От нелокальности Ньютона к квантовой нелокальности и далее.
Может ли теория относительности считаться полной?

Николя Жизэн (Швейцария)

Перевод М.Х.Шульмана

---

arXiv:quant-ph/0512168v1 20 Dec 2005

Can relativity be considered complete ?
From Newtonian nonlocality to quantum nonlocality and beyond

Nicolas Gisin
Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland
(Dated: April 26, 2007)

Рассматривается долгая история нелокальности в физике, причем особое внимание уделяется концептуальным прорывам за последние годы. Так, впервые стало возможным изучать ”нелокальность без обмена информацией” извне, т.е. без учета всей тяжелой артиллерии гильбертова пространства квантовой физики. Подчеркивается, что физика всегда давала нелокальное описание Природы, исключая зазор в 10 коротких лет. Отмечается, что концепция ”нелокальности без обмена информацией” полностью чужда духу теории относительности, которая является строго локальной теорией.

PACS numbers:

I. ВВЕДЕНИЕ

100 лет спустя после года великих открытий Эйнштейна и 70 лет после опубликования статьи ЭПР [1] я склонен думать, что Эйнштейн оценил бы название моей публикации как нечто провокационное. Однако ему, вероятно, не понравились бы ее выводы. Ну, кто может сомневаться в полноте теории относительности? А также в том, что квантовая механика неполна! На самом деле, это две научные теории, а Наука никогда не заканчивается (я действительно верю, что сейчас не конец науки [2]). Да, я сейчас, конечно, пишу не для Эйнштейна, а для тех читателей, которые хотят (и это неизбежно носит субъективный характер) разобраться в мирном сосуществовании [3] между относительностью и квантовой физикой в свете теоретических и экспериментальных успехов науки за последние 10 лет, в обширных перспективах физики и нелокальности после Ньютона [4].

II. НЕЛОКАЛЬНОСТЬ ПО НЬЮТОНУ

Исаак Ньютон, великий Ньютон – создатель Универсальной Теории Тяготения, был не вполне доволен своей теорией. Действительно, он хорошо знал об одном неудобном следствии из нее: если на Луне покатится камень, то наш вес, т.е. вес

каждого из нас здесь, на Земле, немедленно изменится. Ньютона больше всего беспокоила мгновенность этого эффекта, т.е. нелокальность, предсказываемая его теорией. Давайте прочтем, как сам Ньютон описывал это [5] (перевод мой – М.Х.Ш):

> *То, что Тяготение должно быть врожденным, неотъемлемым и существенным свойством Материи, так что одно Тело способно воздействовать на другое на Расстоянии, через Вакуум, без посредничества чего бы то ни было, с помощью чего или через что их Действие и Сила могли бы влиять друг на друга, кажется мне таким великим Абсурдом, что я думаю, нет Человека, компетентного в философских сущностях, который мог бы склониться к этой точке зрения. Тяготение должно вызываться действием некоторого Агента, постоянно действующего в соответствии с определенными Законами, но является ли этот Агент материальным или нет, я не буду обсуждать с моими Читателями.*

Ньютону трудно было бы более ясно выразить свое неприятие нелокальности! Однако большинство физиков не уделяет значительного внимания этому аспекту физики Ньютона. За неимением альтернативы, физика оставалась нелокальной примерно до 1915 года, когда Эйнштейн создал Общую Теорию Относительности. Но начнем десятью годами раньше, с 1905 г.

III. ЭЙНШТЕЙН, ВЕЛИЧАЙШИЙ ИНЖЕНЕР В ОБЛАСТИ МЕХАНИКИ

В 1905 г. Эйнштейн ввел три новые радикальные теории, или модели, в физике. Конечно, имеется в виду и специальная теория относительности, но в этом разделе мы обратим большее внимание на его описание броуновского движения и фотоэлектрического эффекта. Действительно, обе теоретические модели показывают глубокую интуицию Эйнштейна в области механики. Броуновское движение было им объяснено как сложные последовательности столкновений (похожих на столкновения бильярдных шаров) между видимой молекулой – частицей, участвующей в броуновском движении, – и меньшими по размеру невидимыми частицами. Дальнейшие случайные столкновения объясняют ломаную траекторию движения частиц. Подобно этому, получил механическое истолкование фотоэлектрический эффект. Световые лучи состоят из маленьких бильярдных шаров, энергия которых определяет их цвет, т.е. длину световой волны. Эти световые корпускулы (сегодня их называют фотонами и вовсе не считают похожими на бильярдные шары) сталкиваются с электронами на поверхности металла и механически выбивают их оттуда, если им хватает энергии.

Общая теория относительности также может быть истолкована как механическое объяснение гравитации. Когда камень катится по Луне, пучок гравитонов (по современной терминологии) разлетается во всех направлениях с конечной скоростью – скоростью света. Следовательно, лишь секундой позже информация об этом достигнет Земли и только тогда повлияет на наш вес. Я думаю, что это – величайшее достижение Эйнштейна, величайшего инженера[1] всех времен: **Эйнштейн придал физике статус локальной теории!**

---

[1] Мои друзья хорошо знают, что в моих устах слово ”инженер” не несет негативного смысла, скорее, наоборот. С моей точки зрения, физик должен быть хорошим теоретиком и хорошим инженером! Что ж, дорогой читатель, я предупреждал тебя, что эта статья имеет субъективный характер.

IV. КВАНТОВАЯ МЕХАНИКА НЕ ЯВЛЯЕТСЯ МЕХАНИКОЙ

Квантовая механика появилась лишь спустя десять лет после появления общей теории относительности. Это была по-настоящему экстраординарная революция До этого, во многом благодаря гению Ньютона и Эйнштейна, Природа казалась состоящей из большого числа маленьких бильярдных шаров, которые механически сталкиваются друг с другом. Но квантовая механика характеризуется как раз тем, что она больше не дает механического описания Природы. Термин “квантовая механика” – просто историческая ошибка, ее следует называть квантовой физикой, так как это совсем иной способ физического описания Природы.

Но это новое описание снова вводит нелокальность в физику! Все это было для Эйнштейна неприемлемым.

Замечательно, хотя и мало где отмечено, что после Ньютона физика давала локальное описание Природы только в течение 10 лет, между 1915 и 1925 г.г. Все остальное время описание было нелокальным, хотя применительно к квантовой физике это носит совершенно иной характер, нежели в теории тяготения Ньютона. На самом деле новая теория потребовала возможности сколь угодно быстрого обмена сообщениями, тогда как старая запрещает это.

V. НЕЛОКАЛЬНОСТЬ ПО ЭЙНШТЕЙНУ

В 1935 г. в респектабельных журналах появились две знаменитые статьи, обе были написаны известными авторами, в обеих говорилось о (неприемлемых для их авторов) нелокальных предсказаниях квантовой физики [1, 6]. Было много написано о “парадоксе” ЭПР, и мне нечего к этому добавить. Я думаю, что реакцию Эйнштейна легко понять. Человек, сделавший физическую теорию локальной спустя сотни лет после Ньютона, написал свое тревожное послание, он гордился своим достижением и определенно этого заслуживал. Но сейчас, всего лишь небольшое время спустя, нелокальность вернулась! Сегодня следует добавить, что квантовая нелокальность существенно отличается от концепции нелокальности Ньютона, но Эйнштейн полностью еще не осознавал этого.

Эйнштейн и его коллеги видели, что квантовая физика описывает пространственно удаленные частицы как глобальную систему, в которой эти частицы вместе образуют единое логическое целое. Они не осознавали полностью, что при этом не допускается обмен информацией и, следовательно, не возникает прямого конфликта с теорией относительности. В следующем разделе я попытаюсь изложить это с помощью современной терминологии.

Большинство физиков не уделило существенного внимания этому аспекту квантовой физики. Установился своеобразный консенсус, что это – предмет будущих исследований, когда наука продвинется дальше. Общее понимание состояло в том, что квантовая нелокальность – не более, чем научный курьез, а не серьезная физика.

Молодые физики с трудом могут поверить, что такое важное понятие, как квантовая нелокальность, в течение ряда лет серьезно не обсуждалось. Но таково было действительное положение дел: спросите какого-либо старого профессора, значительное большинство их все еще верит, что это не важно. Позвольте добавить к этому две маленькие истории, которые подтверждают, что все так и было. Джон Белл – знаменитый автор неравенств Белла и состояний Белла – никогда не имел

аспирантов, специализирующихся в области квантовой физике. Когда молодой физик подходил к нему и заводил разговор о нелокальности, Джон первым делом спрашивал его: ”А у вас есть постоянное место работы?”. В самом деле, без такой постоянной должности невозможно было осмеливаться заниматься проблемой нелокальности! Отметим, что Джон Белл практически никогда не публиковал свои замечательные и сегодня знаменитые статьи [7] в серьезных журналах: борьба с рецензентами была слишком ... длительной (если не пользоваться более адекватной терминологией). Далее, если бы вы посетили ЦЕРН, где Джон Белл постоянно работал в теоретическом отделе, и спросили первого встречного о вкладе Джона в физику, его работа в области оснований квантовой физики вряд ли была бы упомянута (правда, он внес большой вклад и в других областях физики)[2].

Как бы то ни было, квантовая нелокальность в течение десятилетий оставалась научным курьезом и не привлекала заметного внимания. Однако в 1990-х произошли два изменения. Первый концептуальный прорыв произошел благодаря Артуру Экерту (Artur Ekert) и его руководителю Дэвиду Дейчу (David Deutsch) [9]. Они показали, что квантовая нелокальность может быть использована для создания криптографического ключа между двумя удаленными партнерами, и что конфиденциальность ключа может проверяться с использованием неравенства Белла. Вот это была настоящая революция! Так впервые стало понятно, что квантовая нелокальность не только реальна, но даже может быть практически использована. Второй вклад был внесен в связи с технологическим прогрессом. Появились и повсеместно начали внедряться оптические волокна. В это время группа Мэндела (Mandel’s group) в Рочестерском университете (где я в течение года был на пост-докторантской должности и впервые занялся оптикой) использовала параметрическое понижение частоты для генерации запутанных пар фотонов [10]. Этого оказалось достаточно (при наличии детекторов), чтобы продемонстрировать квантовую нелокальность как нечто, не являющееся научным недоразумением. В 1997 моя группа в Женевском университете продемонстрировала нарушение неравенств Белла в опытах между двумя пригородами Женевы (см. рис. 1), удаленных между собой на расстояние чуть больше 10 км и связанных стандартным телекоммуникационным оптоволоконным кабелем длиной 15 км [11, 12] (с тех пор мы достигли расстояния 50 км [13]). Так что квантовая нелокальность стала политически приемлемой! Но что это такое? Позвольте мне ввести вас в курс дела на примере студентов, сдающих ”квантовые экзамены”.

VI. КВАНТОВЫЕ ЭКЗАМЕНЫ: ЗАПУТЫВАНИЕ (ENTANGLEMENT)

Предположим, что двум студентам – Алисе и Бобу – предстоит сдать некие экзамены. Как всегда бывает на экзаменах, студентам запрещено общаться во время экзамена. Однако, очевидно, им позволяется общаться *до* экзамена. Алисе и Бобу заранее известен перечень вопросов, они также знают, что на этом экзамене разрешено лишь ограниченное число возможных ответов, часто есть лишь двоичный

[2] Другая история произошла со мной, когда будучи молодым пост-докторантом я попытался опубликовать одну свою статью. В статье [8] я писал: ”Квантовая частица может исчезнуть в точке A и одновременно возникнуть в точке B, без какого-либо перемещения между этими точками”. Рецензент принял статью при условии, что эта скандальная фраза будет удалена. Рецензент оценивал свое отеческое отношение так серьезно, что сказал мне: ”Смотрите, как я помог Вам!” (возможно, он старался быть политкорректным).

выбор между *да* и *нет*. Во время экзамена Алиса получает один вопрос из перечня, обозначим его через *x*; Боб получает вопрос *y*. Наконец, обозначим через *a* и *b* соответственно ответы Алисы и Боба. Следовательно, экзамен представляет собой реализацию случайного процесса, описываемого функцией условной вероятности, часто именуемой просто корреляцией:

$$P(a,b|x,y) \qquad (1)$$

Ясно, что выбор вопросов *x* и *y* контролируется преподавателем. Однако, как знают все преподаватели, ответы студентов *a* и *b* *не* контролируются преподавателем! Это похоже на эксперименты: за физиком – выбор эксперимента, но не ответ, даваемый Природой.

Далее мы должны рассмотреть три типа экзаменов, чтобы понять, какие ограничения они накладывают на корреляцию P(*a*, *b*|*x*, *y*).

VI-a. Квантовый экзамен #1

На первом квантовом экзамене Алису просят ответить, какой вопрос задан Бобу, и наоборот. Это неправильный экзамен! Почему? Да потому, что Алиса и Боб не обмениваются информацией. Как им действовать, чтобы вероятность была выше, чем просто случайной[3]? Этот простой пример показывает, что запрет на обмен информацией уже ограничивает набор возможных корреляций P(*a*, *b*|*x*, *y*). Например, вариант P(*a, b*|*x, y*) = *δ*(*a* = *y*)δ(*b* = *x*) исключен. Заметим, что корреляция P(*a, b*|*x, y*) является не связанной с обменом сообщениями, т.е. бессигнальной (non-signaling), если и только если ее предельные вероятности независимы от участника с другой стороны: $\Sigma_{\mathbf{b}}$ P(*a, b*|*x, y*) не зависит от *y*, и $\Sigma_{\mathbf{a}}$ P(*a, b*|*x, y*) не зависит от *x*.

VI-b. Квантовый экзамен #2

Второй квантовый экзамен больше похож на экзамен обычного типа. От Алисы и Боба требуется давать одинаковые ответы, если они получают одинаковые вопросы. Это, очевидно, гораздо проще: мы все ожидаем, что хорошие студенты одинаково отвечают на одинаковые вопросы. Достаточно, чтобы они основательно подготовились к экзамену. Заметим, что рассматриваемый нами квантовый экзамен #2 даже легче, чем обычный экзамен, поскольку в данном случае неважно, дается ли *правильный* ответ или нет. Все, что требуется, так это чтобы Алиса и Боб давали согласованные ответы: достаточно, чтобы они заранее договорились, какой ответ давать на каждый из возможных вопросов.

А теперь главная проблема: могут ли Алиса и Боб уверенно выдержать такой экзамен #2 с помощью иной стратегии, т.е. без предварительного согласования своих ответов? Подумаем об этом. Если вы придумали альтернативный трюк, то, если вы студент, вам следует использовать свой трюк, чтобы пройти следующее испытание: просто примените этот трюк вместе с лучшим студентом, и вы получите

[3] Оказывается, имеется стратегия, при которой вероятности обоих игроков достигают 50%.

такую же оценку, как и он[4]. Но если вы – преподаватель и раскрыли этот трюк, то вы должны немедленно остановить обычный экзамен! Разумеется, в данном случае нет никаких трюков, пригодных для классических студентов.

Корреляции, удовлетворяющие условию P(*a* = *b*|*x* = *y*) = 1, с необходимостью имеют вид

$$P(a,b|x,y) = \sum_{\lambda} \rho(\lambda) Q(a|x,\lambda) Q(b|y,\lambda) \qquad (2)$$

для некоторой функции вероятности *Q* и некоторого распределения *ρ* общих стратегий λ. Исторически λ получило название ”локальных скрытых переменных ”, специалист по компьютерам называет это ”разделяемая (shared) случайность”; мы же подразумеваем под λ общие стратегии.

P(*a* = *b*|*x* = *y*) = 1 дает лишь один пример локальной корреляции, но существует бесконечно много других. Соотношение (2) характеризует все локальные корреляции.

Итак, некоторые экзамены требуют использования общих стратегий; другими словами, некоторые наблюдаемые корреляции *не могут быть объяснены иначе, как за счет общих причин*.

VI-c. Квантовый экзамен #3

Третий квантовый экзамен является наиболее затейливым и интересным. Для (кажущейся) простоты ограничим вопросы и ответы двоичным множеством и сопоставим им биты ”0” и ”1”. На этом экзамене от Алисы и Боба требуется давать одинаковый ответ всегда, за исключением случая, когда оба они получают вопрос с пометкой ”1”; в последнем случае они должны давать несовпадающие ответы. Заметим, что в этом случае ответы Алисы и Боба формально должны удовлетворять равенству $a+b = x \cdot y$ (по модулю 2). Теперь заранее не очевидно, могут ли они с помощью предварительной договоренности принять стратегию, гарантирующую им успех.

Предположим сначала, что эта стратегия побуждает Алису давать ответ, который зависит только от ее собственного вопроса *x*, т.е. стратегия Алисы является детерминистической. Но в этом случае Боб, получив вопрос 1, не может уточнить свой ответ, поскольку он будет зависеть от вопроса Алисы. Далее, если вопрос, полученный Алисой, выбирается наугад, то ясно, что Боб оказывается беспомощным. Следовательно, у Алисы и Боба нет определенной стратегии, гарантирующей успех.

Подчеркнем, что успешная сдача этого экзамена не обязательно предусматривает обмен информацией между Алисой и Бобом. Действительно, предположим, что каким-то образом данные Алисы и Боба всегда удовлетворяют условию $a + b = x \cdot y$. Позволяет ли это Алисе и Бобу косвенно обмениваться информацией между собой? Это зависит от одного обстоятельства! Если ответ Алисы известен Бобу, например, они всегда считают, что *a* = 0, то, как только Боб

[4] Опасность состоит в том, что оба студента могут получить плохую оценку! Но в среднем плохой студент выигрывает.

получает вопрос $y = 1$, он может вычислить вопрос Алисы из уравнения $a + b = x \cdot y$ и из знания ее ответа: $x = b$ в данном примере. Но если ответ Алисы Бобу не известен, например, если он дается чисто случайным образом, то тогда соотношение $a + b = xy$ Бобу уже не поможет. Мы вернемся к этой идее бессигнальной корреляции, удовлетворяющей условию $a + b = x \cdot y$ в разделе X-c.

Определим оценку M квантового экзамена #3 в виде суммы вероятностей успеха [14]:

$$\begin{aligned} M &= P(a+b=xy|x=0,y=0) \\ &+ P(a+b=xy|x=0,y=1) \\ &+ P(a+b=xy|x=1,y=0) \\ &+ P(a+b=xy|x=1,y=1) \end{aligned} \qquad (3)$$

Нетрудно подсчитать, что оптимальная стратегия для Алисы и Боба заключается в предварительной договоренности насчет общего ответа независимо от получаемых ими вопросов. При такой стратегии они могут добиться оценки M = 3. Это действительно оптимальная оценка, достижимая при общей стратегии:

$$M \leq 3 \qquad (4)$$

Это – пример неравенства Белла: ограничение корреляций, вытекающее из наличия общих стратегий. Представляют интерес такие неравенства Белла, которые могут нарушаться квантовой физикой. В случае (4), если частицы Алисы и Боба образуют общее синглетное состояние, то они могут добиться оценки $M_{\text{кв физ}} = 2 + \sqrt{2} \approx 3.41$. Цирельсон доказал, что это наибольшая достижимая величина, когда речь идет о квантовых корреляциях [15].

Соответственно, квантовая теория предсказывает, что в некоторых случаях ее результаты не могут быть объяснены никакой механической локальной моделью, т.е. некоторые экзамены могут быть сданы с более высокой оценкой, чем это возможно с классической точки зрения. Тот факт, что эти случаи были специально придуманы, чтобы показать “превосходство” квантовой физики, никак не влияет на выводы. Как только эти полезные и естественные случаи, конкретизирующие превосходящую мощь квантовой физики по отношению ко всем возможным локальным стратегиям, были найдены, квантовая нелокальность была принята физическим сообществом[5].

VII. ПОДБРАСЫВАНИЕ МОНЕТ НА РАССТОЯНИИ

Иной способ рассказать о нелокальности коллегам, не являющимся физиками, состоит в следующем. Вообразим себе двух игроков, подбрасывающих монеты. Игроки находятся на расстоянии друг от друга и бросают свои монеты один раз в минуту. Каждый раз каждый из них независимо и по свой воле выбирает, делать ли ему бросок левой или правой рукой. При этом они заносят все сведения (время,

[5]Я хочу привести некоторую статистику употребления слов ”Неравенство Белла” и ”нелокальность” в журнале Physical Review Letters. Я установил, что фазовый переход произошел в ранних 1990-х, после статьи Экерта по квантовой криптографии. В 1997 г. я впервые опубликовал в PRL с фразой: ”Квантовая теория нелокальна” и заслужил много упреков в том, что это – провокативное заявление; сегодня то же утверждение можно найти во многих статьях, и это не вызывает никаких претензий.

какой рукой произведено подбрасывание, его результат – орел или решка) в большой черный лабораторный ноутбук (см. рис. 1).

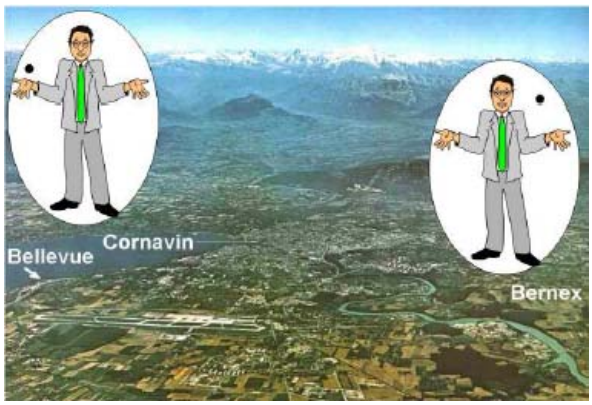

Рисунок 1: Bernex и Bellevue – два пригорода Женевы (один на севере, другой на юге от нее), между которыми в 1997 г. был проведен наш дистанционный (вне лаборатории) эксперимент по проверке неравенства Белла (см. раздел V). На рисунке показаны два игрока, подбрасывающих монеты, как объяснено в разделе VII. В реальном эксперименте монеты были заменены на фотоны, игроки – на интерферометры, их правые и левые руки – на фазовые модуляторы, а орел и решка – на показания двух детекторов. Результаты эксперимента были сходны с результатами игры, но со слабыми нелокальными корреляциями.

После тысячи подбрасываний им это становится скучно. Особенно, если учесть, что не происходит ничего интересного: у каждого из игроков орел и решка выпадают с частотой 50%, независимо от того, какой рукой они подбрасывают монету. Итак, игроки принимают решение сходить в бар и выпить пива. Там, в баре, они сравнивают свои записи и приходят в сильное волнение. Действительно, они быстро замечают, что всякий раз, когда *хотя бы один* из них бросал монету *правой* рукой, то у *обоих* игроков монета падала вверх *одной и той же* стороной (либо орлом, либо решкой). Но когда, по случайному совпадению, они оба делали бросок *левой* рукой, то их результаты всегда были *противоположны*: орел/решка или решка/орел. Очень неординарная корреляция!

Наблюдение корреляций и развитие теоретических моделей, объясняющих их, составляет суть научного метода. Это справедливо не только для физики, но также и для других наук, например, для геологии и медицины. Джон Белл выразился так: ”корреляции вопиют, требуя объяснений!” [16].

Так почему же наши игроки пришли в такое возбуждение от корреляций, которые они выявили? Заметим, что с локальной точки зрения ничего интересного не происходило; в частности, один игрок не влиял на выбор руки другим игроком. Даже если один игрок решил бы всегда пользоваться одной и той же рукой, это не повлияло бы на статистику результатов его коллеги. Следовательно, эта игра и наблюдаемая корреляция не предполагает никакого обмена информацией, т.е. она является бессигнальной. Почему же нам кажется это невозможным? Откровенно говоря, на самом деле мне это не известно!

Классические корреляции всегда объясняются одной из двух причин. Первое объяснение сводится к ”сигнализации”, когда один игрок информирует другого или каким-то образом влияет на него. В данном случае, очевидно, это не так, поскольку

мы предположили, что игроки находятся друг от друга на большом расстоянии (для физиков можно добавить, что интервал между ними является ”пространственно-подобным”). Вторым объяснением для классических корреляций может быть наличие общей причины. Например, все футболисты одновременно прекращают игру потому, что арбитр дал свисток. Это объяснение в точности эквивалентно предположению о наличии общей стратегии, что описывается соотношением (2) и запрещено для данной корреляции неравенством Белла (4). Следовательно, корреляция, выявленная двумя нашими игроками, имеет иную природу. Большой неожиданностью оказывается тот факт, что нечто, выходящее за рамки двух классических объяснений для этой корреляции, действительно существует! А ведь в невозможность этого долгое время верили Эйнштейн и многие другие авторы. Но сегодня, если признать предсказания теории и их экспериментальные доказательства, то возникает следующий непростой вопрос: ”почему же такая корреляция, которую выявили наши гипотетические игроки, не наблюдается в нашем обычном мире?”.

Действительно, квантовая физика (и тензорные произведения гильбертовых пространств) говорит нам, что неравенство Белла (4) может нарушаться, т.е. что не все квантовые корреляции могут быть объяснены двумя классическими причинами корреляций, хотя квантовая физика и не допускает столь сильных корреляций, как наблюдавшиеся нашими гипотетическими игроками. В общем, эта игра иллюстрирует для нас квантовую нелокальность, как мы увидим в разделе X.

VIII. ЭКСПЕРИМЕНТЫ ГОВОРЯТ: БОГ ИГРАЕТ В КОСТИ, ОН ДАЖЕ ИГРАЕТ В НЕЛОКАЛЬНЫЕ КОСТИ

Физика является экспериментальной наукой, а эксперименты снова и снова подтверждают нелокальные предсказания квантовой теории. Были выполнены всевозможные виды экспериментов, как в лаборатории [18], так и за ее пределами [11, 12, 19], с фотонами и массивными частицами [20], с независимыми наблюдателями для затыкания возможной “прорехи” локальности (to close the locality loophole) [11, 12, 17, 19, 21], с квази-идеальными детекторами [20] для затыкания “прорехи” детектирования (to close the detection loophole), с высокой точностью синхронизации для ограничения скорости возможного скрытого обмена информацией [22], с движущимися наблюдателями для проверки альтернативных моделей [23] (мульти-одновременности [24] и Бомовской волны-пилота [25])[6]. Все эти результаты громко говорят, что [вопреки знаменитому утверждению Эйнштейна – прим. пер.] “Бог играет в кости”. Обратим внимание на иронию ситуации: вывод, что Бог играет в кости, дан нам очевидностью эксперимента, подтверждающего квантовую нелокальность, и постулатом Эйнштейна о невозможности передачи информации со сверхсветовой скоростью. В самом деле, как упоминалось в подразделе VI-c, невыполнение условия (4) при детерминистических правилах ведет к факту передачи информации (к сигнализации). Следовательно, экспериментальное нарушение (4) и постулат бессигнальности влечет наличие случайности [26, 27].

[6] Вывод, который следует из всех этих экспериментов, так важен для физических представлений о мире, что очень нужен эксперимент, исключающий одновременно и локальность, и ошибку в детектировании.

Фактически, ситуация даже еще интереснее: Бог не только играет в кости, Он играет в нелокальные кости! **Одинаковая случайность проявляет себя сразу в различных местах**, демонстрируя выполнение соотношения $a + b \approx x \cdot y$ с большей точностью, чем это возможно в рамках классической локальной модели.

Лишь очень небольшое меньшинство физиков еще отказывается признать квантовую нелокальность. Они спрашивают (зачастую с раздражением): *Как можно, находясь в одной (из двух, разделенных в пространстве-времени) точке, узнать, что происходит в другой, не обмениваясь информацией*? Я думаю, это замечательный вопрос! Годами я засыпал, размышляя об этом [28]. Я суммирую свои размышления в следующем разделе.

IX. ЗАПУТЫВАНИЕ КАК ПРИЧИНА КОРРЕЛЯЦИИ

Квантовая физика предсказывает существование совсем нового типа корреляции, которая никогда не сможет быть объяснена с точки зрения механики. И эксперименты это подтверждают: Природа способна демонстрировать одни и те же случайные события в различных местах, возможно, разделенных пространственно-подобным интервалом. Стандартное объяснение состоит в использовании термина ”запутывание”, но это просто слово, правда, имеющее точное техническое определение [29, 30]. Слова все еще полезны для обозначения предметов и понятий. Однако остается понять смысл этого наименования. Запутывание представляет собой новое объяснение корреляций. Квантовые корреляции так же неизбежны, как и другие вещи (огонь обжигает, столкновение со стеной приводит к ушибу, и т.п.). Запутывание возникает на том же концептуальном уровне, как и локальные причины и следствия. Это первичное понятие, не сводимое к локальным причинам и следствиям. Запутывание описывает корреляции без источника корреляции [31] с холистической точки зрения [32]. Иными словами, **квантовая корреляция – это не корреляция между двумя событиями, но единичное событие, проявляющее себя сразу в двух местах**.

Вы удовлетворены моим объяснением того, что такое запутывание? Лично я совсем не удовлетворен! Но что очевидно, так это то, что запутывание существует. Более того, запутывание невероятно прочно! Последнее утверждение может показаться неожиданным, поскольку еще зачастую можно услышать, что запутывание неуловимо, как мечта: как только вы попытаетесь говорить о нем, оно исчезает! Исторически это частично связано с подозрением, что запутывание не является реально чем-то реальным (entanglement was not really real), не более чем некоторые экзотические частицы, которые рождаются случайно и живут в течение мельчайших долей секунды. Но сегодня мы наблюдаем все возрастающее число замечательных экспериментов, подтверждающих существование запутывания.

Запутывание на больших расстояниях [11, 12, 13, 19, 33], запутывание между большим числом фотонов [34] и между большим числом ионов [35], запутывание иона с фотоном [36, 37], запутывание мезоскопических систем (точнее, запутывание между небольшим числом колебательных мод, в которых участвует большое число частиц) [38, 39, 40], переключение запутывания (entanglement swapping) [41, 42, 43], передача запутывания между различными носителями [44], и т.д.

Резюмируем: запутывание существует и начинает влиять на будущие технологии. Это радикально новая концепция, требующая новых терминов и новых понятийных категорий.

X. ОТ КВАНТОВОЙ НЕЛОКАЛЬНОСТИ К ОБЫЧНОЙ

Итак, мы видим, что квантовая физика порождает нелокальные корреляции. И что из этого следует? Ну, хорошо, это может быть использовано для Распространения Квантового Ключа (Quantum Key Distribution) и в других процессах обработки квантовой информации, но это не очень-то помогает нам понять нелокальность. Концептуально мы могли бы изучать нелокальность и без всякого использования инфраструктуры квантовой физики, как-то: гильбертовых пространств, наблюдаемых и тензорных произведений. Нас не должно удивлять, что как только существование нелокальности было обнаружено, то быстро нашелся и концептуальный инструмент для ее изучения. Действительно, такой инструмент уже существовал в математической [45] и даже в физической [26, 27] литературе, дожидаясь, пока общественность проснется! Основной инструмент прост, не требует знания квантовой физики и позволяет, так сказать, изучать квантовую нелокальность ”извне”, т.е. внешним образом по отношению к инфраструктуре квантовой физики.

Вернемся к квантовому экзамену #3 (подраздел VI-c). Предположим, что Алиса и Боб не ограничены квантовой физикой, а ограничены лишь условием, что они не обмениваются сообщениями (no-signaling condition). Следовательно, они все равно провалили бы экзамен #1. Но, соблюдая это более слабое условие, они могли бы успешно сдать квантовый экзамен #3: Алиса и Боб могли бы (каждый из них) формировать выходной бит, который локально казался бы совершенно случайным и независимым от их входных битов. Следовательно, они не обменивались бы сообщениями, но их 2 бита удовлетворяли бы условию $a + b = x \cdot y$, в точности как в игре с подбрасыванием монеток, описанной в разделе VII. Гипотетическая ”машина”, точно воспроизводящая эту корреляцию, служит базовым примером концептуального инструмента, который необходим нам для изучения нелокальности без привлечения квантовой физики. Формально такая функция корреляции определяется соотношением:

$$P(a,b|x,y) = \frac{1}{2}\delta(a+b = x \cdot y) \qquad (5)$$

где функция $\delta(z_1 = z_2)$ принимает значение 1 для $z_1 = z_2$ и значение 0 в противоположном случае.

Корреляция (5) часто упоминается как PR-ящик, в честь основополагающих работ Popescu и Rohrlich [26, 27], или как NL-машина (машина с нелокальными переменными – Non-Local machine[7]). Смысл этой терминологии состоит в том, чтобы подчеркнуть сходство между квантовыми измерениями над двумя максимально запутанными кубитами и корреляцией (5): в обоих случаях результат доступен, как только становится известен соответствующий входной бит. Алисе становится известно значение *a*, как только она вводит входное значение *x* в свою часть машины. Аналогично, Боб узнает значение *b*, как только он введет *y*. Нет необходимости ждать, пока другой введет свое входное значение. Как в квантовой физике, так и в PR-ящике ”машина” не может быть использована больше одного раза

[7] Термин ”машина” используется физиками для обозначения черного ящика со входом и выходом, не обязательно механического. Мне кажется, этот термин появился в квантовой физике в связи с понятием ”оптимальных клонирующих машин”, введенным Buzek и Hillery [46]

(как только Алиса получает на входе *x*, она не может изменить свое мнение и задать на входе иное значение). Заметим еще одну замечательную аналогию: ни квантовая физика, ни NL-машины не позволяют обмениваться сообщениями. Действительно, во всех этих случаях сообщения представляют собой чистый шум, независимо от того, что имеется на входе.

Отметим, что квантовая физика не способна воспроизводить PR – корреляцию (5). Действительно, эта корреляция нарушает неравенство Белла (4) вплоть до алгебраического максимума M = 4, в то время, как теорема Цирельсона [15] утверждает, что квантовые корреляции должны быть ограничены значением $M \leq 2 + \sqrt{2}$. Однако корреляция (5) значительно проще, чем квантовые корреляции, и при этом сохраняет многие их существенные свойства. В частности, (5) нелокальна, но бессигнальна (non-signaling).

Чтобы глубже понять возможности этой гипотетической машины (5) как концептуального инструмента, рассмотрим 3 свойства квантовых корреляций (множество других замечательных аспектов можно найти в [47, 48, 49]). Сначала мы рассмотрим так называемую теорему о невозможности квантового клонирования и увидим, что на самом деле это не квантовая теорема, а теорема, связанная с отсутствием обмена сообщениями. Следующий естественный шаг состоит в анализе квантовой криптографии, надежность которой часто связывают с теоремой о невозможности клонирования, и, как и можно было бы теперь ожидать, мы обнаружим ”бессигнальную криптографию”. Наконец, мы рассмотрим вопрос о затратах на передачу информации при воспроизведении максимальной квантовой корреляции. Но перед всем этим нам необходимо обратиться к некоторым фактам, относящимся к бессигнальным корреляциям.

X-a. Множество бессигнальных корреляций

Рассмотрим вначале множество всех возможных двухчастичных коррелляций P(*a*, *b*|*x*, *y*), где входные значения заданы на конечных алфавитах {*x*} и {*y*}, и подобным же образом выходные значения заданы на конечных алфавитах {*a*} и {*b*}, причем эти корреляции являются бессигнальными:

$$\sum_b P(a,b|x,y) = P(a|x) \quad \text{не зависит от} \quad y \qquad (6)$$

$$\sum_a P(a,b|x,y) = P(b|y) \quad \text{не зависит от} \quad x \qquad (7)$$

Априори это множество кажется огромным. Но оно обладает замечательной структурой. Во-первых, это выпуклое множество: выпуклые комбинации бессигнальных корреляций также являются бессигнальными. Во-вторых, имеется лишь конечное число точек экстремума (математики называют такие множества многогранниками, а точки экстремума – вершинами); соответственно, каждая бессигнальная корреляция может быть представлена в виде (не обязательно единственной) выпуклой комбинации точек экстремума. Тут имеется аналогия с квантовыми смешанными состояниями, которые могут быть представлены в виде выпуклых смесей чистых состояний.

Частью множества бессигнальных корреляций являются локальные корреляции, удовлетворяющие условию (2), аналоги сепарабельных квантовых состояний. Множество локальных корреляций также образует многогранник, под-многогранник бессигнального многогранника. Более того, все вершины локального многогранника являются одновременно вершинами бессигнального многогранника, см. рис. 2 [48]. Грани локального многогранника взаимно-однозначно соответствуют всем возможным неравенствам Белла.

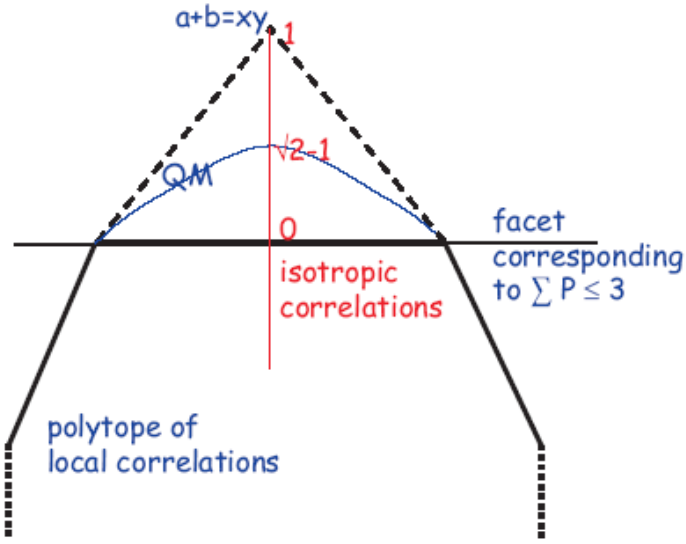

Рисунок 2: Геометрическая точка зрения на множество корреляций. Нижняя часть изображает выпуклое множество (многогранник) локальных корреляций (polytope of local correlations) с верхней гранью (facet corresponding to $\Sigma P \leq 3$), отвечающей неравенству Белла (4). Верхний треугольник соответствует нелокальным бессигнальным корреляциям, нарушающим неравенство Белла. Сплошная (синяя) тонкая кривая ограничивает корреляции, достижимые в квантовой физике (QM). Вершина треугольника отвечает единственной бессигнальной вершине, лежащей выше границы для этого неравенства Белла, т.е. нелокальной PR-машине (5). Тонкая (красная) вертикальная линия изображает изотропные корреляции (isotropic correlations) (8) с указанием некоторых значений p_{NL}.

Проиллюстрируем это на примере простого бинарного случая (которого часто вполне достаточно для данной статьи), т.е. когда *a*, *b*, *x*, *y* представляют собой 4 бита. В этом случае, как известно,іимеется только 8 нетривиальных неравенств Белла (мы не учитываем тривиальные неравенства вида $P(a, b|x, y) \geq 0$), т.е. только 8 релевантных граней локального многогранника. Интересно (это показал Barret с соавторами [48]), что бессигнальный многогранник имеет только на 8 вершин больше, чем локальный многогранник, в точности по одной на каждое неравенство Белла! Каждая из этих 8 вершин эквивалентна PR-корреляции (5), с точностью до элементарной симметрии (замена входа и/или выхода).

Хотя эти многогранники принадлежат 8-мерному пространству[8], их основные свойства могут быть поняты на примере несложной геометрии рисунка 2.

X-b. Теорема о невозможности клонирования

Подробности можно найти в [47], а здесь мы будем просто опираться на интуицию. Предположим, что Алиса (входной и выходной биты x and a, соответственно) разделяет корреляцию (5) как с Бобом (биты y и b), так и с Чарли (биты z и c): $a + b = xy$ и $a + c = xz$. Заметим, что эта ситуация отлична от той, при которой Алиса разделяет одну ”машину” с Бобом, а другую, независимую от первой “машину”, с Чарли: в нашей ситуации Алиса обладает единственным входным битом x и единственным выходным битом a. Как мы сейчас увидим, предположение, согласно которому входной и выходной биты Алисы x и a одновременно коррелируют и с Бобом, и с Чарли, приводит к возникновению обмена информацией. Следовательно, в бессигнальной Вселенной Алиса не может разделять корреляцию (5) более чем с одним партнером: корреляция не может быть клонирована.

Чтобы понять это, предположим, что Боб и Чарли получают одновременно входные биты $y = 1$ и $z = 0$ и выдают на выходе $b + c$. Согласно предположенной нами корреляции (и учитывая, что правило сложения по модулю 2 дает $a + a = 0$), получаем: $b + c = a + b + a + c = xy + xz = x$. Следовательно, они могли бы по своим битам определить входной бит Алисы x, а это означало бы, что Алиса может передать им информацию!

Естественный вопрос состоит в том, при каких условиях корреляция (5) допускает клонирование? Ответ весьма интересен: если корреляция Алиса-Боб нарушает неравенство Белла (4), то корреляция Алиса-Чарли уже не может нарушать его; в противном случае возникает обмен информацией.

Мы только что обнаружили, что CHSH-Bell неравенство (4) является “моногамным”, позволяя сохранять секреты. Сейчас мы увидим, что это не случайно!

X-c. Криптография без обмена информацией

В 1991 открытие Артуром Экертом квантовой криптографии [9], основанной на нарушении неравенства Белла, изменило мир (физиков): запутывание и квантовая нелокальность обрели респектабельность. Сейчас, как мы увидим в этом подразделе, суть безопасности квантовой криптографии выводят не из структуры гильбертова пространства квантовой физики (т.е. не из запутывания), а из бессигнальной корреляции! Тот факт, что квантовая физика предоставляет способ реализовать такую корреляцию, делает идею практически осуществимой. Однако, если бы кто-либо придумал другой способ осуществить подобную бессигнальную корреляцию (сегодня никто не знает другого способа), то это дало бы равную возможность создавать криптографические ключи [51].

Подчеркнем, что речь не идет о каких-либо ограничениях, накладываемых на противника [стремящегося перехватить сообщение – примеч. пер.], например, Еву, исключая требование не обмениваться информацией[9] [52]. Очевидно, если

[8] Более точно, 8 – это размерность пространства бессигнальных корреляций [50].

[9] Отсутствие обмена информацией (no-signaling) должно пониматься здесь как в предшествующем подразделе - теореме о невозможности клонирования. То-есть, даже если две смежные части,

предполагаются дополнительные ограничения для Евы, например, использование только квантовой физики, то Алиса и Боб могут сделать свои данные еще более секретными. Но в качественном отношении ситуация не изменится.

Предположим, что два партнера – Алиса и Боб – имеют устройства, которые позволяют каждому из них формировать входной бит (делать двоичный выбор из чего-либо, например, какой эксперимент осуществить), и каждый из них принимает выходной бит (например, результат эксперимента). Это может быть описано в виде произвольной корреляции: P(*a*, *b*|*x*, *y*), где *a, b, x, y* – четыре бита. Предположим далее, что устройства Алисы и Боба запрещают обмен информацией. Этого простого и очень естественного предположения достаточно, чтобы задать замечательную структуру множества корреляций P(*a*, *b*|*x*, *y*): как было описано в подразделе X-а, это множество является выпуклым и имеет конечное число точек экстремума, называемых вершинами. Замечательное свойство состоит в том, что любая корреляция P(*a*, *b*|*x*, *y*) может быть разложена на выпуклую комбинацию вершин, следовательно, если кто-то знает вершины, то он знает все. Если бы корреляция была локальна, т.е. удовлетворяла условию (2), то она была бы бесполезна для криптографии; действительно, противник Ева могла бы узнать стратегию λ. Итак, предположим, что P(*a*, *b*|*x*, *y*) нарушает неравенство Белла (4). Следовательно, P(*a*, *b*|*x*, *y*) лежит в хорошо определенном угле общего многогранника, в суб-многограннике. Barrett и его сотрудники установили, что этот субмногогранник имеет только 9 вершин [48], причем 8 локальных, для которых M = 3, и только одну нелокальную вершину, которая отвечает нашему концептуальному инструменту, т.е. соотношению *a* + *b* = *xy*, для которого M = 4, см. рис. 2.

В случае максимальной корреляции между Алисой и Бобом (максимальной, но без обмена информацией!), когда их корреляция соответствует нелокальной вершине на рис. 2, интуитивно ясно, что их противник Ева не может быть скоррелирована ни с Алисой, ни с Бобом в силу аргумента о невозможности клонирования, о чем говорилось в предшествующем подразделе. Следовательно, в этом случае Алиса и Боб получают от своих устройств полностью секретные биты. Однако эти биты не всегда скоррелированы: когда *x* = *y* = 1, они анти-коррелированы. Но это может быть легко зафиксировано следующим протоколом. После того, как Алиса и Боб сформировали свои выходные биты, Алиса публично оглашает свой входной бит *x*, а Боб изменяет свой выходной бит на *b′* = *b* + *xy*. Теперь Алиса и Боб идеально коррелируют между собой, а Ева все еще ничего не знает относительно *a* и *b′*.

Рассмотрим теперь случай, когда корреляция между Алисой и Бобом не максимальна:

$$P(a,b|x,y)=\frac{1+p_{NL}}{2}\frac{1}{2}\delta(a+b=x\cdot y)+\frac{1-p_{NL}}{2}\frac{1}{4} \quad (8)$$

При $p_{NL} > 0$ эта корреляция нарушает неравенство (4), при $p_{NL} \le \sqrt{2}-1$ оно может быть реализовано с помощью квантовой физики. Могут ли Алиса и Боб воспользоваться такой корреляцией для криптографического применения, чтобы обеспечить секретность по отношению к любому противнику, ограниченному не квантовой

например, Ева и Боб, находятся рядом, то они не должны обмениваться информацией относительно входного бита третьей частит. Это значит, что Ева.и Боб не должны иметь доступа ко входному биту Алисы.

физикой, а лишь бессигнальной физикой? Полный ответ на этот замечательный вопрос все еще не известен. Однако имеется оптимистический ответ для случая, когда Ева подвергает атаке каждую реализацию независимо от других, т.е. когда речь идет о так называемых индивидуальных атаках. В этом случае можно предположить, что Ева распределяет устройства для отправки Алисе и Бобу. Устройства обычно являются локальными, для них Ева точно знает соотношение между входными и выходными битами как у Алисы, так и Боба. Например, Ева посылает Алисе устройство, которое на выходе выдает всегда 0, а Бобу – устройство, которое воспроизводит на выходе входной бит: $b = y$. В этом примере Ева знает бит a Алисы, но не знает бита Боба. Для некоторой локальной пары устройств Ева знает либо оба бита a и b, либо только b, но не a. Однако, если корреляция Алиса-Боб (8) нарушает неравенство Белла (4), т.е. если $p_{\mathbf{NL}} > 0$, то Ева должна иногда посылать Алисе и Бобу устройства, обеспечивающие максимальную нелокальную корреляцию $a + b = xy$[10], в этом случае она ничего не знает про выходные биты Алисы и Боба a и b. Подробности этого анализа приведены в [51], здесь мы просто приводим результат. При $p_{\mathbf{NL}} > 0.318$ взаимная информация по Шеннону между Алисой и Бобом больше, чем взаимная информация между Евой и Бобом [51]. Следовательно, при $p_{\mathbf{NL}} > 0.318$ Алиса и Боб могут извлечь криптографический секретный ключ из своих данных, безопасно даже по отношению к гипотетическому пост-квантовому противнику, который, однако, должен соответствовать условию бессигнальности.

В работе [51] мы разработали 2-канальный протокол для извлечения ключа, пригодный вплоть до $p_{\mathbf{NL}} > 0.09$. Там также доказывается, что соответствующая информация положительна при всех положительных $p_{\mathbf{NL}}$. Таким образом, можно полагать, что извлечение секретного ключа возможно, если и только если неравенство Белла нарушается[11].

Другой красивый результат заключается в установлении соотношения между приращением и потерей информации, что очень похоже на соотношение неопределенностей Гейзенберга в квантовой физике [54]. Будем по отдельности анализировать случаи, когда Алиса объявляет $x = 0$ и $x = 1$, и обозначим соответствующую частоу появления ошибок в канале Алиса-Боб через $QBER_x$, а взаимную информацию Ева-Боб через $I_x(B,E)$, т.е. $QBER_x = \sum_y P(a \neq b)|x, y)$ и $I_x(B,E) = H(B|x) - H(B|E, x)$. Замечательно, что $I_0(B,E)$ является функцией только $QBER_1$, а $I_1(B,E)$ – только $QBER_0$[12]: приращение информации по одному входу с необходимостью приводит к ошибкам на другом входе, по аналогии с квантовым

[10]Можно было бы предположить, что Ева должна иногда посылать слабую нелокальную машину. Но все такие корреляции являются выпуклыми комбинациями локальных и полностью нелокальных NL-машин. Следовательно, для Евы это будет эквивалентно тому, чтобы всегда посылать любую (локальную или NL-машину), с подходящими вероятностями.

[11] В [47] мы доказали, что корреляция $P(a, b|x, y)$ является нелокальной, если и только если (iff) любые возможные бессигнальные расширения $P(a, b, e|x, y, z)$ имеют положительную условную взаимную информацию в канале Алиса-Боб, условную относительно Евы (has positive Alice-Bob condition mutual information, conditioned on Eve), I(A,B|E), т.е. обладают соответствующей (intrinsic) положительной информацией. Это служит прекрасным дополнением к аналогичному результату относительно запутанных квантовых состояний и очищений (purifications) [53]. В[51] мы доказали, что такое же соотношение между нелокальностью и положительной собственной информацией также выполняется, когда Алиса оглашает свой входной бит, а Боб адаптирует свой выходной бит так, чтобы максимизировать свою взаимную информацию с Алисой. Было бы чудесно доказать это в самом общем случае.

[12]Точнее,: $I_0(B,E) = 2 \cdot QBER_1$ and $I_1(B,E) = 2 \cdot QBER_0$.

случаем, где приращение информации по одному базису с необходимостью разрушает информацию, заключенную в смежном базисе!

В заключение этого подраздела подчеркнем, что распределение корреляции (8) в квантовом случае требует протокола, который отличается от знаменитого протокола BB84 [55]. Действительно, данные, получаемые Алисой и Бобом в соответствии с протоколом BB84, не нарушают какого-либо неравенства Белла, следовательно, протокол BB84 не безопасен по отношению к бессигнальному пост-квантовому противнику. Действительно, даже свободные от шума данные BB84 могут быть получены при квантовых измерениях над сепарабельным состоянием высшей размерности.

Дополнительная размерность могла, в случае с поляризационным кодированием, служить каналом утечки информации, обусловленным случайным дополнительным кодированием по длине волны (be side-channels due to accidental additional wavelength coding). Следовательно, стандартные доказательства безопасности [56, 57] должны учитывать предположения относительно такой размерности релевантных гильбертовых пространств (соответственно, доказательства небезопасности распространения квантового ключа являются безусловными, вопреки широко распространенным утверждениям). Но протокол BB84 легко адаптировать, достаточно, чтобы Алиса измеряла физические величины, отвечающие матрицам Паули σ_z или σ_x, в зависимости от того, равен ли ее входной бит соответственно 0 или 1, точно по протоколу BB84, а Боб измерял их в диагональном базисе: σ_{+45° или σ_{-45° соответственно при $y = 0$ и $y = 1$. При этом данные Алисы и Боба никогда не будут жестко коррелировать, но они могут нарушать неравенство Белла, и поэтому их можно использовать для извлечения секретного ключа, пригодного даже в случае пост-квантовых противников. Заметим, что нарушение неравенства Белла гарантирует отсутствие каналов утечки информации. Далее, в соответствии с этим протоколом, который мы бы хотели называть CHSH-протоколом в честь 4-х авторов [14] наиболее полезной версии неравенства Белла (фактически эквивалентного (4)), Алиса сообщает Асвой входной бит x, т.е. ее базис, как в BB84, но Боб молчит, он всегда в режиме приема и просто инвертирует (flips) свой бит в случае $x = y = 1$. В результате, работая по CHSH-протоколу, Алиса и Боб используют все необработанные биты, однако их данные являются более зашумленными, чем это обеспечивает протокол BB84.

X-d. Затраты на воспроизведение квантовых корреляций

Среди различных вкладов компьютерной науки в квантовую информацию имеется на редкость красивый простой вопрос (фактически угаданный Maudlin [58]): каковы затраты на воспроизведение квантовых корреляций? Более точно, Gilles Brassard, Richard Cleve и их студент Alain Tapp [59], и независимо Michael Steiner [60], сформулировали вопрос: насколько большим числом битов должны обменяться Алиса и Боб чтобы воспроизвести результаты (проективного) измерения, выполненного над квантовыми системами? Вопрос относится к обмену сообщениями во время воспроизведения измерения, ясно, что должны быть достигнуты предварительные договоренности насчет общей стратегии. Если системы находятся в сепарабельном состоянии, то никакого обмена сообщениями не требуется вовсе. Напротив, если состояние допускает измерения, нарушающее неравенство Белла, т.е. если состояние характеризуется квантовой нелокальностью, то его невозможно

воспроизвести без некоторого обмена сообщениями или некоторых других нелокальных ресурсов.

В простейшем случае 2-уровневых систем (2 кубита) эта игра предполагает, что Алиса и Боб принимают на входе значение некоторой возможной наблюдаемой, т.е. некоторый вектор $\vec{a}$ и $\vec{b}$ на сфере Пуанкаре. И они должны сформировать выходной бит, соответствующий двоичному результату измерения ”вверх” или ”вниз” в терминах физика, говорящего о частице со спином ½. Простой способ воспроизвести это квантовое измерение состоит в том, что Алиса сообщает свое входное значение $\vec{a}$ Бобу и формирует предопределенный бит (предопределенный общей стратегией Алисы и Боба). Но информация о векторе соответствует бесконечному множеству битов! Мое первое интуитивное мнение заключалось в том, что нет способа придумать что-либо лучше, в конце концов, входное пространство представляет собой континуум, в то время как в случае неравенств Белла входное множество конечно, обычно даже ограничено двоичным выбором. Однако Brassard с сотрудниками пришли к модели, использующей только 8 битов сообщения!

То был сюрприз: неужели запутывание обходится так дешево? Но это оказалось только началом. Steiner опубликовал модель, пригодную, правда, лишь для векторов, лежащих на экваторе сферы, но эту модель было легко обобщить на целую сферу [61]: она использует только 2 бита! 2 бита, как при плотном кодировании и телепортации: уж это-то предел, подумал я! И вновь я ошибся. Bacon и Toner придумали модель, использующую только один бит сообщения [62]. Прекрасно, но уж теперь-то мы достигли предела, не так ли? Так вот, это не так!

Вернемся к истинно главному вопросу: как Природа ухитряется формировать [одинаковые – прим. пер.] случайные данные в точках, разделенных пространственно-подобным интервалом, которые нельзя объяснить общими причинами? Интересно рассмотреть идею, согласно которой это обеспечивается некоторым скрытым обменом информацией (скрытым от нас, людей).

Моя группа в Женевском университете потратила определенное время, пытаясь разработать эту идею как в экспериментальном, так и в теоретическом плане. Мы смогли установить экспериментальные границы для скорости такого гипотетического скрытого обмена информацией [22]. Мы также исследовали идею, что каждый наблюдатель посылает скрытую информацию о своем результате с произвольно высокой скоростью относительно собственной инерциальной системы отсчета [23]. Измеренные границы скорости гипотетического скрытого обмена информацией оказались очень высокими, а последующее предположение противоречило экспериментам.

Наше теоретическое исследование также породило серьезные сомнения в существовании скрытого обмена информацией. Анализируя сценарий с 3 участниками, мы смогли доказать, что если бы все квантовые корреляции были обусловлены скрытым обменом информацией, то было бы возможным передать сигнал (т.е. скрытый обмен информацией превратился бы в явный) [63, 64]! Следовательно, остается лишь одна альтернатива – Природа использует как скрытый обмен информацией, так и скрытые переменные: каждая из этих возможностей по отдельности противоречит квантовой теории, но совместно могли бы объяснить квантовую физику. Однако это представляется слишком искусственной конструкцией. Итак, мы стоим перед следующей ситуацией: Природа способна формировать нелокальные данные без какого-либо обмена информацией. Но делает

ли она это, используя всю артиллерию квантовой физики? Есть ли там встроенные блоки нелокальности? Частичный ответ приводится ниже.

Вернемся к проблеме моделирования квантовых измерений, но вместо небольшого числа битов сообщения дадим Алисе и Бобу более слабый ресурс: вариант нелокальной машины $a + b = xy$. Это действительно более слабый ресурс, поскольку корреляцию $a + b = xy$ нельзя использовать для передачи какого-либо бита, но посылкой единственного бита легко можно моделировать нелокальную корреляцию (т.к. на входе Алисы имеется только бит x, то достаточно, чтобы она сообщила его Бобу). Замечательный сюрприз состоит в том, такого элементарного ресурса достаточно для моделирования пары проекционных измерений над любым максимально запутанным состоянием 2-х кубитов!

Доказательство читатель может найти в оригинальной статье [65], а в работе [66] представлен элегантный анализ соотношения между двумя этими моделями. Вышеприведенные результаты очень обнадеживают. Создается впечатление, что наконец-то мы начинаем понимать нелокальность без механизма гильбертовых пространств, что наконец-то можно изучать квантовую физику извне, т.е. в перспективе будущих физических теорий (предполагая сохранение эйнштейновых ограничений на скорость обмена информацией), а не с точки зрения старой классической физики. Но еще столько предстоит сделать! Например, неожиданным (и досадным, как я считаю) оказалось, что мы еще не можем моделировать частично запутанные состояния, используя нелокальную корреляцию (сейчас мы можем доказать, что невозможно с единственным этапом корреляции, но есть надежда, что можно моделировать частично запутанную пару кубитов в 2 этапа [67]). Хочу подчеркнуть, что все известные сегодня модели корреляции для частично запутанных кубитов включают в себя некоторый тип передачи сообщения[13] [62], скажем, от Алисы к Бобу. Следовательно, во всех этих моделях Боб не может сформировать свой результат прежде, чем Алиса не сообщит ему свои входные данные. Это контрастирует с ситуацией квантовых измерений, где Бобу не требуется ждать Алису (ему даже не нужно знать о существовании Алисы), и с моделью максимально запутанных кубитов, использующей PR-ящик. Было бы поразительным, если бы частично запутанное состояние не могло быть смоделировано симметричным во времени образом [69].

XI. ЗАКЛЮЧЕНИЕ

История нелокальности в физике замечательна. Она восходит к Ньютону (раздел II). Сначала она испытала ускорение в районе 1935 г. благодаря статьям Эйнштейна (ЭПР) и о кошке Шредингера. Далее она медленно эволюционировала (благодаря работам Джона Белла, Джона Клаузера и Алэна Аспека, а также многих других) от чисто философских дебатов до вопросов, решаемых экспериментальной физикой, или даже экспериментальной метафизикой, как прекрасно выразился Эбнер Шимони [70]. Сейчас, в течение последнего десятилетия, она помчалась на полной скорости. С концептуальной точки зрения произошли два принципиальных прорыва. Вначале появилась статья Артура Экерта в PRL (1991), в которой строго

[13] Используя редукцию некоторого OT-ящика (Переход к PR-ящику без запоминания - Oblivious Transfer to a PR-box) [68], можно смоделировать некоторое 2-кубитное состояние с помощью OT-ящика.

была показана глубокая связь между нелокальностью и криптографией (подраздел X-c). Вторым прорывом, по моему мнению, является открытие PR-ящика (подраздел X-a), пришло понимание того, что бессигнальные корреляции могут анализироваться сами по себе, без необходимости привлекать обычную артиллерию гильбертовых пространств, таким образом, появился простой концептуальный инструмент для обобщения квантовой нелокальности. Мы дали краткий обзор теоремы о невозможности клонирования, соотношения неопределенностей, моногамии предельной корреляции и распространения ключа безопасности. Все свойства, обычно ассоциируемые с квантовой физикой, в действительности являются свойствами бессигнальной теории (раздел X). В частности мы подчеркнули, что второй прорыв – PR-ящик – позволяет подтвердить первый прорыв: имеется тесная связь между нарушением неравенства Белла и безопасностью в квантовой криптографии.

Так может ли теория относительности рассматриваться в качестве полной теории? Что ж, если нелокальность реально существует, как многократно резюмировалось в данной статье, то во всех полных теориях должно найтись для нее место. Следовательно, вопрос должен быть поставлен так: ”Есть ли место в теории относительности для бессигнальных нелокальных корреляций?”

Благодарности

Эта статья основана на моих выступлениях в 2005 г. на IOP конференции по Эйнштейну в Уорвике, QUPON конференции в Вене, Симпозиуме Annus Mirabilis в Цюрихе, на семинаре Парижской обсерватории и на Эренфестовском коллоквиуме в Лейдене. Данная работа выполнена благодаря поддержке EC в рамках проектов RESQ и QAP (контракты IST-2001-37559 и IST-015848), а также Swiss NCCR Quantum Photonics.

Библиография

[1] A. Einstein, B. Podolsky & N. Rosen, Can quantummechanical description of physical reality be considered complete?, Phys. Rev. 47, 777-780 (1935).
[2] In contrast to S.Weinberg, Dreams of a final theory, Vintage/Random House, 1994.
[3] A. Shimony, in Foundations of Quantum Mechanics in the Light of New Technology, ed. S. Kamefuchi, Phys. Soc. Japan, Tokyo, 1983.
[4] For a lively acount of the history of quantum nonlocality and of the people who made it happen, see: The Age of Entanglement, Louisa L. Gilder, Knopf publishing, New-York, 2006
[5] Isaac Newton, Papers & Letters on Natural Philosophy and related documents, page 302, Edited, with a general introduction, by Bernard Cohen, assisted by Robert E. Schofield Harvard University Press, Cambridge, Massachusetts, 1958
[6] E. Schr¨odinger, Naturwissenschaften 23, 807 (1935).
[7] J. S. Bell, Speakable and Unspeakable in Quantum Mechanics: Collected papers on quantum philosophy (Cambridge University Press, Cambridge, 1987, revised edition 2004).
[8] N. Gisin, J. Math. Phys. 24, 1779-1782 (1983).
[9] A.K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[10] L. Mandel, Optical coherent & quantum optics, Cambridge University Press, 1995.
[11] W. Tittel, J. Brendel, N. Gisin and H. Zbinden, Phys. Rev. Lett. 81, 3563-3566 (1998).

[12] Tittel W., Brendel J., Gisin N. & H. Zbinden, Longdistance Bell-type tests using energy-time entangled photons, Phys. Rev. A, 59, 4150-4163 (1999).
[13] Ivan Marcikic, Hugues de Riedmatten, Wolfgang Tittel, Hugo Zbinden, Matthieu Legr´e and Nicolas Gisin, Phys. Rev. Lett. 93, 180502 (2004).
[14] M ≤ 3 is equivalent to the famous CHSH-Bell inequality: J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt, Phys. Rev. Lett. 23, 880 (1969).
[15] B.S. Cirel'son, Lett. Math. Phys. 4, 93 (1980).
[16] J. S. Bell, Speakable and unspeakable in quantum mechanics, page 152, Cambridge: University Press, 1987.
[17] A. Aspect, J. Dalibard and Roger, Phys. Rev. Lett. 49, 1804 (1982).
[18] J. Freedman, and J. F. Clauser, Phys. Rev. Lett., 28,938-941 (1972); A. Aspect, P. Grangier, and G. Roger, Phys. Rev .Lett., 47, 460-463 (1981); Z. Y. Ou and L. Mandel, Phys. Rev. Lett., 61, 50-53 (1988); Shih and Alley, Phys. Rev. Lett. 61, 2921 (1988); P. G. Kwiat, K. Mattle, H. Weinfurter, A.Zeilinger, A. V. Sergienko, and Y. H. Shih, Phys. Rev. Lett., 75 4337 (1995); J. G. Rarity and P. R. Tapster, Phys. Rev. Lett., 64 2495-2498 (1990); J. Brendel, E. Mohler, andW. Martienssen, Europhys. Lett., 20, 575-580 (1992); P. R. Tapster, J. G. Rarity, and P. C. M. Owens, Phys. Rev. Lett., 73, 1923-1926 (1994).
[19] G. Weihs, M. Reck, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett., 81, 5039 (1998).
[20] M.A. Rowe et al., Nature 149 791-794 (2001).
[21] N. Gisin and H. Zbinden, Phys. Lett. A 264 103-107 (1999).
[22] H. Zbinden, J. Brendel, W. Tittel, and N. Gisin, Phys. Rev. A, 63, 022111 (2001); H. Zbinden, J. Brendel, N. Gisin and W. Tittel, J. Phys. A : Math. Gen., 34, 7103-7109 (2001).
[23] N. Gisin, V. Scarani, W. Tittel and H. Zbinden, 100 years of Q theory , Proceedings, Annal. Phys. 9, 831-842 (2000); quant-ph/0009055; Andr´e Stefanov, Hugo Zbinden and Nicolas Gisin, Physical Review Letters 88, 120404 (2002); N. Gisin, Sundays in a Quantum Engi-neer's Life, Proceedings of the Conference in Commemoration of John S. Bell, Vienna 10-14 November 2000; V. Scarani, W. Tittel, H. Zbinden and N. Gisin, Phys. Lett. A 276 1-7 (2000).
[24] A. Suarez & V. Scarani, Phys. Lett.A 232, 9 (1997).
[25] D. Bohm, Phys. Rev., 85, 166-193 (1952); D. Bohm and B.J. Hilley, The Undivided Universe, New York: Routledge, 1993.
[26] S. Popescu and D. Rohrlich, Found. Phys. 24, 379 (1994).
[27] D. Rohrlich and S. Popescu, quant-ph/9508009 and quant-ph/9709026.
[28] N. Gisin, quant-ph/0503007.
[29] R.F. Werner, Phys. Rev. A 40, 4277 (1989).
[30] B.M. Terhal, M.M. Wolf and A.C. Doherty, Physics Today, pp 46-52, April 2003.
[31] N.D. Mermin, quant-ph/9609013 and quant-ph/9801057.
[32] M. Esfeld, Studies in History and Philosophy of Modern Physics 35B, 601-617, 2004.
[33] Cheng-Zhi Peng et al., Phys. Rev. Lett. 94, 150501 (2005).
[34] Zhi Zhao et al., Nature 430, 54-58 (2004).
[35] H. Haeffner et al., Appl. Phys. B 81, 151 (2005).
[36] B.B. Blinov, D.L. Moehring, L.M. Duan and C. Monroe, Nature 428, 153-157 (2004).
[37] J- Volz et al., quant-ph/0511183.
[38] B. Julsgaard, J. Sherson, J.I. Cirac and E.S. Polzik, Nature 432, 482-486 (2004).
[39] E. Altewischer et al., Nature 418, 304 (2002); S. Fasel et al., Phys. Rev. Lett. 94 110501, 2005 and quantph/0512022
[40] C.W. Chou et al., quant-ph/0510055.
[41] J.W.Pan, D. Bouwmeester, H.Weinfurter and A. Zeilinger, Phys. Rev. Lett. 80, 3891 (1998).

[42] T. Jennewein, G. Weihs, J.-W. Pan, and A. Zeilinger, Phys.Rev.Lett. 88, 017903 (2002).
[43] H. de Riedmatten et al., Phys. Rev. A 71, 050302 (2005).
[44] S. Tanzilli et al., Nature 437, 116-120 (2005).
[45] B.S. Tsirelson, Hadronic J. Supplement 8, 329 (1993).
[46] V. Bužek and M. Hillery, Phys. Rev. A 54, 1844 (1996).
[47] L. Masanes, A. Acin and N. Gisin, quant-ph/0508016
[48] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu and D. Roberts, Phys. Rev. A 71, 022101 (2005).
[49] W. van Dam, quant-ph/0501159; S. Wolf and J. Wullschleger, quant-ph/0502030; H. Buhrman, M. Christandl, F. Unger, S. Wehner and A. Winter, quantph/0504133; T. Short, N. Gisin and S. Popescu, quantph/0504134; J. Barrett and S. Pironio Phys. Rev. Lett. 95, 140401 (2005); N.S. Jones and L. Masanes, quantph/0506182; J. Barrett, quant-ph/0508211.
[50] D. Collins and N. Gisin, J. Phys. A: Math. Gen. 37, 1775 (2004).
[51] A. Acin, N. Gisin and L. Masanes, quant-ph/0510094.
[52] For an independent but related work see: J. Barrett, L. Hardy and A. Kent, Phys. Rev. Lett. 95, 010503 (2005).
[53] N. Gisin and S. Wolf, Phys. Rev. Lett. 83, 4200 (1999); N. Gisin and S. Wolf, Proceedings of CRYPTO 2000, Lecture Notes in Computer Science 1880, 482, Springer-Verlag, 2000, quant-ph/0005042; A. Acin and N. Gisin, Phys. Rev. Lett. 94, 020501 (2005); quant-ph/0310054.
[54] V. Scarani, private communication.
[55] C. H. Bennett and G. Brassard, Proc. IEEE Int. Conf. Computers, Systems and Signal Processing, New York, 175 (1984).
[56] P. W. Shor and J. Preskill, Phys. Rev. Lett. 85, 441 (2000).
[57] B. Kraus, N. Gisin and R. Renner, Phys. Rev. Lett. 95, 080501 (2005); quant-ph/0410215.
[58] T. Maudlin, Philosophy of Science Association 1, 404-417, 1992.
[59] G. Brassard, R. Cleve and A. Tapp, Phys. Rev. Lett. 83, 1874 (1999).
[60] M. Steiner, Phys. Lett. A 270, 239 (2000).
[61] B. Gisin, N. Gisin, Phys. Lett. A 260, 323 (1999).
[62] B. F. Toner, D. Bacon, Phys. Rev. Lett. 91, 187904 (2003).
[63] V. Scarani and N. Gisin, Physics Letters A 295, 167-174 (2002); Quant-ph/0110074.
[64] V. Scarani and Nicolas Gisin, Brazilian Journal of Physics 35, 328-332 (2005); quant-ph/0410025.
[65] N. J. Cerf, N. Gisin, S. Massar and S. Popescu Phys. Rev. Lett. 94, 220403 (2005).
[66] J. Degorre, S. Laplante and J. Roland, quantph/0507120.
[67] N. Brunner, N. Gisin and V. Scarani, New Journal of Physics 7, 1-14 (2005); quant-ph/0412109.
[68] S. Wolf and J. Wullschleger, quant-ph/0502030.
[69] For another recent results sustaining the conjecture the partially entangled state are more nonlocal than maximally entangled states see: A. Acin, R. Gill and N. Gisin, Phys. Rev. Lett. 95, 210402 (2005); quant-ph/0506225; and for a recent review read A. Methot and V. Scarani, quant-ph/05XXX???.
[70] Experimental Metaphysics, eds R.S. Cohen, M. Horne and J. Stachel, Kluwer Acad. Press, 1997.