|\,x)d(z'\,|\,y)$ и заметим, что поскольку $\sum\limits_{x,z'}\Delta(x,z')=0$, с необходимостью имеем $\max\limits_{x,z'}\Delta(x,z')\geqslant 0$, ибо в противном случае $\sum\limits_{x,z'}\Delta(x,z') < 0$. Следовательно,

$$\min_d \max_q\Biggl\{\sum_{x,z'} q(x,z')\biggl(p'(z'\,|\,x)-\sum_y p(y\,|\,x)d(z'\,|\,y)\biggr)\Biggr\}=\min_d \max_{x,z'}\Delta(x,z'),$$

т.е. максимум достигается, когда распределение вероятностей $q(x,z')$ сконцентрировано в одном наибольшем значении. Тогда получаем

$$\min_d \max_{x,z'}\Delta(x,z')=0,$$

откуда вытекает существование канала $d(z'\,|\,y)$, такого что

$$\sum_y p(y\,|\,x)d(z'\,|\,y)=p'(z'\,|\,x),\quad \forall x,z',$$

т.е. канал p деградируем в p', что и требовалось. ▲

Главным достоинством этого доказательства по сравнению с доказательством в общем случае является то, что его легко обобщить на аппроксимативный случай – когда существует $\varepsilon\geqslant 0$, такое что для любой случайной величины U и любого совместного распределения вероятностей $q(x,u)$ справедливо

$$P_{\rm guess}(U\,|\,Y)\geqslant P_{\rm guess}(U\,|\,Z)-\varepsilon.$$

Этот случай рассмотрен в Приложении.

§ 5. Второй результат о продолжении: полностью квантовый случай

Лемма 2. *Пусть заданы вполне положительное сохраняющее след отображения* $\mathcal{N}\colon \mathrm{L}(\mathcal{H}_Q)\to \mathrm{L}(\mathcal{H}_R)$ *и линейное отображение* $\mathcal{L}\colon \mathrm{L}(\mathcal{H}_R)\to \mathrm{L}(\mathcal{H}_S)$. *Пусть* $\mathcal{H}_{S'}\cong\mathcal{H}_S$, *и предположим, что* $(\mathrm{id}_{S'}\otimes\mathcal{L})$ *– статистический морфизм отображения* $(\mathrm{id}_{S'}\otimes\mathcal{N})$. *Тогда существует вполне положительное сохраняющее след отображение* $\mathcal{T}\colon \mathrm{L}(\mathcal{H}_R)\to\mathrm{L}(\mathcal{H}_S)$, *такое что*

$$\mathcal{T}\circ\mathcal{N}=\mathcal{L}\circ\mathcal{N}.$$

Доказательство. Так как $(\mathrm{id}_{S'}\otimes\mathcal{L})$ – статистический морфизм $(\mathrm{id}_{S'}\otimes\mathcal{N})$, то согласно определению 5 для любой ПОЗМ $\{\bar P^x_{S'S} : x\in\mathcal{X}\}$ на $\mathcal{H}_{S'}\otimes\mathcal{H}_S\cong\mathcal{H}_S^{\otimes 2}$ существует ПОЗМ $\{P^x_{S'R} : x\in\mathcal{X}\}$ на $\mathcal{H}_{S'}\otimes\mathcal{H}_R$, такая что

$$\mathrm{Tr}\bigl[\{\omega_{S'}\otimes(\mathcal{L}\circ\mathcal{N})(\rho_Q)\}\,\bar P^x_{S'S}\bigr]=\mathrm{Tr}\bigl[\{\omega_{S'}\otimes(\mathcal{N})(\rho_Q)\}\,P^x_{S'R}\bigr]$$

для всех $x\in\mathcal{X}$, всех $\omega_{S'}\in\mathrm{S}(\mathcal{H}_{S'})$ и всех $\rho_Q\in\mathrm{S}(\mathcal{H}_Q)$. По линейности это означает, что

$$\begin{aligned}&\mathrm{Tr}_{S'S}\bigl[\{\Phi^+_{S''S'}\otimes(\mathcal{L}\circ\mathcal{N})(\rho_Q)\}\,\{\mathbb{1}_{S''}\otimes\bar P^x_{S'S}\}\bigr]=\\&=\mathrm{Tr}_{S'R}\bigl[\{\Phi^+_{S''S'}\otimes(\mathcal{N})(\rho_Q)\}\,\{\mathbb{1}_{S''}\otimes P^x_{S'R}\}\bigr]\end{aligned}\tag{3}$$

для всех $x\in\mathcal{X}$ и всех $\rho_Q\in\mathrm{S}(\mathcal{H}_Q)$, где $\Phi^+_{S''S'}=d_S\sum\limits_{i,j=1}^{d_S}|i_{S''}\rangle|i_{S'}\rangle\langle j_{S''}|\langle j_{S'}|$ – максимально сцепленное состояние из $\mathrm{S}(\mathcal{H}_{S''}\otimes\mathcal{H}_{S'})\cong\mathrm{S}(\mathcal{H}_S^{\otimes 2})$.

Из протокола обобщенной телепортации [21] вытекает единственность ПОЗМ $\{B^x_{S''S'} : x \in \mathcal{X}\}$ и унитарных операторов $\{U^x_{S''\to S} : x \in \mathcal{X}\}$, таких что

$$(\mathcal{L} \circ \mathcal{N})(\rho_Q) = \sum_{x\in\mathcal{X}} U^x_{S''\to S} \operatorname{Tr}_{S'S}\bigl[\{\Phi^+_{S''S'} \otimes (\mathcal{L}\circ\mathcal{N})(\rho_Q)\}\,\{\mathbb{1}_{S''} \otimes B^x_{S'S}\}\bigr](U^x_{S''\to S})^\dagger$$

для всех $\rho_Q \in \mathrm{S}(\mathcal{H}_Q)$. Тогда из (3) следует единственность ПОЗМ $\{P^x_{S'R} : x \in \mathcal{X}\}$ на $\mathcal{H}_{S'} \otimes \mathcal{H}_R$, такой что

$$(\mathcal{L} \circ \mathcal{N})(\rho_Q) = \sum_{x\in\mathcal{X}} U^x_{S''\to S} \operatorname{Tr}_{S'R}\bigl[\{\Phi^+_{S''S'} \otimes (\mathcal{N})(\rho_Q)\}\,\{\mathbb{1}_{S''} \otimes P^x_{S'R}\}\bigr](U^x_{S''\to S})^\dagger$$

для всех $\rho_Q \in \mathrm{S}(\mathcal{H}_Q)$. Чтобы доказать это утверждение, определим отображение $\mathcal{T}\colon \mathrm{L}(\mathcal{H}_R) \to \mathrm{L}(\mathcal{H}_S)$ как

$$\mathcal{T}(Z_R) \stackrel{\text{def}}{=} \sum_{x\in\mathcal{X}} U^x_{S''\to S} \operatorname{Tr}_{S'R}\bigl[\{\Phi^+_{S''S'} \otimes Z_R\}\,\{\mathbb{1}_{S''} \otimes P^x_{S'R}\}\bigr](U^x_{S''\to S})^\dagger$$

и заметим, что $\mathcal{T}$, будучи в некотором роде "телепортацией с шумом", действительно является вполне положительным сохраняющим след отображением, что и требовалось. ▲

На самом деле, повторяя рассуждения из [15], нетрудно показать, что условие леммы 2 можно несколько ослабить следующим образом: вместо предположения, что $(\mathrm{id}_{S'} \otimes \mathcal{L})$ – статистический морфизм отображения $(\mathrm{id}_{S'} \otimes \mathcal{N})$, можно предполагать, что $(\mathrm{id}_{S'} \otimes \mathcal{L})$ – статистический морфизм $(\mathcal{D}_{S'} \otimes \mathcal{N})$, где $\mathcal{D}\colon \mathrm{L}(\mathcal{H}_{S'}) \to \mathrm{L}(\mathcal{H}_{S'})$ – некоторое обратимое вполне положительное сохраняющее след отображение в том смысле, что $\mathcal{D}(\mathrm{L}(\mathcal{H}_{S'})) = \mathrm{L}(\mathcal{H}_{S'})$. (Например, канал $\mathcal{D}(\rho) = p\rho + (1-p)\mathbb{1}/d$ обратим, когда $p > 0$.)

Из леммы 2 и предложения 1 немедленно вытекает

С л е д с т в и е 4. *Пусть $\mathcal{N}\colon \mathrm{L}(\mathcal{H}_Q) \to \mathrm{L}(\mathcal{H}_R)$ и $\mathcal{N}'\colon \mathrm{L}(\mathcal{H}_Q) \to \mathrm{L}(\mathcal{H}_S)$ – вполне положительные сохраняющие след отображения. Пусть $\mathcal{H}_{S'}$ – вспомогательное гильбертово пространство, такое что $\mathcal{H}_{S'} \cong \mathcal{H}_S$. Следующие утверждения эквивалентны:*

(i) *Для любой дискретной случайной величины U, любого распределения вероятностей $q(u)$ и любого cq-канала $\mathcal{E} = \{\rho^u_{S'Q} : u \in \mathcal{U}\}$ соответствующие cq-состояния входа-выхода*

$$\sigma_{US'R} = \sum_{u\in\mathcal{U}} q(u)|u\rangle\langle u|_U \otimes (\mathrm{id}_{S'} \otimes \mathcal{N}_Q)(\rho^u_{S'Q})$$

и

$$\tau_{US'S} = \sum_{u\in\mathcal{U}} q(u)|u\rangle\langle u|_U \otimes (\mathrm{id}_{S'} \otimes \mathcal{N}'_Q)(\rho^u_{S'Q})$$

удовлетворяют неравенству

$$H_{\min}(U\,|\,S'R)_\sigma \leqslant H_{\min}(U\,|\,S'S)_\tau,$$

т.е. $P_{\mathrm{guess}}(U\,|\,S'R)_\sigma \geqslant P_{\mathrm{guess}}(U\,|\,S'S)_\tau$;

(ii) *Отображение $\mathcal{N}$ деградируемо в $\mathcal{N}'$, т.е. существует вполне положительное сохраняющее след отображение $\mathcal{T}\colon \mathrm{L}(\mathcal{H}_R) \to \mathrm{L}(\mathcal{H}_S)$, такое что*

$$\mathcal{N}' = \mathcal{T} \circ \mathcal{N}.$$

Для случая cq-каналов получаем

Следствие 5. *Рассмотрим cq-каналы* $\mathcal{E}\colon \mathcal{X} \to \mathrm{S}(\mathcal{H}_R)$ *и* $\mathcal{E}'\colon \mathcal{X} \to \mathrm{S}(\mathcal{H}_S)$, *где* $\mathcal{E} = \{\sigma_R^x : x \in \mathcal{X}\}$ *и* $\mathcal{E}' = \{\tau_S^x : x \in \mathcal{X}\}$. *Введем вспомогательное гильбертово пространство* $\mathcal{H}_{S'} \cong \mathcal{H}_S$, *и пусть* $\mathcal{E}''\colon \mathcal{Y} \to \mathrm{S}(\mathcal{H}_{S'})$ *– cq-канал с* $\mathcal{E}'' = \{\omega_{S'}^y : y \in \mathcal{Y}\}$, *такой что* $\mathrm{span}\{\omega_{S'}^y : y \in \mathcal{Y}\} = \mathrm{L}(\mathcal{H}_{S'})$. *Тогда следующие утверждения эквивалентны*:

(i) *Для любой дискретной случайной величины* U, *любого распределения вероятностей* $q(u)$ *и любого классического канала* $q(y, x \,|\, u)$ *соответствующие cq-состояния входа-выхода*

$$\sigma_{US'R} = \sum_{y\in\mathcal{Y}}\sum_{x\in\mathcal{X}}\sum_{u\in\mathcal{U}} q(u)q(y,x\,|\,u)|u\rangle\langle u|_U \otimes \omega_{S'}^y \otimes \sigma_R^x$$

и

$$\tau_{US'S} = \sum_{y\in\mathcal{Y}}\sum_{x\in\mathcal{X}}\sum_{u\in\mathcal{U}} q(u)q(x\,|\,u)|u\rangle\langle u|_U \otimes \omega_{S'}^y \otimes \tau_S^x$$

удовлетворяют неравенству

$$H_{\min}(U\,|\,S'R)_\sigma \leqslant H_{\min}(U\,|\,S'S)_\tau,$$

т.е. $P_{\mathrm{guess}}(U\,|\,S'R)_\sigma \geqslant P_{\mathrm{guess}}(U\,|\,S'S)_\tau$;

(ii) *Канал* $\mathcal{E}$ *деградируем в* $\mathcal{E}'$, *т.е. существует вполне положительное сохраняющее след отображение* $\mathcal{T}\colon \mathrm{L}(\mathcal{H}_R) \to \mathrm{L}(\mathcal{H}_S)$, *такое что*

$$\tau_S^x = \mathcal{T}(\sigma_R^x), \quad x \in \mathcal{X}.$$

§ 6. Заключение

В статье описана взаимосвязь между теорией статистического сравнения и сравнения каналов с шумом, отличная от рассмотренной в [22]. В частности, показано, как определения 1 и 2 становятся полностью эквивалентными при замене H на $H_{\min}$ в определении 2.

Доказанный результат можно рассматривать как *обращение* леммы об обработке данных: монотонное возрастание информации (измеряемой здесь величиной $H_{\min}$ или, что эквивалентно, величиной P_{guess}) не только необходимо, но и *достаточно* для существования отображения постобработки (сохраняющего след статистического морфизма в общем случае, но мы видели, как дополнительные предположения могут привести к существованию вполне положительного сохраняющего след отображения постобработки).

Как уже отмечалось автором в других работах [17, 23–25], это подход, основанный на теории статистического сравнения, предположительно может играть важную роль в понимании особенности процессов без памяти как теоретико-информационного аналога адиабатических процессов в термодинамике.

ПРИЛОЖЕНИЕ
КЛАССИЧЕСКИЙ СЛУЧАЙ: АППРОКСИМАТИВНАЯ ВЕРСИЯ

В предположении, что

$$P_{\mathrm{guess}}(U\,|\,Y) \geqslant P_{\mathrm{guess}}(U\,|\,Z) - \varepsilon, \quad \varepsilon \geqslant 0,$$

доказательство следствия 3 остается неизменным до того момента, пока не будет доказано неравенство

$$\min_d \max_{x,z'} \Delta(x, z') \leqslant \varepsilon. \tag{4}$$

После этого теперь рассмотрим следующую величину:

$$\max_x \sum_{z'} |\Delta(x, z')|. \tag{5}$$

Эта величина – расстояние, заданное индуцированной ℓ_1-нормой[3], между каналом $p'(z' \,|\, x)$ и деградированным каналом $\sum\limits_y p(y \,|\, x) d(z' \,|\, y)$. Поскольку для всех x выполняется $\sum\limits_{z'} \Delta(x, z') = 0$, имеем

$$\sum_{z'} |\Delta(x, z')| = 2 \sum_{z' \colon \Delta(x,z') \geqslant 0} \Delta(x, z'), \quad \forall x \in \mathcal{X},$$

откуда следует, что для стратегии d, на которой достигается левая часть в (4), справедливо

$$\sum_{z'} |\Delta(x, z')| \leqslant 2|\mathcal{X}| \max_{x,z'} \Delta(x, z') \leqslant 2|\mathcal{X}|\varepsilon, \quad \forall x \in \mathcal{X}.$$

В частности,

$$\max_x \sum_{z'} \left| p'(z' \,|\, x) - \sum_y p(y \,|\, x) d(z' \,|\, y) \right| \leqslant 2|\mathcal{X}|\varepsilon.$$

Обобщим вышесказанное в следующем утверждении.

С л е д с т в и е 6. *Для классических каналов с шумом $p(y \,|\, x)$ и $p'(z \,|\, x)$ и для $\varepsilon \geqslant 0$ предположим, что для любой дискретной случайной величины U, любого распределения вероятностей $q(u)$ и любого канала $q(x \,|\, u)$ совместные распределения вероятностей $q(u)q(x \,|\, u)p(y \,|\, x)$ и $q(u)q(x \,|\, u)p'(z \,|\, x)$ удовлетворяют неравенству*

$$2^{-H_{\min}(U \,|\, Y)} \geqslant 2^{-H_{\min}(U \,|\, Z)} - \varepsilon.$$

Тогда существует деградируемый канал $d(z \,|\, y)$, такой что

$$\max_x \sum_{z} \left| p'(z \,|\, x) - \sum_y p(y \,|\, x) d(z \,|\, y) \right| \leqslant 2|\mathcal{X}|\varepsilon.$$

СПИСОК ЛИТЕРАТУРЫ

1. *Wilde M.M.* Quantum Information Theory. Cambridge, UK: Cambridge Univ. Press, 2013.
2. *Cohen J.E., Kemperman J.H.B., Zbăganu G.* Comparisons of Stochastic Matrices, with Applications in Information Theory, Statistics, Economics, and Population Sciences. Boston: Birkhäuser, 1998.
3. *König R., Renner R., Schaffner C.* The Operational Meaning of Min- and Max-Entropy // IEEE Trans. Inform. Theory. 2009. V. 55. № 9. P. 4337–4347.
4. *Bergmans P.P.* Random Coding Theorem for Broadcast Channels with Degraded Components // IEEE Trans. Inform. Theory. 1973. V. 19. № 2. P. 197–207.

[3] Справедливо равенство (см., например, [26, пример 5.6.4])

$$\max_x \sum_{z'} |\Delta(x, z')| = \max_x \sum_{z'} \left| p'(z' \,|\, x) - \sum_y p(y \,|\, x) d(z' \,|\, y) \right| \stackrel{\mathrm{def}}{=} |||p' - dp|||_1,$$

где $|||A|||_1 \stackrel{\mathrm{def}}{=} \max\limits_{v \colon \|v\|_1 = 1} \|Av\|_1$ – *норма по вариации.* Величина (5) показывает, насколько хорошо статистически различимы $p'(z \,|\, x)$ и $\sum\limits_y p(y \,|\, x) d(y \,|\, z)$.

5. *Körner J., Marton K.* Comparison of Two Noisy Channels // Topics in Information Theory (2nd Colloq., Keszthely, Hungary, 1975). Colloq. Math. Soc. Janos Bolyai. V. 16. Amsterdam: North-Holland, 1977. P. 411–423.
6. *El Gamal A.A.* Broadcast Channels with and without Feedback // Proc. 11th Asilomar Conference on Circuits, Systems and Computers. Pacific Grove, CA. November 7–9, 1977. P. 180–183.
7. *Csiszár I., Körner J.* Information Theory: Coding Theorems for Discrete Memoryless Systems. Cambridge: Cambridge Univ. Press, 2011.
8. *Watanabe S.* Private and Quantum Capacities of More Capable and Less Noisy Quantum Channels // Phys. Rev. A. 2012. V. 85. № 1. P. 012326.
9. *Blackwell D.* Equivalent Comparisons of Experiments // Ann. Math. Statist. 1953. V. 24. № 2. P. 265–272.
10. *Torgersen E.N.* Comparison of Statistical Experiments. Cambridge: Cambridge Univ. Press, 1991.
11. *Liese F., Miescke K.-J.* Statistical Decision Theory: Estimation, Testing, and Selection. New York: Springer, 2008.
12. *Buscemi F., Keyl M., D'Ariano G.M., Perinotti P., Werner R.F.* Clean Positive Operator Valued Measures // J. Math. Phys. 2005. V. 46. № 8. P. 82109.
13. *Shmaya E.* Comparison of Information Structures and Completely Positive Maps // J. Phys. A. 2005. V. 38. № 44. P. 9717–9727.
14. *Chefles A.* The Quantum Blackwell Theorem and Minimum Error State Discrimination // `arXiv:0907.0866v4 [quant-ph]`, 2009.
15. *Buscemi F.* Comparison of Quantum Statistical Models: Equivalent Conditions for Sufficiency // Comm. Math. Phys. 2012. V. 310. № 3. P. 625–647.
16. *Buscemi F., Datta N., Strelchuk S.* Game-Theoretic Characterization of Antidegradable Channels // J. Math. Phys. 2014. V. 55. № 9. P. 092202.
17. *Buscemi F., Datta N.* Equivalence between Divisibility and Monotonic Decrease of Information in Classical and Quantum Stochastic Processes // Phys. Rev. A. 2016. V. 93. № 1. P. 012101.
18. *Matsumoto K.* An Example of a Quantum Statistical Model Which Cannot Be Mapped to a Less Informative One by Any Trace Preserving Positive Map // `arXiv:1409.5658 [quant-ph, math.ST]`, 2014.
19. *Heinosaari T., Jivulescu M.A., Reeb D., Wolf M.M.* Extending Quantum Operations // J. Math. Phys. 2012. V. 53. № 10. P. 102208.
20. *Jenčová A.* Comparison of Quantum Binary Experiments // Rep. Math. Phys. 2012. V. 70. № 2. P. 237–249.
21. *Braunstein S.L., D'Ariano G.M., Milburn G.J., Sacchi M.F.* Universal Teleportation with a Twist // Phys. Rev. Lett. 2000. V. 84. № 15. P. 3486–3489.
22. *Raginsky M.* Shannon Meets Blackwell and Le Cam: Channels, Codes, and Statistical Experiments // Proc. 2011 IEEE Int. Sympos. on Information Theory (ISIT'2011). St. Petersburg, Russia. July 31 – Aug. 5, 2011. P. 1220–1224.
23. *Buscemi F.* All Entangled Quantum States are Nonlocal // Phys. Rev. Lett. 2012. V. 108. № 20. P. 200401.
24. *Buscemi F.* Complete Positivity, Markovianity, and the Quantum Data-Processing Inequality, in the Presence of Initial System-Environment Correlations // Phys. Rev. Lett. 2014. V. 113. № 14. P. 140502.
25. *Buscemi F.* Fully Quantum Second-Law–like Statements from the Theory of Statistical Comparisons // `arXiv:1505.00535 [quant-ph]`, 2014.
26. *Horn R.A., Johnson C.R.* Matrix Analysis. Cambridge: Cambridge Univ. Press, 2013.

Бушеми Франческо
Отделение компьютерных наук и математической информатики,
Нагойский университет, Япония
`buscemi@is.nagoya-u.ac.jp`

Поступила в редакцию
09.02.2016