Об информационном выигрыше при использовании коллективных измерений в квантовой информации

Д.А.Кронберг

Математический институт им. В.А.Стеклова РАН

26 ноября 2018 г

План доклада

- Квантовая теорема кодирования
- Индивидуальные и коллективные измерения
- Двойственность ансамблей квантовых состояний и квантовых наблюдаемых

Квантовая теорема кодирования

- В дальнейшем рассматриваем классически-квантовые (c-q) каналы, где каждому классическому входу соотвествует квантовое состояние на выходе. Для описания явления супераддитивности достаточно простейшего c-q-канала

$$0 \to |\psi_0\rangle,$$

$$1 \to |\psi_1\rangle,$$

где $\langle\psi_0|\psi_1\rangle = \kappa \in \mathbb{R}$.

- Квантовая теорема кодирования утверждает, что классическая взаимная информация передающей и принимающей стороны ограничена величиной Холево

$$\chi(\{\rho_i\},\{p_i\}) = H(\sum_i p_i\rho_i) - \sum_i p_i H(\rho_i), \tag{1}$$

которая для двух чистых равновероятных состояний равна

$$\chi(\{\psi_i\},\{\frac{1}{2},\frac{1}{2}\}) = h_2(\frac{1-\kappa}{2}). \tag{2}$$

Ситуация «хорошего» кода

- Более точно, квантовая теорема кодирования говорит, что для любого ε существует «хороший» код из 2^K кодовых слов $|w_k\rangle$ длины N, для которого скорость кода $R = \frac{K}{N} \approx C$, и наблюдаемая $\{M_k\}$, такие, что максимальная вероятность ошибки при измерении кодовых слов не превосходит ε.
- Скорость этого кода для больших N можно сделать сколь угодно близкой к пропускной способности канала C, однако превосходить пропускную способность скорость кода не может.
- Пропускная способность канала определяется как

$$C = \max_{\{p_i\}} \chi(\{\rho_i\}, \{p_i\}).$$

Важность коллективных измерений

- Чтобы при малой ошибке скорость кода была близка к пропускной способности, важно, чтобы наблюдаемая $\{M_k\}$ на приемной стороне не разлагалась на наблюдаемые, относящиеся к подсистемам.
- Если приемная сторона ограничена лишь индивидуальными измерениями, то максимальная пропускная способность дается пропускной способностью за один шаг C_1.
- Для двух равновероятных чистых состояний

$$C_1 = 1 - h_2(\frac{1}{2}(1 - \sqrt{1 - \kappa^2})).$$

Представление Стайнспринга для измерения

- Вероятность ошибки при оптимальном измерении двух чистых неортогональных состояний зависит от их скалярного произведения и равна

$$q = \frac{1}{2}(1 - \sqrt{1 - \kappa^2}),$$

- Оптимальным измерением является измерение в симметрично расположенном относительно векторов базисе, и его представление Стайнспринга записывается как

$$|0\rangle_A \otimes |\psi_0\rangle_B \to |0\rangle_A \otimes (\sqrt{1-q}|f_0\rangle_B \otimes |\mu_0\rangle_M + \sqrt{q}|f_1\rangle_B \otimes |\mu_1\rangle_M),$$

$$|1\rangle_A \otimes |\psi_1\rangle_B \to |1\rangle_A \otimes (\sqrt{q}|f_0\rangle_B \otimes |\mu_0\rangle_M + \sqrt{1-q}|f_1\rangle_B \otimes |\mu_1\rangle_M),$$

где $\{|0\rangle_A, |1\rangle_A\}$ – классические (т.е. взаимно ортогональные) сигналы Алисы, а $\{|\mu_0\rangle_M, |\mu_1\rangle_M\}$ – взаимно ортогональные состояния окружения, которое можно отождествить как измерительный прибор.

Представление Стайнспринга для индивидуального измерения

- Взаимная информация Алисы и Боба равна

$$I(A,B) = 1 - h_2(q).$$

- Второй член этой величины, $h_2(q)$, является мерой сцепленности системы Боба и его измерительного прибора M. Чем выше эта мера, тем больше ошибка, и тем меньше информация Боба о сигнале Алисы. При индивидуальных измерениях Боб теряет доступ к подпространству M и уже не может восстановить исходные состояния $\{|\psi_0\rangle, |\psi_1\rangle\}$ для проведения лучшего (т.е. коллективного) измерения. Боб имеет только классический сигнал i из состояния $|\mu_i\rangle$ в каждой позиции.

Представление Стайнспринга для «хорошего» кода

- Теперь рассмотрим схожую ситуацию для «хорошего» кода $\{|w_k\rangle\}$ с «хорошей» наблюдаемой $\{|m_k\rangle\}$, которые существуют согласно квантовой теореме кодирования. Для измерения состояний, соответствующих кодовым словам, представление Стайнспринга принимает вид

$$|k\rangle_A \otimes |w_k\rangle_B \to |k\rangle_A \otimes |w_k\rangle_B \otimes |m_k\rangle_M ,$$

  где k принимает целые значения от 1 до 2^K.

- Согласно квантовой теореме кодирования, состояния $\{|w_k\rangle\}$ могут быть различены с ошибкой близкой к нулю. Поэтому, мера сцепленности между Бобом и измерительным прибором равна нулю, и Боб не портит измерением кодовые слова. Это падение сцепленности по сравнению с индивидуальными измерениями, возможно, вызвано сцепленностью векторов наблюдаемой.

Ситуация для кода с повторением

- Можно рассмотреть конкретный код и посмотреть, как меняются вероятность ошибки при использовании индивидуальных и коллективных измерений
- Код с повторением длины N задается набором состояний

$$C = \{|w_0\rangle, |w_1\rangle\} = \{|\psi_0\rangle^{\otimes N}, |\psi_1\rangle^{\otimes N}\}. \tag{3}$$

Здесь $\langle w_0|w_1\rangle = \kappa^N$. $|w_0\rangle$ и $|w_1\rangle$ – неортогональные состояния, и легко найти наблюдаемую для их оптимального различения.

Субоптимальное SRM-измерение

- Один из способов построения наблюдаемой, оптимальной в ряде случаев, является SRM (PGM)-измерение, которое строится через оператор Грама

$$G = \frac{1}{2}(|w_0\rangle\langle w_0| + |w_1\rangle\langle w_1|)$$

Собственные векторы G, отвечающие $\frac{1}{2}(1 \pm \kappa^N)$, равны

$$|\lambda_{0,1}\rangle = \frac{1}{\sqrt{2}\sqrt{1 \pm \kappa^N}}(|\psi_0\rangle^{\otimes N} \pm |\psi_1\rangle^{\otimes N}).$$

$$G^{-\frac{1}{2}} = \frac{\sqrt{2}}{\sqrt{1+\kappa^N}}|\lambda_0\rangle\langle\lambda_0| + \frac{\sqrt{2}}{\sqrt{1-\kappa^N}}|\lambda_1\rangle\langle\lambda_1|,$$

и базис измерения задается как

$$|e_{0,1}\rangle = \frac{1}{\sqrt{2}}G^{-\frac{1}{2}}|w_{0,1}\rangle = \frac{1}{\sqrt{2}}(|\lambda_0\rangle \pm |\lambda_1\rangle).$$

Вероятность ошибки равна

$$Q = |\langle\psi_0|^{\otimes N}|e_1\rangle|^2 = \frac{1}{2}(\sqrt{\frac{1+\kappa^N}{2}} - \sqrt{\frac{1-\kappa^N}{2}})^2 = \frac{1}{2}(1 - \sqrt{1-\kappa^{2N}}).$$

Сравнение индивидуальных и коллективных измерений

- Для $N = 2$ можно легко сопоставить случаи индивидуальных и коллективных измерений, а также заметить связь сцепленности с окружением после измерения со сцепленностью векторов наблюдаемой
- Для коллективных измерений взаимная информация равна

$$I_{2,col}(A, B) = 1 - h_2(\frac{1}{2}(1 - \sqrt{1 - \kappa^4})).$$

- Для индивидуальных измерений можно использовать аналогичные выражения, чтобы получить вид векторов наблюдаемой, выражения для ошибки и взаимной информации. Вероятность ошибки

$$q = |\langle\psi_0|f_1\rangle|^2 = \frac{1}{2}(1 - \sqrt{1 - \kappa^2}),$$

Сравнение индивидуальных и коллективных измерений

- Распределения вероятностей выхода для входов 0 и 1

$$P_{Y|X=0} = \{(1-q)^2, q(1-q), q(1-q), q^2\},$$

$$P_{Y|X=1} = \{q^2, q(1-q), q(1-q), (1-q)^2\},$$

итоговое распределение вероятностей на выходе

$$P_Y = \{\frac{1}{2}((1-q)^2 + q^2), q(1-q), q(1-q), \frac{1}{2}((1-q)^2 + q^2)\},$$

- Взаимная информация равна

$$I_{2,ind}(A, B) = H(Y) - H(Y|X) = 1 + h_2(2q(1-q)) - 2h_2(q) =$$

$$= 1 + h_2(\frac{\kappa^2}{2}) - 2h_2(\frac{1-\sqrt{1-\kappa^2}}{2}).$$

- Мера сцепленности с окружением равна $2h_2(q)$.

Мера сцепленности векторов измерений

- Рассмотрим меру сцепленности для векторов коллективных измерений $\{|e_0\rangle, |e_1\rangle\}$
- По симметрии она одинакова для обоих векторов и равна энтропии фон Неймана частичного состояния $\mathrm{tr}_2|e_0\rangle\langle e_0|$.

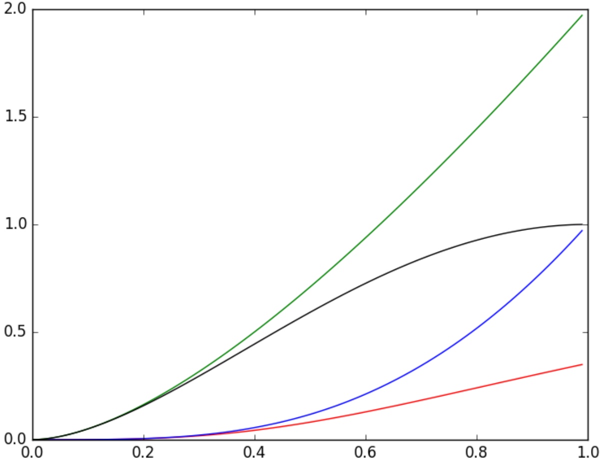
$$|e_0\rangle = \frac{1}{2}[(\frac{1}{\sqrt{1+\kappa^2}}+\frac{1}{\sqrt{1-\kappa^2}})|\psi_0\rangle|\psi_0\rangle+(\frac{1}{\sqrt{1+\kappa^2}}-\frac{1}{\sqrt{1-\kappa^2}})|\psi_1\rangle|\psi_1\rangle] =$$

$$= a|\psi_0\rangle|\psi_0\rangle + b|\psi_1\rangle|\psi_1\rangle,$$

$$A = \mathrm{tr}_2|e_0\rangle\langle e_0| = \frac{1}{2}\begin{pmatrix} 1+\frac{1}{\sqrt{1+\kappa^2}} & \frac{\kappa}{\sqrt{1+\kappa^2}} \\ \frac{\kappa}{\sqrt{1+\kappa^2}} & 1-\frac{1}{\sqrt{1+\kappa^2}} \end{pmatrix}.$$

- Мера сцепленности равна $h_2(\frac{1}{2}(1-\frac{\sqrt{1+2\kappa^2}}{1+\kappa^2}))$.

Связь сцепленности



Мера сцепленности с окружением для коллективных (синяя линия) и индивидуальных (зеленая линия) измерений. Их разность показана черной линией, мера сцепленности векторов измерения – красной линией. По оси X значения κ

Двойственная ситуация

- Разница между индивидуальными и коллективными измерениями может быть проиллюстрирована с помощью двойственности между ансамблями состояний и наблюдаемыми.
- Переход от ансамбля $R = \{p_i, \rho_i\}$ к наблюдаемой $\Pi(R)$ описывается через оператор Грама $G = \sum_i p_i \rho_i$:

$$\Pi(R) = \{p_i G_R^{-\frac{1}{2}} \rho_i G_R^{-\frac{1}{2}}\},$$

- Аналогично, для наблюдаемой $\Lambda = \{\Lambda_i\}$ и оператора плотности σ можно определить ансамбль $R(\Lambda, \sigma)$ как

$$R(\Lambda, \sigma) = \{\mathrm{tr}(\sigma\Lambda_i), \frac{\sigma^{\frac{1}{2}} \Lambda_i \sigma^{\frac{1}{2}}}{\mathrm{tr}(\sigma\Lambda_i)}\}.$$

Для этого ансамбля σ будет оператором Грама
[Informational power of quantum measurements,
M.Dall'Arno, G.M.D'Ariano, and M.F.Sacchi Phys. Rev. A 83, 062304 (2011)]

Двойственная ситуация

- Легко видеть, что $R(\Pi(S), G_S) = S$ для любого ансамбля S с оператором Грама G_S, и, аналогично, $\Pi(R(\Lambda, \sigma)) = \Lambda$.
- Если Алиса готовит ансамбль состояний S, а Боб производит измерение наблюдаемой Π, взаимная информация равна

$$I(S, \Pi) = \sum_{i,j} p_i \mathrm{tr}(\rho_i \Pi_j) \log \frac{\mathrm{tr}(\rho_i \Pi_j)}{\sum_k p_k \mathrm{tr}(\rho_k \Pi_j)}.$$

- Двойственность между ансамблями и наблюдаемыми заключается в том, что

$$I(S, \Lambda) = I(R(\Lambda, G_S), \Pi(S)).$$

- Для коллективных SRM-измерений двойственная ситуация в точности совпадает с исходной, потому что SRM-измерение определяется так же, как и двойственная наблюдаемая. Но для индивидуальных измерений, двойственная ситуация включает SRM-измерение и набор состояний в пространстве исходной (небольшой) размерности

Двойственная ситуация: индивидуальные измерения

- При индивидуальном измерении векторами наблюдаемой будут все 2^N комбинаций из $|f_0\rangle$ и $|f_1\rangle$

$$G^{\frac{1}{2}} = \frac{1}{2}|\lambda_0\rangle(\langle\psi_0|^{\otimes N} + \langle\psi_1|^{\otimes N}) + \frac{1}{2}|\lambda_1\rangle(\langle\psi_0|^{\otimes N} - \langle\psi_1|^{\otimes N})$$

- Для вектора с $N-K$ состояниями $|f_0\rangle$ и K состояниями $|f_1\rangle$ имеем

$$G^{\frac{1}{2}}|f_0\rangle^{\otimes(N-K)} \otimes |f_1\rangle^{\otimes K} = \frac{1}{2}(\sqrt{1-q}^{N-K}\sqrt{q}^{K} + \sqrt{q}^{N-K}\sqrt{1-q}^{K})|\lambda_0\rangle + \\ + \frac{1}{2}(\sqrt{1-q}^{N-K}\sqrt{q}^{K} - \sqrt{q}^{N-K}\sqrt{1-q}^{K})|\lambda_1\rangle.$$

Двойственная ситуация: индивидуальные измерения

- Матрица плотности, соответствующая в двойственной картине исходу с K результатами 1 в базисе $\{|\lambda_0\rangle, |\lambda_1\rangle\}$ имеет вид

$$\rho_K = \frac{1}{(1-q)^{N-K}q^K + q^{N-K}(1-q)^K} \begin{pmatrix} (1-q)^{N-K}q^K & (\sqrt{1-q}\sqrt{q})^N \\ (\sqrt{1-q}\sqrt{q})^N & q^{N-K}(1-q)^K \end{pmatrix},$$

- Вероятность этого в ансамбле равна

$$p_K = \frac{1}{2}((1-q)^{N-K}q^K + q^{N-K}(1-q)^K).$$

- Количество подобных состояний ρ_K равно количеству исходов с K результатами 1, то есть C_N^K. Поэтому, ансамбль, двойственный к индивидуальному измерению, состоит из 2^N состояний, где каждое состояние ρ_K встречается C_N^K раз, и каждое его вхождение имеет вероятность p_K.

Нечетные N: различение по максимуму правдоподобия

- Для кода с повторением и индивидуальных измерений при нечетных N очень простую форму принимает принцип различения по максимуму правдоподобия (MLD): решение принимается в соответствии с большим количеством исходов
- Вероятность ошибки в этом случае равна

$$Q_{MLD} = \sum_{K=0}^{\frac{N-1}{2}} C_N^K q^{N-K} (1-q)^K$$

- Такая схема может быть описана наблюдаемой с двумя операторами: исходу 0 соответствует сумма операторов с преобладанием результатов 0 в частичных позициях, аналогично для исхода 1

Нечетные N: двойственная к MLD ситуация

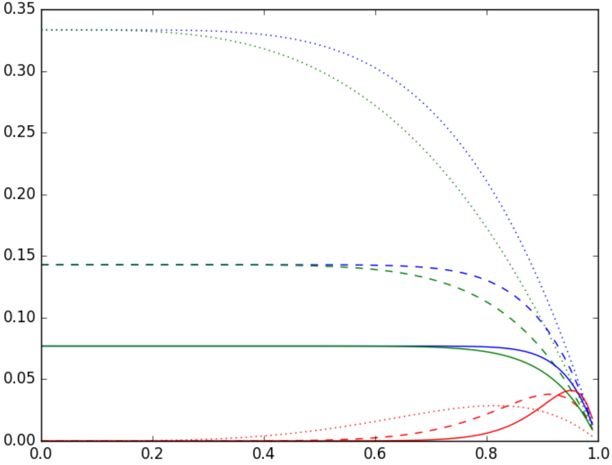
- В ситуации, двойственной к MLD, вместо ансамбля из 2^N состояний, получается ансамбль из двух состояний $\{\rho_0^{MLD}, \rho_1^{MLD}\}$, которые соответствуют решениям о 0 и 1. Состояние ρ_0^{MLD} равно

$$\rho_0^{MLD} = \begin{pmatrix} 1 - Q_{MLD} & \frac{\kappa^N}{2} \\ \frac{\kappa^N}{2} & Q_{MLD} \end{pmatrix}, \quad \rho_1^{MLD} = \begin{pmatrix} Q_{MLD} & \frac{\kappa^N}{2} \\ \frac{\kappa^N}{2} & 1 - Q_{MLD} \end{pmatrix}.$$

- Это смешанные состояния, что очевидно хуже для передачи информации, чем исходные чистые состояния. Это может служить иллюстрацией преимущества коллективных измерений. Падение информации можно описать через минимальное собственное значение ρ_0^{MLD} (входящее в бинарную энтропию), которое равно

$$\lambda_{min} = \frac{1}{2}(1 - \sqrt{1 + \kappa^{2N} - 4Q_{MLD}(1 - Q_{MLD})}).$$

Двойственная к MLD ситуация



Взаимная информация для коллективных (синяя линия) и индивидуальных (зеленая линия) измерений. Минимальное собственное значение двойственного наблюдаемой состояния показано красной линией. Показаны случаи $N = 3$ (пунктирная линия), $N = 7$ (штрихованная линия), $N = 13$ (сплошная линия)

Заключение

- Выигрыш от использования коллективных измерений обуславливается использованием сцепленных наблюдаемых, причем мера сцепленности выглядит связанной с падением ошибки, т.е. сцепленности с окружением
- В двойственной ситуации индивидуальному измерению соответствуют смешанные состояния, что ухудшает характеристики по сравнению с чистыми состояниями для коллективных измерений.

Работа выполнена при поддержке гранта РНФ 17-11-01388

Спасибо за внимание!