# Лекция 6

II. Основные понятия квантовой теории информации (продолжение)

1. Унитарные преобразования и их свойства
2. Теорема о запрете клонирования квантовых состояний. Ее связь с достижимой информацией и различимостью состояний.
3. Граница и информация Холево. Примеры. Априорная и апостериорная энтропии.
4. Передача (transposition) квантовой информации. Понятие квантового канала связи. Точность воспроизведения информации (fidelity). Теорема Б.Шумахера о кодировании при отсутствии шума.

Рассмотрим другое доказательство теоремы о запрете клонирования (W.Wooters W.Zurek 1982).

Пусть квантовый источник (квантовая система *M*) генерирует состояния $|a_M\rangle$.

При квантовом копировании мы хотим создать копии этих состояний в другой квантовой системе *X*. Итак, при копировании исходный сигнал (состояние) квантовой системы *M* не возмущается, а состояние системы *X* становится его копией. Другими словами состояние комбинированной системы развивается по закону:

$$|a_M, 0_X\rangle \to |a_M, a_X\rangle, \qquad (6.1)$$

где $|0_X\rangle$ - это некоторое начальное ("нулевое") состояние системы *X*.

Доказательство. Пусть существует устройство, которое приготавливает копии произвольного состояния системы *M* в системе *X*. Тогда для двух различных состояний системы *M* $|a_M\rangle$ и $|b_M\rangle$ копирующая машина работает следующим образом:

$$|a_M, 0_X\rangle \to |a_M, a_X\rangle,$$

$$|b_M, 0_X\rangle \to |b_M, b_X\rangle.$$

Рассмотри теперь состояние суперпозиции (согласно принципу суперпозиции такое состояние существует):

$|c_M\rangle = |a_M\rangle + |b_M\rangle$ (не будем следить за нормировкой). Если конечное состояние системы *X* есть точная копия, то

$|c_X\rangle = |a_X\rangle + |b_X\rangle$. Но из общих принципов квантовой механики следует, что эволюция квантовой системы должна происходить по линейному закону, т.е. под действием унитарных преобразований.

<u>Замечание.</u> Свойства унитарности преобразований (Д.Бом. Квантовая теория)

1. Нормировка произвольной волновой функции остается неизменной при унитарном преобразовании (т.е. УП соответствует классической операции поворота, при которой сохраняется длина вектора).
2. Унитарное преобразование не меняет ортогональности исходных волновых функций.
3. Связи между преобразованными при УП операторами остаются такими же как и между непреобразованными операторами.

4. Собственные значения матриц не изменяются при УП. В частности не меняется след матрицы, что позволяет вычислять его в удобных представлениях.

Из унитарности преобразований следует, что

$$|c_M, 0_X\rangle = |a_M, 0_X\rangle + |b_M, 0_X\rangle \to$$

$$\to |a_M, a_X\rangle + |b_M, b_X\rangle \neq |c_M, c_X\rangle, \qquad (6.2)$$

Видно, что знак равенства во второй строчке (6.2) невозможен, т.к. $|c_M, c_X\rangle = |a_M, a_X\rangle + |a_M, b_X\rangle + |b_M, a_X\rangle + |b_M, b_X\rangle$. Следовательно, если два различных состояния могут быть копированы точно, то их линейная суперпозиция - нет!

Заметим, что копирование может быть выполнено, если состояния являются взаимно ортогональными (второе и третье слагаемые в 6.2). Например, можно копировать наблюдаемую, у которой собственные состояния являются состояниями системы *M*, а затем, использовать классическую информацию о конечных состояниях для изготовления необходимого количества копий. С другой стороны, квантовый сигнал, представляющий собой набор неортогональных состояний не может быть в точности скопирован.

Мы остановились на теореме о запрете клонирования. Было показано, что квантово-механическая машина, приготавливающая копии квантовых состояний может это сделать лишь для совпадающих или ортогональных состояний. Происходит это из-за того, что как и все квантовые операции, операция клонирования должна быть унитарной и сохранять скалярное (внутреннее) произведение. Мы доказали, что невозможно приготовить совершенную копию неизвестного квантового состояния используя унитарное преобразование (эволюцию). При этом возникает несколько вопросов.

- Что будет, если мы попытаемся копировать смешанное состояние?
- Что будет, если мы захотим получить неточные копии, которые, тем не менее достаточно хороши, с точки зрения потребности конкретной задачи?

Ответ на них составляет предмет отдельной главы теории квантовой информации, которого мы касаться не будем. Лишь вкратце заметим, что даже если в копирующей машине используются неунитарные операции, то по-прежнему невозможно копировать неортогональные чистые состояния, до тех пор пока мы не задумываемся об удовлетворительности соответствия копируемых состояний исходным. То же относится и к смешанным состояниям, хотя для доказательства используется более умозрительный подход даже в таком вопросе “что означает понятие копирования смешанного состояния?”

Рассмотрим проблему копирования несколько с другой стороны. В криптографии при обмене секретными сообщениями необходимо заботиться в возможности перехвата. Тот, кто перехватывает сообщения (обычно, этот персонаж носит имя Ева) должен уметь различить неортогональные состояния, поскольку именно их и передает Алиса.

Пусть Ева приготавливает свой измерительный прибор в исходном состоянии $|F\rangle$. Ее цель - различить неортогональные состояния $|\psi\rangle$ и $|\varphi\rangle$ не возмущая их. Другими словами, она хочет выполнить унитарную операцию:

$$
\begin{aligned}
&|\psi\rangle|F\rangle \to |\psi\rangle|F_\psi\rangle \\
&|\varphi\rangle|F\rangle \to |\varphi\rangle|F_\varphi\rangle
\end{aligned}
\qquad (6.3)
$$

Из унитарности операции следует, что $\langle\psi|\varphi\rangle\langle F|F\rangle = \langle\psi|\varphi\rangle\langle F_\psi|F_\varphi\rangle$, т.е. $\langle F_\psi|F_\varphi\rangle = 1$. Отсюда видно, что конечное значение измерительного прибора будет одинаковым в обоих случаях! Ева не возмутила (не исказила) два неортогональных состояния, но она и не получила никакой информации ою этих состояниях, т.к. $\langle F_\psi|F_\varphi\rangle = 1$. Более общее измерение (но все еще не самое общее!), которое возмущает исходные состояния, так что $|\psi\rangle \to |\psi'\rangle$ и $|\varphi\rangle \to |\varphi'\rangle$, дает

$$
\begin{aligned}
&|\psi\rangle|F\rangle \to |\psi'\rangle|F_\psi\rangle \\
&|\varphi\rangle|F\rangle \to |\varphi'\rangle|F_\varphi\rangle
\end{aligned}
\qquad (6.4)
$$

Из унитарности следует, что $\langle\psi|\varphi\rangle = \langle\psi'|\varphi'\rangle\langle F_\psi|F_\varphi\rangle$. Самый лучший вариант для Евы, в смысле оптимального различения двух состояний, соответствует минимуму выражения $\langle F_\psi|F_\varphi\rangle$. Минимум осуществляется, когда $\langle\psi'|\varphi'\rangle = 1$, что как раз означает неразличимость исходных состояний $|\psi\rangle$ и $|\varphi\rangle$ после операции, выполняемой Евой. Этот пример служит наглядной иллюстрацией связи между *информацией*, извлекаемой при измерении *и возмущением исходных состояний.*

Напоминание (из прошлой лекции)

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 $H(X{:}Y) \leq H(X)$. 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.**

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”.

Какова связь между копированием и достижимой информацией? Пусть Алиса приготавливает одно из двух неортогональных состояний $|\psi\rangle$ и $|\varphi\rangle$ с соответствующими вероятностями $p$ и $(1 - p)$. Предположим, что в этом случае достижимая информация Боба есть $H(p)$, т.е. законами квантовой механики разрешено Бобу получить достаточно информации при его измерении о том, какое из двух состояний $|\psi\rangle$ или $|\varphi\rangle$ было приготовлено Алисой. Боб может копировать состояния очень простым способом. Он бы выполнил измерение, определив, какое состояние $|\psi\rangle$ или $|\varphi\rangle$ было приготовлено Алисой и как только он завершил идентификацию он бы приготовил копии состояний, которые получил от Алисы. Таким образом, теорема о запрете копирования явилась бы следствием того факта, что достижимая информация об этих состояниях строго меньше, чем $H(p)$. Можно обратить эти рассуждения и показать, что из теоремы о запрете клонирования следует, что достижимая информация меньше чем $H(p)$! Это делается так. Представим, что возможно клонировать неортогональные состояния. После получения состояния $|\psi\rangle$ или $|\varphi\rangle$ от Алисы, Боб смог бы повторно применить клонирующее устройство для получения состояния $|\psi\rangle^{\otimes n}$ или $|\varphi\rangle^{\otimes n}$. В пределе больших n эти два состояния становятся практически ортогональными и возможно различить их с произвольной точностью при проективных измерениях.

Таким образом, если было бы возможным копирование, то Боб мог бы идентифицировать с произвольно высокой вероятностью успеха какое из двух состояний $|\psi\rangle$ или $|\varphi\rangle$ было приготовлено Алисой и, таким образом, достижимая информация была бы $H(p)$. <u>Следовательно, теорему о запрете клонирования можно рассматривать как эквивалент утверждения о том, что в квантовой механике достижимая информация для неортогональных состояний в общем случае меньше, чем энтропия приготовления</u>.

Хочется подчеркнуть, что скрытая природа квантовой информации играет центральную роль в мощности квантовых вычислений и достижимая информация есть количественное проявление природы квантовой информации. К сожалению не существует общего рецепта вычисления достижимой информации (по крайней мере он неизвестен). В то же время имеется ряд важных достижимых границ, которые строго обоснованы. Наиболее важная из них - т.н. граница Холево.

***<u>Граница Холево</u>***. Она играет очень важную роль в теории квантовой информации.

<u>Теорема</u> о границе Холево. Предположим, что Алиса приготавливает состояние $\rho_X$, где $X = 0,...n$ с вероятностями $p_0,...p_n$. Пусть Боб выполняет некое измерение этого состояния (т.н. *POVM* - probability-operator-valued measure - дающее максимальное относительно всех вероятностных мер значение взаимной информации = при наилучшем измерении сигнала на выходе) описываемое

множеством элементов $\{E_y\} = \{E_0,...,E_m\}$. Результат измерения Боба есть $Y$. Граница Холево утверждает, что при любых измерениях Боб может достигнуть:

$$H(X:Y) \le S(\rho) - \sum_x p_x S(\rho_x), \tag{6.5}$$

где $\rho = \sum_x p_x \rho_x$.

Таким образом, граница Холево является верхней границей достижимой информации. Величина, фигурирующая в правой части (5.13) настолько важна в квантовой теории информации, что получила отдельное имя - *информация (или количество) Холево*. Иногда ее обозначают как $\chi$.

Граница Холево играет ключевую роль при доказательстве многих положений квантовой теории информации. Рассмотрим несколько примеров.

<u>Пример 1</u>. В теории квантовой информации доказывается теорема (см.**), что

$$S(\rho) - \sum_x p_x S(\rho_x) \le H(X), \tag{6.6}$$

где равенство достигается только для тех состояний $\rho_x$, которые имеют ортогональные основания (т.е. определены на множестве ортогональных состояний). Здесь $\rho = \sum_x p_x \rho_x$, а $p_x$ - набор вероятностей для состояний $\rho_x$ ( т.е. $\rho_x = |x_i\rangle\langle x_i|$ ) . Предположим, что неравенство в (6.6) - строгое.

Тогда, из теоремы о границе Холево сразу следует, что *H(X:Y)* строго меньше *H(X)*. Следовательно невозможно достоверно определить *X*, исходя из результатов измерений *Y*. Это обобщает наше понимание того, что если состояния, приготавливаемые Алисой неортогональны, то Боб не может определить с достоверностью, какое состояние было приготовлено Алисой.

<u>Пример 2.</u> (конкретный)

Пусть Алиса приготавливает единичный кубит в одном из двух квантовых состояний, в соответствии с результатом подбрасывания монеты. При выпадении орла Алиса готовит состояние |0>, если же выпадает решка, то она готовит состояние $\cos\theta|0\rangle + \sin\theta|1\rangle$, где $\theta$ - некоторый действительный параметр. Цель Боба - определить какое из двух состояний было послано.

В базисе |0>, |1> состояние $\rho$ можно записать следующим образом:

$$\rho = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} \cos^2\theta & \cos\theta\sin\theta \\ \cos\theta\sin\theta & \sin^2\theta \end{bmatrix}. \tag{6.7}$$

Чтобы вычислить границу $S(\rho) - \sum_x p_x S(\rho_x)$, найдем S($\rho$). Для этого найдем собственные значения матрицы $\rho$:

$$\rho = \begin{bmatrix} \dfrac{1+\cos^2\theta}{2} & \dfrac{\cos\theta\sin\theta}{2} \\ \dfrac{\cos\theta\sin\theta}{2} & \dfrac{\sin^2\theta}{2} \end{bmatrix}$$

Уравнение на собственные значения:

$$\left(\frac{1+\cos^2\theta}{2}-\lambda\right)\left(\frac{\sin^2\theta}{2}-\lambda\right)-\frac{\cos^2\theta\sin^2\theta}{4}=0$$

$$\frac{\left(1+\cos^2\theta-2\lambda\right)\left(\sin^2\theta-2\lambda\right)}{2}-\frac{\cos^2\theta\sin^2\theta}{4}=0$$

$$\sin^2\theta-2\lambda+\cos^2\theta\sin^2\theta-2\lambda\cos^2\theta-2\lambda\sin^2\theta+4\lambda^2-\cos^2\theta\sin^2\theta=0$$

$$\sin^2\theta-2\lambda-2\lambda\left(\cos^2\theta+\sin^2\theta\right)+4\lambda^2=0$$

$$\sin^2\theta-4\lambda+4\lambda^2=0$$

$$\lambda_{1,2}=\frac{1\pm\cos\theta}{2}$$

Тогда $S(\rho)=-\sum_x\lambda_x\log\left(\lambda_x\right)$ (см. 5.2):

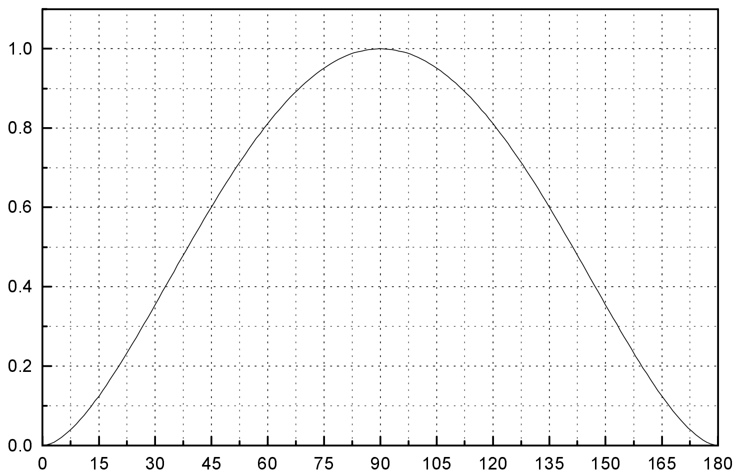
$$S(\rho)=-\left[\frac{1+\cos\theta}{2}\log\left(\frac{1+\cos\theta}{2}\right)+\frac{1-\cos\theta}{2}\log\left(\frac{1-\cos\theta}{2}\right)\right]=$$

$$=H\left(\frac{1\pm\cos\theta}{2}\right)$$

Теперь найдем величину $\sum_x p_x S\left(\rho_x\right)$. Собственные значения каждой из двух матриц плотности, задающих исходное состояние (5.15) и входящих в эту сумму равны $\lambda_x^{(1)}=(0,\,1)$ и $\lambda_x^{(2)}=(0,1)$. Поэтому

$$\sum_x p_x S\left(\rho_x\right)=\frac{1}{2}\left[-\sum_x\lambda_x^{(1)}\log\lambda_x^{(1)}\right]+\frac{1}{2}\left[-\sum_x\lambda_x^{(2)}\log\lambda_x^{(2)}\right]=\left[-\sum_x\lambda_x\log\lambda_x\right]=0$$

Отсюда, граница Холево определяется бинарной энтропией Шеннона $H\left(\frac{1\pm\cos\theta}{2}\right)$. Из рисунка видно, что максимум границы достигается при θ = π/2 и отвечает уровню 1 бит.



По вертикали отложено значение границы Холево (фактически - это бинарная энтропия). По горизонтали - значение параметра θ в град.
Это, в свою очередь, означает, что Алиса готовит состояния, которые выбирает из ортогонального набора |0> либо |1> с равной вероятностью. Значит Боб может достоверно определить какое из (ортогональных) состояний было приготовлено Алисой. Для других значений θ граница Холево строго меньше единицы, т.е. Боб не может определить достоверно, какое из неортогональных состояний было приготовлено. С другой стороны, ясно, что при θ = 9 два состояния неразличимы. Поэтому при этом значении параметра Боб может угадать, какое состояние было послано с вероятностью 50%.

Границу (или информацию Холево) можно ввести несколько по-другому. Переобозначим величины, входящие в определение (6.5): $H(X:Y) \le S(\rho) - \sum_x p_x S(\rho_x)$:

$$S(\rho) = S(\rho)_{apr} \ge H,$$

$$\sum_x p_x S(\rho_x) = S(\rho)_{aps} \ge 0.$$

Первая величина называется априорной (безусловной) энтропией. Она описывается соответствующими диагональными элементами матрицы плотности.
Апостериорная (условная) энтропия - определяет вносимую каналом связи ошибку в классической схеме. В квантовой теории она отвечает за квантовую недетерминированность сигналов, связанную с соотношением неопределенности... В отсутствие классических шумов и помех апостериорная энтропия обращается в нуль. Сигналы на входе и на выходе канала при этом коррелированы и взаимная информация $I(\rho) = S = H$.
Достижимая информация определяется выражением $I_{acc} = S(\rho) = H$, что соответствует случаю, когда сигнал формируется из ортонормированных собственных состояний $\psi_n$, а операторы на выходе коммутируют с оператором плотности, т.е. когда $S(\rho)_{aps} = H(\rho)_{aps} = 0$.

В случае, когда сигналы $\rho_a = \pi_a$ - это чистые состояния с нулевой энтропией, граница Холево просто сводится к утверждению, что

$$H(X:Y) \le S(\rho),$$

где $\rho = \sum_a p(a)\pi_a$ - оператор плотности для ансамбля чистых сигналов (состояний). И хотя Шенноновская энтропия *H(X)* сообщения, посылаемого источником в общем случае больше, чем энтропия фон Неймана $S(\rho)$ ансамбля сигналов, достижимая информация (классическая) ограничена величиной $S(\rho)$.
Таким образом ясно, что граница Холево устанавливает связь между энтропией фон Неймана квантового ансамбля и (***классической***) взаимной Шенноновской информацией ***квантового*** канала связи.
Такая связь, однако, является довольно слабой. Дело в том, что теорема Холево формулируется в виде неравенства. Поэтому, в принципе, можно сконструировать такой источник квантовых сигналов, для которого взаимная информация *H(X:Y)* и близко не достигает $S(\rho)$ при любом выборе наблюдаемой *Y* при декодировании. Поэтому, хотя из теоремы Холево и следует

информационно-теоретическое значение величины $S(\rho)$, она не дает интерпретации $S(\rho)$ в терминах классической теории информации. Например, мы не могли бы использовать теорему Холево при интерпретации квантовой теории некоторого макросостояния термодинамической системы, как дающую меру ресурсов, необходимых для представления информации о микросостояниях системы.
Ответ на этот вопрос дает квантовая теорема кодирования Б.Шумахера (1995). В ней классическая идея о двоичной логике в терминах битов заменяется моделью квантовых битов - двухуровневых систем. Эти квантовые биты являются фундаментальными единицами квантовой информации. В теореме утверждается, что ***энтропия фон Неймана*** $S(\rho)$ ***ансамбля является просто средним числом кубитов, необходимых для кодирования состояний ансамбля при помощи идеальной кодирующей системы***. Теорему можно рассматривать как краеугольный камень альтернативного подхода в квантовой теории информации. Вместо использования классической теории информации к вероятностям, вычисленным по законам квантовой механики (подход Левитина и Холево), мы пересмотрим понятия кодирования и мер информации, которые сами по себе определенно являются квантовыми величинами.

**Теорема о квантовом кодировании при отсутствии шума** (*quantum noiseless coding theorem*)
Пусть $M$ - источник квантового сигнала, который представляется ансамблем. Этот ансамбль описывается оператором плотности $\rho$. Пусть имеются два числа $\delta,\ \varepsilon > 0$.

1. Предположим, что имеется $S(\rho)+\delta$ кубитов. Тогда для достаточно большого $N$, группы из $N$ сигналов из источника $M$ могут быть переданы с помощью имеющегося набора кубитов с качеством $F > 1 - \varepsilon$.
2. Предположим, что имеется $S(\rho)-\delta$ кубитов. Тогда для достаточно большого $N$, при передаче групп из $N$ сигналов от источника с помощью имеющегося набора кубитов, качество передачи будет $F < \varepsilon$.

Комментарии к теореме.
N - это число независимых испытаний с функцией распределения $p_n$.
Энтропию фон Неймана ансамбля сигналов (чистых состояний) можно интерпретировать как число кубитов на сигнал, необходимое для передачи с качеством, близким к единице. Если имеется больше, чем $S(\rho)$ кубитов, при увеличении группы сигналов можно добиться произвольно высокого качества $F$. Если же доступно меньше, чем $S(\rho)$ кубитов, качество $F$ стремиться к нулю.
Более того, $S(\rho)$ является (в некотором смысле) количеством кубитов, необходимым для передачи части перепутанной системы при поддержании качества $F$ всего состояния близким к единице
Таким образом, энтропия $S$ является мерой физических ресурсов, необходимых для представления информационного содержания о системе смешанных состояний. Неважно каким образом получена эта система смешанных состояний - из стохастического процесса или при выбрасывании части перепутанных состояний. **Квантовая энтропия фон Неймана измеряется в кубитах.**
При доказательстве теоремы используется в основном классический аппарат с небольшими изменениями. Вместо распределения вероятностей -

рассматривается набор собственных значений оператора плотности. Кроме того используется две (вспомогательных) леммы, доказанных Б.Щумахером.
Заметим, что в квантовой теории информации рассматриваются и соответствующие теоремы для зашумленных каналов. Кроме того вводится понятие качества для смешанных состояний.

**<u>Перенос (transposition) квантовой информации. Понятие квантового канала связи.</u>**
В квантовой теории информации необходимо различать понятия *копирования* состояний и *перенос* (transposition) информации из системы $M$ в систему $X$. При переносе состояние системы $M$ передается к системе $X$ без сохранения копии начального состояния:

$$\left|a_M, 0_X\right\rangle \to \left|0_M, a_X\right\rangle, \qquad (6.8)$$

где $\left|0_X\right\rangle$ и $\left|0_M\right\rangle$ - некоторые “нулевые” состояния систем $X$ и $M$. После переноса сигнал полностью возникает в кодирующей системе $X$, исчезая в системе $M$. Одним из экзотических примеров переноса служит явление квантовой телепортации.
Перенос является унитарной операцией для произвольных состояний из системы $M$. Это обеспечивает сохранение скалярного (внутреннего) произведения:
$\left\langle a_X \middle| b_X\right\rangle = \left\langle a_M \middle| b_M\right\rangle$ для любых сигналов (состояний) $\left|a_M\right\rangle$ и $\left|b_M\right\rangle$. Это может происходить только, если размерность гильбертова пространства системы $X$ $\mathcal{H}_X$ не меньше чем размерность гильбертова пространства системы $M$ $\mathcal{H}_M$. Как происходит процесс переноса с помощью унитарного преобразования U? Для ответа на этот вопрос необходимо понять как ортогональный базис из гильбертова пространства системы $M$ переходит в ортогональный базис гильбертова пространства системы $X$ (свойство 2 УП). После этого эволюция других состояний будет очевидна из-за линейности.

Перенос является *обратимой операцией*, поскольку состояние сигнала может быть передано назад из $X$ в $M$ посредством унитарного преобразования $U^{-1}$. Поэтому система связи, основанная на переносе, представляется в следующем виде. Со стороны кодирования, сигнал (квантовое состояние), исходящий из системы $M$, поступает в процессе унитарного преобразования U в кодирующую систему $X$. Система $X$ переправляется от передатчика к получателю. С декодирующей стороны выполняется унитарное преобразование $U^{-1}$ для возвращения сигнала из $X$ в $M^*$ - как идентичной копии системы $M$. В символьном виде:

$$M \xrightarrow[U]{} X \xrightarrow[U^{-1}]{} M^*.$$

Система $X$ называется квантовым каналом связи и поддерживает перенос состояний из системы $M$ в систему $M^*$. В общем случае для совершенной передачи (переноса) квантовый канал должен быть достаточно емким: необходимо, чтобы $dim\mathcal{H}_X \geq dim\mathcal{H}_M$. Впрочем, иногда совершенная передача (перенос) не является необходимой; требуется лишь приближенный перенос информации из системы $M$ в систему $M^*$. В зависимости от характеристик сигнала можно требовать от канала связи меньшей емкости - смотря насколько качественно нам нужно его воспроизвести.

Под сигналом далее будем понимать передаваемое квантовое состояние вида:

$$\rho = \sum_a p(a)\pi_a ,$$

где $\pi_a = |a_M\rangle\langle a_M|$ - оператор плотности (для чистого состояния - это оператор проецирования), отвечающий векторам-состояниям $|a_M\rangle$ квантовой системы *M*, передаваемым с вероятностью *p(a)*.

Для того чтобы определить эффективность канала нам нужно ввести меру качества передачи или фиделити (fidelity) В русском языке этот термин не имеет устоявшегося отображения. Будем называть его *качеством* (передачи информации). Пусть начальный передаваемый сигнал системы *M* есть $|a_M\rangle$. Он представляется оператором плотности $\pi_a = |a_M\rangle\langle a_M|$. Конечное состояние *M** будет состоянием, представленным оператором плотности $w_a$. В общем случае это состояние не является чистым, поэтому $w_a$ - необязательно оператор проецирования. Для того, чтобы проверить насколько близко состояние $w_a$ находится к состоянию $\pi_a$ можно произвести контрольное измерение наблюдаемой $\pi_a$. Это измерение имеет два возможных исхода: “1” - показывающее, что конечное состояние совпадает с начальным и “0” - показывающее, что конечное состояние отлично от начального. Тогда вероятность того, что конечное состояние $w_a$ прошло испытание есть $Sp(\pi_a w_a)$.

Определим точность воспроизведения информации - *качество* как общую вероятность того, что набор сигналов (или ансамбль сигналов) приготовленный в *M* и переданный в *M** прошел контрольный тест, сравнивающий его с начальным состоянием:

$$F = \sum_a p(a) Sp(\pi_a w_a). \tag{6.9}$$

Ясно, что *качество* лежит в интервале между 0 и 1. Оно равна единице только в случае, когда передача всех возможных сигналов является совершенной (идеальной). *F* будет близко к единице если:

- сигналы с большой вероятностью *p(a)* искажены несильно при передаче, поэтому $w_a$ приблизительно совпадает с $\pi_a$;
- набор сигналов, который сильно возмущен, т.е. имеющий $w_a$ сильно отличную от $\pi_a$ имеет малую вероятность появления *p(a)*.