ГЛАВА 3

ПРИМЕНЕНИЯ СЦЕПЛЕННЫХ СОСТОЯНИЙ

§ 3.1. Квантовое состояние как информационный ресурс

В этом параграфе нам потребуются элементарные сведения об эволюциях квантовой системы. В дальнейшем, в главе 6 этот вопрос будет рассмотрен углубленно и с общих позиций теории открытых квантовых систем. Математически настроенному читателю мы советуем перейти к главе 4 и вернуться к этому материалу после главы 6. Пока же достаточно знать следующее:

1) Обратимые эволюции квантовой системы описываются унитарными операторами U: вектор исходного чистого состояния ψ преобразуется в результате такой эволюции в $U\psi$. Соответственно, оператор плотности S преобразуется в USU^*.

2) Важнейший пример необратимой эволюции — изменение состояния в результате измерения. Простейшее идеальное квантовое измерение связывается с ортонормированным базисом $|e_x\rangle$, векторы которого индексированы возможными исходами измерения x. Если система перед измерением находится в состоянии S, то в результате такого измерения она переходит с вероятностью $\langle e_x \mid Se_x\rangle$ в состояние $|e_x\rangle\langle e_x|$. Весь статистический ансамбль после измерения разбивается на подансамбли, соответствующие различным исходам x, и описывается состоянием $\langle e_x | S e_x \rangle$

$$S' = \sum_x |e_x\rangle\langle e_x \mid Se_x\rangle\langle e_x|, \tag{3.1}$$

вообще говоря отличным от исходного. Таким образом, квантовое измерение включает неустранимое воздействие на наблюдаемую систему, которое изменяет ее состояние, даже если исходы наблюдения «не считываются». В этом принципиальное отличие квантовых «наблюдаемых» от классических случайных величин, наблюдение которых не изменяет статистический ансамбль, а сводится к простому отбору его представителей.

Квантовое состояние приготавливается макроскопическими устройствами. Изменяя параметры устройства, мы изменяем параметры состояния, и таким образом получаем возможность «записывать» классическую информацию в квантовом состоянии. Простейший квантовый канал связи математически задается семейством (выходных или сигнальных) состояний S_x, где параметр x пробегает входной алфавит. Отображение $x \to S_x$ в сжатой форме содержит описание физического процесса, порождающего состояние S_x. Например, пусть $x = 0, 1$, причем S_1 когерентное состояние поля излучения лазера, а S_0 вакуумное состояние. В этом случае мы имеем канал с двумя чистыми неортогональными состояниями.

Для того чтобы извлечь классическую информацию, содержащуюся в квантовом состоянии, необходимо произвести измерение. В приведенном выше примере такую роль играет любой приемник лазерного излучения с возможной последующей обработкой результатов измерения. Если измерение задается базисом $|e_y\rangle$, то условная вероятность получить исход y, при условии, что был послан сигнал x, дается формулой

$|e_y\rangle$

$$P(y|x) = \langle e_y \mid S_x e_y \rangle. \tag{3.2}$$

Таким образом, для фиксированного измерения мы получаем обычный канал связи. Это дает возможность поставить вопрос о максимальном количестве классической информации, которое может быть передано по данному квантовому каналу связи и о его пропускной способности. Этот вопрос будет детально рассмотрен в главе 5. Отметим здесь лишь один факт, имеющий принципиальное значение:

Пропускная способность любого квантового канала ограничена сверху величиной $\log \dim \mathcal{H}$, причем эта величина достигается для «идеального» канала, сигнальные состояния которого образованы векторами ортонормированного базиса в пространстве $\mathcal{H}$, а измерение задается этим же ортонормированным базисом. Таким образом, размерность гильбертова пространства является мерой максимального информационного ресурса квантовой системы.

Рассмотрим теперь следующий вопрос. Нелокальный, с классической точки зрения, характер ЭПР-корреляций наводит на мысль попытаться использовать их для мгновенной передачи информации. Покажем, что этого невозможно достичь, находясь в рамках квантовой механики (с точки зрения которой ЭПР-корреляции не противоречат локальности). Рассмотрим две квантовые системы A

эбина не передаёта

и B, в пространствах $\mathcal{H}_A$ и $\mathcal{H}_B$ соответственно, которые находятся в сцепленном состоянии S_{AB}. В случае, представляющем интерес, системы пространственно разделены, хотя формально это ни в чем не выражается. Система A получает классическую информацию, содержащуюся в значениях параметра x, которая может быть использована для выполнения произвольных унитарных операций U_x в пространстве $\mathcal{H}_A$. При этом состояние системы AB переходит в $S_x = (U_x \otimes I_B) S_{AB} (U_x \otimes I_B)^*$, таким образом, классическая информация записывается в квантовом состоянии составной системы. В свою очередь, над системой B может быть произведено произвольное измерение, описываемое ортонормированным базисом $|e_y\rangle$ в $\mathcal{H}_B$. Легко видеть, что результирующая переходная вероятность (3.2) не зависит от x, а значит количество передаваемой информации в самом деле равно нулю.

§ 3.2. Сверхплотное кодирование

Хотя ЭПР-корреляции сами по себе не позволяют передавать информацию, оказывается, что наличие таких корреляций между системами позволяет увеличить максимальное количество классической информации, передаваемой от A к B, вдвое, если между системами имеется идеальный квантовый канал связи, т. е. возможность безошибочно передать любое квантовое состояние. Таким образом, ЭПР-корреляции выступают как «катализатор» при передаче классической информации через квантовый канал связи, и с этот точки зрения, также представляют собой особого рода информационный ресурс.

Рассмотрим системы A и B, каждая из которых представляет собой q-бит, между которыми имеется идеальный квантовый канал связи. Из того что было сказано выше в § 3.1, вытекает, что максимальное количество классической информации, которое может быть передано от A к B, равно одному биту, и получается при кодировании бита в два ортогональных вектора, например,

$$0 \to |0\rangle, \quad 1 \to |1\rangle.$$

Протокол «сверхплотного кодирования», предложенный Виснером в 1992 г., имеет в своей основе простой математический факт: базис Белла

$$|e_+\rangle = |00\rangle + |11\rangle,\ |e_-\rangle = |00\rangle - |11\rangle,\ |h_+\rangle = |10\rangle + |01\rangle,\ |h_-\rangle = |10\rangle - |01\rangle$$

в системе из двух q-битов AB (мы используем канонический базис $|0\rangle, |1\rangle$ в пространстве одного q-бита и опускаем нормировочный множитель $1/\sqrt{2}$) может быть получен из одного вектора действием «локальных» унитарных операторов, т. е. операторов, действующих нетривиально только в пространстве q-бита A, например

$$|e_-\rangle = (\sigma_z \otimes I)|e_+\rangle, \quad |h_+\rangle = (\sigma_x \otimes I)|e_+\rangle, \quad |h_-\rangle = -i(\sigma_y \otimes I)|e_+\rangle.$$

Таким образом, если AB изначально находится в состоянии $|e_+\rangle$, A может закодировать 2 бита классической информации в 4 состояния базиса Белла, производя только локальные операции, а затем (физически) послать свой q-бит B по идеальному квантовому каналу. Тогда, производя измерение в базисе Белла, B получает 2 бита классической информации. Конструкции протоколов сверхплотного кодирования и телепортации допускают обобщение на случай пространства произвольной конечной размерности (ср. далее в главе 8).

§ 3.3. Квантовая телепортация

До сих пор говорилось о передаче классической информации через квантовый канал связи. Такая информация может быть «записана» в квантовом состоянии и передана через физический канал. Однако квантовое состояние и само по себе является информационным ресурсом постольку, поскольку имеет статистическую неопределенность. Оказывается, что информация, содержащаяся в неизвестном квантовом состоянии, имеет качественные отличия от классической, и поэтому заслуживает специального термина *квантовая информация*. Наиболее ярким отличием квантовой информации является невозможность копирования (no cloning). Очевидно, что классическая информации может воспроизводиться в любом количестве. Но физический прибор, который бы выполнял аналогичную задачу для квантовой информации, противоречит принципам квантовой механики, так как преобразование

$$|\psi\rangle \to \underbrace{|\psi\rangle \otimes \ldots \otimes |\psi\rangle}_{n}$$

является нелинейным, и не может быть осуществлено унитарным оператором. Конечно, это можно сделать каждый раз специальным прибором для данного конкретного состояния (и даже для фиксированного набора ортогональных состояний), но не существует

не унитарный оператор

универсального прибора, который бы размножал произвольное квантовое состояние.

Каким образом может быть передано квантовое состояние? Очевидно, что можно просто физически переслать саму систему. Гораздо более интересный и нетривиальный способ — *телепортация квантового состояния*, при которой сама система физически не передается, а передается лишь классическая информация [1]. При этом существенным дополнительным ресурсом, который вновь играет роль «катализатора», является ЭПР-корреляция между входом и выходом канала связи. Заметим, что свести передачу произвольного квантового состояния к только передаче классической информации, не используя дополнительного квантового ресурса, невозможно: поскольку классическая информация копируема, это означало бы возможность копирования и квантовой информации.

Сама система не передаётся

Пусть имеются две квантовые системы A и B, описывающие, соответственно, вход и выход канала связи. На вход A поступает произвольное состояние $|\psi\rangle$; можно описать процедуру, при которой исходное состояние B перейдет в $|\psi\rangle$, а входное $|\psi\rangle$ с необходимостью разрушится (иначе мы имели бы копирование).

В простейшей (и основной) версии системы A и B являются двухуровневыми (q-битами).

1) Перед началом передачи система AB приготовляется в состоянии $|00\rangle + |11\rangle$.

2) C посылает A произвольное чистое состояние

$$|\psi\rangle = a|0\rangle + b|1\rangle.$$

Совокупность трех систем CAB описывается состоянием

$$(a|0\rangle + b|1\rangle) \otimes (|00\rangle + |11\rangle).$$

3) Затем

а) A производит некоторое обратимое преобразование состояния системы CA;

б) A производит измерение (с 4 исходами, что составляет 2 бита классической информации). Преобразование и измерение будут описаны ниже.

---

[1] *Bennett C. H., Brassard G., Crépeau C., Jozsa R., Peres A., Wootters W. K.* Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channel // Phys. Rev. Lett. — 1993. — V. 70. — P. 1895–1899.

4) A посылает результат измерения B по классическому каналу связи.

5) В зависимости от полученного результата измерения B производит некоторое преобразование и получает это произвольное $|\psi\rangle$.

Производимые преобразования являются характерными примерами логических операций, используемых в квантовом компьютинге. На 3-м шаге над системой CA производится операция CNOT (контролируемое «нет»):

$$|00\rangle \to |00\rangle, \quad |01\rangle \to |01\rangle, \quad |10\rangle \to |11\rangle, \quad |11\rangle \to |10\rangle,$$

при которой состояние первого q-бита сохраняется, а состояние второго q-бита не изменяется, либо изменяется на противоположное, в зависимости от состояния первого q-бита. При этом базис переходит в базис, следовательно, в четырехмерном пространстве CA этому преобразованию соответствует унитарный оператор. Затем к q-биту A применяется операция Адамара H с унитарной матрицей

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Тогда

$$|0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),$$

т. е. базис поворачивается на угол $\pi/4$.

Начальное состояние всей системы CAB есть

$$a|000\rangle + b|100\rangle + a|011\rangle + b|111\rangle.$$

После действия CNOT на CA получаем

$$a|000\rangle + b|110\rangle + a|011\rangle + b|101\rangle.$$ CNOT на CA

Потом H действует на C

$$a(|000\rangle + |100\rangle) + b(|010\rangle - |110\rangle) + a(|011\rangle + |111\rangle) + b(|001\rangle - |101\rangle).$$

Выделяя состояние системы CA, получаем

$$|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle).$$

Теперь производится измерение в системе CA, проецирующее на один из четырех базисных векторов $|00\rangle, \ldots, |11\rangle$. Результат измерения посылается от A к B по классическому (идеальному) каналу