10 лет Российскому Научному Фонду

МИАН, 16.05.2024

Исследования по квантовой информатике в МИАНе, поддержанные РНФ

научный руководитель: академик РАН А.С.Холево

- квантовые системы и каналы бесконечной размерности и их характеристики
- нахождение пропускных способностей квантовых каналов определенных классов
- положительные операторнозначные меры
- нахождение соотношений между мерами нелокальности и мерами сцепленности
- квантовая криптография: анализ стойкости криптографических протоколов

Квантовые системы

Состояние ρ квантовой системы A – это положительный оператор в банаховом пространстве $\mathfrak{T}(\mathcal{H}_A)$ всех ядерных операторов в сепарабельном гильбертовом пространстве $\mathcal{H}_A$ с нормой $\|X\|_1 = \mathrm{Tr}|X|$.

Составная квантовая система AB описывается гильбертовым пространством $\mathcal{H}_{AB} \doteq \mathcal{H}_A \otimes \mathcal{H}_B$.

Для любого состояния ρ квантовой системы AB частичные состояния определяются формулами:

$$\rho_A = \mathrm{Tr}_{H_B}\rho \quad \text{и} \quad \rho_B = \mathrm{Tr}_{H_A}\rho$$

В состоянии $\rho \otimes \sigma$ ($\rho \in \mathfrak{S}(\mathcal{H}_A)$, $\sigma \in \mathfrak{S}(\mathcal{H}_B)$) системы A и B независимы

Квантовые каналы

Квантовый канал Φ из A в B – это линейное вполне положельное сохраняющее след отображение банахова пространства $\mathfrak{T}(\mathcal{H}_A)$ в банахово пространство $\mathfrak{T}(\mathcal{H}_B)$

полная положительность: $\Phi \otimes \mathrm{Id}_C(\rho) \geq 0$ для всех $\rho \in \mathfrak{S}(\mathcal{H}_{AC})$

Двойственный канал Φ^* – это линейное унитальное вполне положельное отображение из $\mathfrak{B}(\mathcal{H}_B)$ в $\mathfrak{B}(\mathcal{H}_A)$ такое, что

$$\mathrm{Tr}\, \Phi(\rho)B = \mathrm{Tr}\, \Phi^*(B)\rho \quad \forall \rho \in \mathfrak{T}(\mathcal{H}_A), B \in \mathfrak{B}(\mathcal{H}_B)$$

Унитарный канал: $\rho \mapsto U\rho U^*$, U – унитарный оператор

Любой квантовый канал Φ из A в B – редукция унитарного канала из AD в BE: для любого $\Phi : A \to B$ существуют системы D и E такие, что

$$\Phi(\rho) = \mathrm{Tr}_{\mathcal{H}_E}\widehat{\Phi}(\rho \otimes \sigma_0), \quad \rho \in \mathfrak{T}(\mathcal{H}_A), \quad \widehat{\Phi}(\omega) = U\omega U^*,$$

где σ_0 – состояние в $\mathfrak{S}(\mathcal{H}_D)$ и U – унитарный оператор из $\mathcal{H}_{AD}$ в $\mathcal{H}_{BE}$.

О видах сходимости бесконечномерных квантовых каналов

$\{\Phi_n\}$ – последовательность квантовых каналов из A и B.

$\{\Phi_n\}$ равномерно сходится к каналу Φ_0, если

$$\lim_{n\to+\infty} \sup_{\rho\in\mathfrak{S}(\mathcal{H}_A)} \|\Phi_n(\rho) - \Phi_0(\rho)\|_1 = 0.$$

в этом случае $\{\Phi_n\}$ – редукция равномерно сходящейся последовательности $\{\widehat{\Phi}_n\}$ унитарных каналов

$\{\Phi_n\}$ сильно сходится к каналу Φ_0, если

$$\lim_{n\to+\infty} \|\Phi_n(\rho) - \Phi_0(\rho)\|_1 = 0 \quad \forall\rho \in \mathfrak{S}(\mathcal{H}_A)$$

в этом случае $\{\Phi_n\}$ не всегда представима в виде редукции сильно сходящейся последовательности $\{\widehat{\Phi}_n\}$ унитарных каналов

$\{\Phi_n\}$ сильно-* сходится к каналу Φ_0, если $\{\Phi_n\}$ – это редукция некоторой сильно сходящейся последовательности $\{\widehat{\Phi}_n\}$ унитарных каналов

$\{\Phi_n\}$ сильно-* сходится к каналу Φ_0 тогда и только тогда, когда

$$s.o.\text{-}\lim_{n\to+\infty} \Phi_n^*(B) = \Phi_0^*(B) \quad \forall B \in \mathfrak{B}(\mathcal{H}_B)$$

$\{\Phi_n\}$ сильно сходится к каналу Φ_0 тогда и только тогда, когда

$$w.o.\text{-}\lim_{n\to+\infty} \Phi_n^*(B) = \Phi_0^*(B) \quad \forall B \in \mathfrak{B}(\mathcal{H}_B)$$

Цели исследований:

- нахождение достаточных условий сильной-* сходимости для сильно сходящихся последовательностей каналов;

- нахождение простых достаточных условий существования "предельной точки" у последовательности $\{\Phi_n\}$ относительно сильной сходимости;

- нахождение простых достаточных условий существования "предельной точки" у последовательности $\{\Phi_n\}$ относительно сильной-* сходимости.

Нахождение информационных характеристик квантовых каналов определенных классов

Квантовые теоремы кодирования:

- теорема Холево-Schumacher-Westmoreland (классическая пропускная способность)
- теорема Bennett-Shor-Smolin-Thapliyal (классическая пропускная способность с использованием сцепленности)
- теорема Lloyd-Devetak-Shor (квантовая пропускная способность)

Смешанные унитарные квантовые каналы имеют вид

$$\Phi(\rho) = \sum_{U \in \mathcal{U}} \pi_U U \rho U^*,$$

где $\mathcal{U}$ – конечная группа, состоящая из унитарных операторов в конечномерном гильбертовом пространстве H, а π_U – распределение вероятностей на группе $\mathcal{U}$.

Схемой квантовых вычислений называется последовательность действий над набором кубитов или кудитов. Каждое такое действие называется квантовым вентилем. Среди схем квантовых вычислений важное значение имеют клиффордовы схемы, осуществляемых специальным набором вентилей. Предполагается представление клиффордовых квантовых схем в виде действия некоторого квантового канала и исследование его информационных характеристик, в частности, пропускных способностей

Характеристики сцепленности и нелокальности многочастичного состояния. Нахождение соотношений между ними.

Сцепленность состояния $\omega \in \mathfrak{S}(\mathcal{H}_{AB})$ – непредставимость ω в виде выпуклой смеси состояний вида $\rho \otimes \sigma$

Нелокальность состояния $\omega \in \mathfrak{S}(\mathcal{H}_{AB})$ – нарушение этим состоянием одного из неравенств Белла, например, неравенства

$$|\mathbb{E}X_1Y_1 + \mathbb{E}X_1Y_2 + \mathbb{E}X_2Y_1 - \mathbb{E}X_2Y_2| \leq 2,$$

где X_1, X_2, Y_1, Y_2 – случайные величины на вероятностном пространстве $\{\Omega, \mathfrak{F}, \mathbb{P}\}$, принимающие значения в $[0, 1]$.

Атаки на протоколы квантовой криптографии

Полученные ранее результаты по постселективным преобразованиям квантовых состояний позволили построить атаку, демонстрирующую уязвимость практически используемого протокола KPK. В ней противник распоряжается таким ресурсом, как возможность блокировки состояний: для "неудобных"сигналов происходит блокировка, для "удобных-отправка на приёмную сторону. Взаимная информация передающей и подслушивающей стороны I_{AE}^{ps} зависит от возможности постселекции, и в скорости генерации ключа участвует именно она:

$$l_{\text{key}} = I_{AB} - I_{AE}^{\text{ps}}.$$

Планируется построение атаки на другую версию протокола с фазово-временным кодированием, которая использует

8 состояний вместо 4, поэтому более сложна для построения явных атак.

СПАСИБО ЗА ВНИМАНИЕ