Как теорема о запрете клонирования получила свое название

Э. Перес (Израиль)

Перевод М.Х. Шульмана (shulman@dol.ru, www.timeoriigin21.narod.ru)

---

arXiv:quant-ph/0205076v1 14 May 2002

How the No-Cloning Theorem Got its Name

Asher Peres

Department of Physics, Technion—Israel Institute of Technology,
32000 Haifa, Israel
February 1, 2008

Аннотация

Я был рецензентом, который санкционировал публикацию FLASH-статьи Ника Герберта (Nick Herbert), относительно которой было совершено ясно, что она неверна. Я объясняю, почему мое решение было правильно, и даю краткий обзор того прогресса, к которому это привело.

Теорема о запрете клонирования [неизвестного квантового состояния] [1, 2] имеет фундаментальное значение в квантовой теории. Она утверждает, что не существует квантового усилителя, который мог бы удвоить точно два или более неортогональных состояния. Простое доказательство занимает всего лишь несколько строк [3]. Почему эта теорема не была открыта лет за 50 до этого? Какие события привели к ее открытию и публикации?

Здесь приведена история моего личного вклада в эту теорему, которую я публикую впервые более чем за двадцать лет. В начале 1981 года редактор *Foundations of Physics* попросил меня стать рецензентом рукописи Ника Герберта, озаглавленной “FLASH – сверхсветовой коммуникатор, основанный на новом способе измерения”. Мне было ясно, что эта статья не могла быть верной, потому что она противоречила специальной теории относительности. Однако я был уверен, что это было ясно также и автору. Однако, как бы то ни было, ни один из его аргументов не был связан с теорией относительности, так что ошибка могла прятаться где угодно.

Прибор Герберта представлял собой идеализированную лазерную усилительную трубку, которая могла иметь макроскопически различимые выходы, в то время как вход представлял собой единичный произвольно поляризованный фотон. Действительно, слово LASER есть аббревиатура для выражения “”Light Amplification by Stimulated Emission of Radiation – Лазерное усиление за счет вынужденного излучения”. Однако, помимо вынужденного излучения, имеется и *спонтанное излучение*, которое проявляется в виде шума. Утверждение Герберта состояло в том, что шум не должен был мешать идентификации поляризации входного фотона, по крайней мере – статистически. Для этого он использовал понятие “quantum compounds – квантовых структур” [4] и многие понятия лазерной физики, с которыми я не был знаком.

Я рекомендовал редактору *Foundations of Physics* опубликовать эту статью [5]. Я написал ему, что она очевидно неверна, но что я ожидаю значительного интереса к ней, и нахождение ошибки может привести к значительному прогрессу

в нашем понимании физики. Вскоре после этого Wooters и Zurek [1], а также Dieks [2] почти одновременно опубликовали свои версии теоремы о запрете клонирования. Броский лозунг “Единичный квант не может быть клонирован” изобрел Джон Уилер. Как данная статья получила свое название – это отдельная история [6].

Был и другой рецензент – GianCarlo Ghirardi, – который рекомендовал отклонить статью Герберта. Его анонимная рецензия содержала аргумент, который описывался как особый случай теоремы в работах [1, 2]. Вероятно, Ghirardi считал, что его возражения были настолько очевидны, что не нуждались в отдельной публикации в форме статьи (он опубликовал ее в следующем году [7]). Другие возражения выдвинул Glauber [8], а затем и многие другие авторы, которых я не цитирую из-за недостатка места.

Глядя назад, ясно, теорема о запрете клонирования была неявно использована S. Wiesner в основополагающей статье Conjugate Coding (Сопряженное Кодирование), посланной им приблизительно в 1970 г. в *IEEE Transactions on Information Theory* и отклоненной из-за того, что она была написана на специфическом языке, непонятном для специалистов по вычислительной технике (это действительно была статья по физике, хотя и посланная в компьютерный журнал) Работа Wiesner’a в конце концов была опубликована в исходном виде в 1983 году в новостном издании Association for Computer Machinery, Special Interest Group in Algorithms and Computation Theory – ACM SIGACT). Другая ранняя статья – Unforgeable Subway Tokens [10] – также неявно подразумевала, что точное дублирование квантового состояния невозможно. Как это часто бывает в науке, все это было хорошо известно тем, кто был в теме.

Как бы то ни было, теорема о запрете клонирования не содержала оснований для отклонения статьи Герберта. Его рукопись упоминала точное клонирование в качестве теоретического идеала, но было ясно, что в действительности на выходе лазерной усилительной трубки создавалось неидеальное состояние, где многие различные компоненты были запутаны с финальным состоянием лазера.

Теорема о запрете клонирования и ее практические применения в квантовой криптографии породили огромную волну интереса, как я и предсказывал. Каждый месяц одна или несколько статей на эту тему появлялись в разделе quant-ph Электронного Архива или в каких-либо журналах. Типичными обсуждавшимися вопросами были:

- как достичь хотя бы оптимального, если не идеально, клонирования [11], этот вопрос привел к важному понятию квантового незапутывания (quantum disentanglement) [12];
- теорема о нераспространении (no-broadcasting theorem) [13], которая является обобщением запрета клонирования в случае общей матрицы плотности не чистого состояния;
- M→N вероятностное клонирование [14, 15];
- более строгие и более сильные теоремы [16, 17, 18];
- и, в частности, связь оптимального клонирования с невозможностью передачи сигналов (signaling) [19, 20] и границами оценивания состояний, накладываемыми условием бессигнальных коммуникаций [22].

В конце концов был установлен фундаментальный результат: полностью положительные изображения, которые могут быть образованы квантовыми системами, не могут увеличивать разрешимость [23].

Нет сомнений, что термин “сверхсветовой” был одной из причин того, что эта тема стала такой притягательной. Кто не был бы счастлив опрокинуть

релятивистский предел скорости передачи информации? Действительность, сверхсветовые групповые скорости наблюдались при барьерном туннелировании в конденсированном веществе [24, 25]. Однако специальная теория относительности не запрещает, чтобы *групповая скорость* превосходила *c*. Только скорость *фронта* волнового пакета является релевантным критерием для передачи сигнала, и скорость фронта никогда не превосходит *c*.

Очевидно, что термин “сверхсветовой” неприменим ни в сегодняшней практике, ни в теории относительности. Простой вывод таков: пусть даны два наблюдателя с запутанной двухчастичной квантовой системой (или даже со многими такими системами: они эквивалентны единственной системе более высокого порядка); невозможно с помощью локальных квантовых операций (local quantum operations – LQO) передать какую бы то ни было информацию от одного наблюдателя другому без передачи реального материального объекта.

Вот что говорит квантовая механика [26]; но может быть поставлен логический вопрос: а какие модификации квантовой механики разрешали бы передавать информацию с помощью LQO. В дальнейшем я покажу, что нелинейная эволюция матрицы плотности ρ способна обеспечить такой результат. К аналогичному выводу пришел также Svetlichny [27], который, однако, рассматривал только специальный случай начального максимально запутанного чистого состояния и сделал дальше ограничивающие допущения (он тоже использовал термин “сверхсветовой” без всякой апелляции к теории относительности).

Рассмотрим наших хорошо знакомых двух наблюдателей Алису и Боба, которые имеют двухчастичную квантовую систему в хорошо известном состоянии ρ. Они выполняют локальные квантовые операции, которым математически соответствуют положительные операторно-значные измерения (POVM)[1] с элементами $\sum A_j = \mathbb{1}$ и $\sum B_\mu = \mathbb{1}$ соответственно. Вероятность совместного результата $j\mu$ равна

$$P_{j\mu} = \mathrm{Tr}_A \mathrm{Tr}_B \, (\rho \, A_j \otimes B_\mu), \tag{1}$$

где двойной след берется по индексам Алисы и Боба. Если Боб не знает, что Алиса получила результат j, то вероятность получения им результата μ равна

$$\sum_j P_{j\mu} = \mathrm{Tr}(\rho_B B_\mu), \tag{2}$$

где $\rho_B = \mathrm{Tr}_A(\rho)$ есть редуцированная матрица плотности Боба. Этот результат не зависит от выбора POVM Алисой. Так гласит квантовая механика, и все это хорошо всем известно.

Если Боб знает, что Алиса получила результат j, то из (1) следует, что то вероятность получения им результата μ равна $\mathrm{Tr}_B(\rho_j B_\mu)$, где

$$\rho_j = \mathrm{Tr}_A(\rho A_j)/p_j. \tag{3}$$

Здесь знаменатель $p_j = \sum_\nu P_{j\nu}$ - это вероятность того, что Алиса получает результат j, так что ρ_j имеет единичный след, как и должно быть.

Следовательно, все происходит так, как если бы состояние подсистемы Боба действительно было ρ_j . Квантовая механика не утверждает, что это верно, но также не дает возможности увидеть, что эта реалистическая точка зрения является ложной. Это вопрос веры. Bernard d’Espagnat называет редуцированную

[1] Их значениями являются неотрицательные самосопряженные операторы в гильбертовом пространстве, интеграл от них является оператором тождества [см. Википедию].

матрицу Боба “несобственной” смесью [28]. Я также рассматривал подобные ситуации в [4], где я различал чистые состояния, смеси и “компаунды” (compounds – смеси, имеющие единственное разложение на чистые состояния, имеется дополнительная информация. Здесь я даю немного более общую формулировку: редуцированная матрица Боба может быть расщеплена единственным образом на другие матрицы плотности (не обязательно чистые состояния), если Алиса сообщает ему, какой результат она получила.

Вопрос состоит в том, может ли Боб осуществить это без помощи Алисы и, таким образом, выявить, какое именно POVM она выбрала для выполнения. Для этого придется нарушить квантовую механику каким-то способом, таким, например, как клонирование, что как раз и предложил Ник Герберт в своей статье. Здесь существенным является предположение, что клонирование является “несобственной” смесью (“компаундом”), позволяющим клонировать каждый компонент раздельно, как если бы состояние реально было бы одним из таких компонентов с вероятностью ρ_j , а мы просто игнорировали бы остальные.

Предположим, что Боб может выполнить сохраняющее след нелинейное преобразование

$$\rho_j \to \tilde{\rho}_j, \tag{4}$$

над неизвестными “истинными” состояниями своей подсистемы. Тогда его редуцированная матрица плотности эволюционирует как

$$\rho_B = \sum_j p_j \rho_j \to \sum_j p_j \tilde{\rho}_j. \tag{5}$$

Заметим, что результат не определяется одним только ρ_B, но существенным является и разложение ρ_B на определенный набор ρ_j . В частности, этот результат зависит от конкретного выбора POVM, сделанного Алисой, как явно показывает уравнение (3).

Если Алиса выбирает различные POVM, $\sum A_s = \mathbb{1}$, дающие Бобу состояния $\mathrm{Tr}_A(\rho A_s)/p_s$ с вероятностями p_s, то Боб должен получить после этого гипотетического нелинейного преобразования

$$\rho_B = \sum_s p_s \rho_s \to \sum_s p_s \tilde{\rho}_s. \tag{6}$$

Обозначим правые части последних двух выражений ρ' и ρ'' соответственно. В общем случае они не равны между собой и могут быть удовлетворительным образом различимы. Если Бобу поступает достаточное число копий, он должн быть способен узнать, какое POVM выбрала Алиса.

Излишне говорить, что предположение о нелинейной эволюции ρ противоречит квантовой механике. Напротив, если ρ эволюционирует линейно, то $\rho' = \rho''$, и таким способом информация не может быть передана. Заметим, что все обсуждение относится к матрице плотности ρ. Вполне возможно иметь нелинейную эволюцию чистых состояний, которая соответствует линейной эволюции ρ. Например, эволюция

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} \to \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{7}$$

нелинейна в терминах чистых состояний, поскольку

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} \equiv \alpha\begin{pmatrix}1\\ 0\end{pmatrix} + \beta\begin{pmatrix}0\\ 1\end{pmatrix}, \tag{8}$$

и правая сторона должна давать $(\alpha+\beta)\binom{1}{0}$, если бы эволюция была линейной.

С другой стороны, та же эволюция, выраженная в терминах матрицы плотности, имеет вид

$$\begin{pmatrix} a & b\\ b^* & 1-a\end{pmatrix} \to \begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}. \tag{9}$$

Это – линейная операция, порожденная парой матриц Крауса

$$\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} \quad \text{и} \quad \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}. \tag{10}$$

В итоге ошибочная статья Ника Герберта оказалась искрой, которая привела к огромному прогрессу. Появилось и много других ошибочных статей, которые были опубликованы в авторитетных журналах, некоторые из них принадлежали известным ученым. Их негативное влияние может сказываться годами. Но за них я не несу никакой ответственности. Я не был рецензентом этих статей и не могу защищать репутацию их авторов.

Я благодарен Erika Andersson, Gilles Brassard, Dagmar Bruß, Chris Fuchs, GianCarlo Ghirardi, Nobu Imoto, Danny Terno и Bill Wootters за многие разъясняющие комментарии и за помощь, позволившую мне привести некоторые из следующих далее ссылок. Работа была поддержана фондом Gerard Swope Fund и фондом поощрения исследований.

Ссылки

[1] W. K. Wootters and W. H. Zurek, Nature 299 (1982) 802.
[2] D. Dieks, Phys. Letters 92A (1982) 271.
[3] A. Peres, Quantum Theory: Concepts and Methods (Kluwer, Dordrecht, 1995) p. 279.
[4] A. Peres, in Mathematical Foundations of Quantum Theory, ed. by A. R. Marlow (Academic Press, New York, 1978), p. 357.
[5] N. Herbert, Found. Phys. 12 (1982) 1171.
[6] R. Kipling, Just So Stories (MacMillan, London, 1902).
[7] G. C. Ghirardi and T. Weber, Nuovo Cimento 78B (1983) 9.
[8] R. J. Glauber, in New Techniques and Ideas in Quantum Measurement Theory, ed. by D. M. Greenberger, Ann. New York Acad. Sci. 480 (1986) 336.
[9] S. Wiesner, SIGACT News, 15 (1983) 78.
[10] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, in Advances in Cryptology (Proceedings of Crypto-82, Plenum, New York, 1983) p. 267.
[11] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, Phys. Rev. A57 (1998) 2368.
[12] D. R. Terno, Phys. Rev. A59 (1999) 3320.
[13] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. 76 (1996) 2818.
[14] L.-M. Duan and G.-C. Guo, Phys. Rev. Lett. 80 (1998) 4999.
[15] N. J. Cerf and S. Iblisdir, Phys. Rev. A 62 (2000) 040301.

[16] G. Lindblad, Lett. Math. Phys. 47 (1999) 189.
[17] M. Koashi and N. Imoto, quant-ph/0101144.
[18] R. Jozsa, quant-ph/0204153.
[19] N. Gisin, Phys. Lett. 242A (1998) 1.
[20] S. Ghosh, G. Kar, and A. Roy, Phys. Letters 261A (1999) 17.
[21] D. Bruß, G. M. D'Ariano, C. Macchiavello, and M. F. Sacchi, Phys. Rev. A 62 (2000) 062302.
[22] S. M. Barnett and E. Andersson, Phys. Rev. A 65 (2002) 044307.
[23] C. A. Fuchs and J. van de Graaf, IEEE Trans. Info. Theory 45 (1999) 1216.
[24] R. Y. Chiao and A. M. Steinberg, in Progress in Optics XXXVII , ed. by E. Wolf (Elsevier, Amsterdam, 1997); Physica Scripta T76 (1998) 61.
[25] J. C. Garrison, M. W. Mitchell, R. Y. Chiao, and E. L. Bolda, Phys. Letters 245A (1998) 19.
[26] A. Peres, Phys. Rev. A 61 (2000) 022117.
[27] G. Svetlichny, Found. Phys. 28 (1998) 131.
[28] B. d'Espagnat, Veiled Reality (Addison-Wesley, Reading, 1995) p. 105.