5. Квантовая теория информации

Основным понятием квантовой теории информации является энтропия фон Неймана квантового состояния ρ, которая определяется следующей формулой:

$$S(\rho) \equiv -\mathrm{Tr}(\rho \log_2 \rho). \tag{5.1}$$

Если λ_i — собственные значения ρ, то определение фон Неймана можно переписать в виде $S(\rho) = -\sum_i(\lambda_i \log_2 \lambda_i)$, где подразумевается, что $0 \log_2 0 = 0$.

Смешивание увеличивает энтропию фон Неймана. Энтропия взвешенной смеси состояний больше или равна взвешенной сумме энтропий составляющих (вогнутость энтропии):

$$S(p_1\rho_1 + p_2\rho_2) \geqslant p_1 S(\rho_1) + p_2 S(\rho_2), \quad p_1 + p_2 = 1. \tag{5.2}$$

Корреляция уменьшает энтропию фон Неймана. Энтропия квантовой системы, состоящей из двух подсистем, меньше или равна сумме энтропий двух подсистем (субаддитивность энтропии):

$$S(\rho_{AB}) \leqslant S(\rho_A) + S(\rho_B). \tag{5.3}$$

Редукция может как увеличить, так и уменьшить энтропию фон Неймана. Разность энтропий двух подсистем не может превышать энтропию полной системы (неравенство треугольника):

$$S(\rho_{AB}) \geqslant |S(\rho_A) - S(\rho_B)|. \tag{5.4}$$

Таким образом, в отличие от классической энтропии Шеннона (см. приложение), квантовая энтропия фон Неймана полной системы может быть меньше энтропии составляющих подсистем. В частности, если составная система находится в чистом состоянии, то $S(\rho_{AB}) = 0 \Rightarrow S(\rho_A) = S(\rho_B)$, но не обязательно $S(\rho_A) = S(\rho_B) = 0$.

5.1. Докажите следующие свойства энтропии фон Неймана: 1) Энтропия неотрицательна и обращается в нуль только тогда, когда система находится в чистом состоянии; 2) Энтропия не меняется при унитарных преобразованиях; 3) Если размерность гильбертова пространства равна d, то энтропия не превышает значения $\log_2 d$, причем максимум достигается только тогда, когда система находится в максимально смешанном (однородном) состоянии $\rho = I/d$.

5.2. Вычислите энтропию фон Неймана для следующих состояний:

$$\rho = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \rho = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \quad \rho = \frac{1}{3}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}.$$

5.3. Вычислите энтропию фон Неймана для состояния Вернера

$$\rho(p) = p|\mathrm{Bell}\rangle\langle\mathrm{Bell}| + \frac{1-p}{4}I,$$

где $0 \leqslant p \leqslant 1$ и $|\mathrm{Bell}\rangle$ — любое из состояний Белла.

5.4. Докажите, что формула (5.2) превращается в равенство тогда и только тогда, когда состояния ρ_i совпадают.

5.5. Докажите, что формула (5.3) превращается в равенство тогда и только тогда, когда состояния ρ_i некоррелированы, т.е. подсистемы независимы.

5.6. Докажите, что чистое состояние $|\psi_{AB}\rangle$ системы, состоящей из двух подсистем A и B, является перепутанным тогда и только тогда, когда $S(A|B) < 0$, где $S(A|B) = S(\rho_{AB}) - S(\rho_B)$ — так называемая условная энтропия.

5.7. Покажите, что вогнутость энтропии фон Неймана является следствием субаддитивности. Для доказательства введите вспомогательную квантовую систему.

5.8. Энтропия фон Неймана является, прежде всего, мерой неопределенности квантового состояния. Для одиночного кубита, размерность гильбертова пространства которого $d = 2$, энтропия $S(\rho) = 0$ в случае чистого состояния $\rho = |\psi\rangle\langle\psi|$ и $S(\rho) = 1$ в случае максимально смешанного (однородного) состояния $\rho = I/2$. Аналогичным образом неопределенность квантового состояния кубита можно описывать степенью чистоты $P(\rho) = \mathrm{tr}(\rho^2)$ (см. задачу 1.10). Есть ли взаимно-однозначное соответствие между энтропией и степенью чистоты? В чем преимущество и недостатки каждой величины как меры неопределенности квантового состояния?

Предположим, что имеется некоторый источник квантовой информации — черный ящик, который при каждом обращении к нему выдает состояние $|x\rangle$ с вероятностью $p(x)$, причем результаты разных обращений являются статистически независимыми. Состояния $|x\rangle$, создаваемые источником, не обязательно являются ортогональными и принадлежат некоторому конечному набору состояний, именуемому алфавитом. Источник однозначно характеризуется ансамблем $E = \{|x\rangle, p(x)\}$, порождающим оператор плотности $\rho = \sum_x p(x)|x\rangle\langle x|$. В результате n-кратного обращения к источнику создается последовательность состояний $|x_1\rangle$, $|x_2\rangle, \ldots,$ $|x_n\rangle$, которую можно рассматривать как квантовое сообщение длиной n. Если сообщение не является случайным, в том смысле, что $\rho \neq I/2$, то его можно сжать, т.е. преобразовать в более короткую последовательность кубитов, без потери информации. Последнее означает, что степень совпадения исходного факторизованного состояния n кубитов и состояния, которое получается из сжатого при его развертывании, стремится к единице при $n \to \infty$. Минимальная длина сжатого сообщения в пределе $n \to \infty$ равна $nS(\rho)$, где $S(\rho)$ — энтропия фон Неймана. В этом состоит суть теоремы кодирования Шумахера для нешумящего квантового канала. Таким образом, энтропия фон Неймана определяет наименьшее (в отсутствии шумов и в пределе $n \to \infty$) количество физических ресурсов (кубитов), необходимых для передачи или хранения квантового сообщения, создаваемого источником, который описывается оператором плотности ρ.

5.9. Имеется некоторый источник классической информации, выдающий значения битов 0 и 1 с вероятностями $p_0 = p_1 = 1/2$. Последовательность битов кодируется через неортогональные чистые состояния кубитов $|0\rangle$ и $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Во сколько раз можно сжать создаваемое таким образом квантовое сообщение? Найдите чистое состояние, дающее максимальную степень совпадения с исходным, и вычислите эту степень совпадения.

5.10. Предположим, что нам необходимо закодировать три цвета — красный, зеленый и голубой — через три соответствующих квантовых состояния кубита $|R\rangle$, $|G\rangle$ и $|B\rangle$. Какие состояния нужно взять, чтобы получить наиболее экономичные квантовые сообщения, т.е. требующие наименьшее количество ресурсов?

Предположим, что у Алисы есть источник классической информации, выдающий символы $X = x_1, x_2, \ldots, x_n$ в соответствии с распределением вероятностей $p_1, p_2, \ldots, p_n$. Алиса кодирует классическое сообщение через квантовые состояния $|x_1\rangle, |x_2\rangle, \ldots, |x_n\rangle$ и предоставляет это сообщение Бобу. Боб производит измерение полученного сообщения и получает набор символов $Y = y_1, y_2, \ldots, y_n$. Задача Боба — как можно лучше определить X на основе результата измерения Y. Для этого Боб должен выбрать измерение, с помощью которого достигается максимальное значение взаимной информации $H(X:Y)$ (см. приложение), наиболее близкое к $H(X)$. Такое измерение называется оптимальным. Максимум взаимной информации $H(X:Y)$ по всем возможным схемам POVM-измерений называется *доступной информацией*. Можно показать, что верхняя оценка доступной Бобу информации $I_{\text{дост}}$ имеет вид

$$I_{\text{дост}} \leqslant S(\rho). \tag{5.5}$$

Если состояния, приготовленные Алисой, не ортогональны, то $S(\rho) < H(X) \Rightarrow I_{\text{дост}} < H(X)$ и Боб не может с уверенностью определить, какое состояние приготовила Алиса. В случае ортогональных состояний $S(\rho) = H(X)$, так что при оптимальной схеме измерения доступной оказывается вся посланная информация.

5.11. Предположим, что имеется некоторый источник классической информации, выдающий значения битов 0 и 1 с вероятностями $p_0 = p_1 = 1/2$. Последовательность битов кодируется через неортогональные чистые состояния кубитов $|0\rangle$ и $\cos\theta|0\rangle + \sin\theta|1\rangle$, где θ — вещественный параметр. Рассчитайте максимум доступной информации и проанализируйте его зависимость от параметра θ.

Полученные выше оценки для сжимаемости сообщений и доступной информации можно обобщить на случай, когда источник квантовой информации выдает не чистые, а смешанные состояния и описывается, следовательно, ансамблем $E = \{\rho_x, p(\rho_x)\}$. В этом случае энтропия фон Неймана заменяется энтропией Холево

$$\chi(E) = S\left(\sum_x p_x \rho_x\right) - \sum_x p_x S(\rho_x). \tag{5.6}$$

Можно показать, что энтропия Холево удовлетворяет неравенству

$$\chi(E) \leqslant H(X), \tag{5.7}$$

где $H(X)$ — энтропия Шеннона классического источника информации и равенство имеет место только тогда, когда носители состояний ρ_x ортогональны. Таким образом, при использовании смешанных состояний для передачи информации минимальное количество кубитов, необходимых для передачи или хранения квантового сообщения длиной n в пределе $n \to \infty$, будет равно $n\chi(E)$, а верхняя оценка доступной информации будет равна $\chi(E)$.

5.12. Докажите неотрицательность энтропии Холево исходя из субаддитивности энтропии фон Неймана.

5.13. Предположим, что имеется некоторый источник классической информации, выдающий значения битов 0 и 1 с вероятностями $p_0 = p_1 = 1/2$. Последовательность битов кодируется через неортогональные состояния кубитов $|0\rangle\langle 0|$ и $\cos\theta|0\rangle\langle 0| + \sin\theta|1\rangle\langle 1|$, где θ — вещественный параметр. Рассчитайте максимум доступной информации и проанализируйте его зависимость от параметра θ.

5.14. Одной из возможных ситуаций, когда для кодирования используются смешанные состояния, является следующая. Предположим, что Алиса посылает Бобу кубиты в чистых квантовых состояниях, но через неидеальный (шумящий) канал. Из-за потери когерентности в канале Боб получает кубиты в смешанных состояниях, которые он и должен раскодировать. В этом случае величина $\chi(E)$ будет описывать максимальное количество информации, которую можно передать Бобу через неидеальный канал, используя заданное число кубитов.

Пусть Алиса посылает в канал с затуханием фазы (см. задачу 3.5) равномерную смесь чистых состояний $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ и $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Рассчитайте максимум доступной информации и проанализируйте его зависимость от вероятности ошибки p.