УДК 530.145

РАЗЛИЧЕНИЕ, ТОЧНОЕ КЛОНИРОВАНИЕ И РАЗДЕЛЕНИЕ ДВУХ КВАНТОВЫХ СОСТОЯНИЙ С ПРОИЗВОЛЬНЫМИ АПРИОРНЫМИ ВЕРОЯТНОСТЯМИ

А.Э. Растегин, О.Н. Солдатенко

DISTINCTION, EXACT CLONING AND SEPARATION OF TWO QUANTUM STATES WITH ARBITRARY PRIOR PROBABILITIES

A.E. Rastegin, O.N. Soldatenko

Рассмотрены вероятностные квантовые операции свободного от ошибок различения и точного клонирования квантовых состояний в рамках общей схемы разделения состояний. Сформулирована задача оптимального разделения состояний, имеющих произвольные априорные вероятности. При оптимальной процедуре максимизируется вероятность успешного разделения. В качестве общего решения задачи найден максимум полученной нелинейной функции в области допустимых значений переменных. Эта область задается внешними параметрами конкретной поставленной задачи. Исследована зависимость максимальной вероятности успешного разделения от входных параметров.

Probabilistic quantum operations of the error-free distinction and the exact cloning are considered in the general scheme of quantum state separation. We formulate the problem of optimal separation of states with arbitrary prior probabilities. The optimal procedure maximizes the probability of successful separation. The general solution is given in terms of maximization of certain nonlinear function in a domain of acceptable values of variables. This domain is fixed by input parameters of the task of quantum information processing. A dependence of the maximum probability of successful separation on input parameters is studied.

Начиная с 80-х гг. прошлого столетия в мире проводятся активные теоретические и экспериментальные исследования в сфере использования квантового состояния как информационного ресурса. В этом направлении были достигнуты впечатляющие успехи. Сейчас есть все основания полагать, что на квантовом уровне можно конструировать новые, гораздо более мощные по сравнению с классическими средства для передачи и обработки информации [1]. Квантовая криптография является, по существу, воплощенной на практике и апробированной технологией. Некоторые квантовые криптосистемы уже предлагаются для коммерческого использования. Достижения в области создания квантовых компьютеров носят пока теоретический характер, хотя сделаны значимые шаги и по их реализации. Так, 13 февраля 2007 г. появилось сообщение о том, что частной канадской компанией D-Wave Systems был запущен первый в мире квантовый компьютер Orion с разрядностью 16 кубитов. Независимо от того, как скоро использование квантовых информационных технологий станет повсеместным, квантовая теория информации заслуживает внимательного изучения, так как она ставит перед учеными новые, подчас совершенно неожиданные вопросы, как теоретические, так и экспериментальные.

В свете открывающихся перспектив значительно возрос интерес к потенциальным возможностям и ограничениям манипуляций с микросостояниями. К числу задач, имеющих принципиальное значение, относится проблема различения квантовых состояний. В простейшем варианте она формулируется так. Дано множество $\{\,|\Psi_1\rangle, |\Psi_2\rangle\}$ двух (неидентичных) квантовых состояний. Мы знаем, что система находится в одном из этих двух состояний, но не знаем, в каком именно. Производя над системой какие-либо измерения, нам нужно определить это состояние. За исключением ситуации, когда $|\Psi_1\rangle$ и $|\Psi_2\rangle$ ортогональны, не существует процедуры, которая во всех испытаниях дает безошибочный ответ. Широко известны два подхода к проблеме различения.

В подходе Хелстрома [3] вероятность ложной идентификации отлична от нуля (кроме случая ортогональности), но процедура всегда выдает определенный ответ, то есть либо «1», либо «2». В этом подходе минимизируется вероятность ложной идентификации. Альтернативный подход был предложен независимо Ивановичем [4], Диксом [5] и Пересом [6]. Оказывается, если допустить неопределенный ответ «не знаю» (далее «НЗ»), можно исключить ложную идентификацию. А именно, если процедура выдает ответ «1», состояние системы (до измерения) было действительно $|\Psi_1\rangle$, если же ответ «2», то состояние было действительно $|\Psi_2\rangle$. Но в некоторых испытаниях процедура будет выдавать неопределенный ответ «НЗ», и в оптимальном измерении вероятность ответа «НЗ» должна быть минимизирована.

Еще одним важным аспектом является изучение ограничений квантового клонирования. Интерес к этому направлению стимулирован прежде всего проблемами стойкости квантовых криптосистем. Существуют два типа квантовых клонеров: универсальные и состояние-зависимые [7]. В наиболее простой своей постановке задача состояние-зависимого клонирования формулируется так. На вход клонера подается какое-либо одно из пары $\{\,|\Psi_1\rangle, |\Psi_2\rangle\}$ состояний, причем неизвестно, какое именно (но сами эти два состояния нам известны). Клонер должен выдать две копии вводимого состояния. Если процедура детерминированная, т. е. выполняется унитарное преобразование, то копии не могут быть точными. Тогда необходимо минимизировать ошибку в соответствии с заданным критерием для оценки качества клонов. Следует отметить, что клонеры, оптимальные с точки зрения одного

критерия, не являются таковыми с точки зрения других [7, 8]. Дуан и Гуо предложили другую схему клонирования, в которой вслед за унитарным преобразованием выполняется специально подобранное измерение над вспомогательной системой [9]. Это позволяет генерировать точные клоны, но только вероятностным образом. При таком подходе должна быть максимизирована вероятность успешного клонирования.

Авторами статьи [10] была предложена вероятностная процедура общего типа – разделение квантовых состояний. Ее специальными случаями являются свободное от ошибок различение квантовых состояний и точное клонирование. Однако в работе [10] был рассмотрен только случай равновероятных состояний. Сформулируем задачу вероятностного разделения двух неортогональных квантовых состояний с произвольными априорными вероятностями. Для осуществления этого процесса интересующая нас система приводится во взаимодействие с вспомогательной системой – «пробой *P*»; затем над вспомогательной системой производится измерение.

Пусть $|\Psi_+\rangle$ и $|\Psi_-\rangle$ – два состояния со скалярным произведением $|\langle\Psi_+|\Psi_-\rangle| = a$ и с априорными вероятностями p_+ и p_- соответственно ($p_+ + p_- = 1$). Мы хотим путем унитарного преобразования U и последующего измерения M преобразовать $|\Psi_+\rangle$ и $|\Psi_-\rangle$ в квантовые состояния $|\Phi_+\rangle$ и $|\Phi_-\rangle$ со скалярным произведением $|\langle\Phi_+|\Phi_-\rangle| = b$, где $a > b$:

$$|\Psi_\pm\rangle \xrightarrow{U+M} |\Phi_\pm\rangle \qquad (1)$$

Действуя унитарным преобразованием U на состояния $|\Psi_\pm\rangle\ |m_0\rangle$, где $|m_0\rangle$ – начальное состояние пробы *P*, получим:

$$U\left(|\Psi_\pm\rangle|m_0\rangle\right) = \mu_\pm|\Phi_\pm\rangle|m_0\rangle + \nu_\pm|\Gamma_\pm\rangle|m_1\rangle, \qquad (2)$$

где $|\mu_\pm|^2 + |\nu_\pm|^2 = 1$. Производя над пробой *P* измерение, в случае исхода m_0 мы получим желаемый результат, т. е. состояния $|\Phi_\pm\rangle$. В случае другого исхода система перейдет в состояния $|\Gamma_\pm\rangle$ и процесс разделения потерпит неудачу. Вероятность получения желаемого результата равна

$$P_{\text{sep}} = p_+|\mu_+|^2 + p_-|\mu_-|^2. \qquad (3)$$

Для равновероятного случая ($p_+ = p_- = 1/2$) вероятность разделения получена Чефлесом и Барнеттом [10] в следующем виде:

$$P = \frac{1-|\langle\Psi_+|\Psi_-\rangle|}{1-|\langle\Phi_+|\Phi_-\rangle|}. \qquad (4)$$

Рассмотрим более общую задачу – разделение неравновероятных квантовых состояний ($p_+ \neq p_-$). Вычисление оптимальной вероятности успешного разделения сводится к нахождению максимума нелинейной функции двух переменных

$$P_{\text{sep}} = \frac{1}{2}\left[1 + x^2 - y^2 + \Delta p\sqrt{1-(x-y)^2}\sqrt{1-(x+y)^2}\right] \qquad (5)$$

в определенной области изменения переменных, которая задается входными параметрами задачи ($\Delta p = p_+ - p_-$). Эту задачу можно преобразовать к исследованию на максимум функции одной переменной

$$P_{sep} = \frac{1}{2}\left[1 + x^2 - (a-bx)^2 + \Delta p\sqrt{1-(x-(a-bx))^2} \times \right.$$
$$\left. \times\sqrt{1-(x+(a-bx))^2}\right]. \qquad (6)$$

Поскольку полученное выражение зависит сразу от трех параметров *a*, *b* и Δp, которые задаются конкретными начальными условиями, будем графически исследовать зависимость $P(a, b, \Delta p)$ (рис. 1, 2).

На графиках четко наблюдаются следующие закономерности:

1) с увеличением степени разделения двух квантовых состояний (т. е. с уменьшением $b = \langle\Phi_+|\Phi_-\rangle$ при фиксированном $a = \langle\Psi_+|\Psi_-\rangle$) вероятность успешного разделения P_{sep} уменьшается;

2) с увеличением разности между априорными вероятностями двух состояний Δp P_{sep} увеличивается;

3) при фиксированных *a* и *b*, P_{sep} принимает минимальное значение при $\Delta p = 0$ (состояния равновероятны) и максимальное значение при $\Delta p = 1$ (априорная

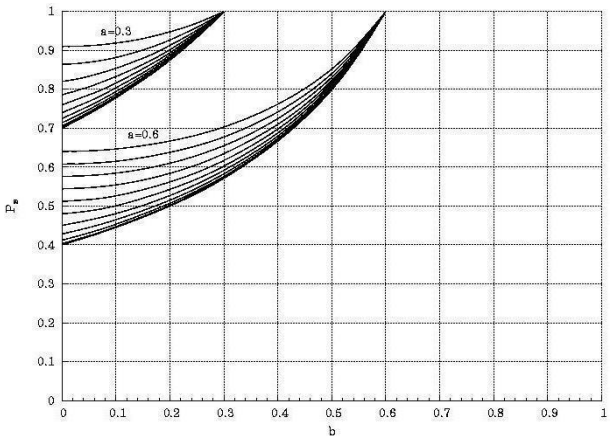

Рис. 1.

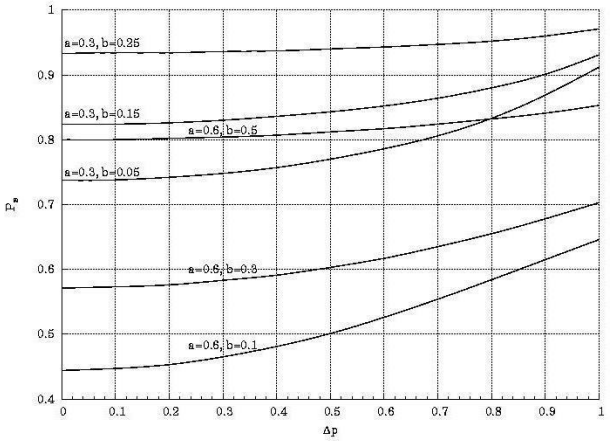

Рис. 2.

вероятность одного из состояний равна нулю).

Чтобы исследовать качественную зависимость вероятности успешного разделения от исходных параметров задачи, используем квазиоптимальный процесс разделения, удовлетворяющий специфическому свойству композиции, который существенно упрощает исследование многошаговых квантовых операций:

$$P_{\text{sep}}\left(a \to b\right) = P_{\text{sep}}\left(a \to b + \Delta b\right) P_{\text{sep}}\left(b + \Delta b \to b\right) \qquad (7)$$

Максимальное значение вероятности успешного разделения при таком процессе разделения равна:

$$P_{\text{sep}}\left(a \to b\right) = \sqrt{\left|\frac{1-a^2}{1-b^2}\right|}\sqrt{\left|\frac{a-\sqrt{1-\Delta p^2\left(1-a^2\right)}}{a+\sqrt{1-\Delta p^2\left(1-a^2\right)}}\right|}\times$$

$$\times\sqrt{\left|\frac{b+\sqrt{1-\Delta p^2\left(1-b^2\right)}}{b-\sqrt{1-\Delta p^2\left(1-b^2\right)}}\right|}\times \qquad (8)$$

$$\times\left|\frac{a\Delta p+\sqrt{1-\Delta p^2\left(1-a^2\right)}}{b\Delta p+\sqrt{1-\Delta p^2\left(1-b^2\right)}}\right|^{\Delta p}.$$

Полученный результат хорошо согласуется с уже исследованными частными случаями (например, с разделением равновероятных состояний) и позволяет качественно оценить зависимость вероятности успешного разделения двух квантовых состояний от входных параметров задачи, т. е. от угла между начальными и конечными состояниями и от априорных вероятностей квантовых состояний.

СПИСОК ЛИТЕРАТУРЫ

1. Валиев К.А., Кокин А.А. Квантовые компьютеры: надежды и реальность. М.: НИЦ «Регулярная и хаотическая динамика», 2002. 320 с.

2. D-Wave Systems/http://www.dwavesys.com

3. Хелстром К. Квантовая теория проверки гипотез и оценивания. М.: Мир, 1979. 344 с.

4. Ivanovic I.D. How to differentiate between non-orthogonal states // Phys. Lett. A. 1987. V. 123. P. 257–259.

5. Dieks D. Overlap and distinguishability of quantum states // Phys. Lett. A. 1988. V. 126. P. 303–306.

6. Peres A. How to differentiate between non-orthogonal states // Phys. Lett. A. 1988. V. 128. P. 19.

7. Brив D., DiVincenzo D.P., Ekert A., et al. Optimal universal and state-dependent quantum cloning // Phys. Rev. A. 1998. V. 57. P. 2358–2378.

8. Rastegin A.E. relative error of state-dependent cloning // Phys. Rev. A. 2002. V. 66. P. 042304.

9. Duan. L.M., Guo G.C. Probabilistic cloning and identification of linearly independent quantum states // Phys. Rev. Lett. 1998. V. 80. P. 4999–5002.

10. Chefles A., Barnett S.M. Quantum state separation, unambiguous discrimination and exact cloning // J. Phys. A: Math. Gen. 1998. V. 31. P. 10097–10103.

Иркутский государственный университет, Иркутск.