Письма в ЖЭТФ, том 99, вып. 7, с. 488 – 492

О сжатии информации классического источника при помощи побочной квантовой и классической информации

С. Н. Молотков[+*×1)], *Т. А. Потапова*[○]

[+]*Институт физики твердого тела РАН, 142432 Черноголовка, Россия*

[*]*Академия криптографии РФ, 121552 Москва, Россия*

[×]*Факультет вычислительной математики и кибернетики, МГУ им. Ломоносова, 119991 Москва, Россия*

[○]*Факультет информационных технологий и вычислительной техники, Национальный исследовательский университет "Высшая школа экономики", 101000 Москва, Россия*

Поступила в редакцию 11 марта 2014 г.

Рассмотрена задача сжатия классической информации, когда приемник имеет доступ только к побочным квантовым состояниям, ассоциированным с классическими состояниями источника, которые непосредственно не доступны. Для того чтобы приемник мог восстановить всю информацию источника требуется некоторое дополнительное количество побочной классической информации. Простыми средствами получена граница на минимально необходимое количество побочной классической информации.

DOI: 10.7868/S0370274X14070133

Введение. Источник информации может генерировать либо классические, либо квантовые состояния. Одним из фундаментальных результатов классической теории информации является теорема о сжатии информации, называемая также теоремой кодирования Шеннона для классического источника [1]. В квантовой области ситуация оказывается более разнообразной [2]. Классическую информацию можно передавать при помощи квантовых состояний. Например, в квантовой криптографии ключ (случайная классическая битовая строка), передается при помощи квантовых состояний. Верхняя граница классической информации, которую можно извлечь из ансамбля квантовых состояний, дается фундаментальной границей Холево (теорема кодирования Холево [3]). Сначала данная граница была получена для чистых состояний, затем – для смешанных [4, 5]. Кодирование (сжатие квантовой информации) по Шумахеру [6] отвечает на вопрос о минимальной размерности гильбертова пространства состояний квантового канала связи, в которое можно вложить квантовые состояния источника как таковые без потери квантовой информации (искажения исходных квантовых состояний). Квантовая механика позволяет осуществлять перенос неизвестного квантового состояния с одной квантовой системы на другую при помощи заранее распределенного запутанного состояния (телепортация квантового состояния – квантовой информации). При этом совместно используются квантовый канал и вспомогательный классический канал связи. Телепортация была предсказана в [7] и экспериментально продемонстрирована в полном белловском базисе в [8]. Данное явление принципиально не имеет классического аналога. Квантовая механика позволяет передавать классическую информацию при помощи запутанного состояния и дополнительного классического канала (сверхплотное кодирование [9]).

Ниже нас будет интересовать сжатие классической информации в ситуации, когда сами состояния классического источника не доступны непосредственно. Доступны лишь побочные квантовые состояния, однозначно ассоциированные с классическими состояниями источника. Такая ситуация возникает, например, в квантовой криптографии. Имея доступ только к побочным квантовым состояниям, которые в общем случае являются неортогональными, приемник принципиально не может идентифицировать все последовательности состояний, генерируемые источником. Вопрос, на который требуется ответить, состоит в том, *какое минимальное количество классической побочной информации дополнительно к квантовой необходимо для достоверного различения (в асимптотическом пределе) всех исходных классических последовательностей.*

Данная проблема является квантовым аналогом классической задачи, рассмотренной Слепяном и Вольфом [10]. Она формулируется следующим образом. Имеются два коррелированных классических

1) e-mail: sergei.molotkov@gmail.com

источника. Каждый источник посылает состояния одному приемнику. Имея доступ только к одному из двух источников, можно указать верхнюю границу информации, которую может извлечь приемник. Вопрос состоит в получении верхней границы информации, которой может достичь приемник, имея доступ сразу к двум источникам. В такой ситуации один из них может рассматриваться как источник побочной информации по отношению к другому источнику. В квантовом случае задача о сжатии классической информации с побочной квантовой рассматривалась в работе Винтера и Деветяка [11] с использованием метода проекций на типичное пространство. В работе Ренеса и Реннера [12] данная задача решалась с помощью языка min и max энтропий фон Неймана.

Ниже простыми средствами будет показано, что решение указанной задачи может быть получено как обобщение замечательной теоремы кодирования Холево для *квантового источника* [2–4]. Данный путь является наиболее прямым и позволяет получить более точные оценки вероятности ошибки.

Классический источник. Пусть имеется классический источник, который генерирует состояния в соответствии с алфавитом $X = \{x_1, x_2, \ldots, x_m\}$ и заданным над ним распределением вероятностей $p_X(x)$. Источник используется n раз, где n достаточно велико. Пусть последовательности длины n – $X^n = (x_{i_1}, x_{i_2}, \ldots, x_{i_n})$ посылаются через идеальный канал без памяти. Полное число последовательностей длины n равно $2^{n\log m}$ (здесь и далее логарифмы берутся по основанию 2). Все последовательности можно разбить на типичные и нетипичные. Множество типичных последовательностей $T_{\delta,\varepsilon}$ имеет размерность

$$2^{n[H(X)-\delta]} < |T_{\delta,\varepsilon}| < 2^{n[H(X)+\delta]}, \tag{1}$$

начиная с некоторой длины $n > n_0(\delta,\varepsilon)$ (где δ, ε – любые сколь угодно малые величины). Вероятности появления каждой из типичных последовательностей $p(X^n)$ примерно одинаковы (асимптотическая равнораспределенность):

$$2^{-n[H(X)+\delta]} < p(X^n) < 2^{-n[H(X)-\delta]}. \tag{2}$$

При больших n существует $(1-\varepsilon)2^{n[H(X)-\delta]}$ типичных слов. Вероятность остальных нетипичных последовательностей составляет не более ε. Количество информации в битах, которое генерирует источник, в пересчете на посылку в асимптотическом пределе длинных последовательностей ($n \to \infty$) составляет $nH(X)$ (где $H(X) = -\sum_{i=1}^{m} p_X(x_i)\log p_X(x_i)$).

Неформально теорема кодирования источника (сжатия классической информации) означает, что для того, чтобы перенумеровать все типичные последовательности, достаточно целых чисел из диапазона $1 \le J \le 2^{nH(X)}$. Для представления этих чисел требуется не более $[nH(X)]+1$ двоичных разрядов (где [...] – целая часть числа), каждый из которых несет один бит информации. Вместо того чтобы передавать n позиций, которые генерирует источник, приемник и передатчик могут заранее договориться об общей кодовой таблице – соответствии каждой типичной последовательности $X_J = (x_{i_1}, x_{i_2}, \ldots, x_{i_n})$ и $[nH(X)]+1$-битного номера J. Нумерация типичных последовательностей в силу их равнораспределенности может быть произвольной. Если источник генерирует одну из типичных последовательностей, то посылается не сама последовательность, а ее номер J. По кодовой таблице приемник однозначно восстановит сгенерированную последовательность. Если источник генерирует нетипичную последовательность, то она отбрасывается и ничего не посылается. В асимптотическом пределе потери информации не происходит. *Для сжатия информации принципиально важно наличие у передатчика и приемника заранее оговоренной кодовой таблицы.*

Квантовый источник. Классическая информация может передаваться при помощи квантовых состояний. Классическому источнику с алфавитом $X = (x_1, x_2, \ldots, x_m)$ и распределением вероятности $p_X(x)$ над ним сопоставляется квантовый алфавит $Q = (\rho_{x_1}, \rho_{x_2}, \ldots, \rho_{x_m})$ $(x_i \to \rho_{x_i})$ с тем же распределением вероятности. Количество классической информации, которое может быть получено из такого источника, ограничено фундаментальной величиной Холево [2–4]. При n-кратном использовании канала из всех $2^{nH(X)}$ классических типичных последовательностей, которым сопоставляются квантовые состояния, могут быть достоверно различимы лишь $2^{n\chi(\overline{\rho})}$ квантовых последовательностей, где

$$\begin{gathered}\chi(\overline{\rho}) = H(\overline{\overline{\rho}}) - \sum_{x}^{m} p_X(x) H(\rho_x),\\ \overline{\rho} = \sum_{x}^{m} p_X(x)\rho_x, \quad H(\rho) = -\mathrm{Tr}\{\rho\log\rho\}\end{gathered} \tag{3}$$

(здесь и ниже энтропию Шеннона и фон Неймана, в зависимости от контекста, мы обозначаем одной буквой H, что не должно приводить к путанице). Точнее говоря, из всех $2^{nH(X)}$ квантовых последовательностей длины n $(\rho_{x_{i_1}}, \rho_{x_{i_2}}, \ldots, \rho_{x_{i_n}})$, достоверно различимо (со сколь угодно малой вероятностью ошибки в асимптотическом пределе $n \to \infty$) не более $2^{n\chi(\overline{\rho})}$ последовательностей. Существуют код (кодовая таблица последовательностей и их номеров) размером не более $2^{n\chi(\overline{\rho})}$ и набор квантовомеханических измерений, которые при наличии заранее оговоренной кодовой таблицы у передатчика и приемника позволяют безошибочно различить все кодовые последовательности. Иначе говоря, фундаментальная граница Холево достижима [2, 4].

Таким образом, *приемник и передатчик должны заранее договориться о кодовой таблице. В соответствии с данной кодовой таблицей источник генерирует сначала классические, а затем квантовые состояния. Приемник строит измерения (декодер), позволяющие различать квантовые последовательности только внутри кодовой таблицы (кодовые слова).*

Классический источник с побочными квантовыми и классическими состояниями. *В ряде важных задач квантовой информатики возникает необходимость различения последовательностей квантовых состояний, когда приемник не имеет заранее оговоренной кодовой таблицы.* Например, это имеет место в квантовой криптографии, когда передатчик посылает в канал связи последовательности квантовых состояний согласованные с классическими состояниями:

$$(x_{i_1}, x_{i_2}, \ldots, x_{i_n}) \to (|\phi_{x_{i_1}}\rangle, |\phi_{x_{i_2}}\rangle \ldots |\phi_{x_{i_n}}\rangle), \qquad (4)$$

а подслушиватель не имеет у себя кодовой таблицы. Классические состояния остаются в распоряжении приемника, а квантовые поступают в канал связи. Передатчик генерирует $\approx 2^{nH(x)}$ классических слов. Однако если квантовые состояния неортогональны (что имеет место в квантовой криптографии), то число безошибочно различимых последовательностей *даже при наличии кодовой таблицы* оказывается не более $\approx 2^{n\chi(\overline{\rho})}$ ($2^{n\chi(\overline{\rho})} < 2^{nH(x)}$). В отсутствие кодовой таблицы приемник "видит" ансамбль состояний, который описывается матрицей плотности

$$\rho_{XQ} = \sum_{x_{i_1},\ldots x_{i_n}} p_X(x_{i_1}) \ldots p_X(x_{i_n}) |x_{i_1}\rangle\langle x_{i_1}| \otimes \ldots \otimes$$
$$\otimes |x_{i_n}\rangle\langle x_{i_n}| \otimes \rho_{x_{i_1}} \otimes \ldots \otimes \rho_{x_{i_n}} =$$
$$= \left[\sum_x p_X(x) |x\rangle\langle x| \otimes \rho_x \right]^{\otimes n}, \qquad (5)$$

причем приемнику доступны только побочные квантовые состояния (подсистема Q) и недоступны классические состояния X.

Вопрос, на который требуется ответить, состоит в том, какое минимальное количество дополнительной (побочной) классической информации должно быть доступно приемнику для безошибочного различения всех $2^{n \log m}$ последовательностей. Источник генерирует классическую строку и ставит ей в соответствие последовательность квантовых состояний (квантовый источник). Кроме того, передатчик дополнительно сообщает приемнику вспомогательную побочную классическую информацию от второго классического источника, коррелированного определенным образом с квантовым источником. (В задаче Слепяна–Вольфа имеются два классических коррелированных источника. В данной задаче коррелированных источников также два: квантовый и классический.) Вспомогательный источник имеет свой алфавит Z и распределение вероятностей над ним $p_Z(z)$. *Как будет видно из дальнейшего, размер алфавита и тип распределения не важны. Важна лишь энтропия Шеннона данного источника.* Поэтому достаточно взять простейший бинарный алфавит $Z = \{0, 1\}$, $p_Z(0) = q$ и $p_Z(1) = 1 - q$. *Побочная классическая информация генерируется на каждую квантовую последовательность*, например при помощи несимметричной монеты, которая подбрасывается n раз. Энтропия такого источника есть $nH(q) = nh(q)$ (где $h(q) = -q \log q - (1 - q) \log(1 - q)$ – бинарная энтропийная функция).

Побочная классическая информация может быть представлена *ортогональными квантовыми состояниями* $|z\rangle$ ($z = 0, 1$):

$$(x_{i_1}, x_{i_2}, \ldots, x_{i_n}) \to \qquad (6)$$
$$\to (|\phi_{x_{i_1}}\rangle \otimes |z_{i_1}\rangle, |\phi_{x_{i_2}}\rangle \otimes |z_{i_2}\rangle \ldots |\phi_{x_{i_n}}\rangle \otimes |z_{i_n}\rangle) =$$
$$= (|\phi_{x_{i_1}, z_{i_1}}\rangle \otimes |\phi_{x_{i_2}, z_{i_2}}\rangle \ldots |\phi_{x_{i_n}, z_{i_n}}\rangle) = |\Phi_{J_{(x,z)}}\rangle.$$

На каждый акт генерации квантового состояния $|\phi_{x_{i_k}}\rangle$ генерируется побочное классическое состояние $|z_{i_k}\rangle$. Для дальнейшего удобно обозначить набор индексов как $J_{(x,z)} = ((x_{i_1}, z_{i_1}); (x_{i_2}, z_{i_2}); \ldots; (x_{i_n}, z_{i_n}))$. Всего существует $2^{n \log m}$ наборов индексов по числу генерируемых последовательностей $(x_{i_1}, x_{i_2}, \ldots, x_{i_n})$. К каждой позиции квантовых состояний "подцепляется" вспомогательная классическая информация, которая в пересчете на одну позицию составляет $h(Q)$ бит. Задача состоит в определении минимального количества $h(Q)$ побочной классической информации, при котором приемник, имея доступ к квантовым состояниям и побочной классической информации $(z_{i_1}; z_{i_2}; \ldots; z_{i_n})$, сможет с использованием квантовомеханических измерений безошибочно различить все генерируемые источником последовательности $(|\phi_{x_{i_1}}\rangle, |\phi_{x_{i_2}}\rangle \ldots |\phi_{x_{i_n}}\rangle)$ и, соответственно, $(x_{i_1}, x_{i_2}, \ldots, x_{i_n})$.

Ниже мы покажем, что ответ на поставленный вопрос фактически является следствием теоремы Холево [2–4]. При этом мы ограничимся случаем чистых состояний и прямой теоремой. Случай смешанных состояний может быть рассмотрен аналогично и является его следствием [4]. Обратная теорема кодирования (сильное обращение) может быть доказана методом Огавы и Нагаоке [13].

Важно отметить, что передатчик и приемник используют побочные квантовые состояния и побочную классическую информацию для общей кодовой квантово-классической таблицы. Зная эту таблицу (соответствие индекса $J(x,z)$ некоторой квантово-классической последовательности), приемник конструирует измерения. Измерения состояний (6) даются разложением единицы:

$$I = \sum_{J_{(x,z)}}^{N} M_{J_{(x,z)}}, \tag{7}$$

где $M_{J_{(x,z)}}$ – положительные операторнозначные меры, N – число наборов индексов $J_{(x,z)}$. Условная вероятность того, что послана последовательность состояний $|\Phi_{J_{(x,z)}}\rangle$, а получен исход измерений $J'_{(x,z)}$, есть $\Pr(J'_{(x,z)}|J_{(x,z)}) = \langle \Phi_{J_{(x,z)}}|M_{J'_{(x,z)}}|\Phi_{J_{(x,z)}}\rangle$.

Средняя вероятность ошибки по всем последовательностям равна

$$P_{\mathrm{err}}(N) = \frac{1}{N}\sum_{J_{(x,z)}}^{N}\left(1-\langle \Phi_{J_{(x,z)}}|M_{J_{(x,z)}}|\Phi_{J_{(x,z)}}\rangle\right), \tag{8}$$

где N – число последовательностей. Субоптимальные измерения (*pretty good measurements*) выбираются в виде

$$\begin{gathered} M_{J_{(x,z)}} = |\widehat{\Phi}_{J_{(x,z)}}\rangle\langle\widehat{\Phi}_{J_{(x,z)}}|, \\ |\widehat{\Phi}_{J_{(x,z)}}\rangle = \Gamma^{-1/2}|\Phi_{J_{(x,z)}}\rangle, \\ \Gamma = \sum_{J_{(x,z)}}^{N}|\Phi_{J_{(x,z)}}\rangle\langle\Phi_{J_{(x,z)}}|, \end{gathered} \tag{9}$$

где Γ – оператор Грама. С учетом (9) формула (8) может быть записана как

$$\begin{gathered} P_{\mathrm{err}}(N) = \frac{1}{N}\sum_{J_{(x,z)}}^{N}\left(1-|\langle\widehat{\Phi}_{J_{(x,z)}}|\Phi_{J_{(x,z)}}\rangle|^2\right) \le \\ \le \frac{2}{N}\sum_{J_{(x,z)}}^{N}\left(1-|\langle\widehat{\Phi}_{J_{(x,z)}}|\Gamma^{1/2}|\widehat{\Phi}_{J_{(x,z)}}\rangle|^2\right) = \\ = \frac{2}{N}\mathrm{Tr}\left(\Gamma-\Gamma^{1'2}\right). \end{gathered} \tag{10}$$

В (10) было использовано равенство $\mathrm{Tr}\left((\ldots)|\widehat{\Phi}_{J_{(x,z)}}\rangle\langle\widehat{\Phi}_{J_{(x,z)}}|\right) = \langle\widehat{\Phi}_{J_{(x,z)}}|\left((\ldots)\right)|\widehat{\Phi}_{J_{(x,z)}}\rangle$. Далее, $2(\Gamma-\Gamma^{1/2}) \le \Gamma^2-\Gamma$ (см., например, [4, 14]). Вычислим среднюю вероятность ошибки по всевозможным реализациям классического источника в соответствии с распределениями вероятностей $p_X(x)$ и $p_Z(z)$ над побочным квантовым и классическим алфавитами:

$$\begin{gathered} \overline{P_{\mathrm{err}}(N)} \le \frac{1}{N}\overline{\mathrm{Tr}\left(\Gamma-\Gamma^{1/2}\right)} = \\ = \frac{1}{N}\overline{\mathrm{Tr}\left\{\left(\sum_{J_{(x,z)}}^{N}|\Phi_{J_{(x,z)}}\rangle\langle\Phi_{J_{(x,z)}}|\right)\times\right.} \\ \overline{\left.\times\left(\sum_{J'_{(x,z)}}^{N}|\Phi_{J'_{(x,z)}}\rangle\langle\Phi_{J'_{(x,z)}}|\right) - \sum_{J_{(x,z)}}^{N}|\Phi_{J_{(x,z)}}\rangle\langle\Phi_{J_{(x,z)}}|\right\}}, \end{gathered} \tag{11}$$

где усреднение по распределениям $p_X(x)$ и $p_Z(z)$ означает

$$\begin{gathered} \overline{(\ldots)} = \sum_{x_{i_1},\ldots,x_{i_n}}\ \sum_{z_{i_1},\ldots,z_{i_n}}[p_X(x_{i_1})p_X(x_{i_2})\ldots p_X(x_{i_n})]\times \\ \times[p_Z(z_{i_1})p_Z(z_{i_2})\ldots p_Z(z_{i_n})](\ldots), \end{gathered} \tag{12}$$

$$\begin{gathered} \overline{P_{\mathrm{err}}(N)} \le \frac{1}{N}\mathrm{Tr}\Bigg\{\sum_{J_{(x,z)}\neq J'_{(x,z)}}^{N}\times \\ \times\overline{\left(|\Phi_{J_{(x,z)}}\rangle\langle\Phi_{J_{(x,z)}}|\right)}\ \overline{\left(|\Phi_{J'_{(x,z)}}\rangle\langle\Phi_{J'_{(x,z)}}|\right)}\Bigg\} = \\ = (N-1)\mathrm{Tr}\Bigg\{\Bigg(\sum_{x_{i_1},x_{i_2},\ldots,x_{i_n}}p_X(x_{i_1})p_X(x_{i_2})\ldots \\ \ldots p_X(x_{i_n})|\phi_{x_{i_1}}\rangle\langle\phi_{x_{i_1}}|\otimes|\phi_{x_{i_2}}\rangle\langle\phi_{x_{i_2}}|\otimes\ldots\otimes|\phi_{x_{i_n}}\rangle\langle\phi_{x_{i_n}}|\Bigg)\times \\ \times\Bigg(\sum_{z_{i_1},z_{i_2}\ldots z_{i_n}}p_Z(z_{i_1})p_Z(z_{i_2})\ldots \\ \ldots p_Z(z_{i_n})|z_{i_1}\rangle\langle z_{i_1}|\otimes|z_{i_2}\rangle\langle z_{i_2}|\otimes\ldots\otimes|z_{i_n}\rangle\langle z_{i_n}|\Bigg)\Bigg\} = \\ = 2(N-1)\mathrm{Tr}\left(\overline{\rho_x}^2\right)^{\otimes n}\cdot\mathrm{Tr}\left(\overline{\rho_z}^2\right)^{\otimes n}, \end{gathered}$$

где

$$\overline{\rho}_x = \sum_x p_X(x)|\phi_x\rangle\langle\phi_x|, \quad \overline{\rho}_z = \sum_z p_Z(z)|z\rangle\langle z|. \tag{13}$$

Воспользовавшись неравенством $\min(a\cdot b) \le a^s\cdot b^{1-s}$, где $0\le s\le 1$ (детали см. в [4], а также [14]), получаем

$$\begin{gathered} \overline{P_{\mathrm{err}}(N=2^{nR})} \le 2(N-1)^s\mathrm{Tr}\left(\overline{\rho_x}^{1+s}\right)^{\otimes n}\cdot\mathrm{Tr}\left(\overline{\rho_z}^{1+s}\right)^{\otimes n} \le \\ \le 2\max_{0\le s\le 1}2^{-n\left(\max_s\{-\log[\mathrm{Tr}(\overline{\rho_x}^{1+s})]\}-\log\mathrm{Tr}(\overline{\rho_z}^{1+s})-R\right)}, \end{gathered} \tag{14}$$

где R – количество информации в битах, генерируемое классическим источником, в пересчете на одну посылку. Если учитываются только типичные последовательности, то $R = H(X)$, если все, то $R = \log m$.

Поскольку $-\log[\mathrm{Tr}\,(\overline{\rho_x}^{1+s})]$ и $-\log[\mathrm{Tr}\,(\overline{\rho_z}^{1+s})]$ являются выпуклыми вверх функциями s и

$$\begin{aligned} &\frac{1}{ds}\left\{-\log\left[\mathrm{Tr}\left(\overline{\rho_x}^{1+s}\right)\right]\right\}_{s=0} = H(\overline{\rho}_x), \\ &\frac{1}{ds}\left\{-\log\left[\mathrm{Tr}\left(\overline{\rho_z}^{1+s}\right)\right]\right\}_{s=0} = H(\overline{\rho}_z), \end{aligned} \tag{15}$$

при $H(\overline{\rho}_x) + H(\overline{\rho}_z) > R$, вероятность ошибки декодирования с ростом n стремиться к нулю.

Другими словами, если заданы энтропия исходного классического источника R и квантовые состояния, то минимальное количество побочной классической информации $H(\overline{\rho}_z)$, необходимое для того, чтобы приемник смог различить все классические последовательности, имея доступ только к побочной квантовой и побочной классической информации, составляет

$$H(\overline{\rho}_z) > R - H(\overline{\rho}_x). \tag{16}$$

Как видно из приведенных выше рассуждений, конкретный тип источника дополнительной побочной классической информации несущественен. Важна только энтропия источника. Один из авторов (С.Н.М.) выражает благодарность Д.А. Кронбергу за полезные дискуссии.

1. C. E. Shannon, Bell Syst. Tech. Jour. **27**, 397 (1948); **27**, 623 (1948).
2. А. С. Холево, *Квантовые системы, каналы, информация*, МЦМО, М. (2010).
3. A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973); Probl. Inf. Transm. **15**, 247 (1979).
4. A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998); А. С. Холево, УМН **53**, 193 (1998).
5. B. Schumacher and M. D.Westmoreland, Phys. Rev. A **56**, 131 (1997).
6. B. Schumacher, Phys. Rev. A **51**, 2738 (1995).
7. C. H. Bennett, G. Brassard, C .Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
8. Y.-Ho. Kim, S. P. Kulik, and Y. Shih, Phys. Rev. Lett. **86**, 1370 (2001).
9. C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
10. D. Slepian and J. K. Wolf, IEEE Trans. Inf. Theory **IT-19**, 471 (1973).
11. I. Devetak and A. Winter, quant-ph/0209029.
12. J. M. Renes and R. Renner, quant-ph/1008.0452.
13. T. Ogawa and H. Nagaoka, quant-ph/9808063.
14. X. Zhan, *Matrix Inequalities, Lecture Notes in Mathematics*, ed. by J.-M. Morel, F. Takens, and B. Teissier, Springer, Berlin (2002), v. 1790.