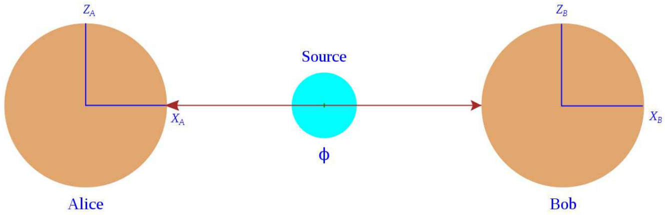
Квантовая телепортация

М. В. Волков

Уральский федеральный университет
Институт естественных наук и математики
кафедра алгебры и фундаментальной информатики

2022/2023 учебный год

В статье 1935 г. (A. Einstein, B. Podolsky, N.Rosen, Can Quantum-Mechanical Description of Physical Reality be Considered Complete? Physical Review 47(10):777–780 (1935)) Эйнштейн, Подольский и Розен описали некоторый мысленный эксперимент, который по их мнению показывал, что квантово-механические представления противоречат некоторым фундаментальным законам природы, а именно, невозможности мгновенной передачи информации на сколь угодно большие расстояния. Упрощенно их аргумент был таков. Квантовая система может состоять из двух разлетающихся в разные стороны частиц:



Если один наблюдатель (Алиса) измерит «свою» частицу, то вторая половина системы должна в тот же самый момент измениться соответствующим образом, и второй наблюдатель (Боб) может это зарегистрировать.

Неравенство Белла, эксперименты и протокол Беннета и др.

В 1964 г. Белл (J. S. Bell, On the Einstein Podolsky Rosen Paradox. Physics Physique Физика. 1(3): 195–200 (1964)) превратил аргументы Эйнштейна, Подольского и Розена в некоторое неравенство, которое допускало экспериментальную проверку.

Начиная с 1972 г. разные группы физиков провели эксперименты, которые показали, что неравенство Белла *нарушается*. Это означает, что явление, которое Эйнштейн, Подольский и Розен считали очевидно невозможным, может происходить в реальности. «Парадокс» Эйнштейна–Подольского–Розена стал *эффектом Эйнштейна–Подольского–Розена*.

В 1993 г. Беннет, Брассар, Крепо, Йожа, Перес и Вуттерс (C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. K. Wootters, Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. Physical Review Letters. 70(13):1895–1899 (1993)) предложили протокол передачи квантовых состояний с использованием эффекта Эйнштейна–Подольского–Розена. Такую передачу и принято называть *квантовой телепортацией*.

Телепортация по протоколу Беннета и др. осуществлена экспериментально, причем расстояние передачи быстро растет (рекорд 2020 года — 1400 км).

Алиса хочет передать Бобу сообщение, закодированное вектором $|\psi\rangle = \begin{bmatrix}\alpha\\ \beta\end{bmatrix} = \alpha|0\rangle + \beta|1\rangle$, где $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$.

Алиса инициализирует систему $H := H_2 \otimes H_2 \otimes H_2$ состоянием $|\psi\rangle|0\rangle|0\rangle$.

Шаг 1: Алиса применяет преобразование Адамара $R = R_2$ ко 2-му кубиту:

$$|\psi\rangle|0\rangle|0\rangle \xrightarrow{R} \frac{1}{\sqrt{2}}|\psi\rangle\left(|0\rangle + |1\rangle\right)|0\rangle.$$

Контролируемый XOR — это унитарный оператор в $H_2 \otimes H_2$, который определен так: $|a\rangle|b\rangle \mapsto |a\rangle|a \oplus b\rangle$.

Шаг 2: Алиса применяет контролируемый XOR ко 2-му и 3-му кубитам:

$$\frac{1}{\sqrt{2}}|\psi\rangle\left(|0\rangle + |1\rangle\right)|0\rangle \xrightarrow{\text{XOR}} \frac{1}{\sqrt{2}}|\psi\rangle\left(|00\rangle + |11\rangle\right).$$

Шаг 3: Алиса посылает Бобу 3-й кубит *по квантовому каналу* и применяет контролируемый XOR ко 1-му и 2-му кубитам:

$$\frac{1}{\sqrt{2}}|\psi\rangle\left(|00\rangle + |11\rangle\right) = \frac{1}{\sqrt{2}}\left(\alpha|0\rangle + \beta|1\rangle\right)\left(|00\rangle + |11\rangle\right) \xrightarrow{\text{XOR}}$$

$$\xrightarrow{\text{XOR}} \frac{1}{\sqrt{2}}\left(\alpha\left(|000\rangle + |011\rangle\right) + \beta\left(|110\rangle + |101\rangle\right)\right).$$

Шаг 4: Алиса применяет преобразование $L := \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$ ко 1-му кубиту:

$$\frac{1}{\sqrt{2}}\left(\alpha\left(|000\rangle + |011\rangle\right) + \beta\left(|110\rangle + |101\rangle\right)\right) \xrightarrow{L}$$
$$\xrightarrow{L} \frac{1}{2}\left(\alpha\left(|000\rangle - |100\rangle + |011\rangle - |111\rangle\right) + \beta\left(|010\rangle + |110\rangle + |001\rangle + |101\rangle\right)\right).$$

Шаг 5: Алиса замеряет первые два кубита и посылает результаты измерений Бобу *по классическому каналу*.

Шаг 6: Боб применяет контролируемый XOR ко 2-му и 3-му кубитам.

Шаг 7: Боб применяет к 1-му кубиту преобразование $S := \begin{bmatrix} i & 0 \\ 0 & 1 \end{bmatrix}$.

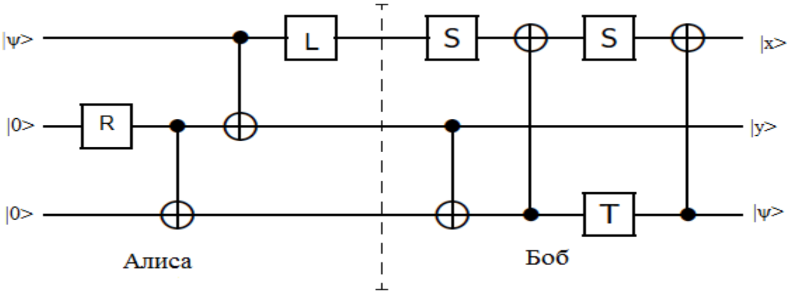
Шаг 8: Боб применяет контролируемый XOR к 3-му и 1-му кубитам.

Шаг 9: Боб снова применяет S к 1-му кубиту, а к 3-му кубиту применяет преобразование $T := \begin{bmatrix} -1 & 0 \\ 0 & -i \end{bmatrix}$.

Шаг 10: Боб снова применяет контролируемый XOR к 3-му и 1-му кубитам.

Протокол квантовой телепортации (3)

Следующая схема изображает весь протокол ($\oplus$ изображает XOR):



Утверждается, что после его выполнения в 3-м кубите у Боба возникнет исходный вектор $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$!

Заметим, что злоумышленник не сможет перехватить этот сообщение, даже если он имеет доступ к классическому каналу, по которому Алиса посылает результаты измерений, а по квантовому каналу ничего секретного не передается. Именно с этим связаны большие надежды на практическое применение квантовой телепортации в криптографии.

Перед измерением (после шага 4) состояние системы было таким:

$$\frac{1}{2}\left(\alpha\left(|000\rangle - |100\rangle + |011\rangle - |111\rangle\right) + \beta\left(|010\rangle + |110\rangle + |001\rangle + |101\rangle\right)\right).$$

Случай 1: Алиса передала $|0\rangle|0\rangle$.

$$\frac{1}{2}\left(\alpha\left(\underbrace{|000\rangle} - |100\rangle + |011\rangle - |111\rangle\right) + \beta\left(|010\rangle + |110\rangle + \underbrace{|001\rangle} + |101\rangle\right)\right).$$

Боб работает с $\frac{1}{2}|0\rangle|0\rangle\left(\alpha|0\rangle + \beta|1\rangle\right)$. Сначала Боб XORит 2-й и 3-й кубиты, а к 1-му применяет $S = \begin{bmatrix} i & 0 \\ 0 & 1 \end{bmatrix}$:

$\frac{1}{2}|0\rangle|0\rangle\left(\alpha|0\rangle + \beta|1\rangle\right) \xrightarrow{\text{XOR},S} \frac{i}{2}|0\rangle|0\rangle\left(\alpha|0\rangle + \beta|1\rangle\right)$. Затем Боб XORит 3-й и 1-й кубиты: $\frac{i}{2}|0\rangle|0\rangle\left(\alpha|0\rangle + \beta|1\rangle\right) \xrightarrow{\text{XOR}} \frac{i}{2}\alpha|0\rangle|0\rangle|0\rangle + \frac{i}{2}\beta|1\rangle|0\rangle|1\rangle$. Затем Боб применяет S к 1-му кубиту, $T = \begin{bmatrix} -1 & 0 \\ 0 & -i \end{bmatrix}$ к 3-му, после чего снова XORит 3-й и 1-й кубиты:

$$\frac{i}{2}\alpha|0\rangle|0\rangle|0\rangle + \frac{i}{2}\beta|1\rangle|0\rangle|1\rangle \xrightarrow{S,T} \frac{1}{2}\alpha|0\rangle|0\rangle|0\rangle + \frac{1}{2}\beta|1\rangle|0\rangle|1\rangle \xrightarrow{\text{XOR}} \frac{1}{2}|0\rangle|0\rangle\left(\alpha|0\rangle + \beta|1\rangle\right).$$

Случай 2: Алиса передала $|0\rangle|1\rangle$:

$$\frac{1}{2}\left(\alpha\left(|000\rangle - |100\rangle + \underbrace{|011\rangle} - |111\rangle\right) + \beta\left(\underbrace{|010\rangle} + |110\rangle + |001\rangle + |101\rangle\right)\right).$$

Боб работает с $\frac{1}{2}|0\rangle|1\rangle\left(\alpha|1\rangle + \beta|0\rangle\right)$.

Сначала Боб XORит 2-й и 3-й кубиты, а к 1-му применяет S:

$$\frac{1}{2}|0\rangle|1\rangle\left(\alpha|1\rangle + \beta|0\rangle\right) \xrightarrow{\mathrm{XOR}} \frac{1}{2}|0\rangle|1\rangle\left(\alpha|0\rangle + \beta|1\rangle\right) \xrightarrow{S} \frac{i}{2}|0\rangle|1\rangle\left(\alpha|0\rangle + \beta|1\rangle\right).$$

Затем Боб XORит 3-й и 1-й кубиты:

$$\frac{i}{2}|0\rangle|1\rangle\left(\alpha|0\rangle + \beta|1\rangle\right) \xrightarrow{\mathrm{XOR}} \frac{i}{2}\alpha|0\rangle|1\rangle|0\rangle + \frac{i}{2}\beta|1\rangle|1\rangle|1\rangle.$$

Затем Боб применяет S к 1-му кубиту, T к 3-му и XORит 3-й и 1-й кубиты:

$$\frac{i}{2}\alpha|0\rangle|1\rangle|0\rangle + \frac{i}{2}\beta|1\rangle|1\rangle|1\rangle \xrightarrow{S,T} \frac{1}{2}\alpha|0\rangle|1\rangle|0\rangle + \frac{1}{2}\beta|1\rangle|1\rangle|1\rangle \xrightarrow{\mathrm{XOR}} \frac{1}{2}|0\rangle|1\rangle\left(\alpha|0\rangle + \beta|1\rangle\right).$$

Случай 3: Алиса передала $|1\rangle|0\rangle$:

$$\frac{1}{2}\left(\alpha\left(|000\rangle-\underbrace{|100\rangle}+|011\rangle-|111\rangle\right)+\beta\left(|010\rangle+|110\rangle+|001\rangle+\underbrace{|101\rangle}\right)\right).$$

Боб работает с $\frac{1}{2}|1\rangle|0\rangle\left(-\alpha|0\rangle+\beta|1\rangle\right)$.

Сначала Боб XORит 2-й и 3-й кубиты, а к 1-му применяет S. В данном случае оба эти преобразования ничего не меняют.
Затем Боб XORит 3-й и 1-й кубиты:

$$\frac{1}{2}|1\rangle|0\rangle\left(-\alpha|0\rangle+\beta|1\rangle\right)\xrightarrow{\mathrm{XOR}}-\frac{1}{2}\alpha|1\rangle|0\rangle|0\rangle+\frac{1}{2}\beta|0\rangle|0\rangle|1\rangle.$$

Затем Боб применяет S к 1-му кубиту, T к 3-му и XORит 3-й и 1-й кубиты:

$$-\frac{1}{2}\alpha|1\rangle|0\rangle|0\rangle+\frac{1}{2}\beta|0\rangle|0\rangle|1\rangle\xrightarrow{S,T}\frac{1}{2}\alpha|1\rangle|0\rangle|0\rangle+\frac{1}{2}\beta|0\rangle|0\rangle|1\rangle\xrightarrow{\mathrm{XOR}}\frac{1}{2}|1\rangle|0\rangle\left(\alpha|0\rangle+\beta|1\rangle\right).$$

Случай 4: Алиса передала $|1\rangle|1\rangle$:

$$\frac{1}{2}\left(\alpha\left(|000\rangle - |100\rangle + |011\rangle - \underbrace{|111\rangle}\right) + \beta\left(|010\rangle + \underbrace{|110\rangle} + |001\rangle + |101\rangle\right)\right).$$

Боб работает с $\frac{1}{2}|1\rangle|1\rangle\left(-\alpha|1\rangle + \beta|0\rangle\right)$.

Сначала Боб XORит 2-й и 3-й кубиты, а к 1-му применяет S:

$$\frac{1}{2}|1\rangle|1\rangle\left(-\alpha|1\rangle + \beta|0\rangle\right) \xrightarrow{\text{XOR},S} \frac{1}{2}|1\rangle|1\rangle\left(-\alpha|0\rangle + \beta|1\rangle\right).$$

Затем Боб XORит 3-й и 1-й кубиты:

$$\frac{1}{2}|1\rangle|1\rangle\left(-\alpha|0\rangle + \beta|1\rangle\right) \xrightarrow{\text{XOR}} -\frac{1}{2}\alpha|1\rangle|1\rangle|0\rangle + \frac{1}{2}\beta|0\rangle|1\rangle|1\rangle.$$

Затем Боб применяет S к 1-му кубиту, T к 3-му и XORит 3-й и 1-й кубиты:

$$-\frac{1}{2}\alpha|1\rangle|1\rangle|0\rangle + \frac{1}{2}\beta|0\rangle|1\rangle|1\rangle \xrightarrow{S,T} \frac{1}{2}\alpha|1\rangle|1\rangle|0\rangle + \frac{1}{2}\beta|0\rangle|1\rangle|1\rangle \xrightarrow{\text{XOR}} \frac{1}{2}|1\rangle|1\rangle\left(\alpha|0\rangle + \beta|1\rangle\right).$$

Видим, что во всех случаях в 1-м и 2-м кубитах окажется то, что передала Алиса, а в 3-м действительно возникнет исходный вектор $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.