

ЛИНЕЙНЫЕ ОПТИЧЕСКИЕ КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

Г. П. Мирошниченко

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург, Россия

gpmirosh@gmail.com

Представлен обзор работ за последнее десятилетие, где разработан протокол линейных оптических квантовых вычислений, экспериментально продемонстрировано функционирование отдельных компонентов, предложены усовершенствования оптической архитектуры первоначально введенного в 2001 году протокола, а также дана оценка его отказоустойчивости.

Ключевые слова: оптическая квантовая информатика, линейные оптические квантовые вычисления, почти детерминированная квантовая телепортация, квантовые коды коррекции ошибок.

1. Введение

Любое направление деятельности человека связано с использованием информации. Раздел науки — информатика — занимается изучением методов передачи, хранения, обработки информации. Информация должна долго храниться, передаваться без искажений, обрабатываться быстро и без потерь. Идет постоянное совершенствование методов информатики. В дополнение к классической информатике развивается новое направление — квантовая информатика. Число научных работ по этому направлению неуклонно растет. Ясно, что классическая информатика не может обойтись без квантовых законов, так как все процессы так или иначе ими определяются. Достаточно вспомнить такие приборы информатики, как современные компьютеры, работа которых основана на квантовых законах поведения носителей в полупроводниках, поведения спиновых степеней свободы в магнитном поле и так далее. И тем не менее это классический компьютер. То есть сложная электрическая схема, содержащая макроскопические базисные нелинейные элементы — биты — имеющие два устойчивых логических классических состояния (значение тока, напряжения, намагниченности) и набор универсальных вентилях — гейтов — служащих для управления битами. Универсальный классический компьютер — это машина, работающая по принципу машины Тьюринга [1], имеющей программное управление, память, пошаговый способ действий, в которой логические операции производятся с классическими булевыми состояниями, отображающими одну совокупность состояний битов в другую совокупность булевых состояний.

Квантовая информатика предлагает принципиально новый подход к информационным процессам. Первые идеи нового подхода связывают с работами Ю.И. Манина [2] и Р. Феймана [3]. Естественно, человек потребляет информацию, представленную в классической форме. В квантовой информатике предлагается эту классическую информацию отобразить (записать, скопировать) в квантовые состояния квантовых элементарных носителей — кубитов, каждый из которых действует в 2-мерном гильбертовом пространстве. Затем над этим когерентным квантовым состоянием квантового регистра предлагается одновременно производить квантовые унитарные операции согласно опять таки квантовому алгоритму.

Этот алгоритм или протокол позволяет преобразовать, передать, запомнить квантовое состояние, а затем, с помощью набора квантовых измерений, превратить преобразованную квантовую информацию в классическую, для ее осмысления человеком.

Итак, для функционирования квантовой информатики необходим софт — алгоритмы, программы, протоколы и хард — конкретная физическая реализация кубитов и соответствующих квантовых гейтов (квантовый логический базис). Предложено несколько направлений реализации квантовых битов информации. Основные из них, это: ионы или атомы в оптоэлектронных лазерных ловушках. В ловушку можно поместить два или большее число ионов на расстоянии несколько микрон друг от друга и управлять каждым из них в отдельности. Организовать взаимодействие между ионами можно, используя коллективные колебательные моды ионов [4]. Это ядерные спины в молекулах жидкости. Для создания логического базиса можно использовать последовательности импульсов магнитного поля. В этом случае используется хорошо разработанная экспериментальная техника ядерного магнитного резонанса. Экспериментально продемонстрирована возможность когерентного управления системой из пяти ЯМР-кубитов — пока рекордное достижение в физике квантовых вычислений [5]. Это мезоскопические твердотельные системы, например, мезоскопические сверхпроводники. Экспериментально реализован зарядовый кубит. Такая система получила название *single Cooper-pair box*, или SCPB [6]. Это фазовые кубиты [7] — джозефсоновские кубиты, состояния которых различаются по токам в переходах. Это состояния примесей в кремнии [8] и квантовых точек в полупроводниковых гетероструктурах [9]. Это «топологически устойчивые» кубиты, предложенные А. Китаевым в 1997 году [10]. Наконец 11 мая 2011 года представлен компьютер D-Wave One, созданный на базе 128-кубитного процессора.

Существует и успешно развивается альтернативное направление к полупроводниковой кремниевой вычислительной базе [11]. Это направление разрабатывает классические оптические процессоры и компьютеры, где, вместо потока электронов, как в кремниевых чипах, используется поток фотонов — лазерное диодное излучение, параметры которого — фаза, амплитуда, поляризация — модулируются электрооптическими, волноводными (и другими) модуляторами, преобразующими информацию, передаваемую по световому лучу. Биты создаются на основе бистабильных нелинейных оптических устройств (резонаторов Фабри-Перро, интерференционных волноводных модуляторов, полупроводниковых квантовых точек и т.д.). В 2003 году компания Lenslet создала первый в мире гибридный (ядро процессора — оптическое, а входная и выходная информация электронная) оптический коммерческий процессор EnLight256, производительностью в 8×10^{12} операций в секунду. Ядро процессора — оптическая матрица VMM, представляет собой пространственный пиксельный модулятор, осуществляет векторно-матричную логику. Огромная производительность и параллельность вычислений — существенные достоинства этих машин.

Принципы квантовой оптики, рассматривающей свет, как квантовый объект, могут быть применены и для целей квантовой информатики. Это направление естественно назвать оптическая квантовая информатика. Здесь носителями квантовой информации являются квантовые степени свободы квантов света — фотонов (поляризация, волновой вектор, временной центр фотонного пакета, фаза и другие). Существует направление, в рамках которого логический базис гейтов в оптической квантовой информатике строится на основе линейных оптических элементов и фотодетекторов. По этому направлению развивается квантовые коммуникации и линейные оптические квантовые вычисления (ЛОКВ). И об этом направлении пойдет речь ниже.

2. Преобразование вычислительного базиса с помощью линейных оптических элементов

Вторичное квантование электромагнитного излучения (в гамильтоновом подходе) начинается с выбора модового базиса с помощью решения волнового уравнения в объеме, где распространяются световые волны (с соответствующими граничными условиями) и введения операторов рождения и уничтожения квантов света — фотонов, носящих квантовые индексы рассматриваемых мод [12]. Это бозе - операторы с коммутационным соотношением алгебры Гейзенберга-Вейля

$$[\hat{a}, \hat{a}^\dagger] = 1, \quad [\hat{a}, \hat{a}] = 0, \quad [\hat{a}^\dagger, \hat{a}^\dagger] = 0 \quad (1)$$

Линейные оптические элементы оптических сетей являются пассивными устройствами, сохраняющими число распространяющихся фотонов, и служат для создания интерференции оптических состояний. Каждый оптический элемент имеет вход и выход (один или несколько), и правило преобразования операторов мод с входа на выход имеет (линейный) вид

$$\hat{b}_j^\dagger = \sum_k M_{j,k} \hat{a}_k^\dagger \quad (2)$$

Здесь унитарная матрица $M_{j,k}$ определяется с помощью унитарной матрицы U , определяемой эффективным гамильтонианом элемента H , с помощью соотношения

$$\hat{b}_j^\dagger = U \hat{a}_j^\dagger U^\dagger, \quad U = \exp(i\theta H) \quad (3)$$

Квантовое состояние мод преобразуется с входа элемента на выход согласно правила

$$|\varphi_{out}\rangle = U |\varphi_{in}\rangle \quad (4)$$

Основными линейными оптическими элементами, используемыми в протоколах ЛОКВ, являются фазовращатель и светоделитель. Гамильтониан фазовращателя (один вход и один выход $j = 1$) имеет вид

$$H_{PS} = \hat{a}_j^\dagger \hat{a}_j, \quad |n\rangle_{out} = U_{PS} |n\rangle_{in} = \exp(i\theta n) |n\rangle_{in}, \quad M_{j,k}^{PS} = \exp(i\theta) \delta_{j,k} \quad (5)$$

Здесь $|n\rangle$, $n = 0, 1, 2, \dots$ — фокковский базис. Гамильтониан светоделителя (два входа и два выхода, $j = 1, 2$) имеет вид

$$H_{BS} = \exp(i\vartheta) \hat{a}_1^\dagger \hat{a}_2 + (h.c.) \quad (6)$$

Матрица (2) имеет вид

$$M^{BS} = \begin{pmatrix} \cos \theta & \exp(-i\vartheta) \sin \theta \\ -\exp(i\vartheta) \sin \theta & \cos \theta \end{pmatrix} \quad (7)$$

Оптическая схема, описываемая унитарной матрицей размерности N , представляет собой N модовый интерферометр, состоящий из $N(N+1)/2$ светоделителей (7) и фазовращателей (5). Такое устройство, как было показано [13], может совершать любую унитарную операцию (2) над N оптическими модами (рис. 1 взят из работы [14])

Унитарная матрица $M_{j,k}$ интерферометра рис.1 размерности $N \times N$ разбивается на произведение матриц $N \times N$, отвечающих каждому светоделителю схемы $M_{(p,q)}^{BS}$ (здесь индексы p, q обозначают номера мод, связанных данным светоделителем), и диагональной матрицы D фазовращателей N мод

$$M = (M_{(N,N-1)}^{BS} \cdot M_{(N,N-2)}^{BS} \cdot \dots \cdot M_{(N,1)}^{BS} \cdot M_{(N-1,N-2)}^{BS} \cdot \dots \cdot M_{(2,1)}^{BS} \cdot D)^{-1} \quad (8)$$

Матрица $M_{(p,q)}^{BS}$ — это единичная матрица размерности $N \times N$, где в элементы с номерами строк и столбцов, взятых из множества $\{p, q\}$, вставлены соответствующие элементы

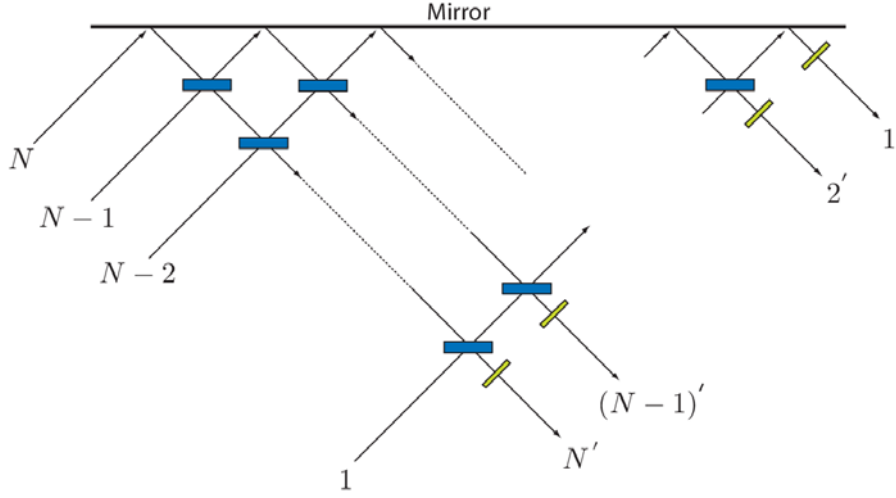


РИС. 1. N – портовый интерферометр, способный выполнить любую унитарную (из группы $U(N)$) операцию над N оптическими модами. Обозначения линейных оптических элементов: горизонтальные прямоугольники – светоделители, наклонные прямоугольники – фазовые пластинки

матрицы (7) (с соответствующими данному светоделителю углами). Например, для $N=3$, матрица $M_{(3,1)}^{BS}$ имеет вид

$$M_{(3,1)}^{BS} = \begin{pmatrix} \cos \theta & 0 & \exp(-i\vartheta) \sin \theta \\ 0 & 1 & 0 \\ -\exp(i\vartheta) \sin \theta & 0 & \cos \theta \end{pmatrix} \quad (9)$$

С помощью светоделителя двухмодовый фоковский вектор $|1, 1\rangle_{in}$ преобразуется по правилу

$$|1, 1\rangle_{out} = -\sqrt{2}e^{i\vartheta} \cos \theta \sin \theta |2, 0\rangle_{in} + (\cos^2 \theta - \sin^2 \theta) |1, 1\rangle_{in} + \sqrt{2}e^{-i\vartheta} \cos \theta \sin \theta |0, 2\rangle_{in} \quad (10)$$

Векторы $|1, 0\rangle_{in}$, $|0, 1\rangle_{in}$ преобразуются

$$\begin{aligned} |1, 0\rangle_{out} &= \cos \theta |1, 0\rangle_{in} + e^{-i\vartheta} \sin \theta |0, 1\rangle_{in} \\ |0, 1\rangle_{out} &= \cos \theta |0, 1\rangle_{in} - e^{i\vartheta} \sin \theta |1, 0\rangle_{in} \end{aligned} \quad (11)$$

Поперечные моды излучения могут различаться по поляризациям. Общеприняты обозначения $(n_H(n_V) - n)$ фотонов горизонтально (вертикально) поляризованы

$$|H\rangle \equiv |1_H, 0_V\rangle, \quad |V\rangle \equiv |0_H, 1_V\rangle, \quad |F\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), \quad |S\rangle = \frac{1}{\sqrt{2}}(|V\rangle - |H\rangle) \quad (12)$$

Преобразования (11) для поляризаций осуществляются поляризаторами по правилу

$$\begin{aligned} |H\rangle_{out} &= \cos \theta |H\rangle_{in} + e^{-i\vartheta} \sin \theta |V\rangle_{in}, \\ |V\rangle_{out} &= \cos \theta |V\rangle_{in} - e^{i\vartheta} \sin \theta |H\rangle_{in} \end{aligned} \quad (13)$$

и поляризационными светоделителями – горизонтальными и наклонными, с двумя входами 1 и 2 (HV-PBS и FS-PBS), по правилу

$$\begin{aligned} |H_1\rangle_{out} &= |H_1\rangle_{in}, \quad |H_2\rangle_{out} = |H_2\rangle_{in}, \quad |V_1\rangle_{out} = |V_2\rangle_{in}, \quad |V_2\rangle_{out} = |V_1\rangle_{in}, \\ |F_1\rangle_{out} &= |F_1\rangle_{in}, \quad |F_2\rangle_{out} = |F_2\rangle_{in}, \quad |S_1\rangle_{out} = |S_2\rangle_{in}, \quad |S_2\rangle_{out} = |S_1\rangle_{in} \end{aligned} \quad (14)$$

Формулы (11) и (13) математически эквивалентны, и при определении вычислительного базиса определяют так называемые поляризационную (13) и двухрельсовую (11) логики, с помощью которых можно сформировать любые однокубитовые операции. С помощью линейных оптических операций можно конструировать обширные оптические сети, вычислительные циклы, где имеется входное состояние вовлеченных в процесс мод, и конечное их состояние, свойства которого изучаются с помощью квантовых измерений.

Вышеприведенные формулы переписываются на логическом языке, при определении квантовых битов информации – кубитов. Кубит это базис $SU(2)$ группы. Для ее реализации можно использовать пространственные моды (различающиеся волновым вектором) и поляризационные моды, различающиеся типом поляризации. В качестве кубита со значением «0» («1») в двурельсовой кодировке выбирают

$$|0\rangle_c = |1, 0\rangle \quad (|1\rangle_c = |0, 1\rangle) \quad (15)$$

(один фотон в первой пространственной моде и ноль фотонов во второй и наоборот). В поляризационной кодировке выбирают кубиты со значением «0» («1»)

$$|0\rangle_c = |H\rangle \quad (|1\rangle_c = |V\rangle). \quad (16)$$

Для построения логического базиса необходимы и двухкубитовые операции. Но с помощью линейной оптики нельзя построить перепутанные состояния кубитов (15), (16) детерминистическим образом [15]. Если же поменять кодировку, например, взяв кубиты со значением «0» («1»)

$$|0\rangle_c = |0\rangle \quad (|1\rangle_c = |1\rangle) \quad (17)$$

то двухкубитная операция легко совершается с помощью светоделителя (один фотон на одном входе, ноль фотонов на противоположном входе) так как такая операция сохраняет число фотонов. Но однокубитная операция общего вида средствами линейной оптики не совершается детерминистически. Авторы Книлл, Лафламме, Милбурн предложили вводить нелинейность для совершения двухкубитных операций с помощью квантовых измерений над вспомогательными модами [20]. Но тогда такие операции становятся вероятностными.

3. Элементы немасштабируемого протокола ЛОКВ

Первые предложения по ЛОКВ сформулированы в работе [16]. Здесь оптический квантовый компьютер конструировался как сеть из N оптических мод, каждая из которых представляет собой битовую струну, которой приписывается значение «0» или «1». Каждая мода имеет обозначение из последовательности нулей и единиц в двоичном коде. Если число кубитов n , то число мод $N \approx 2^n$. В сеть запускается один фотон, который находится в суперпозиции N мод. Занятая фотоном мода (битовая струна) определяет текущее состояние регистра. Легко построить полный вычислительный одно и двухкубитовый базис в таком оптическом компьютере [17]. Но два обстоятельства требуют рассматривать такое устройство, как модель полуклассического компьютера. Во первых это не масштабируемый вариант, то есть для совершения любой логической операции над одним кубитом сети требуется применить $N \approx 2^n$ линейных оптических элементов, то есть такой протокол требует экспоненциально большое (по числу кубитов) число ресурсов. Ускорение, связанное с параллельностью действия «съедается» экспоненциально большим количеством элементов. Во вторых, суперпозиция одного фотона в N модах, это по существу классическая суперпозиция одиночного импульса света, так как уравнение движения одного фотона формально совпадают с классическими уравнениями Максвелла. Такой интерференционный квантовый эффект, как двухфотонный Hong-Ou-Mandel эффект [18] в данном случае отсутствует.

Второй протокол оптических квантовых вычислений связан с предложением использования керровской нелинейности среды [19] для конструирования двухкубитных операций над оптическими кубитами. Гамильтониан вещества с кросс-керровской нелинейностью можно представить в виде

$$H_{Kerr} = \hat{a}_a^\dagger \cdot \hat{a}_a \cdot \hat{a}_b^\dagger \cdot \hat{a}_b \quad (18)$$

Здесь a и b – две взаимодействующие через нелинейность среды моды излучения. Операторы мод преобразуются (3) в среде согласно соотношению

$$\hat{a}_{a'} = \exp\left(-i\theta\hat{a}_b^\dagger \cdot \hat{a}_b\right)\hat{a}_a, \quad \hat{a}_{b'} = \exp\left(-i\theta\hat{a}_a^\dagger \cdot \hat{a}_a\right)\hat{a}_b \quad (19)$$

С помощью соединенных через нелинейную среду двух интерферометров Маха-Цандера (использующих поляризационные светоделители (14)) можно получить двухкубитную операцию CZ, где кубиты выполнены в поляризационной кодировке (рис.2 взят из работы [17]).

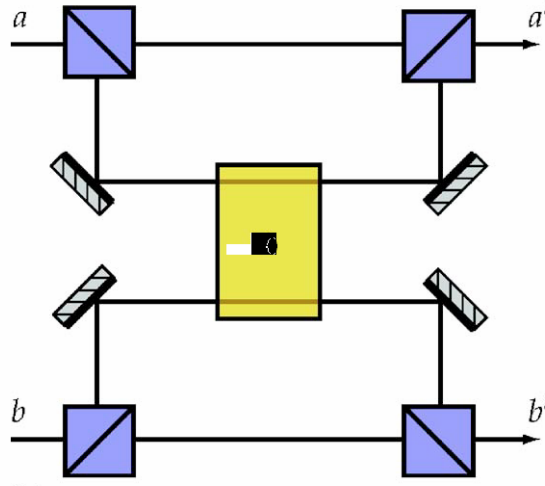


РИС. 2. Протокол двухкубитной операции CZ на двух связанных через кросс-керровскую нелинейность интерферометров Маха-Цандера. Прямоугольник в центре – кросскерровская среда, обеспечивающая сдвиг фаз на θ ; a , b – однофотонные входы, a' , b' – однофотонные выходы; прямоугольники по краям – поляризационные светоделители, работающие по схеме (14). Вычислительный базис представлен в поляризационной горизонтальной кодировке (12)

Схема на рис.2 создает операцию CZ, матрица которой, в вычислительном базисе, имеет вид

$$W_{CZ} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \quad (20)$$

Эта матрица действует на базисные двухкубитные векторы $|0,0\rangle_c$, $|0,1\rangle_c$, $|1,0\rangle_c$, $|1,1\rangle_c$ (16), записанные в координатной форме

$$|0\rangle_c = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle_c = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad |n, m\rangle_c = |n\rangle_c \otimes |m\rangle_c \quad (21)$$

Здесь \otimes — знак прямого произведения векторов. Трудность реализации протокола с керровской нелинейностью связана с малостью параметра нелинейности и необходимостью использования больших оптических путей для создания сдвига фаз $\theta = \pi$, что, в свою очередь, приводит к уменьшению соотношения сигнал-шум на выходе.

4. Телепортационный протокол ЛОКВ Knill-Laflamme-Milburn

Альтернативные протоколы для ЛОКВ состоят в том, что вместо того, чтобы строить многокубитные вычисления с одним фотоном в сети, можно закодировать кубит в один фотон, занимающий две оптические моды (поляризационные, пространственные или другие). Масштабируемый (число ресурсов полиномиально зависит от количества битов) протокол ЛОКВ предложен в работе [20] Протокол Книлла, Лафламме, Милбурна основан на линейных оптических элементах, фотодетекторах, вероятностном гейте CZ (20), основанном на гейте NS, методе телепортации вероятностного гейта в вычислительную цепь для достижения высокой вероятности успешного срабатывания гейта, и протокола, корректирующего ошибки гейта. Рассмотрим работу вероятностного гейта NS. Оптическая схема гейта NS представлена на рис.3 (взятого из работы [17])

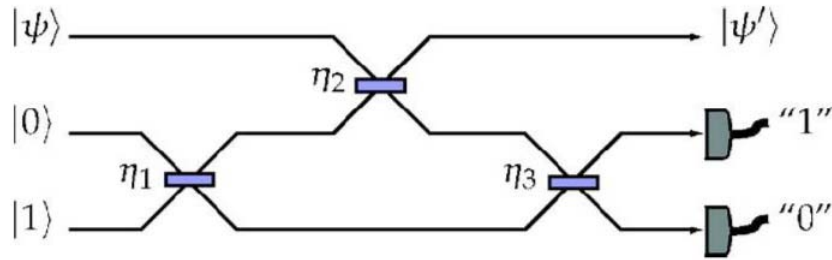


РИС. 3. Вероятностный гейт NS, имеющий входную моду в состоянии $|\psi\rangle$, выходную моду в состоянии $|\psi'\rangle$, три светоделителя с коэффициентами пропускания $\eta_1 = \eta_3 = \frac{1}{4-2\sqrt{2}}$, $\eta_2 = 3 - 2\sqrt{2}$, два (идеальных) фотодетектора, различающие фоковские состояния $|n\rangle$ с числами фотонов 0,1,2,3. и двух вспомогательных мод в состояниях $|0\rangle$ и $|1\rangle$. Конфигурация успешного события показана на рисунке

Правильная работа NS гейта состоит в следующем преобразовании состояния входной моды

$$|\psi'\rangle = \alpha |0\rangle + \beta |1\rangle - \gamma |2\rangle = W_{NS} |\psi\rangle = W_{NS} (\alpha |0\rangle + \beta |1\rangle + \gamma |2\rangle) \quad (22)$$

Если детекторы, контролирующие состояния вспомогательных мод, обнаружат одновременно один фотон в первой вспомогательной моде и ноль фотонов во второй, то такая конфигурация срабатывания «переведет» состояние входной моды в требуемое, согласно протокола (22). Вероятность такого события равна $\frac{1}{4}$. С помощью гейта NS предлагается протокол гейта CZ, оптическая схема которого приводится на рис.4. взятом из работы [17]

На входы CZ гейта подаются два фотона в произвольных состояниях (в двухрельсовой кодировке (15))

$$|\psi\rangle_1 \otimes |\varphi\rangle_2 = (\alpha |0, 1\rangle_1 + \beta |1, 0\rangle_1) \otimes (\gamma |0, 1\rangle_2 + \delta |1, 0\rangle_2) \quad (23)$$

Гейт вводит сдвиг фаз, равный π , в состоянии $|1, 0\rangle_1 \otimes |1, 0\rangle_2$, оставляя прочие базисные векторы без изменения. Как следствие, совершается вероятностная операция CZ с матрицей

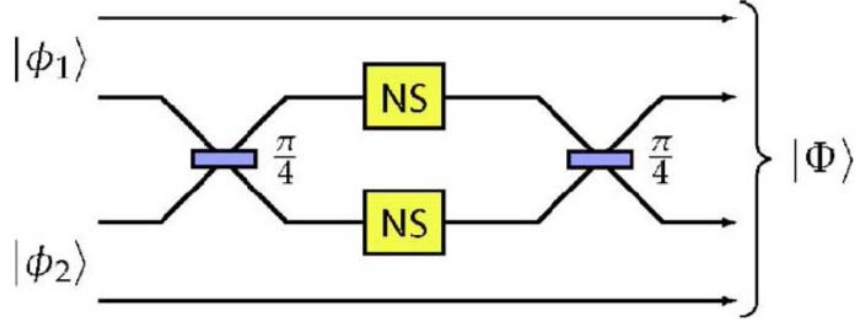


РИС. 4. Оптическая схема двухкубитного CZ гейта, имеющего два однокубитных входа (входные состояния кубитов $|\psi\rangle_1$ и $|\varphi\rangle_2$, выходное двухкубитное перепутанное состояние $|\Phi\rangle_{1,2}$). Схема содержит два светоделителя с коэффициентом пропускания $\frac{1}{\sqrt{2}}$ и два гейта NS

(20) в вычислительном базисе, то есть факторизованное состояние $|\psi\rangle_1 \otimes |\varphi\rangle_2$ переходит в перепутанное

$$|\Phi\rangle_{1,2} = \alpha\gamma |0, 1, 0, 1\rangle_{1,2} + \alpha\delta |0, 1, 1, 0\rangle_{1,2} + \beta\gamma |1, 0, 0, 1\rangle_{1,2} - \beta\delta |1, 0, 1, 0\rangle_{1,2} \quad (24)$$

Вероятность такого гейта равна $\frac{1}{16}$. CZ — это основной двухкубитный гейт, с помощью которого, а также с помощью однокубитных гейтов, можно построить полный логический базис ЛОКВ. Основная проблема состоит в малой вероятности успешного результата в работе этой схемы. Ряд альтернативных предложений по вероятностному гейту NS не существенно улучшают его возможности.

В протоколе Книлла, Лафламме, Милбурна присутствует еще одна находка, которую иногда называют «телепортационный трюк». Суть ее состоит в следующем. Протокол телепортации состояния первой моды удобно кратко записать в виде

$$|\psi\rangle_1 \otimes |\Psi_{00}\rangle_{2,3} \rightarrow X_3^n Z_3^m |\psi\rangle_3 \otimes |\Psi_{nm}\rangle_{1,2} \quad (25)$$

Здесь белловское состояние $|\Psi_{00}\rangle_{2,3}$ второй и третьей моды (в измерительном базисе, индекс с удален)

$$|\Psi_{00}\rangle_{2,3} = \frac{1}{\sqrt{2}} (|00\rangle_{23} + |11\rangle_{23}) \quad (26)$$

X, Y, Z — обозначения однокубитных матриц Паули $\sigma_x, \sigma_y, \sigma_z$ соответствующей моды, $nm = 0, 1$. Запись (25) означает, что после белловского измерения, результат которого задается парой чисел $nm = 0, 1$, обнаружившего моды 1 и 2 в белловском состоянии $|\Psi_{nm}\rangle_{1,2}$, входное состояние трех мод (левая часть формулы (25)) переходит в выходное состояние (правая часть формулы (25)). Состояние $|\psi\rangle_1$ первой моды телепортируется (с точностью до известного однокубитного поворота) в состояние третьей моды $|\psi\rangle_3$. Подействуем трехмодовой унитарной операцией

$$W_{123} = I_1 \otimes I_2 \otimes U_3 \quad (27)$$

где U_3 - произвольная унитарная операция, I_1, I_2 - тождественные операции, на входное состояние протокола, получим

$$W_{123} |\psi\rangle_1 \otimes |\Psi_{00}\rangle_{2,3} \rightarrow U_3 X_3^n Z_3^m |\psi\rangle_3 \otimes |\Psi_{nm}\rangle_{1,2} \quad (28)$$

Формула (28) определяет выходное состояние протокола

$$|\psi_{out}\rangle = U X^n Z^m |\psi\rangle \quad (29)$$

Далее, на моду 3 можно подействовать компенсирующим преобразованием, получим протокол телепортации гейта U

$$|\psi_{out}\rangle = Z^{-m} X^{-n} U X^n Z^m |\psi\rangle = \tilde{U} |\psi\rangle \quad (30)$$

Другими словами, гейт U не применяется прямо к третьей моде, а телепортируется по ЭПР каналу, и эту процедуру можно рассматривать как процедуру приготовления состояния третьей моды, а не как процедуру действия на нее гейта. Существенный момент протокола, это возможность выполнения полного белловского измерения над 1 и 2 модами. Формула (30) описывает протокол телепортации однокубитного гейта. По аналогии можно построить протокол телепортации двухкубитного гейта. Для этого нужны два ЭПР канала, по которым телепортируется соответствующий кубит, и к четырехкубитному каналу применим двухкубитную операцию, которую надо телепортировать. Двойной телепортационный протокол запишется в виде

$$|\psi\rangle_1 \otimes |\psi_{00}\rangle_{23} \otimes |\psi_{00}\rangle_{45} \otimes |\varphi\rangle_6 \rightarrow X_3^n Z_3^m |\psi\rangle_3 \otimes X_4^k Z_4^l |\varphi\rangle_4 \otimes |\Psi_{nm}\rangle_{1,2} \otimes |\Psi_{kl}\rangle_{5,6} \quad (31)$$

Применим двухкубитный гейт U_{34} к 3 и 4 модам, получим протокол телепортации двухкубитного гейта

$$|\psi_{out}\rangle = U_{34} \cdot X_3^n Z_3^m \otimes X_4^k Z_4^l |\psi, \varphi\rangle_{34} \quad (32)$$

Нас будет интересовать случай, когда $U_{34} = W_{CZ}$ (20). Получаем протокол телепортации CZ гейта. На рис.5. взятом из работы [17], изображена оптическая схема протокола телепортации CZ гейта

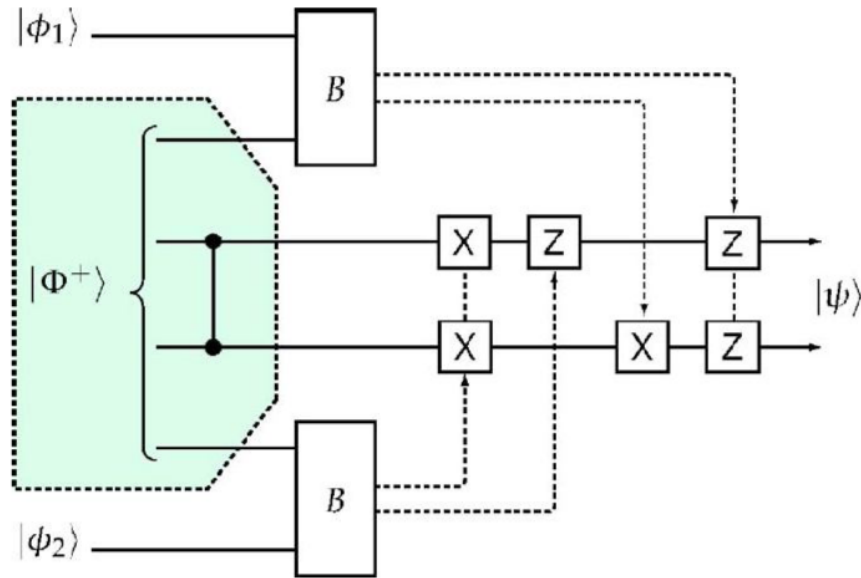


Рис. 5. Схема протокола телепортации CZ гейта. Прямоугольники B — полные белловские анализаторы двух двухкубитных состояний, прямоугольники X , Z — компенсирующие (в зависимости от результата белловского измерения) однокубитные матрицы Паули, пунктирные стрелки — управления компенсирующими преобразованиями в зависимости от классического исхода измерений. Выделенная пунктиром область — область приготовления двух ЭПР каналов, на которые действует двухкубитная CZ операция (изображенная жирными точками, соединенными жирной линией)

Привлекательность данного протокола состоит в том, что разделяются области приготовления ЭПР каналов и области действия гейта. Так, если даже гейт CZ вероятностный, то можно заранее приготовить в квантовой памяти достаточное число четырехкубитных ЭПР каналов, к которым применена сработавшая операция CZ. На рис. 5 этот заранее приготовленный канал выделен пунктирной областью приготовления. Затем, в нужный момент, запускаются белловские анализаторы, и на выходе устройства получаем требуемый результат

$$|\Psi\rangle_{out} = W_{CZ} |\phi_1, \phi_2\rangle \quad (33)$$

Так работает «телепортационный трюк» Книлла, Лафламме, Милбурна. Тем не менее данный протокол имеет существенный недостаток. Методами линейной оптики невозможно построить полный белловский анализатор [15] (альтернатива, тем не менее, существует [21]). А это означает, что мы возвращаемся снова к той же проблеме. Но теперь протокол становится вероятностным из-за свойств белловских анализаторов.

Протокол Книлла, Лафламме, Милбурна пытается справиться и с этой проблемой. Показано, что телепортация кубита с помощью неполных белловских измерений возможна с близкой к единице вероятностью, при условии, что в процессе участвуют много вспомогательных мод. На рис. 6, взятом из работы [22], представлена схема N – модовой телепортации состояния $|\psi\rangle = \alpha |0, 1\rangle_{0,a} + \beta |1, 0\rangle_{0,a}$, где $|0\rangle, |1\rangle$ – фоковские векторы.

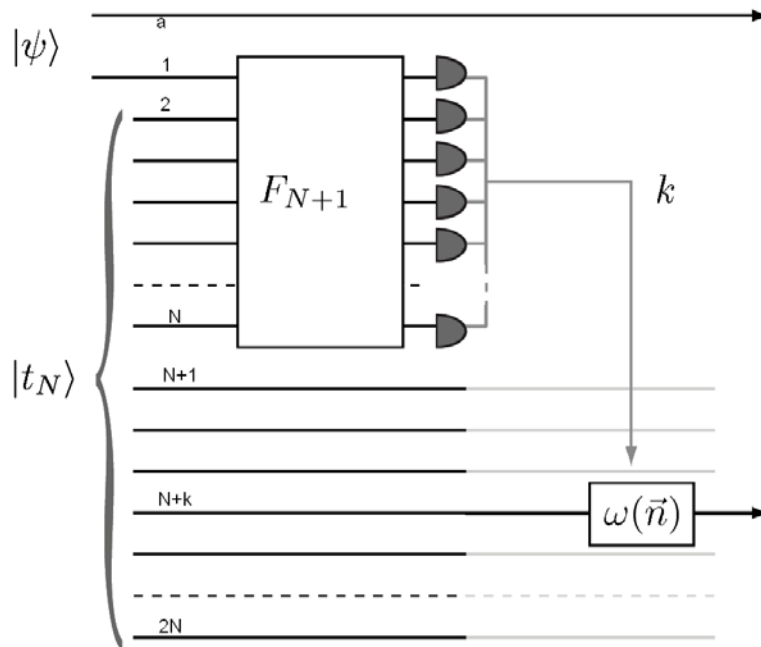


РИС. 6. Схема N модовой телепортации состояния $|\psi\rangle = \alpha|0, 1\rangle_{0,a} + \beta|1, 0\rangle_{0,a}$ с вероятностью ошибки $1/N + 1$. При срабатывании k детекторов, состояние $|\psi\rangle$ телепортируется в $N+k$.а моды (с точностью до фазового преобразования $\omega(\vec{n})$, $\vec{n} = (n_0, n_1 \dots n_N)$ (где n_i – число детектированных фотонов в моде i))

В представленном протоколе используется N пар перепутанных мод, приготовленных в состоянии $|t_N\rangle$

$$|t_N\rangle = \frac{1}{\sqrt{N+1}} \sum_{j=1}^N |1\rangle_1 \otimes \dots \otimes |1\rangle_j \otimes |0\rangle_{j+1} \otimes \dots \otimes |0\rangle_N \otimes |0\rangle_{N+1} \otimes \dots \otimes |0\rangle_{N+j} \otimes |1\rangle_{N+j+1} \otimes \dots \otimes |1\rangle_{2N} \quad (34)$$

Кубиты вспомогательных мод кодируются на состояниях пары мод с номерами $\{j, N+j\}$, $j = 1 \dots N$. Первые моды каждой пары и телепортируемая (нулевая) мода пропускаются через $N+1$ модовый преобразователь (линейное квантовое преобразование Фурье, N модовый интерферометр рис.1). Правило преобразования состояния пары мод j и k имеет вид (в формуле (2) матрица M переобозначена как матрица F_{N+1})

$$(F_{N+1})_{j,k} = \frac{1}{\sqrt{N+1}} \exp\left(2\pi i \frac{j \cdot k}{N+1}\right), \quad j, k = 0 \dots N \quad (35)$$

Такое преобразование «стирает» информацию о том по какому пути конкретные фотоны приходят на систему из $N+1$ детектора. Такое преобразование является обобщением преобразования (7) для двухкубитного светоделителя. Тогда, если идеальные, различающие фоковские состояния, N детекторов дали суммарный отсчет в k фотонов, где $0 < k < N+1$, то исходное состояние мод 0 , а будет телепортировано в состояние мод $N+k$, а. Тогда моды с номерами $N+1 \dots N+k-1$, будут в состоянии вакуума $|0\rangle$, а моды с номерами $N+k+1 \dots 2N$ будут в состоянии $|1\rangle$. Можно ввести вектор распределения детектированных k фотонов по модам $\vec{n} = (n_0, n_1 \dots n_N)$, $\sum_j n_j = k$. Тогда, для завершения протокола, необходимо выполнить дополнительное фазовое преобразование моды $N+k$ по формуле (см. рис. 6)

$$\omega(\vec{n}) = \exp\left(\frac{2\pi i}{N+1} N \sum_{j=0}^j n_j\right) \quad (36)$$

Для примера, матрица F_3 имеет вид

$$F_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \exp\left(\frac{2\pi i}{3}\right) & \exp\left(\frac{-2\pi i}{3}\right) \\ 1 & \exp\left(\frac{-2\pi i}{3}\right) & \exp\left(\frac{2\pi i}{3}\right) \end{pmatrix} \quad (37)$$

Другими словами, при обнаружении k фотонов можно заключить, что k мод отдали свои фотоны. Если у телепортируемой моды 0 детекторы «увидели» вакуумное состояние (заселенное с вероятностью $|\alpha|^2$), то это будет означать, что в моде с номером $N+k$ присутствует точно 0 фотонов. Если у телепортируемой моды детекторы «увидели» однофотонное состояние (заселенное с вероятностью $|\beta|^2$), то это будет означать, что в моде с номером $N+k$ присутствует точно 1 фотон. Это означает, что в состояние мод с номером $N+k$ произошла телепортация состояния $|\psi\rangle$. Неудачными для протокола являются два события: $k = 0$, $k = N+1$. Вероятность такой неудачи $1/N+1$. Чтобы убедиться в этом, рассмотрим существенные для данных событий, слагаемые в прямом произведении $|\psi\rangle \otimes |t_N\rangle$ векторов на входе

$$|\psi\rangle \otimes |t_N\rangle = \left(\alpha |0, 1\rangle_{0,a} + \beta |1, 0\rangle_{0,a}\right) \otimes (|0\dots 0\rangle_{1..N} \otimes |1..1\rangle_{N+1..2N} + |1\dots 1\rangle_{1..N} \otimes |0..0\rangle_{N+1..2N} + \dots) \quad (38)$$

Из анализа этих слагаемых ясно, что если $N+1$ детектор не обнаружил ни одного фотона, то есть $k=0$, то это возможно тогда, когда детекторы «увидели» состояние $\alpha |0, 1\rangle_{0,a} \otimes |0\dots 0\rangle_{1..N} \otimes |1..1\rangle_{N+1..2N}$ и после измерения получаем состояние $\alpha |1\rangle_{0,a} \otimes |1..1\rangle_{N+1..2N}$, то

есть телепортация не произошла. Вероятность такого исхода $|\alpha|^2/(N+1)$. Если детекторы обнаружили $N+1$ фотон, то такое состояние могло произойти только от слагаемого $\beta|1,0\rangle_{0,a} \otimes |1\dots 1\rangle_{1\dots N} \otimes |0\dots 0\rangle_{N+1\dots 2N}$, а так как оно одно, то полная вероятность его обнаружения равна $|\beta|^2/(N+1)$. Поэтому полная вероятность неудачи протокола равна $1/N+1$. Используя данный протокол, Книлл, Лафламме, Милбурн показали, что если приготовить $4N$ модовое состояние

$$|CZ_N\rangle = \sum_{j,k=1}^N (-1)^{(N-j)(N-k)} |1,0\rangle_1 \otimes \dots \otimes |1,0\rangle_j \otimes |0,1\rangle_{j+1} \otimes \dots \otimes |0,1\rangle_N \otimes |1,0\rangle_1 \otimes \dots \otimes |1,0\rangle_k \otimes |0,1\rangle_{k+1} \otimes \dots \otimes |0,1\rangle_N \quad (39)$$

то, применяя процедуру телепортации, аналогичную (35) к $2N+2$ модам, получаем протокол телепортации CZ операции. Состояние (39) получается с помощью последовательного применения N вероятностных CZ преобразований между модами $N+k$, $2N+k$ для $k=1\dots N$ в состоянии $|t_N, t_N\rangle$. На этапе приготовления, согласно протоколу [23], вероятность получения состояния (39) равна $1/16^N$. Окончательно, вероятность телепортации CZ гейта оказывается равной $N^2/(N+1)^2$. Итак, согласно протокола Книлла, Лафламме, Милбурна, почти детерминированная двухкубитная операция CZ возможна, но ценой привлечения значительного числа вспомогательных мод. Известны состояния протокола рис. 6, приводящие к ошибке. Это обнаружение 0 или $N+1$ фотон в состоянии телепортируемой и вспомогательных мод. Как следует из анализа, при таких событиях телепортируемое состояние $|\psi\rangle = \alpha|0,1\rangle_{0,a} + \beta|1,0\rangle_{0,a}$ трансформируется в состояние с помощью проектирования на элементы Z базиса. Если обнаружено 0 фотонов в детекторах, то состояние $|\psi\rangle$ проектируется на состояние $|0,1\rangle_{0,a}$, а при обнаружении $N+1$ фотон — проектируется на состояние $|1,0\rangle_{0,a}$. Перепишем протокол N модовой телепортации (38) для поляризационной кодировки кубитаов. Допустим, нам надо телепортировать однокубитовое состояние

$$|\psi\rangle = \alpha|H\rangle_0 + \beta|V\rangle_0 \quad (40)$$

здесь $|0\rangle_c = |H\rangle_0$, $|1\rangle_c = |V\rangle_0$ — вычислительный базис горизонтально и вертикально поляризованных состояний моды 0. Телепортация производится с помощью вспомогательных мод, разбитых на пары, в состоянии, подобном (34), где, однако, используется поляризационная кодировка и для этого необходимо иметь два фотона на пару (в отличие от (34), где приходится 1 фотон на пару перепутанных мод). Состояние $|t_N\rangle$ в этом случае имеет вид

$$|t_N\rangle = \frac{1}{\sqrt{N+1}} \sum_{j=1}^N |V\rangle_1 \otimes \dots \otimes |V\rangle_j \otimes |H\rangle_{j+1} \otimes \dots \otimes |H\rangle_N \otimes |H\rangle_{N+1} \otimes \dots \otimes |H\rangle_{N+j} \otimes |V\rangle_{N+j+1} \otimes \dots \otimes |V\rangle_{2N} \quad (41)$$

Определим операторы поляризационных мод

$$\hat{a}_k^\dagger |0\rangle = |V\rangle_k, \quad \hat{b}_k^\dagger |0\rangle = |H\rangle_k \quad (42)$$

и формулы преобразования Фурье для операторов V , H мод

$$F_{N+1}^V(\hat{a}_k^\dagger) = \frac{1}{\sqrt{N+1}} \sum_{l=0}^N \exp\left(\frac{2\pi i}{N+1} \cdot k \cdot l\right) \hat{a}_l^\dagger, \quad (43)$$

$$F_{N+1}^H(\hat{b}_k^\dagger) = \frac{1}{\sqrt{N+1}} \sum_{l=0}^N \exp\left(\frac{2\pi i}{N+1} \cdot k \cdot l\right) \hat{b}_l^\dagger$$

Операторы V , H мод преобразуются независимо. Как и в случае (38), в прямом произведении $|\psi\rangle \otimes |t_N\rangle$ состояний (40) и (41) первые $N+1$ мод подвергаются преобразованию Фурье (43), причем V , H моды преобразуются независимо с использованием неполяризованных

светоделителей, таких, как на рис.1. Затем, на выходе, фотоны кубитов (в каждой моде по фотону) пропускаются через поляризационные светоделители (14). На каждом выходе светоделителя поляризованные фотоны измеряются. Полное число измеренных фотонов (если пренебречь потерями) всегда равно $N+1$. Это свойство протокола весьма полезно, так как с его помощью можно контролировать потери фотонов. Допустим, что в моде j найдено v_j вертикальных фотонов и h_j горизонтальных. Для того чтобы понять, какое состояние мод формируется после акта измерения, рассмотрим случай $\sum_{j=0}^N v_j = N + 1$ (все детектированные фотоны вертикальны). Из вида начального состояния $|\psi\rangle \otimes |t_N\rangle$ ясно, что единственное слагаемое, ответственное за такое событие равно

$$\beta |V\rangle_0 \otimes |V\rangle_1 \otimes \dots \otimes |V\rangle_N \otimes |H\rangle_{N+1} \otimes \dots \otimes |H\rangle_{2N} \quad (44)$$

Такое состояние отвечает измерению нашего кубита в Z вычислительном базисе (в результате процедуры обнаружено состояние $\beta |V\rangle_0$ информационного кубита). Суперпозиция разрушена, телепортация не происходит, такое событие является неудачей протокола. Аналогичное событие связано со слагаемым

$$\alpha |H\rangle_0 \otimes |H\rangle_1 \otimes \dots \otimes |H\rangle_N \otimes |V\rangle_{N+1} \otimes \dots \otimes |V\rangle_{2N} \quad (45)$$

которое обнаруживается, если выполнено $\sum_{j=0}^N h_j = N + 1$. Таким образом, как и в случае двухрельсового протокола (38), вероятность неудачи равна $1/N + 1$. Все остальные события отвечают условию

$$\sum_{j=0}^N v_j = k, \quad \sum_{j=0}^N h_j = N + 1 - k, \quad k \neq 0, N + 1 \quad (46)$$

Легко убедиться, что телепортация произошла в моду с номером $N+k$ (как и в случае (38)). Протокол телепортации гейта CZ строится по аналогии с (39) [24].

Авторы протокола ЛОКВ предлагают способ оптимизации их идеи. Для снижения вероятности ошибки протокола телепортации CZ гейта можно использовать квантовый код коррекции ошибок. Так как тип ошибки телепортационного протокола известен, то это позволяет создать корректирующий код. Идею корректирующего кода рассмотрим в поляризационной кодировке, для уменьшения громоздкости записи. Согласно [20], для получения квантового корректирующего кода вводится следующее логическое кодирование

$$|0\rangle_L = |HH\rangle + |VV\rangle, \quad |1\rangle_L = |HV\rangle + |VH\rangle \quad (47)$$

Рассмотрим произвольный логический кубит в этой кодировке $\alpha |0\rangle_L + \beta |1\rangle_L$, требующий для своего создания два кубита

$$|\psi\rangle = \alpha |0\rangle_L + \beta |1\rangle_L \quad (48)$$

Если в результате измерения в Z базисе над любым кубитом получаем состояние $|H\rangle$, то закодированное от Z измерения состояние $|\psi\rangle$ (48) преобразуется в состояние обычного, до применения корректирующего кода, состояние кубита

$$\alpha |0\rangle_L + \beta |1\rangle_L \rightarrow \alpha |H\rangle + \beta |V\rangle \quad (49)$$

То есть исходный кубит из-за появившейся ошибки не теряется. Если результат измерения $|V\rangle$, то получаем декодеровку

$$\alpha |0\rangle_L + \beta |1\rangle_L \rightarrow \alpha |V\rangle + \beta |H\rangle \quad (50)$$

Применение X преобразования восстанавливает исходный кубит. Рассмотрим работу корректирующего ошибки кода (47) на примере $|t_1\rangle$ телепортации (41). Оптическая схема представлена на рис.7 [25].

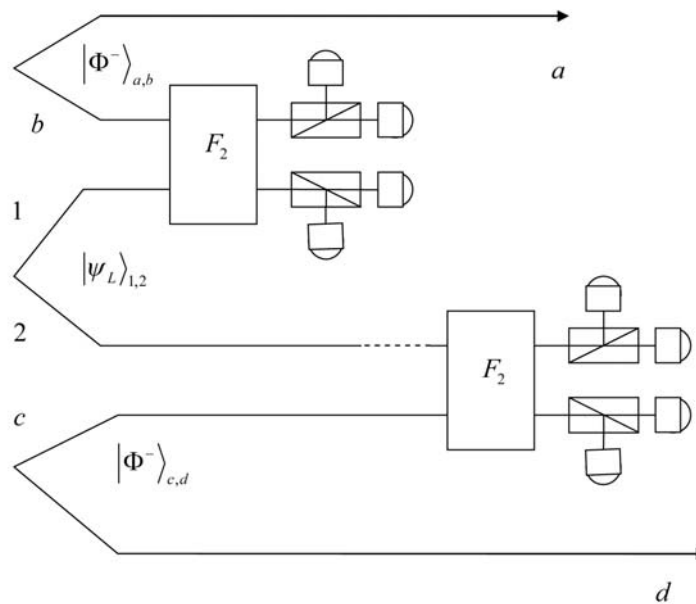


Рис. 7. Схема $|t_1\rangle$ телепортации кубита с кодом коррекции ошибок в состоянии $|\psi_L\rangle_{1,2} = \alpha |0_L\rangle_{1,2} + \beta |1_L\rangle_{1,2}$. Белловские перепутанные состояния $|\Phi^-\rangle_{a,b} = \frac{1}{\sqrt{2}} (|H, V\rangle_{a,b} - |V, H\rangle_{a,b})$ и $|\Phi^-\rangle_{c,d} = \frac{1}{\sqrt{2}} (|H, V\rangle_{c,d} - |V, H\rangle_{c,d})$. Используются поляризационные светоделители и фотодетекторы, различающие фоковские состояния на каждом выходе светоделителей

Если детекторы мод b и 1 сработали успешно (условие (46) выполнено), то измеряя состояние моды 2 и в зависимости от результата, корректируя состояние моды a, получаем в моде a телепортируемое состояние кубита $\alpha |H\rangle_a + \beta |V\rangle_a$. Если детекторы мод b и 1 показали ошибку, то есть выполнено условие $k = 0$ или $k = N + 1$ в формуле (46), то код коррекции ошибки срабатывает по схеме (49) или (50), и, выполнив соответствующую коррекцию (на рис. 7 не показаны), предпринимаем еще один акт телепортации с помощью измерений с детекторами 2 и с. В случае успеха получаем телепортируемое состояние в моде d. В случае неудачи акт телепортации невозможен. Итак, полная ошибка телепортации в протоколе рис.7 с двухступенчатой коррекцией кода при $N=1$ равна $1/4$ (без коррекции - $1/2$). Вероятность успеха - $3/4$, что совпадает с вероятностью успеха схемы без коррекции при $N=3$. Но схема с $N=3$ требует больше ресурсов, чем схема с коррекцией, в чем и состоит польза квантового кода коррекции ошибок.

5. Заключение, последние достижения

Итак, для функционирования протокола ЛОКВ необходимы: недетерминированный нелинейный гейт NS; возможность приготовления состояния $|t_N\rangle$, необходимого для почти

детерминированной телепортации; телепортация кубита с вероятностью ошибки $1/N + 1$; телепортация CZ гейта с вероятностью успеха $(N/N + 1)^2$; применение квантового корректирующего кода для повышения вероятности успеха протокола телепортации; коды, корректирующие фазовые ошибки; коды, корректирующие ошибки потери фотонов; коды коррекции с каскадной структурой; оптимизированные архитектуры квантовой оптической сети, осуществляющей ЛОКВ.

Хотя в принципе предложенный протокол масштабируем, то есть число элементов полиномиально зависит от числа кубитов, тем не менее требует большой затраты ресурсов. Ряд предложений, связанных с введением кодов, корректирующих ошибки, открытием кластерных состояний, существенно улучшают конструкцию квантового оптического компьютера. Кроме вышесказанного, существенно необходимо повысить эффективность источников единичных фотонов, развить технологию изготовления оптических сетей с низким поглощением, создать высокоэффективные детекторы одиночных фотонов, различающие фоковские состояния света. За последнюю декаду, с момента формулирования протокола ЛОКВ в 2001 году [20], возможность отдельных элементов протокола экспериментально и теоретически обоснована. Разработаны несколько моделей ЛОКВ. Токовая (циклическая) модель представляет собой последовательность унитарных операций, совершаемых, согласно квантовому алгоритму, над N – кубитным состоянием регистра. Любая унитарная операция над N – кубитным состоянием может быть разбита на элементарные одно и двухкубитные операции, набор которых должен быть полным. Носители информации – кубиты – различимы. Поэтому можно ввести траекторию, по которой производится алгоритм – вычислительная процедура – от начального состояния до конечного. Такой протокол называется токовой моделью. Функционирование отдельных элементов токовой модели продемонстрировано в ряде работ. В работах [26-29] экспериментально показана возможность создания вероятностной операции контролируемого НЕТ методами линейной оптики на единичных фотонах, основной операции в протоколе ЛОКВ. В работах [30,31] разработаны новые теоретические протоколы квантовой коррекции ошибок против Z измерений и потери фотонов, в работах [32,33] работа кодов, корректирующих ошибки в состояниях оптических кубитов, продемонстрирована экспериментально. В 2001 году была предложена альтернатива токовой модели [34]. Здесь вычисление в квантовом компьютере начинается с большого перепутанного состояния многих кубитов (кластерное состояние), над кубитами производится однокубитовые измерения, слева на право, постепенно считывая и телепортируя информацию по состоянию направо. Теория кластерной архитектуры была усовершенствована в работах [35,36]. Экспериментально перепутанные оптические кластерные состояния были получены в работах [37-40]. Для успешной работы протокола ЛОКВ необходимы, близкие к идеальным, однофотонные элементы – детекторы и источники. Пути оптимизации этих приборов намечены в работе [41]. Источники одиночных фотонов с приемлемыми характеристиками, основанные на азотных вакансиях в алмазе, квантовых точках в полупроводнике, на излучении отдельных атомов, захваченных в ловушках, продемонстрированы в работах [42-44]. Предложено несколько экспериментальных схем фотодетекторов, различающих фоковские состояния фотонов в работах [45-48]. Для создания оптических сетей, на которых будет функционировать протокол ЛОКВ, обладающих улучшенными характеристиками по поглощению, требованиями миниатюризации, масштабированности, стабильности, контролируемости, воспроизводимости, необходимо использовать архитектуру интегральной оптики. Оптические чипы, удовлетворяющие этим требованиям. Получены экспериментально в работах [49-54]. В заключение сошлемся на весьма оптимистичную работу [55], где дана оценка порога устойчивости работы протокола ЛОКВ при использовании неидеальных детекторов и источников одиночных фотонов.

Здесь показано, что если произведение эффективности используемого детектора и источника больше $2/3$, то протокол ЛОКВ эффективен. Эта оценка существенно более оптимистична, чем это обычно допускается при анализе отказоустойчивости тестируемой аппаратуры.

Работа частично поддержана ФЦП «Научные и научно-педагогические кадры инновационной России» (контракты Р689 НК-526Р, 14.740.11.0879 и 16.740.11.0030, грант 2012-1.2.2-12-000-1001-047), грантом 11-08-00267 РФФИ, ФЦП «Исследования и разработки по приоритетным направлениям развития научного и технологического комплекса России 2007-2013» (контракт 07.514.11.4146).

Литература

- [1] Хопкрофт Дж., Мотвани Р., Ульман Дж. Введение в теорию автоматов, языков и вычислений. — М.: «Вильямс», 2002. — 528с.
- [2] Манин Ю. И. Вычислимое и невычислимое. — М.: Сов. Радио, 1980. — 128с.
- [3] Feynman R. Simulating Physics with Computers // Inter. Jour. Theor. Phys. — 1982. — V.21, №6/7. — P. 467–488.
- [4] Cirac J.I., Zoller P. Quantum Computations with Cold Trapped Ions // Phys. Rev. Lett. — 1995. — V.74. — P.4091–4094.
- [5] Gershenfeld N.A., Chuang I.L. Bulk spin resonance quantum computation // Science. — 1997. — V.275. — P.350–356.
- [6] Yu. A. Pashkin, T. Yamamoto, O. Astafiev, Y. Nakamura, D. V. Averin, J. S. Tsai. Quantum oscillations in two coupled charge qubits. // Nature. — 2003. — P.421 823.
- [7] J. Martinis, S. Nam, J. Aumentado, and C. Urbina. Rabi oscillations in a large Josephson-junction qubit // Phys. Rev. Lett. — 2002. — V.89. — P.117901.
- [8] B. Kane. A silicon-based nuclear spin quantum computer// Nature. — 1998. — V.393. — P.133.
- [9] D. Loss and D. P. DiVincenzo, "Quantum computation with quantum dots"// Phys. Rev. — 1998. — V.57. — P.120.
- [10] Kitaev A. Yu., quant-ph/9707021
- [11] Оптические вычисления. Под ред. Р. Аратуна. — М.: Мир, 1993. — 441 с.
- [12] Скалли М. О., Зубайри М. С. Квантовая оптика: Пер. с англ. / Под ред. В.В. Самарцева. — М.: ФИЗМАТЛИТ, 2003. — 512с.
- [13] Reck M., Zeilinger A., Bernstein H. J., and Bertani P. Experimental realization of any discrete unitary operator// Phys. Rev. Lett. — 1994. — V.73, №58.
- [14] Casey Robert Myers. Investigating Photonic Quantum Computation. A thesis of the degree of Doctor of Philosophy in Physics // Waterloo, Ontario, Canada, 2007.
- [15] Lutkenhaus N., Calsamiglia J., Suominen K. A. Bell measurements for teleportation // Phys. Rev. A. — 1999. — V.59. — 3295.
- [16] Cerf, N. J., Adami C., Kwiat P. G. // Phys. Rev. A — 1998. — V.57. — R1477.
- [17] Pieter Kok, Munro W. J., Kae Nemoto, Ralph T. C., Jonathan P. Dowling, Milburn G. J. Linear optical quantum computing with photonic qubits // Rev. Mod. Phys. — 2007. — V.79, №1.
- [18] Hong C. K., Ou Z. Y., Mandel L. Measurement of subpicosecond time intervals between two photons by interference // Phys. Rev. Lett. — 1987. — V.59. — P.2044–2046.
- [19] Milburn, G. J. Quantum Optical Fredkin Gate // Phys. Rev. Lett. — 1998. — V.62. — 2124.
- [20] Knill E., Laflamme R. Milburn G. J. A scheme for efficient quantum computation with linear optics // Nature London. — 2001. — 409, 46.
- [21] Miroshnichenko G. P. Discrete photodetection for protocols of linear optical quantum calculations and communications // Journal of Experimental and Theoretical Physics. — 2011. — V.112, № 6. — P.923–931.
- [22] Pieter Kok & Brendon W. Lovett. Introduction to Optical Quantum Information Processing. — Cambridge University Press, 1 edition, May 31, 2010.
- [23] Franson J.D., Donegan M.M., Jacobs B.C. Generation of entangled ancilla states for use in linear optics quantum computing // Phys. Rev. A. — 2004. — V.69. — P.052328.
- [24] Federico M. Spedalieri, Hwang Lee, Jonathan P. Dowling. High-fidelity linear optical quantum computing with polarization encoding // Physical Review A. — 2006. — V.73. — P.012334.
- [25] O'Brien J. L., Pryde G. J., White A. G., Ralph T. C. High-Fidelity Z-Measurement Error Correction of Optical Qubits. arXiv:quant-ph/0408064v1 10 Aug 2004.

- [26] Pittman T. B., Fitch M. J., Jacobs B. C., Franson J. D. Experimental controlled-NOT logic gate for single photons in the coincidence basis. // *Physical Review A*. — 2003. — V.68. — P.032316.
- [27] O'Brien J. L., Pryde G. J., White A. G., Ralph T. C., Branning D. Demonstration of an all-optical quantum controlled-NOT gate // *Nature*. — 2003. — V.426. — 264.
- [28] O'Brien J. L., Pryde G. J., Gilchrist A., James D. F.V., Langford N. K., Ralph T. C., White A.G. Quantum Process Tomography of a Controlled-NOT Gate // *Phys. Rev. Lett.* — 2004. — V.93. — P.080502.
- [29] Sara Gasparoni, Jian-Wei Pan, Philip Walther, Terry Rudolph, and Anton Zeilinger. Realization of a Photonic Controlled-NOT Gate Sufficient for Quantum Computation // *Phys. Rev. Lett.* — 2004. — V.93. — P.020504.
- [30] Ben Criger, Osama Moussa, Raymond Laamme. Quantum Error Correction with Mixed Ancilla Qubits. arXiv:1201.1517v2 [quant-ph] 8 Mar 2012.
- [31] Ralph T. C., Hayes A. J. F., Gilchrist A. Loss-Tolerant Optical Qubits // *Phys. Rev. Lett.* — 2005. — V.95. — P.100501.
- [32] O'Brien J. L., Pryde G. J., White A. G., Ralph T. C. High-fidelity Z -measurement error encoding of optical qubits // *Phys. Rev. A*. — 2005. — V.71. — P.060303.
- [33] Pittman T. B., Jacobs B. C., Franson J. D. Demonstration of quantum error correction using linear optics // *Phys. Rev. A*. — 2005. — V.71. — P.052332.
- [34] Robert Raussendorf and Hans J. Briegel. A One-Way Quantum Computer // *Phys. Rev. Lett.* — 2001. — V.86. — 5188.
- [35] Michael A. Nielsen. Optical Quantum Computation Using Cluster States // *Phys. Rev. Lett.* — 2004. — V.93. — P.040503.
- [36] Daniel E. Browne and Terry Rudolph. Resource-Efficient Linear Optical Quantum Computation // *Phys. Rev. Lett.* — 2005. — V.95. — P.010501.
- [37] Walther P., Resch K. J., Rudolph T., Schenck E., Weinfurter H., Vedral V., Aspelmeyer M., Zeilinger A. Experimental one-way quantum computing // *Nature*. — 2005. — V.434. — 169.
- [38] Nikolai Kiesel, Christian Schmid, Ulrich Weber, Geza Toth, Otfried Gühne, Rupert Ursin, and Harald Weinfurter. Experimental Analysis of a Four-Qubit Photon Cluster State. *Phys. Rev. Lett.* 95, 210502 (2005).
- [39] Robert Prevedel, Philip Walther, Felix Tiefenbacher, Pascal Bohi, Rainer Kaltenbaek, Thomas Jennewein, Anton Zeilinger. High-speed linear optics quantum computing using active feed-forward // *Nature*. — 2007. — V.445. — 65.
- [40] C.Y. Lu et al. Experimental entanglement of six photons in graph states // *Nat. Phys.* — 2007. — V.3. — 91.
- [41] Thomas Jennewein, Marco Barbieri, Andrew G. White. Single-photon device requirements for operating linear optics quantum computing outside the post-selection basis // *Journal of Modern Optics*. — 2011. — V.58. — P.276–287.
- [42] Sylvain Fasel, Olivier Alibart, Sebastien Tanzilli, Pascal Baldi, Alexios Beveratos, Nicolas Gisin, Hugo Zbinden. High-quality asynchronous heralded single-photon source at telecom wavelength // *New J. Phys.* — 2004. — 6.
- [43] Markus Hiljkema, Bernhard Weber, Holger P. Specht, Simon C. Webster, Axel Kuhn, and Gerhard Rempe. A single-photon server with just one atom // *Nature Phys.* — 2007. — V.3. — P.253–255.
- [44] Andrew J. Shields. Semiconductor quantum light sources // *Nature Photon.* — 2007. — V.1. — P.215–223.
- [45] Kardynal B. E., Yuan Z. L., Shields A. J. An avalanche-photodiode-based photon-number-resolving detector // *Nature photonics*. — 2008. — V.2. — 425.
- [46] Adriana E. Lita, Aaron J. Miller, Sae Woo Nam. Counting near-infrared single-photons with 95% efficiency // *Opt. Express*. — 2008. — V.16. — P.3032–3040.
- [47] Miki S., Fujiwara M., Sasaki M., Baek B., Miller A. J., Hadfield R. H., Nam S. W., Wang Z. Large sensitive-area nbn nanowire superconducting single-photon detectors fabricated on single-crystal MgO substrates // *Appl. Phys. Lett.* — 2008. — V.92. — P.061116.
- [48] Aleksander Divochiy, Francesco Marsili, David Bitauld, Alessandro Gaggero, Roberto Leoni, Francesco Mattioli, Alexander Korneev, Vitaliy Seleznev, Nataliya Kaurova, Olga Minaeva, Gregory Gol'tsman, Konstantinos G. Lagoudakis, Moushab Benkhaoul, Francis Levy, Andrea Fiore. Superconducting nanowire photon-number-resolving detector at telecommunication wavelengths // *Nature Photon.* — 2008. — V.2. — P.302–306.
- [49] Brian J. Smith, Dmytro Kundys, Nicholas Thomas-Peter, Smith P. G. R., Walmsley I. A. Phase-controlled integrated photonic quantum circuits. arXiv:0905.2933v2 [quant-ph] 23 Sep 2009.
- [50] Alberto Politi, Martin J. Cryan, John G. Rarity, Siyuan Yu, Jeremy L. O'Brien. Silica-on-Silicon Waveguide Quantum Circuits // *Science*. — 2008. — V.320. — 646.

- [51] Alberto Politi, Jonathan C. F. Matthews, Jeremy L. O'Brien. Shor's Quantum Factoring Algorithm on a Photonic Chip // Science. — 2009. — V.325. — 1221.
- [52] Alberto Peruzzo et al. Quantum Walks of Correlated Photons // Science. — 2010. — V.329. — 1500.
- [53] Ryo Okamoto, Jeremy L. O'Brien, Holger F. Hofmann, Shigeki Takeuchi Realization of a Knill-Laflamme-Milburn C-NOT gate –a photonic quantum circuit combining effective optical nonlinearities. arXiv:1006.4743v1 [quant-ph] 24 Jun 2010.
- [54] Damien Bonneau et al. Quantum interference and manipulation of entanglement in silicon wire waveguide quantum circuits. arXiv:1201.6537v1 [quant-ph] 31 Jan 2012.
- [55] Michael Varnava, Daniel E. Browne, and Terry Rudolph. How good must single photon sources and detectors be for efficient linear optical quantum computation? arXiv:quant-ph/0702044v2 20 Jul 2007.