Доказательство гипотезы о квантовых гауссовских оптимизаторах

А. С. Холево
Математический институт им. В. А. Стеклова, Москва

Резюме

Дано решение, в позитивном смысле, проблемы квантовых гауссовских оптимизаторов, возникшей в квантовой информатике более 15 лет назад: средствами некоммутативной теории вероятностей показано, что выпуклый функционал общего вида (включая энтропии фон Неймана, Реньи и нормы Шаттена), заданный на области значений гауссовского вполне положительного отображения (канала) на алгебре канонических коммутационных соотношений, достигает глобального экстремума на когерентных состояниях, причем когерентные состояния характеризуются этим свойством [1,2]. Этот результат позволил вычислить пропускные способности и описать оптимальные методы кодирования для математических моделей каналов связи, наиболее употребительных в квантовой информатике и квантовой оптике [3,4].

1. А. С. Холево, “Гауссовские оптимизаторы и проблема аддитивности в квантовой теории информации”, УМН,70:2(422) (2015), 141-180.

2. V. Giovannetti, A. S. Holevo, R. Garcia-Patron, “A solution of Gaussian optimizer conjecture for quantum channels”,Comm. Math. Phys., 334:3 (2015), 1553-1571.

3. A. Mari, V. Giovannetti, A. S. Holevo, “Quantum state majorization at the output of bosonic Gaussian channels”, Nature Communications, 5 (2014), 3826.

4. V. Giovannetti, R. Garcia-Patron, N. J. Cerf, A. S. Holevo, “Ultimate classical communication rates of quantum optical channels”, Nature Photonics, 8:10 (2014), 216.

В классическом (коммутативном) анализе известен принцип, который кратко формулируется следующим образом:

Гауссовские ядра имеют гауссовские максимизаторы

(Lieb 1990, основываясь на работах К.И.Бабенко, Beckner, Carlen и др.). Речь идет о том, что норма интегрального оператора из L_p в L_q с гауссовским ядром (при определенных ограничениях) достигается (только) на гауссовской функции. Проблема нетривиальна, поскольку речь идет о *максимуме* выпуклой функции; доказательства существенно опираются на мультипликативность классических L_p-норм и на характеризацию гауссовских функций.

Некоммутативным аналогом гауссовского интегрального оператора является бозонный гауссовский канал – вполне положительное отображение Φ состояний на алгебре канонических коммутационных соотношений, которое оставляет инвариантным множество гауссовских состояний. В цитированных работах найдено решение гипотезы о квантовых гауссовских оптимизаторах: показано, что *выпуклый функционал общего вида от* $\Phi[\rho]$ *достигает глобального максимума на чистых гауссовских (когерентных) состояниях* ρ, *причем когерентные состояния характеризуются этим свойством*.

Другими словами, спектр выходных состояний, отвечающих когерентным входным, *мажорирует* спектр любых других выходных состояний.

Попутно установлена *мультипликативность*, относительно тензорных произведений, некоммутативных L_p-норм (норм Шаттена), а также *аддитивность* выходных энтропий Реньи и фон Неймана гауссовского отображения Ф. Эти свойства á priori не выполняются для произвольных квантовых каналов, поэтому классические методы доказательства не допускают обобщения на некоммутативный случай.

Потребовался принципиально новый метод, эксплуатирующий полугрупповую структуру множества бозонных гауссовских каналов, а также специальные свойства спектров комплементарных каналов. Решение дано для калибровочно - ко(контра)вариантных каналов, согласованных с фиксированной комплексной структурой.

Бозонные гауссовские системы

Классическое фазовое пространство: $Z = \mathbb{C}^s$, рассматриваемое как $2s-$мерное вещественное симплектическое пространство с кососимметричной формой $2\mathrm{Im}\, z^* z'$.

Квантование Вейля задается унитарными операторами сдвигов $D(z) = \exp\left(\mathbf{a}^\dagger z - z^* \mathbf{a}\right)$, где $\mathbf{a}$ is вектор операторов уничтожения для s бозонных мод. Канонические коммутационные соотношения Вейля:

$$D(z)D(z') = \exp\left(-i\,\mathrm{Im}\, z^* z'\right) D(z+z').$$

Гауссовские состояния

Гауссовские калибровочно-ковариантные состояния задаются характеристическими функциями

$$\chi_\rho(z) \equiv \mathrm{Tr}\rho D(z) = \exp\left(-z^*\alpha z\right),$$

где α корреляционная матрица, $\alpha \geq I/2$.

Вакуумное состояние $|0\rangle\langle 0|$ соответствует $\alpha = I/2$.

Когерентные состояния $|z\rangle\langle z| = D(z)|0\rangle\langle 0|D(z)^*$.

Гауссовские каналы

Ковариантные каналы

$$\Phi : \chi_\rho(z) \to \chi_\rho(Kz) \exp\left(-z^* \mu z\right); \qquad \mu \geq \pm\frac{1}{2}\left(I - K^* K\right) \qquad (*)$$

Контравариантные каналы

$$\Phi : \chi_\rho(z) \to \chi_\rho(-\overline{Kz}) \exp\left(-z^* \mu z\right); \qquad \mu \geq \frac{1}{2}\left(I + K^* K\right) \qquad (**)$$

K задает изменение амплитуд, μ задает шум в канале.

Если μ минимальное решение неравенства, то канал *экстремален* в выпуклом множестве всех каналов.

Мажоризация

Теорема Пусть Φ гауссовский калибровочно-ковариантный или контравариантный канал, f вогнутая функция на $[0,1]$, $f(0)=0$, тогда для любого оператора плотности ρ

$$\mathrm{Tr} f(\Phi[\rho]) \geq \mathrm{Tr} f(\Phi[|z\rangle\langle z|]) = \mathrm{Tr} f(\Phi[|0\rangle\langle 0|]).$$

Если f строго вогнута и канал Φ таков, что K обратима, а неравенство (*) (соотв. (**)) строгое, то равенство достигается только если ρ когерентное состояние.

Эквивалентно, последовательность собственных чисел оператора плотности $\Phi[|z\rangle\langle z|]$ *мажорирует* соответствующую последовательность оператора $\Phi[\rho]$, для любого $\rho \in \mathfrak{S}(\mathcal{H})$.
Когерентный вход порождает *наименее хаотический* выход для “фазо-нечувствительных” бозонных гауссовских каналов.

Точные значения и аддитивность

Следствие Для $p > 1$ и любого гауссовского калибровочно-ко(контра)вариантного канала Φ, полагая $g(x) = (x+1)\log(x+1) - x\log x$, имеем

$$\min_{\rho} S(\Phi[\rho]) = \mathrm{tr} g(\mu + (K^*K - I)/2)$$

$$\|\Phi\|_{1\to p} = \left[\det\left[(\mu + K^*K/2 + I/2)^p - (\mu + K^*K/2 - I/2)^p\right]\right]^{-1/p}$$

Свойство мультипликативности для норм $\|\cdot\|_{1\to p}$, как и аддитивность минимальных энтропий Реньи и фон Неймана, выполняется для любой пары гауссовских калибровочно-ко (контра)вариантных каналов.
Следует из мажоризационной теоремы при $f(x) = -x^p$, $f(x) = -x\log x$, с использованием мультипликативности вакуума.

Классическая пропускная способность

Следствие Классическая пропускная способность с ограничением на входе канала Φ:

$$C(\Phi; F, E) = C_{\chi}(\Phi; F, E)$$

$$= \max_{\nu:\, \mathrm{tr}\nu\epsilon \leq E} \mathrm{tr}\, g(K^{*}\nu K + \mu + (K^{*}K - I)/2) - \mathrm{tr} g(\mu + (K^{*}K - I)/2),$$

где ϵ матрица энергии. Оптимальное кодирование задается ансамблем когерентных состояний $\rho_z = |z\rangle\langle z|$, с калибровочно-инвариантным гауссовским распределением на Z, с корреляционной матрицей ν, на которой достигается максимум в правой части.

Одна мода (квантовая формула Шеннона)

Все калибровочно-ковариантные каналы описываются формулой:

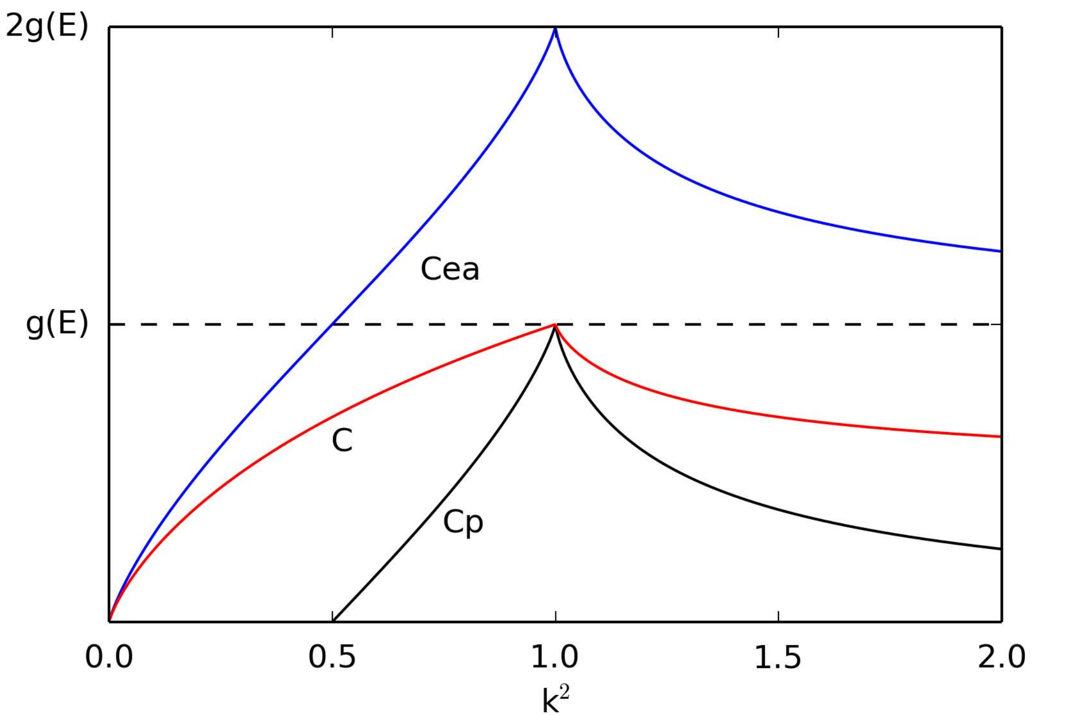
$$\Phi^*[D(z)] = D(kz) \exp\left[-\left(|k^2 - 1|/2 + N\right)|z|^2\right],$$

где $N \geq 0$ уровень шума, $k \geq 0$ коэффициент, соответствующий ослаблению ($k < 1$), усилению ($k > 1$), или классическому аддитивному шуму ($k = 1$). Во всех случаях минимальная выходная энтропия равна

$$\min_\rho S(\Phi[\rho]) = g(N'),$$

где $N' = N + \max\{k^2 - 1, 0\}$, а пропускная способность с ограничением на входе

$$C(\Phi; a^\dagger a, E) = C_\chi(\Phi; a^\dagger a, E) = g(k^2 E + N') - g(N').$$


2g(E)
g(E)
Cea
C
Cp
0.0
0.5
1.0
1.5
2.0
k²

Definition of channel

Channel is a linear completely positive trace-preserving map
$\Phi : \mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}(\mathcal{H}_B)$.

Complete positivity: $\Phi \otimes \mathrm{Id}_{(n)}$ positive for all $n = 1, 2, \ldots$

Channel = dynamical map = noncommutative Markov map

Composition of channels $\Phi_2 \circ \Phi_1$

Tensor product $\Phi_1 \otimes \Phi_2 = (\Phi_1 \otimes \mathrm{Id}_2) \circ (\mathrm{Id}_1 \otimes \Phi_2)$

Representations of CP maps

The **Stinespring representation** for CP maps of C*-algebras.

Corollary:
Let Φ:$\mathfrak{T}(\mathcal{H}_A) \mapsto \mathfrak{T}(\mathcal{H}_B)$ be a channel. There exist a Hilbert space $\mathcal{H}_E$ and an isometric operator $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$, such that

$$\Phi(\rho) = \mathrm{Tr}_E V \rho V^*; \quad \rho \in \mathfrak{T}\left(\mathcal{H}_A\right).$$

Complementary channel

$$\tilde{\Phi}(\rho) = \mathrm{Tr}_B V \rho V^*; \quad \rho \in \mathfrak{T}\left(\mathcal{H}_A\right).$$

Dilation to unitary dynamics of open quantum system interacting with environment.

The minimal output entropy

The von Neumann entropy $S(\rho) = -\mathrm{Tr}\rho \log \rho$ is nonnegative concave function of density operator ρ.

The minimal output entropy of the quantum channel Φ (purity of the output)

$$\check{S}(\Phi) = \inf_{\rho} S(\Phi(\rho)).$$

The *additivity conjecture* for the min-out entropy

$$\check{S}\,(\Phi_1 \otimes \Phi_2) \stackrel{?}{=} \check{S}\,(\Phi_1) + \check{S}\,(\Phi_2)\,.$$

$(1 \to p)-$Schatten norms and Rényi entropies

Related to multiplicativity of $(1 \to p)-$ *norms*

$$\|\Phi\|_{1\to p} = \sup_{\|X\|_1 \le 1} \|\Phi[X]\|_p = \sup_{\rho \in \mathfrak{S}(\mathcal{H})} \left(\mathrm{Tr}\Phi([\rho]^p)\right)^{1/p}$$

or additivity of the *minimal output Rényi entropy*

$$\check{R}_p(\Phi) = \inf_{\rho \in \mathfrak{S}(\mathcal{H})} R_p(\Phi[\rho]) = \frac{p}{1-p} \log \|\Phi\|_{1\to p}\,.$$

In finite dimensions $\lim_{p\downarrow 1} \check{R}_p(\Phi) = \check{S}(\Phi)$.

The χ–capacity

A noncommutative analog of the Shannon capacity:

$$C_\chi(\Phi) = \sup_\pi \left\{ S\left(\Phi\left[\bar{\rho}\right]\right) - \int_{\mathfrak{S}(\mathcal{H})} S(\Phi\left[\rho\right]))\pi(d\rho) \right\} \leq \sup_{\bar{\rho}} S\left(\Phi\left[\bar{\rho}\right]\right) - \check{S}(\Phi), \tag{1}$$

$\bar{\rho} = \int \rho\pi(d\rho)$, with possible input constraint on $\bar{\rho}$: $\mathrm{Tr}\bar{\rho}H \leq E$.

The basic *additivity conjecture* for χ-capacity:

$$C_\chi(\Phi_1 \otimes \Phi_2) \stackrel{?}{=} C_\chi(\Phi_1) + C_\chi(\Phi_2).$$

In the case of interest, the inequality in (1) becomes *equality*, implying *equivalence* of this to the additivity of the minimal output entropy $\check{S}(\Phi)$.

The classical capacity of quantum channel

The *classical capacity* of a quantum channel is defined as the maximal transmission rate per use of the channel, with coding and decoding chosen for increasing number n of independent uses of the channel

$$\Phi^{\otimes n} = \underbrace{\Phi \otimes \cdots \otimes \Phi}_{n}$$

such that the error probability goes to zero as $n \to \infty$.

HSW Theorem

$$C(\Phi) = \lim_{n\to\infty}(1/n)C_\chi(\Phi^{\otimes n}).$$

If the additivity holds, then $C(\Phi) = C_\chi(\Phi)$.

The global additivity is false

Theorem (Shor, 2004) The additivity of min-out entropy and capacity are globally equivalent: if one holds for all channels Φ_1, Φ_2, then the other also holds for all channels.

Hastings (2008) (following Winter, Hayden): **Additivity fails in very high dimensions**. Proof: large deviation and measure concentration techniques for operator-valued processes.

Szarek et al.: insight via **Dvoretzky-Mil'man's theorem** on almost spherical sections of high-dimensional convex bodies.

Bosonic Gaussian ($d = \infty$) channels? Present talk.

Application: Wehrl's conjecture

Berezin-Lieb inequality for quantum entropy $S(\rho) = -\,\mathrm{Tr}\rho \log \rho$:

$$\cdots \leq S(\rho) \leq -\int_{\mathbb{C}} \langle z|\rho|z\rangle \,\mathrm{log}\langle z|\rho|z\rangle \frac{d^2 z}{\pi} \equiv S_{cl}(\rho),$$

where $|z\rangle$ are Glauber's coherent vectors. Lieb (1978) used exact constants in the Hausdorff-Young inequality (Fourier transform) and Young inequality (convolution) to prove Wehrl's conjecture:

$S_{cl}(\rho)$ **is minimized by any coherent state** $\rho = |\zeta\rangle\langle\zeta|$.

Lieb and Solovej (2012): coherent states minimize *any* concave functional, not only the entropy (“majorization”).

Majorization for the output of Gaussian q-c channel

$\rho \to \langle z|\rho|z\rangle$ is a "quantum-classical Gaussian channel"
Wehrl entropy=output entropy, minimized by pure Gaussian ρ.

For any $c > 0$ consider "measure-prepare" channel

$$\Phi_c[\rho] = \int_{\mathbb{C}} \langle z|\rho|z\rangle |cz\rangle\langle cz| \frac{d^2 z}{\pi}.$$

This is Gaussian gauge-covariant channel, hence

$$\mathrm{Tr} f(\Phi_c[\rho]) \geq \mathrm{Tr} f(\Phi_c[|z\rangle\langle z|])$$

for all states ρ and any coherent state $|z\rangle\langle z|$. The majorization for Gaussian measurement is obtained by taking the limit $c \to \infty$ and showing that both sides of Berezin inequalities converge.

Idea of Proof of the Majorization Theorem

Lemma 1. Let Φ be gauge-covariant, then $\Phi = \mathcal{A} \circ \mathcal{B}$, where $\mathcal{A}$ is *extreme amplifier*

$$K_2^* K_2 \geq I, \qquad \mu = \frac{1}{2}\left(K_2^* K_2 - I\right),$$

and $\mathcal{B}$ is *extreme attenuator*

$$K_1^* K_1 \leq I, \qquad \mu = \frac{1}{2}\left(I - K_1^* K_1\right).$$

If (*) is strict and K invertible, then $0 < |K_1| < 1$, $|K_2| > 1$.
Similar result for gauge-contravariant channel.

Proof: Composition rules: $\quad K = K_1 K_2, \quad \mu = K_2^* \mu_1 K_2 + \mu_2.$

Additivity for complementary channels

Folklore, related to Schmidt decomposition. Let ρ_{AB} be pure state in $\mathcal{H}_A \otimes \mathcal{H}_B$, then partial states ρ_A, ρ_B have the same nonzero spectrum (notation: $\rho_A \sim \rho_B$), in particular, $S(\rho_A) = S(\rho_B)$.

Corollary. For complementary channels, $\Phi(P_\psi) \sim \tilde{\Phi}(P_\psi)$ for all ψ. Hence $\check{S}(\Phi) = \check{S}(\tilde{\Phi})$, and additivity of min-out entropy simultaneously holds or not for complementary channels.

The case of extreme amplifier

Lemma 2. For an extreme amplifier $\mathcal{A}$ there is an extreme attenuator $\mathcal{B}$ such that for all $\psi \in \mathcal{H}$

$$\mathcal{A}(P_\psi) \sim (\mathcal{A} \circ \mathcal{B})\,(P_\psi).$$

Proof:

$$\mathcal{A}(P_\psi) \sim \tilde{\mathcal{A}}(P_\psi) \sim \left(\mathsf{T} \circ \tilde{\mathcal{A}}\right)(P_\psi),$$

where T is the transposition: $\mathsf{T}\,(D(z)) = D(-\bar{z})$.

$\mathsf{T} \circ \tilde{\mathcal{A}}$ is gauge-covariant Gaussian channel.
Decomposition from Lemma 1 gives $\mathsf{T} \circ \tilde{\mathcal{A}} = \mathcal{A} \circ \mathcal{B}$.

End of proof of theorem

$$\mathrm{Tr} f\left(\mathcal{A}(P_\psi)\right) \overset{(L2)}{=} \mathrm{Tr} f\left(\left(\mathcal{A}\circ\mathcal{B}\right)\left(P_\psi\right)\right) \geq \sum_j p_j \mathrm{Tr} f\left(\mathcal{A}(P_{\psi_j})\right),$$

where $\mathcal{B}(P_\psi) = \sum_j p_j P_{\psi_j}$, $p_j > 0$. If ψ is a minimizer, then for strictly concave f , the states $\mathcal{A}(P_{\psi_j})$ all coincide implying $P_{\psi_j} = P_\phi$.

Lemma 3. Let $\mathcal{B}$ be an extreme attenuator with $0 < |K| < 1$. Then $\mathcal{B}(P_\psi) = P_\phi$ (pure state) iff P_ψ is a coherent state.

Thus $\min_\psi \mathrm{Tr} f\left(\mathcal{A}(P_\psi)\right) = \mathrm{Tr} f\left(\mathcal{A}(|z\rangle\langle z|)\right) = \mathrm{Tr} f\left(\mathcal{A}(|0\rangle\langle 0|)\right).$ $\square$