07

Безошибочное различение когерентных состояний двухмодового оптического поля

© М.М. Эскандери, Д.Б. Хорошко¶, С.Я. Килин

Институт физики им. Б.И. Степанова НАН Беларуси,
220072 Минск, Беларусь

¶ e-mail: horoshko@dragon.bas-net.by

Поступила в редакцию 11.03.2020 г.
В окончательной редакции 11.03.2020 г.
Принята к публикации 28.03.2020 г.

Исследована процедура квантового измерения — безошибочного различения — четырех двухмодовых когерентных состояний оптического поля, представляющих интерес для передачи информации по оптическому каналу связи. Показано, что комплексное сопряжение амплитуды одной из мод приводит к лучшей различимости состояний. Предложена интерферометрическая схема безошибочного различения таких состояний и найдена вероятность успешного различения. Обсуждены применения рассмотренного набора состояний в квантовой криптографии, квантовой телепортации и оптической связи с высоким уровнем потерь.

Ключевые слова: квантовые измерения, безошибочное различение состояний, квантовая криптография, квантовый канал связи.

DOI: 10.21883/OS.2020.08.49716.83-20

Введение

Оптические поля широко используются в современных системах передачи информации, в которых сигнал передается как по оптическому волокну, так и по открытому пространству. Хотя в ряде случаев светодиоды могут быть использованы в качестве источников света, наибольшая емкость оптического канала связи достигается при использовании лазерных источников поля и когерентных оптических приемников. Таким образом, в современной оптической линии связи состояния носителя информации представляют собой несколько когерентных состояний одной моды оптического поля. При квантовом описании света когерентное состояние с безразмерной комплексной амплитудой α представляется [1] в виде

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle, \qquad (1)$$

где $|n\rangle$ представляет собой n-фотонное состояние поля (состояние Фока). Перекрытие двух когерентных состояний дается формулой $|\langle\alpha|\beta\rangle|^2 = e^{-|\alpha-\beta|^2}$. Таким образом, при достаточной близости амплитуд два когерентных состояния являются существенно неортогональными, и их различение при измерении связано с возможной ошибкой, обусловленной квантовым шумом. В подобном случае канал передачи информации рассматривают как квантовый канал связи [2] и для определения уровня ошибок привлекают квантовую теорию измерений [3].

В типичной современной системе волоконно-оптической связи состояния носителя информации можно считать практически ортогональными. Действительно, при использовании всего двух когерентных состояний с противоположной фазой, что соответствует популярной схеме фазового манипулирования BSPK [4], величина перекрытия состояний равна $|\langle\alpha| - \alpha\rangle|^2 = e^{-4N}$, где $N = |\alpha|^2$ — среднее число фотонов в одном окне модуляции. Следовательно, в данной схеме квантовое рассмотрение становится необходимым только при очень низком уровне сигнала. По мере распространения сигнала в оптическом волокне его мощность уменьшается из-за потерь, и когда она становится сравнимой с пределом чувствительности фотодетектора, используемого в когерентном оптическом приемнике, сигнал подвергается усилению на оптическом повторителе. Типичные значения частоты модуляции и чувствительности приемника в современных волоконно-оптических сетях составляют $f = 10\,\mathrm{GHz}$ и $P = 1\,\mu\mathrm{W}$ соответственно [5]. Таким образом, средняя энергия поля в окне модуляции может быть оценена в $E = P/f = 10^{-16}\,\mathrm{J}$, в то время как энергия одного фотона на длине волны $\lambda = 1.5\,\mu\mathrm{m}$ составляет $E_{ph} = 2\pi\hbar c/\lambda \sim 10^{-19}\,\mathrm{J}$. Это означает, что поле на приемнике содержит в среднем $N = E/E_{ph} = 1000$ фотонов на один передаваемый бит информации. Перекрытие двух когерентных состояний в данном случае ничтожно мало, и рассмотрение квантового шума не требуется. Однако быстрый прогресс в области телекоммуникаций приводит к использованию модуляторов с частотой $f = 25\,\mathrm{GHz}$ и фотоприемников с чувствительностью $P = 0.1\,\mu\mathrm{W}$, что снижает среднее число фотонов до $N = 40$. Кроме того, необходимость повышения емкости каналов связи приводит к внедрению прогрессивных форматов фазового и амплитудного манипулирования, в которых в одном окне модуляции может передаваться несколько битов информации [4–6]. При этом перекры-

тие соседних когерентных состояний уже определяется не только уровнем сигнала, но и геометрией расположения состояний на комплексной плоскости. Так, в перспективном формате M-PSK используется M значений фазы [4,5], причем амплитуды когерентных состояний имеют вид $\alpha_k = \sqrt{N}e^{i2\pi k/M}$ и перекрытие соседних состояний дается формулой $|\langle\alpha_k|\alpha_{k+1}\rangle|^2 = e^{-4N\sin^2(\pi/M)}$, что равно примерно $2 \cdot 10^{-3}$ для $N = 40$, $M = 16$. Подобное перекрытие приводит к ошибке в дискриминации состояний порядка 10^{-3}, что близко к максимально допустимому уровню ошибок, исправляемых кодами коррекции ошибок [5]. Таким образом, в ближайшем будущем квантовый шум может стать существенным для массовых сетей телекоммуникаций. Кроме того, квантовый шум имеет большое значение для оптической связи через открытое пространство, при которой усиление сигнала невозможно. В частности, для спутниковой оптической связи требуется разработка специальных приемников на основе детекторов одиночных фотонов, в которых квантовый шум играет ключевую роль [7]. Еще одним важным приложением, требующим квантового анализа оптического канала связи, является квантовая криптография, в которой состояния поля намеренно создаются неортогональными уже на входе в канал связи с целью сделать незаметный перехват информации невозможным [8]. Таким образом, разработка методов различения перекрывающихся когерентных состояний является весьма актуальной современной задачей с широкой областью применения.

Существуют три подхода к решению задачи различения M неортогональных состояний квантовой системы. Первый подход основан на максимизации извлекаемой информации, точный расчет которой в большинстве случаев весьма сложен и верхняя граница которой была установлена Холево [9]. Эта граница достижима в большинстве случаев только при проведении коллективных квантовых измерений над блоками состояний в пределе бесконечно длинных блоков [10]. При анализе стойкости схем квантовой криптографии обычно предполагается, что противник имеет возможность проводить подобные измерения. В практических системах передачи информации проводятся индивидуальные измерения каждого носителя, и поэтому извлекаемая информация, как правило, гораздо ниже предела Холево. В этом случае существует два подхода — различение состояний с минимальной ошибкой (РСМО) и безошибочное различение состояний (БРС). При РСМО процедура измерения M неортогональных состояний дает M исходов и подбирается так, чтобы минимизировать среднюю вероятность ошибки. В случае чистых квантовых состояний, что типично для оптических линий связи, где когерентное состояние остается чистым при любом уровне потерь, оптимальное для РСМО измерение представляется проекторами на чистые состояния, а оптимальная средняя вероятность ошибки дается пределом Холстрома [3]. Этот предел, как правило, лежит гораздо ниже средней ошибки гомодинного приема, реализованного в современных массовых волоконно-оптических линиях связи. Разработка когерентных приемников, понижающих вероятность ошибки до предела Холстрома, является перспективным направлением исследований [11]. При БРС процедура измерения M неортогональных состояний дает $M + 1$ исход, из которых M в точности (без ошибок) соответствуют измеряемым состояниям, а один исход с вероятностью P_e является нерешающим, т.е. не дает никакой информации о состоянии системы [12,13]. Как правило, P_e превышает предел Холстрома для заданного набора состояний, но ключевым преимуществом БРС является знание позиций нерешающих исходов, тогда как при РСМО позиции ошибок неизвестны. Особую важность БРС имеет для моделирования атак на систему квантовой криптографии, в которых перехват информации маскируется под потери квантового канала связи. В этом случае вероятность БРС $P_D = 1 - P_e$ определяет минимально допустимое пропускание канала [14,15]. В ряде протоколов квантовой криптографии используются две моды оптического поля [16–18]. Недавно было установлено, что вероятность БРС двухмодовых когерентных состояний существенно повышается, когда амплитуды двух мод являются взаимно комплексно-сопряженными [13]. В настоящей работе будет проведено детальное исследование данного явления и предложена схема оптического интерферометра, осуществляющего БРС четырех двухмодовых когерентных состояний оптического поля.

Расчет структуры состояний

Рассмотрим две моды оптического поля A и B, находящиеся в одном из четырех сигнальных состояний $|\psi_k\rangle = |\alpha_k\rangle_A|\alpha_k^*\rangle_B$, где $\alpha_k = \sqrt{N}e^{i\pi k/2}$ и индекс k принимает значения от 0 до 3. Состояние каждой моды несет два бита информации, записанные в формате 4-PSK, упомянутом выше, однако амплитуды обеих мод являются взаимно комплексно-сопряженными. Такие состояния создаются фазовым электрооптическим модулятором бегущей волны сразу на двух боковых частотах модулированного светового пучка [19], но для простоты анализа в настоящей работе мы будем полагать, что они создаются двумя модуляторами на одной несущей оптической частоте. Также возможен вариант, при котором две моды представляют собой два последовательных временных окна с полем в когерентном состоянии с амплитудой $\alpha_0 = \sqrt{N}$, и модулятор записывает фазу $\pi k/2$ в первом окне и фазу $-\pi k/2$ во втором. Все четыре состояния имеют одинаковую вероятность $1/4$, т.е. система сигнальных состояний является равновероятной. Вероятность БРС для такого набора состояний равна $P_D = (1 - e^{-2N})^2$ [13]. При малом значении $N \ll 1$, типичном для квантовой криптографии, вероятность БРС квадратична по среднему числу фотонов, $P_D = 4N^2 + O(N^3)$. Для сравнения мы

будем рассматривать альтернативную систему четырех состояний $|\tilde{\psi}_k\rangle = |\alpha_k\rangle_A|\alpha_k\rangle_B$, в которой амплитуда моды B в точности повторяет амплитуду моды A. Эта система может быть переведена унитарным преобразованием [20] в систему $|\tilde{\psi}'_k\rangle = |\sqrt{2}\alpha_k\rangle_A|0\rangle_B$, и, так как унитарное преобразование не меняет вероятность БРС, для обеих систем эта вероятность дается выражением $\tilde{P}_D = 2e^{-2N}(\sinh 2N - \sin 2N) = 16/3N^3 + O(N^4)$ [13]. Эта вероятность значительно меньше P_D при малом N, откуда следует, что использование комплексно-сопряженной амплитуды для второй моды существенно повышает различимость набора квантовых состояний.

Оптимальное БРС соответствует квантовому измерению, характеризуемому проекторами на состояния, взаимные сигнальным [12,13]. Состояние $|\psi_k^{\perp}\rangle$ взаимно состоянию $|\psi_k\rangle$, если оно принадлежит линейной оболочке сигнальных состояний и ортогонально всем состояниям, кроме $|\psi_k\rangle$. Когда сигнальные состояния являются когерентными, как в рассматриваемом случае, взаимные состояния представляют собой суперпозиции когерентных состояний [21] и относятся к классу состояний „кота Шредингера“. Состояния этого класса очень чувствительны к потерям и требуют специальных мер защиты от разрушения [22,23]. Проведение проективного измерения в базисе подобных состояний является крайне сложной технической задачей. Гораздо больший практический интерес представляет проведение измерения на базе интерферометра и детекторов одиночных фотонов, не различающих их число. Для когерентных состояний одной моды такое измерение было недавно реализовано экспериментально [24], а его двухмодовый вариант будет представлен в следующем разделе. В данном типе измерений на вход интерферометра подаются сигнальное поле в одном из возможных состояний и вспомогательное поле в когерентном состоянии, фаза которого привязана к фазе сигнальных состояний. Вспомогательное поле необходимо для проведения фазочувствительных измерений. Мы будем описывать это поле как моду C, находящуюся в когерентном состоянии $|\gamma\rangle_C$ с положительной амплитудой γ, сравнимой по величине с α_k. На практике данная мода может быть разбита светоделителями на несколько мод и сдвинута по фазе, но так как эти операции унитарны, они не изменят вероятность БРС. Таким образом, на входе в интерферометр имеется трехмодовое поле в одном из четырех состояний $|\varphi_k\rangle = |\alpha_k\rangle_A|\alpha_k^*\rangle_B|\gamma\rangle_C$, $k = 0, 1, 2, 3$. Все выходы интерферометра, обозначим их число через J, контролируются детекторами одиночных фотонов, не различающими число фотонов, так что фотоотсчет детектора соответствует присутствию в измеряемом поле как минимум одного фотона. Одна реализация квантового измерения характеризуется фиксацией некоторого количества L фотоотсчетов на всех фотодетекторах. В пределе низкого числа фотонов наиболее вероятным значением является $L = 0$. Этот результат, очевидно, является нерешающим. Менее вероятна фиксация одного фотоотсчета, т. е. $L = 1$. В этом случае имеется J исходов измерения, соответствующих фиксации отсчета на одном из J детекторов. Однако эти исходы не могут различить четыре сигнальных состояния, так как вероятность одного отсчета имеет вероятность, убывающую в пределе малого числа фотонов как $O(N)$, а вероятность различения имеет порядок $O(N^2)$. Следовательно, все исходы с $L = 1$ также являются нерешающими. Следующая по степени вероятности возможность — фиксация двух отсчетов, что может произойти $J(J-1)$ способами. Вероятность данного события имеет порядок $O(N^2)$, что соответствует порядку вероятности различения, а значит, БРС может быть реализовано при фиксации всего двух фотоотсчетов. Очевидно, что для альтернативного набора состояний $|\tilde{\varphi}_k\rangle = |\alpha_k\rangle_A|\alpha_k\rangle_B|\gamma\rangle_C$ требуется три отсчета, так как вероятность различения в этом случае на порядок ниже.

Для лучшего понимания данного явления представим состояния различаемого набора в виде ряда по суммарному числу фотонов в обеих модах и ограничимся первыми тремя членами данного разложения, что является хорошим приближением для $N \ll 1$:

$$\begin{pmatrix} |\varphi_0\rangle \\ |\varphi_1\rangle \\ |\varphi_2\rangle \\ |\varphi_3\rangle \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} |0\rangle_A|0\rangle_B|0\rangle_C$$

$$+ \mathbf{\Phi}_1 \begin{pmatrix} |1\rangle_A & |0\rangle_B & |0\rangle_C \\ |0\rangle_A & |1\rangle_B & |0\rangle_C \\ |0\rangle_A & |0\rangle_B & |1\rangle_C \end{pmatrix} + \mathbf{\Phi}_2 \begin{pmatrix} |2\rangle_A & |0\rangle_B & |0\rangle_C \\ |0\rangle_A & |2\rangle_B & |0\rangle_C \\ |0\rangle_A & |0\rangle_B & |2\rangle_C \\ |1\rangle_A & |1\rangle_B & |0\rangle_C \\ |1\rangle_A & |0\rangle_B & |1\rangle_C \\ |0\rangle_A & |1\rangle_B & |1\rangle_C \end{pmatrix}, \tag{2}$$

где матрицы $\mathbf{\Phi}_1$ и $\mathbf{\Phi}_2$ задаются соотношениями

$$\mathbf{\Phi}_1 = e^{-N-\gamma^2/2} \begin{pmatrix} \alpha & \alpha & \gamma \\ i\alpha & -i\alpha & \gamma \\ -\alpha & -\alpha & \gamma \\ -i\alpha & i\alpha & \gamma \end{pmatrix}, \tag{3}$$

$$\mathbf{\Phi}_2 = \frac{1}{\sqrt{2}} e^{-N-\gamma^2/2} \times \begin{pmatrix} N & N & \gamma^2 & \sqrt{2}N & \sqrt{2}\alpha\gamma & \sqrt{2}\alpha\gamma \\ -N & -N & \gamma^2 & \sqrt{2}N & i\sqrt{2}\alpha\gamma & -i\sqrt{2}\alpha\gamma \\ N & N & \gamma^2 & \sqrt{2}N & -\sqrt{2}\alpha\gamma & -\sqrt{2}\alpha\gamma \\ -N & -N & \gamma^2 & \sqrt{2}N & -i\sqrt{2}\alpha\gamma & i\sqrt{2}\alpha\gamma \end{pmatrix} \tag{4}$$

и введено обозначение $\alpha = \sqrt{N}$. Ранг матрицы $\mathbf{\Phi}_1$ не может превышать число ее столбцов, т. е. 3, а значит, если мы ограничим наше разложение нулевым и первым

порядками, то четыре сигнальных состояния окажутся линейно зависимыми. Как известно, линейно зависимые состояния не могут быть безошибочно различены [12,13]. Интерферометр может изменить распределение фотонов по модам, но оставляет общее число фотонов неизменным. Таким образом, можно сказать, что сигнальные состояния неразличимы в однофотонном подпространстве [14]. Структура состояний в двухфотонном подпространстве задается матрицей $\mathbf{\Phi}_2$, ранг которой равен 4, что означает линейную независимость сигнальных состояний при ограничении разложения тремя первыми членами. Именно ранг матрицы $\mathbf{\Phi}_2$, совпадающий с числом сигнальных состояний, определяет возможность реализации БРС на основании всего двух отсчетов и квадратичную зависимость вероятности различения от N.

Для сравнения проведем подобный расчет для альтернативного набора сигнальных состояний $|\tilde{\varphi}_k\rangle_A = |\alpha_k\rangle_A|\alpha_k\rangle_B|\gamma\rangle_C$:

$$\begin{pmatrix} |\tilde{\varphi}_0\rangle \\ |\tilde{\varphi}_1\rangle \\ |\tilde{\varphi}_2\rangle \\ |\tilde{\varphi}_3\rangle \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} |0\rangle_A|0\rangle_B|0\rangle_C + \tilde{\mathbf{\Phi}}_1 \begin{pmatrix} |1\rangle_A & |0\rangle_B & |0\rangle_C \\ |0\rangle_A & |1\rangle_B & |0\rangle_C \\ |0\rangle_A & |0\rangle_B & |1\rangle_C \end{pmatrix}$$

$$+\tilde{\mathbf{\Phi}}_2 \begin{pmatrix} |2\rangle_A & |0\rangle_B & |0\rangle_C \\ |0\rangle_A & |2\rangle_B & |0\rangle_C \\ |0\rangle_A & |0\rangle_B & |2\rangle_C \\ |1\rangle_A & |1\rangle_B & |0\rangle_C \\ |1\rangle_A & |0\rangle_B & |1\rangle_C \\ |0\rangle_A & |1\rangle_B & |1\rangle_C \end{pmatrix}, \qquad (5)$$

где

$$\tilde{\mathbf{\Phi}}_1 = e^{-N-\gamma^2/2} \begin{pmatrix} \alpha & \alpha & \gamma \\ i\alpha & i\alpha & \gamma \\ -\alpha & -\alpha & \gamma \\ -i\alpha & -i\alpha & \gamma \end{pmatrix}, \qquad (6)$$

$$\tilde{\mathbf{\Phi}}_2 = \frac{1}{\sqrt{2}} e^{-N-\gamma^2/2} \times \begin{pmatrix} N & N & \gamma^2 & \sqrt{2}N & \sqrt{2}\alpha\gamma & \sqrt{2}\alpha\gamma \\ -N & -N & \gamma^2 & -\sqrt{2}N & i\sqrt{2}\alpha\gamma & i\sqrt{2}\alpha\gamma \\ N & N & \gamma^2 & \sqrt{2}N & -\sqrt{2}\alpha\gamma & -\sqrt{2}\alpha\gamma \\ -N & -N & \gamma^2 & -\sqrt{2}N & -i\sqrt{2}\alpha\gamma & -i\sqrt{2}\alpha\gamma \end{pmatrix}. \qquad (7)$$

Ранг матрицы $\tilde{\mathbf{\Phi}}_2$ равен 3, что означает линейную зависимость ее строк и соответственно сигнальных состояний в двухфотонном подпространстве. Поэтому состояния альтернативного набора не могут быть различены при фиксации всего двух отсчетов, а требуют трех отсчетов, что и было продемонстрировано в эксперименте [24]. Таким образом, мы показали, что сопряжение амплитуды второй моды приводит к изменению структуры квантовых состояний и лучшей различимости при заданном среднем числе фотонов.

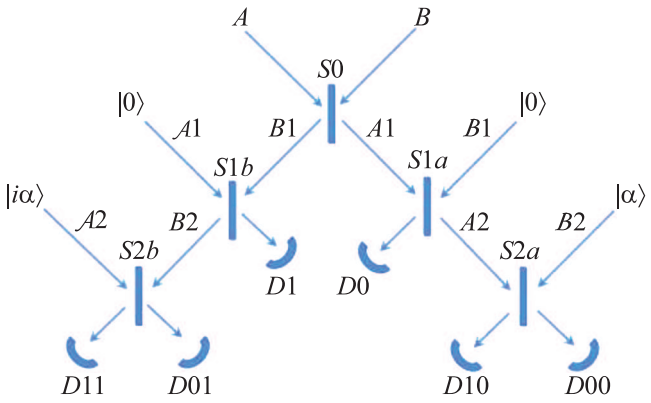

Схема интерферометра, реализующего БРС для четырех когерентных состояний мод A и B, имеющих вид $|\psi_k\rangle = |\alpha_k\rangle_A|\alpha_k^*\rangle_B$. Буквой S обозначены светоделители, буквой D — фотодетекторы. Стрелки обозначают моды оптического поля.

Схема измерения

На рисунке изображена схема интерферометрического измерения, осуществляющего БРС для исследуемого набора состояний. Она состоит из пяти симметричных светоделителей и шести детекторов одиночных фотонов. Для понимания принципа ее действия следует иметь в виду, что преобразование поля на симметричном светоделителе является унитарным преобразованием с оператором эволюции $U = e^{\pi/4\,(a^+b - ab^+)}$, где a и b — операторы уничтожения фотонов входящих мод светоделителя, а a^+ и b^+ — операторы рождения фотонов этих мод. На выходе светоделителя полевые операторы имеют вид $a' = U^+aU = (a+b)/\sqrt{2}$ и $b' = U^+bU = (a-b)/\sqrt{2}$.

Несложно заметить, что смешение мод A и B на светоделителе $S0$ приводит к образованию следующих состояний:

$$U|\pm\alpha\rangle_A|\pm\alpha\rangle_B = |\pm\sqrt{2}\alpha\rangle_{A1}|0\rangle_{B1}, \qquad (8)$$

$$U|\pm i\alpha\rangle_A|\mp i\alpha\rangle_B = |0\rangle_{A1}|\pm i\sqrt{2}\alpha\rangle_{B1}, \qquad (9)$$

т.е. состояния $|\psi_0\rangle$ и $|\psi_2\rangle$ приводят к деструктивной интерференции на левом выходе светоделителя $S0$, а состояния $|\psi_1\rangle$ и $|\psi_3\rangle$ приводят к деструктивной интерференции на его правом выходе. Таким образом, фиксация отсчета на детекторе $D0$ означает четное k и оставляет моду $A2$ в состоянии $|\pm\alpha\rangle_{A2}$, в то время как фиксация отсчета на детекторе $D1$ означает нечетное k и оставляет моду $B2$ в состоянии $|\pm i\alpha\rangle_{B2}$. Вспомогательная мода $\mathscr{B}2$, приготовленная в состоянии $|\pm i\alpha\rangle_{B2}$, помогает различить два возможных состояния моды $A2$: фиксация отсчета на детекторе $D00$ соответствует $|\psi_0\rangle$,

тогда как фиксация отсчета на детекторе $D10$ соответствует $|\psi_2\rangle$. Аналогично в другом плече интерферометра вспомогательная мода $\mathcal{A}2$, приготовленная в состоянии $|i\alpha\rangle$, помогает различить два возможных состояния моды $B2$: фиксация отсчета на детекторе $D01$ соответствует $|\psi_1\rangle$, тогда как фиксация отсчета на детекторе $D11$ соответствует $|\psi_3\rangle$. При этом индекс детекторов Dyx соответствует записи номера сигнального состояния в двоичной системе исчисления $k = (xy)_2$. Таким образом, детекторы Dx декодируют значение младшего бита числа k, а детекторы Dyx декодируют значение его старшего бита.

Вероятность различения

Найдем вероятность успешного различения состояний в предложенной схеме измерения. Вероятность фиксации отсчета на $D0$ или $D1$ равна $P_1 = 1 - e^{-N}$. При условии фиксации отсчета на Dx вероятность срабатывания Dyx равна $P_2 = 1 - e^{-2N}$. Мы не рассматриваем возможные отсчеты детекторов $Dy\bar{x}$ (верхняя черта означает инверсию бита), следующие за отсчетом детектора Dx, так как сигнальное состояние в соответствующем плече интерферометра спроектировано на вакуум, как показывают уравнения (8), (9), и данные отсчеты происходят из-за фотонов вспомогательного поля. Итого, вероятность различения всех четырех сигнальных состояний равна $P'_D = P_1P_2 = (1 - e^{-N})(1 - e^{-2N}) = 2N^2 + O(N^3)$. Данная схема измерения не является оптимальной, так как P'_D в пределе малого N в два раза меньше оптимального значения P_D, приведенного в предыдущем разделе. Однако эта схема имеет существенное практическое преимущество — она может быть реализована на основе линейного интерферометра и детекторов одиночных фотонов. Подобная схема неоптимального линейно-оптического различения для альтернативного набора сигнальных состояний была реализована в работе [24].

Полученный результат важен для нескольких направлений современных исследований. Во-первых, он показывает, что системы квантовой криптографии, использующие две моды поля в сопряженных когерентных состояниях [16–18], могут быть подвергнуты атаке БРС [14,15], которая в данном случае является одной из самых эффективных и является основным ограничивающим фактором для допустимого уровня потерь в канале связи. Для борьбы с данной атакой требуется разработка специальных мер защиты [25,26] либо блокировка одной из передаваемых мод. Во-вторых, различение неортогональных состояний является важной частью протоколов квантовой телепортации [27,28]. Повышенная различимость сопряженных двухмодовых состояний может значительно повысить вероятность успеха телепортации. В частности, удвоение когерентных состояний используется в протоколе квантовой телепортации на основе обобщенных квазибелловских состояний поля [29], и его замена на удвоение с сопряжением значительно увеличит вероятность успеха, особенно при малом среднем числе фотонов. В-третьих, применение сопряжения амплитуды к сжатым когерентным полям представляет интерес для более эффективной передачи многомодового квантового сигнала [30]. Кроме того, повышенная различимость позволяет проведение РСМО на уровне, приближенном к пределу Хелстрома, что говорит о перспективности рассмотренного набора состояний для использования в когерентных приемниках, предназначенных для работы на однофотонном уровне.

Заключение

Исследовано безошибочное различение четырех двухмодовых когерентных состояний оптического поля и показано, что комплексное сопряжение амплитуды одной из мод приводит к лучшей различимости состояний. Предложена интерферометрическая схема безошибочного различения таких состояний и найдена вероятность успешного различения, которая квадратична по среднему числу фотонов. Данные результаты имеют значение для разработки систем квантовой криптографии и квантовой телепортации на дальние расстояния, а также для систем оптической передачи информации, связанных с детектированием низкого уровня оптического сигнала.

Финансирование работы

Белорусский республиканский фонд фундаментальных исследований (грант Ф20КИ-035).

Конфликт интересов

Авторы заявляют, что у них нет конфликта интересов.

Список литературы

[1] *Килин С.Я.* Квантовая оптика. Поля и их детектирование. М.: Едиториал УРСС, 2003. 176 с.
[2] *Килин С.Я.* // УФН. 1999. Т. 169. С. 507. doi 10.3367/UFNr.0169.199905b.0507; *Kilin S.Ya.* // Phys. Usp. 1999. V. 42. P. 435. doi 10.1070/PU1999v042n05ABEH000542
[3] *Helstrom C.W.* Quantum Detection and Estimation Theory. Academic Press, 1976. 309 p. Перевод: Хелстром К. Квантовая теория проверки гипотез и оценивания. М.: Мир, 1979. 344 с.
[4] *Proakis J.* Digital Commun. McGraw-Hill, 2000. 928 p. Перевод: Прокис Дж. Цифровая связь. М.: Радио и связь, 2000. 800 с.
[5] *Muciaccia T., Gargano F., Passaro V.M.N.* // Photonics. 2014. V. 1. P. 323. doi 10.3390/photonics1040323
[6] *Burenkov I.A., Tikhonova O.V., Polyakov S.V.* // Optica. 2018. V. 5. P. 227. doi 10.1364/OPTICA.5.000227
[7] *Khan I., Elser D., Dirmeier T., Marquardt C., Leuchs G.* // Phil. Trans. Roy. Soc. A. 2017. V. 375. P. 20160235.

[8] Квантовая криптография: идеи и практика / Под ред. Килина С.Я., Хорошко Д.Б., Низовцева А.П. Минск: Белорусская наука, 2007. 391 с.
[9] *Holevo A.S.* Probabilistic and Statistical Aspects of Quantum Theory. Elsevier, 1982. 324 p. Перевод: Холево А.С. Вероятностные и статистические аспекты квантовой теории. М.: Наука, 1980. 324 с.
[10] *Hausladen P., Jozsa R., Schumacher B., Westmoreland M., Wootters W.K.* // Phys. Rev. A. 1996. V. 54. P. 1869. doi 10.1103/PhysRevA.54.1869
[11] *Becerra F.E., Fan J., Baumgartner G., Goldhar J., Kosloski J.T., Migdall A.* // Nature Phot. 2013. V. 7. P. 147. doi 10.1038/nphoton.2012.316
[12] *Chefles A.* // Phys. Lett. A. 1998. V. 239. P. 339. doi 10.1016/S0375-9601(98)00064-4
[13] *Horoshko D.B., Eskandari M.M., Kilin S.Ya.* // Phys. Lett. A. 2019. V. 383. P. 1728. doi 10.1016/j.physleta.2019.03.006
[14] *Dušek M., Jahma M., Lütkenhaus N.* // Phys. Rev. A. 2000. V. 62. P. 022306. doi 10.1103/PhysRevA.62.022306
[15] *Эскандери М.М., Хорошко Д.Б., Килин С.Я.* // ЖПС. 2019. Т. 86. С. 717; *Eskandari M.M., Horoshko D.B., Kilin S.Ya.* // J. Appl. Spectr. 2019. V. 86. P. 806. doi 10.1007/s10812-019-00897-z
[16] *Mérolla J.-M., Mazurenko Y., Goedgebuer J.-P., Rhodes W.T.* // Phys. Rev. Lett. 1999. V. 82. P. 1656. doi 10.1103/PhysRevLett.82.1656
[17] *Miroshnichenko G.P., Kozubov A.V., Gaidash A.A., Gleim A.V., Horoshko D.B.* // Opt. Express. 2018. V. 26. P. 11292. doi 10.1364/OE.26.011292
[18] *Chistiakov V., Kozubov A., Gaidash A., Gleim A., Miroshnichenko G.* // Opt. Express. 2019. V. 27. P. 36551. doi 10.1364/OE.27.036551
[19] *Horoshko D.B., Eskandary M.M., Kilin S.Ya.* // J. Opt. Soc. Am. B. 2018. V. 35. P. 2744. doi 10.1364/JOSAB.35.002744
[20] *Horoshko D.B., De Bièvre S., Kolobov M.I., Patera G.* // Phys. Rev. A. 2016. V. 93. P. 062323. doi 10.1103/PhysRevA.93.062323
[21] *Sanders B.C.* // Phys. Rev. A. 1992. V. 45. P. 6811. doi 10.1103/PhysRevA.45.6811
[22] *Horoshko D.B., Kilin S.Ya.* // J. Mod. Opt. 1997. V. 44. P. 2043. doi 10.1080/09500349708231866
[23] *Horoshko D.B., Kilin S.Ya.* // Opt. Express. 1998. V. 2. P. 347. doi 10.1364/OE.2.000347
[24] *Becerra F.E., Fan J., Migdall A.* // Nature Commun. 2013. V. 4. P. 2028. doi 10.1038/ncomms3028
[25] *Gaidash A., Kozubov A., Miroshnichenko G.* // J. Opt. Soc. Am. B. 2019. V. 36. P. B16. doi 10.1364/JOSAB.36.000B16
[26] *Gaidash A., Kozubov A., Miroshnichenko G.* // Phys. Scr. 2019. V. 94. P. 125102. doi 10.1088/1402-4896/ab3277
[27] *Braunstein S.L., Kimble H.J.* // Phys. Rev. Lett. 1998. V. 80. P. 869. doi 10.1103/PhysRevLett.80.869
[28] *Horoshko D.B., Kilin S.Ya.* // Phys. Rev. A. 2000. V. 61. P. 032304. doi 10.1103/PhysRevA.61.032304
[29] *Horoshko D.B., Patera G., Kolobov M.I.* // Opt. Commun. 2019. V. 447. P. 67. doi 10.1016/j.optcom.2019.04.088
[30] *Аверченко В.А., Голубева Т.Ю., Голубев Ю.М., Fabre C.* // Опт. и спектр. 2008. Т. 105. № 5. С. 831–843; *Averchenko V.A., Golubeva T.Yu., Golubev Yu.M., Fabre C.* // Opt. Spectrosc. 2008. V. 105. N 5. P. 758–770.