Запутанные (entangled) состояния, парадокс Эйнштейна-Подольского-Розена, неравенство Белла, квантовая теорема о невозможности клонирования, квантовые компьютеры.

Имеем систему с двумя степенями свободы, или систему, состоящую из двух подсистем A и B, каждая из которых – одну имеет степень свободы.

У этой системы возможны состояния

$$\Psi = \Psi_\alpha(q_1) \cdot \Psi_\beta(q_2) -$$

факторизованные. Однако, не любое состояние может быть факторизовано

$$\Psi = \frac{1}{\sqrt{2}} \left(\Psi_{\alpha_1}(q_1) \cdot \Psi_{\beta_1}(q_2) + \Psi_{\alpha_2}(q_1) \Psi_{\beta_2}(q_2) \right) -$$

(entangled)

пример запутанного состояния. В этом состоянии имеется жесткая корреляция степеней свободы, они „запутаны". С вероятностью 1/2 мы при измерении обнаружим A в состоянии α_1 (при этом B – обязательно в состоянии β_1), или A в α_2, а B – в β_2.

ЭПР первыми обратили внимание на парадоксальность запутанных состояний. Они аргументировали, что квантовая механика – не полная теория, что она не может описать все относящиеся к делу физические реальности.

Речь идет о фундаментальном квантово-механическом индетерминизме.

Пусть спин находится в состоянии

$$\chi = \frac{1}{\sqrt{2}}\left(\chi_{+z} + \chi_{-z} \right).$$

z здесь означает, что обсуждается проекция спина на ось z. При измерении S_z мы равновероятно обнаружим $\pm \hbar/2$. Эта неопределенность при поверхностном взгляде „похожа" на неопределенность при подбрасывании монеты. Но, при подбрасывании монеты мы, изучив детально её полет, собрав достаточно много информации о полете и поверхности, куда она падает, можем 100% предсказать исход. В квантовой механике, имея максимально-возможную информацию о так-сказать „полете", т.е. о состоянии системы, имеем неопределенность 50:50.

Это многим не нравится и сейчас:
„Бог в кости не играет".
Эйнштейн долго искал аргумент, доказывающий, что такая квантовая механика не полна, и почти нашел. И оказался неправ.

Вот суть парадокса, „опровергающего" квантовую механику:

Пусть мы имеем две частицы со спином 1/2 в синглетном состоянии

$$|\chi\rangle = \frac{1}{\sqrt{2}}\left(|a: +z;\ b: -z\rangle - |a: -z;\ b: +z\rangle \right).$$

$$\chi = \frac{1}{\sqrt{2}}\left(\chi^a_{z\uparrow}\chi^b_{z\downarrow} - \chi^a_{z\downarrow}\chi^b_{z\uparrow} \right).$$

Алиса измерила проекцию спина на ось $\vec{n}_a$

одной из частиц, назвала её частицей „а"; спина другой частицы, „в", на ось $\vec{u}_в$ измерил проекцию Боб.

Результаты их измерений скоррелированы. Допустим, $\vec{u}_а = \vec{u}_в = \vec{e}_z$. С вероятностью 1/2 Алиса получит $\hbar/2$, а Боб $(-\hbar/2)$; либо наоборот. У них никогда не могут получиться одинаковые результаты. Это – абсолютная корреляция, или, если угодно, – антикорреляция.

Можно показать, что то же самое получится, если Алиса и Боб выберут $\vec{u}_а = \vec{u}_в = \vec{e}_x$: результаты обязательно отличаются знаком.

Подобная корреляция бывает сплошь и рядом и в обычной „классической" жизни. Пусть мы имеем две карты – пиковый и бубновый тузы. Помешаем эту маленькую колоду, и дадим Алисе и Бобу по одной карте. Когда Алиса откроет карту, у неё с 50% вероятностью окажется туз бубновый. В этом случае у Боба – 100% туз пик. При этом Бобу даже не нужно переворачивать карту. И здесь ЭПР произносят ключевое утверждение: (в знач. мере философское!!)

Если, без какого либо вмешательства в систему, мы можем 100% предсказать значение физической величины, тогда существует элемент физической реальности, соответствующий этой физической величине.

Бобу не надо вмешиваться в систему и переворачивать свою карту, он просто спросит у Алисы цвет её карты. ~~Это не важно~~ И 100% знает, что у него туз пик. Значит имеется физическая реальность — в его конверте туз пик.

Аналогично, Бобу не надо измерять проекцию спина на ось z частицы, оставшейся после её ~~его~~ измерения. Он просто спросит у Алисы о её результате. Значит — у оставшейся частицы имеется физически реальный $S_z^b = -S_z^a$. Ведь он знал это, не трогая частицу „b". И то же самое относится к S_x.

Значит, есть <u>две</u> физические реальности, соответствующие S_x^b и S_z^b, а операторы $\hat{S}_x$ и $\hat{S}_z$ — не коммутируют.

<u>Диагноз</u>: квантовая механика — не полная теория — она не может описать две физические реальности одновременно.

<u>Ответ Бора</u>: измерение Алисы есть вмешательство в <u>двухчастичную</u> систему. Классическое понятие „изолированной системы" нуждается в пересмотре. Даже если частицы „a" и „b" разнесены очень далеко друг от друга, „измерение Алисы есть вмешательство в судьбу <u>обеих</u> частиц.

Очень важно, что это вмешательство мгновенно. При этом принцип относительности Эйнштейна не нарушается. В этой игре Алиса должна передать Бобу информацию о своем измерении <u>обычным</u> способом

Бор и Эйнштейн не смогли договориться. Рассудим их эксперимент, показавший нарушение неравенства Белла. Эйнштейн был неправ.

Неравенство Белла.

Когда я учился квантовой механике, многие физики разделяли точку зрения Эйнштейна. И сейчас некоторые из них, незнакомые с неравенством Белла и современными экспериментами, полагают что **Невозможно** экспериментально установить кто прав, Бор или Эйнштейн. Действительно, как проверить, влияет ли измерение Алисой S_z своей частицы на результат измерений Боба. ~~Ведь если проводить~~ Действительно ли утверждение о том, что до измерений Алисы у Боба сохранялись шансы на оба результата его измерения.

Оказывается, можно!

Если прав Эйнштейн, то в „полной" теории должен присутствовать некий параметр λ, который отличает синглетные состояния пар (a,b). Если λ лежит в некоем интервале $\lambda_1 < \lambda < \lambda_2$, то у частицы „a" $S_z = \hbar/2$, а у „b" $-(-\hbar/2)$. А если λ вне этого интервала, то наоборот. Должны существовать функция,

$$A(\lambda, \vec{a}) = \begin{cases} \hbar/2, & \lambda_1 < \lambda < \lambda_2 \\ -\hbar/2, & \text{в иных случаях,} \end{cases}$$

которая дает результаты измерения Алисы S_z^a, и ~~такая~~ подобная функция и Боба,

$$B(\lambda, \vec{a}) = \begin{cases} -\hbar/2, & \lambda_1 < \lambda < \lambda_2, \\ \hbar/2, & \text{otherwise} \end{cases}$$

Здесь очень важную роль играет локальность: A зависит от λ и $\vec{U}_a$, но не зависит от $\vec{U}_b$ – направления, которое ~~выберет~~ может выбрать Боб потом, после измерений Алисы.

Параметр λ в супер-теории может быть для разных синглетных пар различным, в то время как в квантовой механике все (синглетные) (a,b) пары одинаковы, и, согласно Бору, нет способа отличить одну такую пару от другой. Поэтом λ называют "скрытым параметром".

Неравенства Белла – это ограничения, накладываемые на теорию скрытых параметров.

Введем корреляционную функцию $E(\vec{U}_a, \vec{U}_b)$, которая равна среднему произведению $(S^a_{u_a} \cdot S^b_{u_b})$, деленному на $(\hbar^2/4)$. Очевидно, что

$$|E(\vec{U}_a, \vec{U}_b)| \leqslant 1, \text{ ибо } S^a_{u_a} \cdot S^b_{u_b} = \pm \hbar^2/4.$$

В супер-теории

$$E(\vec{U}_a, \vec{U}_b) = \frac{4}{\hbar^2} \int P(\lambda) A(\lambda, \vec{U}_a) B(\lambda, \vec{U}_b) d\lambda,$$

где $P(\lambda)$ – неизвестная функция распределения, такая, что $P(\lambda) \neq 0$, $\int P(\lambda) d\lambda = 1$. Очень важно, что $P(\lambda)$ не зависит от $\vec{U}_a$ и $\vec{U}_b$. Действительно, $\vec{U}_a$ и $\vec{U}_b$ Алиса с Бобом могут выбрать после того, как создана пара (a,b). $P(\lambda)$ характеризует количество пар с разным λ в ансамбле.

В рамках квантовой механики,

$$E(\vec{a}, \vec{b}) = \frac{4}{\hbar^2} \langle \chi | \hat{\vec{S}}_a \vec{a} \cdot \hat{\vec{S}}_b \vec{b} | \chi \rangle = -\vec{a}\cdot\vec{b}$$

Теорема Бэлла утверждает (1964), что

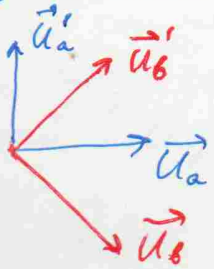
1) В супер-теории

$$S = E(\vec{a}, \vec{b}) + E(\vec{a}, \vec{b}') + E(\vec{a}', \vec{b}') - E(\vec{a}', \vec{b})$$

всегда удовлетворяет неравенству Белла:

$$|S| \leqslant 2$$

2) В квантовой механике оно может быть нарушено, например для



$$-S = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} - \left(-\frac{1}{\sqrt{2}}\right) = +2\sqrt{2}.$$

Утверждение (1) доказывается просто:

$$S = \frac{4}{\hbar^2} \int P(\lambda)\, S(\lambda)\, d\lambda, \quad \text{где } S(\lambda) = A(\lambda, \vec{a}) B(\lambda, \vec{b}) + A(\lambda, \vec{a}) B(\lambda, \vec{b}') + A(\lambda, \vec{a}') B(\lambda, \vec{b}') - A(\lambda, \vec{a}') B(\lambda, \vec{b})$$

$$S(\lambda) = A(\lambda, \vec{a}) \left[B(\lambda, \vec{b}) + B(\lambda, \vec{b}') \right] + A(\lambda, \vec{a}') \left[B(\lambda, \vec{b}') - B(\lambda, \vec{b}) \right].$$

Одна из квадратных скобок обязательно нуль, а вторая – $\pm\hbar$. Поэтому $S(\lambda) = \pm \hbar^2/2$.

$$S = \pm \frac{4}{\hbar^2} \cdot \frac{\hbar^2}{2} \int P(\lambda) \left(\pm 1\right)_\lambda d\lambda. \quad |S| \leqslant 2.$$

Эксперимент показал, что S бывает больше 2.

Квантовая криптография.

Задача криптографии – передать сообщение от Алисы к Бобу, минимизируя риск перехвата информации шпионом. Классическая криптография использует хитрые методы, которые не могут быть „взломаны" в разумное время современными компьютерами.

Квантовая криптография важна в другом отношении. Она позволяет на 100% убедиться, что перехвата не было.

Сообщение кодируется нулями и единицами. Каждая единица или нуль – 1 бит информации. В качестве носителя бита можно использовать частицу со спином 1/2. Алиса шлет частицы с определенными S_z одну за другой. Боб ориентирует приемный аппарат типа Штерна-Герлаха и получает цепь единичек и нулей.

Эта процедура не несет квантовых особенностей и может быть перехвачена шпионом так, что следов перехвата не останется. Он ловит частицы с определенным S_z и такие же отправляет Бобу.

Ситуация меняется радикально, если Алиса шлет частицы попеременно: то с определенным S_z, то с определенным S_x, никому, даже Бобу, не сообщая о выборе (x, z) для каждой частицы.

Например, Алиса выслала 16 частиц, и пока еще не решила, какие из частиц несут полезную информацию.

Что может сделать Боб? Он произвольно ориентирует прибор то вдоль x, то вдоль z. Получает цепочку нулей и единиц (в среднем их поровну).

Ту частицу, которую Алиса послала с заданным $S_x = +1/2$ Боб примет 100% как единицу, если он у нее измеряет S_x, и 50% примет как единицу, если измеряет S_z.

Далее Боб открыто сообщает Алисе результаты своих измерений; а также какую проекцию он измерял, S_x или S_z, для каждой частицы. Эта информация позволит Алисе узнать, был ли перехват. Ведь шпион, в случае если он пытался организовать перехват, еще не знает, что фиксировала Алиса, S_x или S_z для частиц. И получив 1, ~~он не знает~~ измерив S_x, он не знает, что фиксировала Алиса для этой частицы. Он пошлет Бобу частицу с $S_x = 1$. Тогда, если Алиса таки фиксировала S_x — это счастье шпиона. А если она фиксировала S_z, и Боб вздумает измерять S_z, то 50% на то, что Боб намерет не то, что послала Алиса. И Алиса об этом узнает. В итоге, для каждой частицы:

(50%) 50% - шанс, что шпион угадал ось. - ОК

(25%) Из оставшихся 50%, (когда шпион не угадал ось, половина случаев), когда и Боб тоже выбрал не ту же ось, что Алиса - ОК

(12,5%) Из оставшихся 25%, ~~половину~~ когда шпион не угадал ось, а Боб угадал, Боб все-таки получит правильный бит — ОК

(12,5%)!! Шпион не угадал ось, а Боб угадал, и вместо 1 принял 0. — не ОК.

Если был перехват, 1/4 всех битов испорчена шпионом, и при этом половина из них, всего 1/8

1/8 посланных Алисой битов покажут Алисе, что был перехват.

Заметим, что пока записка еще не послана. Шпион ничего не узнал, а Алиса уже знает, что был взлом.

Только убедившись, что перехвата не было, открыто Алиса сообщает Бобу, какие номера частиц он должен вычеркнуть, а какие являются запиской. При этом Алиса выберет не те частицы, о которых ей говорил открыто Боб. Всего частиц было, скажем, 10000, а Боб послал ей информацию о своем выборе оси и результатах измерения – только для 1000.

Теорема о невозможности клонирования

Выше мы предполагали, что шпион наугад выставлял свой прибор и выбирал ось для перехвата. А почему бы ему не попытаться подетальнее изучить перехватываемую частицу, а затем отправить Бобу в точно том же состоянии (клонирование).

К счастью для Алисы и Боба, это невозможно.

Обозначим $|\alpha_1\rangle$ состояние, которое нужно клонировать, а $|\phi\rangle$ - начальное состояние системы, переводимое затем тоже в $|\alpha_1\rangle$. Клонирование осуществляется действием некоторого Гамильтониана.

Запишем эту операцию.

$$\hat{H}\cdot\left(|\alpha_1\rangle\otimes|\phi\rangle\right)=\left(|\alpha_1\rangle\otimes|\alpha_1\rangle\right)$$

Для состояния $|\alpha_2\rangle$ мы должны иметь:

$$\hat{H}\left(|\alpha_2\rangle\otimes|\phi\rangle\right)=\left(|\alpha_2\rangle\otimes|\alpha_2\rangle\right).$$

А как насчет исходного состояния $\left(|\alpha_1\rangle+|\alpha_2\rangle\right)/\sqrt{2}$?

Мы получим, в силу линейности $\hat{H}$:

$$\hat{H}\cdot\left(\frac{1}{\sqrt{2}}(|\alpha_1\rangle+|\alpha_2\rangle)\otimes|\Phi\rangle\right)=\frac{1}{\sqrt{2}}\left((|\alpha_1\rangle\otimes|\alpha_1\rangle+|\alpha_2\rangle\otimes|\alpha_2\rangle\right)$$

вместо

$$\frac{1}{\sqrt{2}}(|\alpha_1\rangle+|\alpha_2\rangle)\otimes\frac{1}{\sqrt{2}}(|\alpha_1\rangle+|\alpha_2\rangle).$$

Итоговое состояние – запутанное !!!

Квантовый компьютер.

Очень популярный сейчас термин „Q-bit" не очень богат содержанием – это квантовая система, которая может находиться только в двух ортогональных состояниях и их суперпозициях. Например, спиновое состояние электрона. ~~Фотон~~ В качестве Q-bita можно взять двух-уровневую систему.

Однако манипулирование большим числом Q-битов очень интересно.

Можно использовать очень упрощенное определение компьютера как системы, которая оперирует наборами N-битов – регистрами. Регистр содержит бинарные N-слова. Для $N=3$ мы имеем 8 возможных слов. $8=2^N=2^3$. Это если регистр не квантовый.

В случае же Q-битов, 2^N слов составляют лишь базисные квантовые состояния регистров. Всего же возможных Q-слов, которые могут быть записаны в регистре, неизмеримо больше.

Когда Q-компьютер оперирует Q-регистром, он на самом деле выполняет параллельные операции над 2^N классическими числами. Этот параллелизм есть основа эффективности Q-компьютеров.

Возникают вопросы, какие операции можно выполнять с помощью Q-компьютера, и какого типа алгоритмы можно использовать с таким устройством. И, наконец, как его построить, и, вообще, возможно ли это?

Алгоритм Шора.

В обычной, неквантовой криптографии, используются алгоритмические протоколы. Один из них основан на том, что некоторые арифметические действия гораздо легче выполняются в прямом направлении, чем в обратном. Легко, например, перемножать многозначные числа. А разложить большое число на множители очень трудно даже мощным компьютерам. Делается это перебором, и нужно выполнить порядка $\sqrt{N}$ операций деления. Компьютерное время

$$t \sim \exp(\text{число разрядов в } N).$$

Если 300 разрядов – компьютер не справляется. Такая "необратимость" – источник криптографического метода (Rivest, Shamir, Adleman (RSA)), используемого в кредитных карточках, банковских трансакциях и т.п.

В 1994 году Peter Shor поверг всех криптографов, особенно военных, в шок. Он показал, что Q-компьютер потребует для факторизации числа N много меньше времени,

$$t \sim (\text{число разрядов в } N).$$

Базовый принцип работы Q-компьютера сводится к эволюции системы с неким Гамильтонианом. Процедура начинается с некого стартового состояния и заканчивается Измерением состояния Q-регистра, что прерывает эволюцию. Поскольку результат квантового измерения принципиально неоднозначен, Q-компьютер может "ошибиться". Например, в алгоритме Шора, Q-компьютер выдает „возможный вариант ответа", который, однако, компьютер сам же легко проверит.

Шор доказал, что требуемое число попыток растет всего лишь линейно с ростом числа разрядов факторизуемого числа.

Гамильтониан, „ведущий вычисления", зависит от времени, он сам эволюционирует тоже, подчиняясь часам, которые задают ритм вычислений. Оказывается, создать такой Гамильтониан не очень сложно. На самом деле, вычисления декомпозируются на простые операции — logical gates, — обычные YES, AND, OR.

Но существуют и необычные, сугубо квантовые логические операции. Например, $\sqrt{NOT}$. Этот gate трансформирует Q-биты 0 и 1 в симметричную и антисимметричную линейные комбинации. Повторное действие этой операции инвертирует 0 и 1, что соответствует NOT.

Декогеренция.

Глобальное квантовое состояние Q-компьютера должно быть суперпозицией большого числа состояний базисных, и эта суперпозиция должна долго сохраняться и контролироваться. Любое запутывание с окружающим миром разрушает суперпозицию.

2 пути.

1) Изоляция.
2) Корректировка.