Лекция 5

II. Основные понятия квантовой теории информации (продолжение)

1. Энтропия фон Неймана, ее неотрицательность, максимальное значение. Квантовая относительная энтропия. Неравенство Клейна.
2. Композиционные системы. Субаддитивность и вогнутость энтропии. Энтропия смеси состояний. Совместная энтропия. Условная энтропия. Взаимная информация. Примеры. Различие между классической и квантовой информацией.
3. Достижимая информация.
4. Теорема о запрете клонирования квантовых состояний. Ее связь с достижимой информацией.
5. Граница и информация Холево. Примеры. Априорная и апостериорная энтропии.

На прошлых лекциях было введено понятие классической (Шенноновской) и квантовой (фон Неймана) энтропий. Шенноновская энтропия (далее будем обозначать ее буквой H) дает меру неопределенности, связанную с классическим распределением вероятностей. Квантовые состояния описываются схожим образом, только вместо распределения вероятностей используются операторы плотности. Мы определили энтропию фон Неймана квантового состояния ρ соотношением:

$$S(\rho) \equiv -Sp\left(\rho \log \rho\right). \qquad (5.1)$$

Напомним, что в теории информации логарифмы принято брать по основанию “2” (а в статистической физике - по основанию “е” - “наты”).

Если λ_x - собственные значения матрицы плотности ρ, то выражение (5.1) для энтропии фон Неймана можно переписать по-другому:

$$S(\rho) \equiv -\sum_x \lambda_x \log \lambda_x, \qquad (5.2)$$

где, как обычно, считается, что $0 \log 0 \equiv 0$ (как и для Шенноновской энтропии). При вычислениях удобнее пользоваться последней формулой. Например, как было показано на прошлой лекции для полностью смешанного состояния в N-мерном пространстве энтропия равна $\log N$.

Пример. Сравнение квантовой и классической энтропии. Вычислим энтропию состояния

$$\rho = p|0\rangle\langle 0| + (1-p)\frac{\left(|0\rangle+|1\rangle\right)\left(\langle 0|+\langle 1|\right)}{2}.$$ (Сравнить результат с Шенноновской энтропией $H(p, 1-p)$).

Решение.

Учтем, что

$$|0\rangle\langle 0| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}, \qquad |1\rangle\langle 1| = \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix},$$

$$|0\rangle\langle 1| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 1\\0 & 0\end{pmatrix}, \qquad |1\rangle\langle 0| = \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} = \begin{pmatrix}0 & 0\\1 & 0\end{pmatrix}.$$

$$\rho = p\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \frac{1-p}{2}\left[|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |0\rangle\langle 1|\right] =$$

Тогда $$= p\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \frac{1-p}{2}\left[\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} + \begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix} + \begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right] =$$

$$= p\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \frac{1-p}{2}\left[\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\right] = \begin{pmatrix}\frac{1+p}{2} & \frac{1-p}{2}\\ \frac{1-p}{2} & \frac{1-p}{2}\end{pmatrix}.$$

Видно, что S, вычисленная из последней матрицы отличается от *H(p, 1-p)*.

Квантовая относительная энтропия.

Как и для энтропии Шеннона, полезно ввести квантовый аналог относительной энтропии. Пусть ρ и σ -два оператора плотности. Относительная энтропия состояний (операторов) ρ и σ (ρ относительно σ) называется величина:

$$S(\rho \| \sigma) \equiv Sp(\rho \log \rho) - Sp(\rho \log \sigma) = -S(\rho) - Sp(\rho \log \sigma). \qquad (5.3)$$

Как и соответствующая классическая величина, квантовая относительная энтропия может принимать бесконечные значения.

Так, относительная энтропия определяется как бесконечная, если *ядро* (*kernel*) оператора σ (векторное пространство собственных векторов σ с нулевыми собственными значениями) имеет нетривиальное пересечение с *основанием* (*support*) оператора ρ (векторное пространство образованное собственными векторами ρ с ненулевыми собственными значениями). В других случаях относительная энтропия конечна.

Квантовая относительная энтропия неотрицательна (неравенство Клейна):

$$S(\rho \| \sigma) \geq 0, \qquad (5.4)$$

равенство достигается, когда ρ = σ.

Перечислим основные свойства энтропии фон Неймана.

1. Энтропия неотрицательна. Она принимает нулевые значения только для чистых состояний (доказательство следует из определения).
2. В *N* - мерном гильбертовом пространстве энтропия максимальное значение энтропии log*N*. Энтропия равна log*N* только если система находится в (полностью) смешанном состоянии *I/d*.
3. Предположим, что композиционная система *AB* находится в чистом состоянии. Тогда *S(A) = S(B).*
4. Предположим, что p_i - это вероятности, а состояния ρ_i - раскладывается по собственным векторам с ненулевыми собственными значениями (имеют *основание)* в ортогональном базисе. Тогда

$$S\left(\sum_i p_i \rho_i\right) = H(p_i) + \sum_i p_i S(\rho_i).$$

Док-во. Пусть λ_i^j и $\left|e_i^j\right\rangle$ - собственные значения и собственные векторы состояния ρ_i. Видно, что $p_i\lambda_i^j$ и $\left|e_i^j\right\rangle$ - собственные значения и собственные векторы состояния $\sum_i p_i\rho_i$, поэтому

$$S\left(\sum_i p_i\rho_i\right) = -\sum_{i,j} p_i\lambda_i^j \log p_i\lambda_i^j = -\sum_i p_i \log p_i - \sum_j p_i \sum_i \lambda_i^j \log \lambda_i^j =$$

$$H\left(p_i\right) + \sum_i p_i S(\rho_i).$$

5. Теорема о совместной энтропии: Предположим, что p_i - вероятности, $\left|i\right\rangle$ - ортогональные состояния для системы A и ρ_i - любой набор операторов плотности для другой системы B, Тогда

$$S\left(\sum_i p_i \left|i\right\rangle\left\langle i\right| \otimes \rho_i\right) = H\left(p_i\right) + \sum_i p_i S\left(\rho_i\right).$$

(Доказывается аналогично (4)).

6. Субаддитивность энтропии. Пусть различные квантовые системы A и B имеют общее состояние ρ^{AB}. Тогда совместная энтропия для двух систем удовлетворяет следующим неравенствам:

$S\left(A,B\right) \le S(A) + S(B)$ - причем равенство имеет место только если системы A и B некоррелированы, т.е. $\rho^{AB} = \rho^A \otimes \rho^B$

$S\left(A,B\right) \ge \left|S(A) - S(B)\right|$ - т.н. неравенство треугольника или Араки-Льеба. Это, фактически, квантовый аналог неравенства $H(X:Y) \ge H(X)$ для энтропии Шеннона.

7. Вогнутость энтропии. Пусть p_i - неотрицательные действительные числа, такие, что $\sum_i p_i = 1$, а ρ_i - соответствующие операторы плотности. Тогда энтропия удовлетворяет неравенству:

$S\left(\sum_i p_i\rho_i\right) \ge \sum_i p_i S\left(\rho_i\right)$ - следует из св-ва (4).

Интуитивно ясно, что $\sum_i p_i\rho_i$ выражает состояние квантовой системы, которая находится в неизвестном состоянии ρ_i с вероятностью p_i. Неопределенность нашего знания о такой смеси состояний должна быть больше, чем средняя неопределенность состояний ρ_i, поскольку состояние $\sum_i p_i\rho_i$ дает вклад в неопределенность не только из-за наличия состояний ρ_i но и благодаря усреднению по индексу i.

8. Энтропия смеси квантовых состояний. Обратная сторона условия вогнутости проявляется в некоей полезной теореме, дающей верхнюю границу для энтропии смеси квантовых состояний. А именно, что для смеси $\sum_i p_i\rho_i$ квантовых состояний ρ_i выполняется следующее неравенство:

$$\sum_i p_i S(\rho_i) \le S\left(\sum_i p_i \rho_i\right) \le \sum_i p_i S(\rho_i) + H(p_i)$$

Что можно сказать о верхней границе или о правой части неравенства? Интуитивно ясно, что неопределенность состояния $\sum_i p_i \rho_i$ не может быть больше, чем средняя неопределенность состояния ρ_i плюс дополнительный вклад за счет $H(p_i)$, который представляет собой максимально возможный вклад в неопределенность об индексе i в общую неопределенность Сформулируем теперь теорему о верхней границе

Теорема. Предположим, что $\rho_i = \sum_i p_i \rho_i$, где p_i - некоторый набор вероятностей, а ρ_i - операторы плотности. Тогда

$$S(\rho) \le \sum_i p_i S(\rho_i) + H(p_i), \qquad (**)$$

причем равенство достигается, если состояния ρ_i образуют ортогональный набор.

По аналогии с классическим случаем (энтропия Шеннона) для композиционных систем можно определить *квантовые совместную* и *условную энтропии*, а также *квантовую взаимную информацию*. ***Совместная энтропия*** *S(A, B)* для композиционной системы, состоящей из двух компонент *A* и *B*, определяется как и в классике:

$$S(A,B) \equiv -Sp\left(\rho^{AB} \log\left(\rho^{AB}\right)\right), \qquad (5.5)$$

где ρ^{AB} - матрица плотности системы *AB*. Напоминание:
в классике условной энтропией называлась величина

$$S(Y \mid X) = -\sum_x p(x) \sum_y p(y \mid x) \log p(y \mid x) = -\sum_x \sum_y p(x,y) \log p(y \mid x), \qquad (+)$$

где во втором равенстве использовано понятие совместной вероятности
$p(x,y) = p(y \mid x) p(x)$ - есть вероятность того, что *X* принимает значение *x*, а *Y* принимает значение *y*.
Из определения (+) следует, что *S(Y|X)* есть мера того, сколько информации, в среднем, оставалось бы в *Y* при условии, что мы бы знали *X*. Заметим, что всегда *S(Y|X)* ≤ *S(Y)* и обычно *S(Y|X)* ≠ *S(X|Y)*. (конец напоминания)
Определим ***условную энтропию***, как

$$S(A \mid B) \equiv S(A,B) - S(B). \qquad (5.6)$$

Определим ***взаимную информацию***, как

$$S(A:B) \equiv S(A) + S(B) - S(A,B) = S(A) - S(A \mid B) = S(B) - S(B \mid A). \qquad (5.7)$$

Некоторые свойства энтропии Шеннона не переносятся на энтропию фон Неймана и отсюда следуют интересные следствия квантовой теории информации. Например, для случайных переменных *X* и *Y* имеет место неравенство: *H(X) ≤ H(X, Y)*. Интуитивно, это понятно: не может быть большей неопределенности состояния *X*, чем для совместного состояния *X* и *Y*. Это

интуитивное понимание не годится для квантовых состояний. Рассмотрим систему *AB* двух кубитов в перепутанном состоянии :

$\left(|00\rangle+|11\rangle\right)/\sqrt{2}$. (*)

Это чистое состояние, поэтому *S(A, B) = 0*. С другой стороны, система *A* имеет оператор плотности *I/2* (*I* - единичный оператор) и поэтому ее энтропия равна единице. Действительно, волновой функции состояния (*) не существует, это состояние максимально смешанное. Другой способ озвучивания этого результата состоит в том, что для этой системы величина (условная энтропия) $S(B|A) \equiv S(A,B) - S(A)$ - отрицательная. Это соотношение может трактоваться как критерий перепутывания: Если $|AB\rangle$ - чистое состояние композиционной системы, то $|AB\rangle$ находится в перепутанном состоянии если и только если $S(A|B) < 0$.

Классическая теория информации, в основном, затрагивает проблему пересылки классических сообщений - букв алфавита, текстов, строк битов - через каналы связи, которые работают в соответствии с законами классической физики. Как изменится картина, если будут использоваться квантовые каналы связи? Можно ли передать информацию более эффективно? Можно ли использовать законы квантовой механики для того, чтобы передавать секретную информацию, защищенную от подслушивания? Такого рода вопросы возникают, когда мы используем каналы связи, работающие по законам квантовой механики. Такое переопределение того, что же есть канал связи вызвано необходимостью переосмысления основных положений классической теории информации .

Квантовая теория информации нацелена на исследование каналов связи, но она имеет гораздо более широкую область применения. Можно обозначить три фундаментальные цели, которые стоят перед теорией квантовой информации:

- идентифицировать элементарные классы статических ресурсов в квантовой механике (или типы “информации”)
- идентифицировать элементарные классы динамических процессов в квантовой механике (или типы информационных процессов)
- характеризовать ресурсы, с помощью которых можно реализовать элементарные динамические процессы.

Оказывается, что квантовая теория информации гораздо глубже и богаче классической теории информации потому, что квантовая механика включает в себя гораздо больше элементарных классов статических и динамических ресурсов, которые не просто соответствуют известным классическим типам, но и описывают целые новые типы состояний, например, перепутанные состояния, которые не имеют аналога в классике.

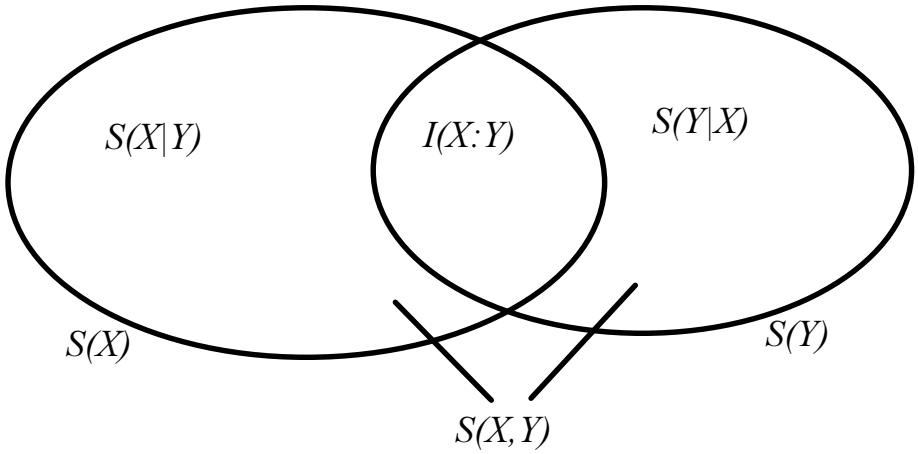
Рассмотрим на некоторых примерах разницу в описании между квантовой и классической информацией.

Принцип соответствия. “Законы квантовой физики должны быть сформулированы таким образом, что в классических границах, когда в процесс вовлечено много квантов, эти законы приводили бы к классическим уравнениям для усредненных величин.” (Д.Бом. Квантовая теория)

Предположим, что Алиса имеет классический источник информации, который выдает символы $X = 0, \ldots n$ с соответствующим распределением вероятностей $p_0, \ldots, p_n$. Цель Алисы и Боба состоит в том, чтобы Боб смог определить величину *X* наилучшим образом. Для того, чтобы достигнуть этого. Алиса приготавливает квантовое состояние ρ_X выбирая его из некоторого фиксированного набора $\rho_0, \ldots \rho_n$, и посылает это состояние Бобу, который выполняет квантовое измерение над этим состоянием. Затем, он пытается сделать лучшее предположение о том, как идентифицировать *X*, основываясь над результатах своих измерений *Y*.

Хорошей мерой того, сколько информации получено Бобом о величине *X* из его измерений - это взаимная информация между *X* и результатом измерения *Y*. Мы помним из предыдущих лекций, что Боб может сделать заключение об *X* по результатам измерения *Y* только, если и только если *H(X:Y) = H(X)*, и что в общем случае $H(X:Y) \le H(X)$. Далее мы покажем, что близость величины *H(X:Y)* к *H(X)* не самом деле дает хорошую меру того, как Боб смог определить *X*. Цель Боба - выбрать измерение, которое максимизирует величину *H(X:Y)* и тем самым приближая ее к *H(X)*. Для этого, определим *достижимую информацию* (*accessible information*), как максимальную величину *взаимной информации*. **Достижимая информация - это мера того, насколько хорошо Боб смог сделать вывод о приготовленном Алисой состоянии, которая она послала ему.**

КЛАССИКА (см. лекцию 3)



Квантовая информация	Классическая информация
Условная энтропия: $S(A\mid B)\equiv S(A,B)-S(B).$ МОЖЕТ БЫТЬ ОТРИЦАТЕЛЬНОЙ!!	Условная энтропия: $H(A\mid B)\equiv H(A,B)-H(B).$ $H(B\|A) \le H(B)$
Совместная энтропия: $S(A,B)\equiv -Sp\left(\rho^{AB}\log\left(\rho^{AB}\right)\right)$	Совместная энтропия: $H(B) \le H(B\|A)$
Взаимная информация: $S(A:B)\equiv S(A)+S(B)-S(A,B)=$ $S(A)-S(A\mid B)=S(B)-S(B\mid A).$	Взаимная информация: $H(A:B)\equiv H(A)+H(B)-H(A,B)=$ $H(A)-H(A\mid B)=H(B)-H(B\mid A).$

В теории классической информации, достижимая информация не так интересна. Если на практике различение пары классических состояний может встретить определенные трудности, то в принципе, это всегда можно сделать. В отличие от этого, в квантовом случае, далеко не всегда возможно различить два состояния даже в принципе. Например. не существует однозначной процедуры, позволяющей различить два неортогональных состояния. Будем “выражаться” в терминах достижимой информации. Если Алиса готовит состояние $|\psi\rangle$ с вероятностью *p* и другое неортогональное состояние $|\varphi\rangle$ с вероятностью *1 - p*,

то достижимая информация при таком приготовлении уж точно меньше, чем *H(p)*, поскольку Боб не может определить принадлежность состояния с полной достоверностью. В классике - если Алиса готовит два классических состояния, например, бит - в состоянии “0” с вероятностью *p* или “1” с вероятностью *1 - p*, то не существует фундаментального закона, запрещающего Бобу различить эти состояния; поэтому достижимая информация оказывается такой же как и энтропия приготовления, т.е. *H(p)*.

Существует важное замечание, относящееся к этой дискуссии - когда концепция достижимой информации имеет классический смысл. Суть его - в различении распределений вероятностей. Представим, что Алиса готовит состояние “0” или “1” с двумя распределениями вероятностей либо с (*p, 1 - p*) либо с (*q, 1 - q*). Получая состояние Боб должен определить, какое распределение вероятности использовала Алиса для приготовления состояния. Очевидно, что Боб не всегда способен определить это с достоверностью 100%. Тем не менее, этот пример (по аналогии с достижимой информацией для квантовой системы, приготавливаемой в одном состоянии из набора смешанных состояний) очень важен. Что является наиболее важным и замечательным - так это то, что фундаментальные объекты в квантовой механике - чистые квантовые состояния - обладают свойствами различимости, что является существенно отличным и существенно богатым свойством, нежели чем для фундаментальных объектов классической теории информации, таких как “0” и “1”.

Теорема о запрете копирования (клонирования)

Теорема о запрете клонирования сулит другую перспективу в плане ограничения на достижимую квантовую информацию, по сравнению с классической. Классическая информация, безусловно, может быть копирована. Это точно можно сделать с цифровой информацией, например. создавая копии файлов с текстами, заложенными в компьютер. Теорема о запрете клонирования утверждает, что квантовая механика не позволяет точно копировать неизвестное квантовое состояние и накладывает некоторые ограничения на возможность создания примерных копий.

На первый взгляд, теорема о запрете клонирования выглядит довольно странно. В конце концов, не является ли классическая физика частным случаем квантовой механики? Почему мы можем копировать классическую информацию, если нельзя копировать квантовую? Ответ состоит в том, что эта теорема не запрещает копировать все квантовые состояния. Она лишь утверждает, что нельзя копировать неортогональные квантовые состояния. Далее, теорема подразумевает, что невозможно построить квантовый прибор так, что бы при наличии на входе состояний $|\psi\rangle$ и $|\varphi\rangle$, на выходе будет две копии входного состояния $|\psi\rangle|\psi\rangle$ или $|\varphi\rangle|\varphi\rangle$. С другой стороны, если $|\psi\rangle$ и $|\varphi\rangle$ ортогональны, то теорема не запрещает их копирование. Действительно, довольно просто сконструировать квантовые схемы, которые копируют такие состояния. Это замечание разрешает кажущееся противоречие между теоремой о запрете клонирования и способностью копировать классическую информацию. Для различных состояний классическая информация может восприниматься как представляемая ортогональными состояниями!

Доказательство теоремы.

Предположим, что у нас есть квантовое устройство с двумя портами (slots), обозначенными *A* и *B*. Порт *A* - это *порт данных*. В него помещается неизвестное, но чистое квантовое состояние $|\psi\rangle$. Это состояние требуется скопировать на порте *B* - это т.н. *порт - мишень*. Предположим, что порт - мишень изначально находится в некоем стандартном чистом состоянии $|s\rangle$.Таким образом, начальное состояние всего копирующего устройства есть:

$$|\psi\rangle\otimes|s\rangle. \qquad (5.8)$$

Процедура копирования подвергается некоторой унитарной эволюции *U*. В идеальном случае

$$|\psi\rangle\otimes|s\rangle\rightarrow(U)\rightarrow U\left(|\psi\rangle\otimes|s\rangle\right)=|\psi\rangle\otimes|\psi\rangle. \qquad (5.9)$$

Предположим, что процедура копирования работает для каких-нибудь двух особых чистых состояний $|\psi\rangle$ и $|\varphi\rangle$. Тогда,

$$U\left(|\psi\rangle\otimes|s\rangle\right)=|\psi\rangle\otimes|\psi\rangle. \qquad (5.10)$$

$$U\left(|\varphi\rangle\otimes|s\rangle\right)=|\varphi\rangle\otimes|\varphi\rangle. \qquad (5.11)$$

Находя скалярное (= внутреннее) произведение этих двух уравнений, получаем, что

$$\left(\langle\varphi|\otimes\langle s|\right)U^{\dagger}U\left(|\psi\rangle\otimes|s\rangle\right)=\left(\langle\psi|\otimes\langle\psi|\right)\left(|\varphi\rangle\otimes|\varphi\rangle\right).$$

Унитарность дает $U^{\dagger}U=I$, а раскрывая прямое произведение векторов, и учитывая, что $\langle s|s\rangle=I$ получаем:

$$\langle\psi|\varphi\rangle=\left(\langle\psi|\varphi\rangle\right)^{2}. \qquad (5.12)$$

Но уравнение $x^2 = x$ имеет только два решения: $x = 0$ и $x = 1$, поэтому $|\psi\rangle = |\varphi\rangle$ или $|\psi\rangle$ и $|\varphi\rangle$ - ортогональны! Следовательно, копирующее устройство может копировать только состояния ортогональные друг другу. Отсюда - в общем случае квантовые состояния нельзя копировать (клонировать). Например, квантовый клонер не может клонировать состояния кубита $|\psi\rangle = 0$ и $|\varphi\rangle=\left(|0\rangle+|1\rangle\right)/\sqrt{2}$ т.к. эти состояния неортогональны.