PACS: 03.67.Lx, 03.67.Ac, 03.67.Pp

ТОПОЛОГИЧЕСКИЕ МЕТОДЫ В КВАНТОВЫХ ВЫЧИСЛЕНИЯХ

С.А. Дуплий[1], И.И. Шаповал[2]
[1]*Харьковский национальный университет*
пл. Свободи 4, Харьков, 61077, Украина
e-mail: sduplij@gmail.com
[2]*Национальный научный центр "Харьковский Физико-Технический Институт"*
ул. Академическая 1, Харьков, 61108, Украина
e-mail: ishapoval@kipt.kharkov.ua
Поступила в редакцию 1 сентября 2007 г.

Рассмотрены основные концепции квантовой теории информации, принципы квантовых вычислений и возможность создания на их основе уникального по вычислительной мощности и принципу функционирования устройства — квантового компьютера. Представлены основные блоки квантовой логики, схемы реализации квантовых вычислений, а также известные сегодня эффективные квантовые алгоритмы, которые призваны воплотить преимущества квантовых вычислений над классическими. Среди них особое место занимают алгоритм Шора факторизации чисел и алгоритм Гровера поиска в неупорядоченных базах данных. Описано явление декогеренции, её влияние на стабильность квантового компьютера и методы коррекции квантовых ошибок. Изложена концепция топологического квантового вычисления, которое не обладает большей вычислительной мощностью по сравнению с обычным квантовым вычислением, но обладает естественной помехоустойчивостью. Показана необходимость анионной статистики его кубитов и представлена наглядная анионная модель реализации топологического квантового вычисления.
КЛЮЧЕВЫЕ СЛОВА: квантовые вычисления, квантовые алгоритмы, помехоустойчивость, декогеренция, топологические квантовые вычисления, теория кос, анионы.

Развитие квантовой физики показало, что, если в XX веке квантовая теория осуществила переворот в понимании природы, то в XXI — может осуществить революцию в теории компьютерных вычислений. Исходя из «закона Мура» (об экспоненциальной миниатюризации), к 2020 году процесс уменьшения размеров элементной базы вычислительной техники может столкнуться с тем, что элементарные блоки устройств-носителей информации и процессоров классического (тьюрингового) компьютера достигли размеров, сравнимых с атомными, и более не могут корректно описываться в рамках классической физики и соответствующих методов вычислений. Так что очевидно — дальнейшее развитие компьютерных технологий невозможно без смены аппарата теории вычислений, основывающейся на классической физике, на аппарат, базирующийся на квантовой механике.

Существенное отличие квантовых законов от классических требует пересмотра всей теории вычислений, чтобы составить представление об особенностях в принципах функционирования квантового компьютера, о его преимуществах и недостатках по сравнению с обычным компьютером. И уже сегодня ясно, что, преодолевая проблему миниатюризации компьютерных устройств и переходя к квантовой модели обработки данных, приобретается нечто гораздо большее, чем возможность дальнейшего уменьшения аппаратных составляющих компьютера. А именно, получаем доступ к потенциально огромному вычислительному ресурсу, существующему исключительно благодаря квантово-механическим свойствам физических систем (суперпозиции квантовых состояний и их запутыванию) и квантовых механизмов, позволяющих оперировать квантовой информацией. Переход от классического носителя информации (бита) к квантовому (кубиту) приводит к тому, что информационный «объём» квантового регистра экспоненциально возрастает при увеличении числа кубитов. К примеру, квантовый регистр, содержащий 300 кубитов, может нести в себе информацию о 10^{90} классических 300-битовых состояниях, что намного больше числа атомов во Вселенной. И, что ещё важнее, само вычисление на n-кубитном квантовом компьютере, которое осуществляется в процессе унитарной эволюции квантовой системы, происходит по 2^n каналам общей волновой функции одновременно, поскольку в этом случае она является суперпозицией 2^n возможных классических состояний битов [1].

В настоящее время известно уже несколько задач, в решении которых квантовый компьютер мог бы оказаться более эффективным по сравнению с классическим компьютером. Прежде всего, это проблема факторизации больших чисел на простые множители. На классических компьютерах наилучшие известные алгоритмы факторизации выполняются за $O\left[exp\left[(64/9)^{1/3}(\ln N)^{1/3}(\ln\ln N)^{2/3}\right]\right]$ шагов, где N — входное число, а $\ln N$ — длина входа [2]. Таким образом, такого рода алгоритмы растут экспоненциально с размером входных данных N, что является непреодолимой преградой для современной компьютерной техники уже для 250–значного числа. Для примера скажем, что в 1994 году было успешно факторизовано 129–значное число (известное как ключ RSA129) с использованием такого алгоритма на приблизительно 1600 классических компьютерах [3]. Полная факторизация заняла 8 месяцев. Факторизация уже, например, 250–значного числа (ключ RSA250) на этом же

кластере заняла бы $8 \cdot 10^5$ лет, а 1000-значного — 10^{25} лет (что значительно превышает возраст Вселенной). Однако в том же 1994 году был разработан алгоритм для факторизации чисел на квантовом компьютере, который реализуется за $O[(\log N)^{2+e}]$ шагов, где e — некоторое малое число [4]. Впоследствии он получил название алгоритма Шора. Он приблизительно квадратично зависит от размера входных данных (что принято считать быстрым алгоритмом), поэтому факторизация 1000–значного числа с помощью такого алгоритма потребует лишь несколько миллионов шагов (а факторизация числа $N \sim 2^{800}$ при скорости вычислений 10^6 операций в секунду потребовала бы всего несколько дней). Следует отметить, что это представляет собой прямую угрозу для большинства современных криптосистем (RSA, EIGamal, DiffieHellman), основанным на факторизации. Например, 250–значный открытый код считается нефакторизуемым за «разумное» время на современной вычислительной технике. Экспоненциальное улучшение временных характеристик квантовых алгоритмов происходит за счёт квантового параллелизма. Таким образом, полученное на выходе квантового компьютера решение представляет собой интерференцию результатов параллельных вычислений.

Другим наиболее важным для физиков применением квантового компьютера может стать моделирование квантово-механических систем. Увеличение производительности подобных алгоритмов может быть того же порядка, что и для алгоритмов факторизации. В этом применении квантовый компьютер станет важнейшим инструментом моделирования в таких областях науки, как квантовая физика, химия, материаловедение, нанотехнологии, биология и медицина. Все они сегодня ограничены низкой скоростью моделирования квантовых систем. Так, в 1982 году Р. Фейнман показал [5], что квантовая система не может быть адекватно промоделирована классическими методами, и что для этих целей необходим квантовый компьютер. В качестве примера подобного применения квантового компьютера может служить исследование квантового хаоса. Оказывается, что квантовое baker-map, являющееся прототипом отображений, появляющихся в теории квантового хаоса, относительно просто реализуется с помощью квантовых гейтов, и его экспериментальная реализация представляется возможным в ближайшем будущем. Для подобных исследований достаточно уже 3–кубитного квантового компьютера. В результате возможно найти экспериментальное доказательство для сверхчувствительности к возмущениям — предполагаемой теоретико-информационной характеристики квантового хаоса [6, 7].

Не столь большое преимущество как в предыдущих алгоритмах, будет иметь квантовый компьютер над классическим и в проблеме поиска в неупорядоченных базах данных. Алгоритм, созданный для этих целей, получил название алгоритма Гровера. Чтобы выделить искомый элемент в неупорядоченной базе данных с вероятностью большей, чем 50%, любой классический алгоритм (как детерминистический, так и вероятностный) потребует обращения к базе данных как минимум *N/2* раз. Квантово-механическая система же может находиться в суперпозиции состояний и одновременно проверять множество элементов. При надлежащем задании программы поиска вычисления искомого состояния на каждом этапе усиливают друг друга, в то время как остальные интерферируют случайным образом. В результате нужный элемент может быть найден лишь за $O\left[\sqrt{N}\right]$ обращений к базе данных, в то время как классический поиск осуществляется за $O[N]$ шагов, что говорит о квадратичном преимуществе квантового механизма поиска [8].

Ясно, что реализация квантового компьютера представляет собой нетривиальную техническую задачу. Перечисленные квантовые алгоритмы — одни из наиболее перспективных разработанных приложений, которые могут быть реализованы на квантовых компьютерах. Дополнительно можно указать на следующие: поиск разложений целого *N* по уравнению Пелла ($x^2 - dy^2 = N$, где *x*, *y*, *d* — целые числа) с экспоненциальным ускорением, поиск периода (вычисления в теории групп), Гауссовы суммы, задача смещённого символа Лежандра, алгоритм Раза (распределённое моделирование), управление сложностью: непересекающиеся подмножества, конечно-циклические интерактивные доказательства, псевдо-телепатия (неравенства Белла, ведение игры), квантовая криптография, квантовая защита информации и скрытое разделение ресурсов, квантовая цифровая подпись. Но представляется, что самым эффективным использованием квантовых машин станет моделирование реальных квантовых систем, что найдет применение в химии, материаловедении, нанотехнологиях, биологии и медицине. Поэтому для реализации производства первых полнофункциональных, а затем и серийных квантовых компьютеров, необходимы междисциплинарные усилия на новом технологическом уровне.

В данной работе рассмотрена краткая история становления, основные принципы функционирования квантового компьютера, перечисленные выше алгоритмы. Более подробно остановимся на основной проблеме осуществления экспериментальных реализаций квантовых компьютеров и методах её преодоления. Вторая часть обзора будет посвящена наиболее обещающей концепции борьбы с разрушающим воздействием внешней среды на квантовое вычисление — топологическому квантовому вычислению. Вначале сделаем небольшой исторический экскурс развития области квантовых вычислений.

КРАТКАЯ ИСТОРИЯ КВАНТОВЫХ ВЫЧИСЛЕНИЙ

1970-ые годы

1970 г. — Стивен Виснер изобретает сопряженное кодирование [9].

1973 г. — Александр Холево издаёт статью, в которой показывает, что *L* кубитов не может нести больше информации, чем *L* классических битов (результат, известный как "теорема Холево" или "предел Холево") [10].

1975 г. — Р.П. Поплавский издаёт статью «Термодинамические модели обработки информации» [11], где показывает невыполнимость адекватного численного моделирования квантовых систем на классических компьютерах, обусловленную принципом суперпозиции.

1976 г. — польский математик Роман Ингарден, в одной из первых попыток создания квантовой теории информации, показывает, что теория информации Шеннона не может непосредственно быть обобщена на квантовый случай, и необходимо построить обобщение теории Шеннона для создания квантовой теории информации [12].

1980-ые годы

1980 г. — Ю.И. Манин, издаёт "Вычисляемое и невычисляемое", Москва, Советское Радио. В этой работе используется экспоненциальное число базисных состояний, необходимых для описания эволюции квантовой системы, и обсуждается потребность в теории квантового вычисления, которая охватывает фундаментальные принципы вычисления без обращения к физической реализации.

1981 г. — Р. Фейнман в докладе на первой конференции по физике вычислений, проведённой в Массачусетском технологическом институте, отметил, что невозможно моделировать эволюцию квантовой системы на классическом компьютере эффективным способом [5]. Он предложил элементарную модель квантового компьютера, который будет способен провести такое моделирование. Томмазо Тоффоли ввёл обратимые гейты Тоффоли [13], которые вместе с гейтами NOT и XOR составляют универсальное множество необходимое для квантового вычисления.

1984 г. — Чарльз Беннетт и Жилль Брассард используют сопряженное кодирование Виснера для распределения криптографических ключей [14].

1985 г. — Дэвид Дойч описал первый универсальный квантовый компьютер [15]. Так же, как универсальная машина Тьюринга может эффективно моделировать любую другую машину Тьюринга, так и универсальный квантовый компьютер в состоянии моделировать любой другой квантовый компьютер с не более чем полиномиальным замедлением.

1990-ые годы

1991 г. — Артур Экерт разрабатывает безопасную коммуникацию, основывающуюся на запутанности квантовых состояний [16].

1993 г. — Дэн Саймон из университета Монреаля, выдвигает проблему оракула, в решении которой квантовый компьютер будет экспоненциально быстрее, чем обычный компьютер. Этот алгоритм вводил основные идеи, которые затем были положены в основу алгоритма факторизации Питера Шора.

1994 г. — Питер Шор в Нью-Джерси разработал замечательный алгоритм для квантового компьютера, предназначенный для факторизации больших целых чисел и решения проблемы дискретного логарифма [4]. Применением алгоритма Шора может стать взлом многих из используемых сегодня криптосистем. Его разработка привела к рождению огромного интереса к квантовым компьютерам, даже вне физического сообщества. В декабре, Игнасио Сирак из университета Сьюдад-Реаль и Питер Золлер из университета Иннсбрука предложили экспериментальную реализацию гейта "управляемое-НЕ" (CNOT) на удерживаемых в ловушке ионах [17].

1995 г. — Питер Шор и Эндрю Стин предложили первые схемы коррекции квантовых ошибок — подход к созданию таких квантовых компьютеров, которые могли бы проводить квантовые вычисления используя большое количестве кубитов в течении продолжительного промежутка времени [18]. Ошибки всегда вводятся средой, но квантовая коррекция ошибок могла бы преодолеть эту проблему и стать ключом для технологии построения крупномасштабных рабочих квантовых компьютеров. Эти ранние предложения имели множество ограничений. Они могли исправлять некоторые ошибки, но не те, которые возникают непосредственно в процессе самого исправления. Предложено множество усовершенствований, и продолжается активное исследование этого вопроса. Была найдена альтернатива квантовой коррекции ошибок: вместо того чтобы активно исправлять ошибки, вызванные взаимодействием со средой, можно использовать специальные состояния, которые имеют "иммунитет" к ошибкам. Этот подход, основывающийся на свободных от декогеренции подпространствах состояний, предполагает, что есть некоторая симметрия во взаимодействии компьютер-среда. Кристофер Монро и Дэвид Винеланд в Национальном институте стандартов и технологии (Валун, Колорадо) экспериментально реализуют первый квантовый логический гейт CNOT на удерживаемых в ловушке ионах согласно предложению Золлера и Сирака [19].

1996 г. — Лов Гровер из научно-исследовательской лаборатории Белла, создаёт квантовый алгоритм поиска в неупорядоченной базе данных [8]. Квадратичное ускорение здесь не является столь же драматическим как ускорение факторизации, решения проблемы дискретного логарифма или моделирования квантовой физики. Однако алгоритм может быть применен к намного более широкому спектру проблем. Любая задача, которая должна была решаться случайным поиском (решение задачи "в лоб"), может теперь иметь квадратичное ускорение в своём решении.

1997 г. — Дэвид Корай, Амр Фахмай и Тимоти Хавэль [20], и в то же самое время Нейл Джершенфелд и Айзек Л. Чуанг в Массачусетском технологическом институте [21], опубликовали первые статьи о квантовых компьютерах, основанных на объёмном спиновом резонансе, или тепловых ансамблях. В их постановке компь-

ютер — это фактически единственная молекула, которая кодирует кубиты в спинах её протонов и нейтронов. Триллионы триллионов из них могут плавать в чашке воды. Эта чашка помещается в ЯМР-устройство (ЯМР-ядерный магнитный резонанс), подобное ЯМР-томографам, используемым в медицине. Такая совокупность комнатно-температурных (тепловых) молекул (ансамбля) обладает большой степенью дублирования, которая позволяет поддерживать когерентность состояний в течение нескольких секунд, что намного лучше показателей других предложенных систем.

1998 г. — первый рабочий 2-кубитный ЯМР-компьютер, продемонстрированный Джонатаном А. Джонсом и Микеле Моска в Оксфордском университете [22], и в то же время Айзеком Л. Чуангом в исследовательском центре Альмадена (*IBM*) вместе с сотрудниками Стэнфордского Университета и Массачусетского технологического института [23].

Первый рабочий 3-кубитный ЯМР-компьютер. Первое выполнение алгоритма Гровера [24].

2000-ые годы

2000 г. — первый рабочий 5-кубитный ЯМР-компьютер демонстрируется в Техническом Университете Мюнхена.

Первое осуществление нахождения порядка (часть алгоритма Шора) в исследовательском центре Альмадена и Стэнфордском университете.

Первый рабочий 7-кубитный ЯМР-компьютер демонстрируется в национальной лаборатории Лос-Аламоса.

2001 г. — первое выполнение алгоритма Шора в исследовательском центре Альмадена (*IBM*) и Стэнфордском университете. Было факторизовано число 15, используя 10^{18} идентичных молекул, содержащих 7 активных ядерных спинов.

2002 г. — Проект Ориентиров Квантовой Информатики и Технологии, вовлекший некоторых из основных разработчиков данной области, концентрирующий стратегию развития Квантовой информатики [25].

2004 г. — первый рабочий квантовый ЯМР-компьютер на чистых состояниях (основанный на параводороде) демонстрируется в Оксфордском университете и университете Йорка [26].

2005 г. — д-р Мэтью Селларс Центра лазерной физики в австралийском Национальном университете в Канберре замедлила световой импульс до нескольких сотен метров в секунду. Замедление скорости света позволяет отобразить информацию на световой импульс, подобно операциям с памятью обычного компьютера. Чтобы замедлять свет, исследователи использовали силикатный кристалл, смешанный с редкоземельным металлом празеодимием [27].

В статье, изданной в ноябрьском выпуске журнала *Nature*, исследователи Грузинского технологического института сообщили о получении экспериментального доказательства того, что когерентность также распространяется на внутренние спиновые степени свободы в атомном конденсате Бозе-Эйнштейна.

Учёные из университета Иллинойса в Urbana-Champaign демонстрируют квантовую запутанность нескольких характеристик, потенциально позволяющую кодирование нескольких кубитов в одной частице.

Две группы физиков впервые измерили ёмкость джозефсоновского перехода. Методы могут использоваться для измерения состояний кубитов в квантовом компьютере, не нарушая само состояние [28].

В декабре, объявлено создание первого квантового байта, или кубайта, учёными из института Квантовой Оптики и Квантовой Информации в университете Инсбрука (Австрия) [29].

Исследователи из университета Гарварда и Грузинского технологического института преуспели в передаче квантовой информации между "квантовыми блоками памяти" — от атомов фотонам и наоборот.

Ученые из Национального Института Стандартов и Технологии добились ориентировки спинов шести атомов в двух противоположных направлениях одновременно.

Масштабируемый квантово-компьютерный полупроводниковый чип, удерживающий ионные кубиты, был впервые сконструирован исследователями университета Мичигана, что подало надежды на построение практического квантового компьютера, используя обычную полупроводниковую технологию.

2006 г. — группа по обработке квантовой информации лаборатории *Hewlett-Packard* находит способы использования фотонов, или лёгких частиц, для обработки информации, а не электронов, используемых в цифровых электронно-вычислительных машинах сегодня. Их работа подаёт надежды на разработку более быстрых, более мощных и более безопасных компьютерных сетей.

Питер Золлер из университета Инсбрука в Австрии, обнаруживает, что метод использования криогенных полярных молекул делает квантовые блоки памяти стабильными [30].

Профессор Винпенни в Манчестерской школе химии впервые продемонстрировал, как металлосодержащие кольца, которые обладают свойствами, необходимыми для функционирования в роли кубитов, могут быть связаны вместе с использованием и органических, и металлоорганических фрагментов. Исследователи Кембриджского университета и компании Тошиба представляют новое квантовое устройство, которое генерирует запутанные фотоны.

Джон Мортон и Саймон Бенжамин из Оксфордского факультета материаловедения, заперли кубит в фуллерене. Это изолировало кубит до некоторой степени, но недостаточно [31]. Следующий шаг, который сделали исследователи, состоял в применении так называемого «скорострельного» метода (“bang-bang method”): кубит неоднократно обстреливается интенсивным микроволновым импульсом, который полностью меняет характер взаимодействия кубита со средой, но позволяет сохранять состояние кубита. Метод "bang-bang" — шаг на пути к построению квантовых прототипов суперкомпьютеров, сконструированных на основе высокотемпературных сверхпроводников, который мог бы стать, согласно экспериментам, выполненным физиками технологического университета Чалмерса (Гетеборг, Швеция), основой квантовой вычислительной техники. Работая с группой из итальянского университета Аквилы, физики непосредственно наблюдали макроскопические квантовые эффекты в высокотемпературных джозефсоновских переходах. Физики университета Техаса в Остине используют лазерную ловушку, чтобы последовательно захватить и измерить одинаковое небольшое количество атомов.

Исследователи университета Питтсбурга разрабатывают способ создания островков полупроводника с размером меньше, чем 10 нанометров, известных как квантовые точки. Островки, сделанные из германия и размещенные на поверхности кремния в нужной конфигурации с точностью до 2 нанометров, способны удерживать отдельные электроны.

Ученые университета Штата Огайо обнаруживают, как осуществить когерентное распространение света между квантовыми точками, облегчая коммуникацию в оптических квантовых компьютерах.

Исследователи университета Иллинойса используют квантовый эффект Зенона (впервые сформулированный так: непрерывное наблюдение за процессом радиоактивного распада делает распад невозможным [32]), неоднократно измеряя свойства фотона, чтобы постепенно изменить их, фактически не позволяя фотону завершить задачу, выполнять поиск базы данных, фактически без "работы" квантового компьютера.

Влатко Ведрал из университета Лидса и его коллеги в университетах Порто и Вены нашел, что фотоны в обычном лазере могут быть квантовомеханически запутанны колебаниями макроскопического зеркала, независимо от температуры зеркала.

Профессор Сэм Бронстейн из университета Йорка вместе с университетом Токио и агентством Науки и Техники Японии дал первую экспериментальную демонстрацию квантового телеклонирования [33].

Профессора университета Шеффилда разрабатывают метод генерирования и управления индивидуальными фотонами с высокой эффективностью при комнатной температуре.

IBM разрабатывает спектроскопию спин-возбуждений, чтобы управлять магнетизмом индивидуальных атомов.

Открыт новый метод проверки ошибок [34].

Разработан метод подсчёта одиночных электронов [35].

Сконструирован первый 12-кубитный квантовый компьютер [36].

Разработана двумерная ионная ловушка для квантового компьютера [37].

В университете Бонна семь атомов выстраивают в устойчивую линию: шаг на пути к построению квантовых гейтов [38].

Разработана синхронизация квантовых свойств электронов на концах нанотрубки.

Группа в Дельфтском технологическом университете в Нидерландах, используя обычную технологию изготовления микрокристалла, создала устройство, которое может управлять спиновым состоянием электронов в квантовых точках [39].

Возникновение новой теории, показывающей как можно контролировать спин частицы не используя сверхпроводящие магниты, что становится очередным шагом в развитии спинтроники и технологии построения квантовых компьютеров [40].

Учёные университетов Копенгагена и Южной Калифорнии разрабатывают квантовую телепортацию между фотонами и атомами, и новый метод квантовой коррекции ошибок [41].

Учёные университета Камерино развивает теорию запутанности макроскопического объекта, которая могла бы позволить использовать "ретрансляторы" в квантовых компьютерах [42].

Учёные университета Иллинойса находят, что квантовая когерентность возможна в несоизмеримых электронных системах [43].

В университете Юты показывают, что возможно считать данные, закодированные в ядерных спинах [44].

Наблюдаются электроны, взаимодействующие с индивидуальными примесными атомами в кремнии: шаг к квантовым компьютерам, базирующимся на кремнии.

2007 г. — университет Мичигана осуществляет запутывание двух ионов, находящихся на расстоянии метра друг от друга.

Первый 16-кубитный адиабатический квантовый компьютер, реализованный компанией *D-Wave Systems*.

Первая реализация алгоритма Д. Дойча на квантовом компьютере кластерного состояния [45].

Разработан алмазный квантовый регистр [46].

На двух сверхпроводящих квантовых кубитах реализован квантовый гейт CNOT [47].

Для квантовых вычислений использован атом азота в фуллерене [48].

Разработан новый метод удержания фотонов [49].

Разработан фотонный транзистор для квантового компьютера.

Двумя независимыми лабораториями разработана квантовая шина для прямого обмена информацией между двумя сверхпроводниковыми кубитами [50, 51].

ОТ БИТОВ К КУБИТАМ

Бит — базовая единица представления и обработки информации современной вычислительной техникой, построенной на основе классических моделей вычислений. Независимо от его физического представления, бит имеет два различимых состояния, которые должны иметь достаточно большой энергетический барьер, чтобы вероятность спонтанного перехода между состояниями, который «вреден» для обработки информации, была минимальна. Бит всегда несет два логических значения, а именно, либо “0”, либо “1”, поэтому бит — классичен. Так регистр, который состоит из n битов, несёт одно из возможных 2^n определённых состояний в любой момент времени, например, $\underbrace{"101\ldots10"}_{n}$.

Квантовый аналог бита (квантовый бит, или кубит) обладает квантово-механическими особенностями поведения. Почти любая квантовая система (обладающая, по крайней мере, двумя состояниями) может выступать в роли кубита. Его пространством состояний является гильбертово пространство — линейная оболочка, натянутая на два (или больше) базисных вектора, которые записываются в дираковских обозначениях как квантовые состояния $|0\rangle$ и $|1\rangle$. Как известно, общее состояние квантовой системы с двумя состояниями может быть представлено суперпозицией базисных состояний

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad (1)$$

причём $|\alpha|^2 + |\beta|^2 = 1$ (см. рис.1, 2). Аналогично можно использовать трёхуровневые квантовые системы (называемые кутритами) для формирования квантовых регистров, или в общем случае кудиты (для d–уровневой системы) [52]. Однако увеличение числа уровней системы наряду с увеличением пропускной способности квантового канала передачи информации влечёт за собой значительные технические трудности её реализации, поэтому пока в первых прототипах квантовых компьютеров и в экспериментах по квантовой коммуникации наибольшее распространение получили кубиты.

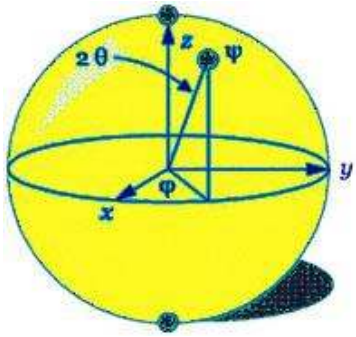

Рис.1. Представление состояния ψ кубита квантового компьютера в виде сферы Блоха

Рассмотрим регистр, составленный из L двухуровневых кубитов. Он может хранить одновременно до 2^L чисел в квантовой суперпозиции. Поэтому, если пополнить регистр дополнительными кубитами, то объём хранимой информации в нём увеличится экспоненциально. Например, 250-кубитный регистр, обладающий атомарными размерами, будет способен хранить больше чисел, чем существует атомов в известной Вселенной. Более того, это преуменьшенная оценка количества квантовой информации, содержащейся в квантовом регистре, так как вектора суперпозиции находятся в непрерывно варьируемой пропорции — каждый с его собственной фазой. Даже в этом случае, если измерить состояние регистра, то получим только одно из тех чисел. Однако исключительность квантового вычисления состоит в том, что можно осуществить некоторое нетривиальное квантовое вычисление, пользуясь суперпозицией — можно выполнить серию математических операций, каждая из которых оперирует всеми хранимыми данными одновременно.

О состоянии L–кубитного регистра можно думать как о 2^L-мерном комплексном векторе. Алгоритм для квантового компьютера должен инициализировать этот вектор в некоторой указанной форме (зависящей от модели квантового компьютера). На каждом шаге алгоритма, этот вектор модифицируется унитарной матрицей, которая определяется физикой устройства. Унитарность матрицы гарантирует её обратимость (таким образом, каждый шаг обратим). После завершения алгоритма, 2^L–мерный комплексный вектор, сохраненный в регистре, должен быть считан из кубитного регистра квантовым измерением. Однако согласно законам квантовой механики, результатом этого измерения будет случайная строка L битов (и измерение разрушит конечное состояние). Эта случайная строка может быть использована в вычислении значения функции потому, что (в соответствии с моделью) распределение вероятности измеренной битовой строки является асимметричным в сторону правильного значения функции. Повторными запусками квантового компьютера и последующего измерения выхода, может быть определено правильное значение с большой вероятностью.

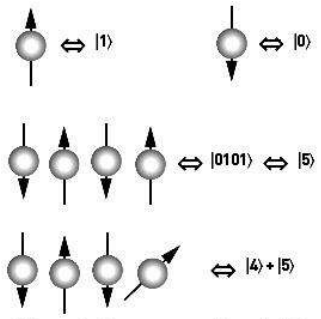

Рис. 2. Кубиты реализуются в контролируемых физических системах (чаще всего в удерживаемых электронах и ионах) с использованием средств контроля над их состоянием

Квантовый алгоритм осуществляется выполнением соответствующих последовательных унитарных операций. Отметим, что для данного алгоритма, операции будут всегда выполняться точно в том же самом порядке. Нет

логического условия "IF, THEN" , чтобы варьировать последовательность, поскольку нет никакого пути считывать состояние кубита до заключительного измерения. Но есть условные операции, реализуемые гейтом controlled-NOT (или просто CNOT) [53, 54]. Краткое введение в теорию квантовой информации и квантовых алгоритмов можно найти в [55].

УНИВЕРСАЛЬНЫЙ КВАНТОВЫЙ КОМПЬЮТЕР

После ознакомления с основными понятиями можно перейти к рассмотрению реализующего объекта квантовой теории информации. В первую очередь квантовый компьютер является устройством, которое существует пока лишь в теории, в мысленном эксперименте, чья задача сводится к формальному анализу обработки квантовой информации. Опираясь на работу Д. Дойча [15], приведём требования, предъявляемые квантовому компьютеру. Квантовый компьютер представляет множество, состоящее из n кубитов, для которого практически определены следующие операции:

1) Каждый кубит может быть инициализирован в известном состоянии (например, состоянии $|0\rangle$).
2) Каждый кубит может быть измерен в базисе $\{|0\rangle, |1\rangle\}$.
3) Универсальный квантовый гейт (см. ниже) (или множество гейтов) может воздействовать на любое ограниченное подмножество кубитов.
4) Состояние кубитов не изменяется кроме как посредством вышеуказанных преобразований.

Данное описание не затрагивает определенных технологических сторон, но содержит основные идеи квантового компьютера.

Теоретическая модель вычислений является сетевой. В ней осуществляется последовательное воздействие логическими гейтами на множество кубитов. Логические гейты классического электронного компьютера расположены на монтажной плате отдельно друг от друга, в квантовом компьютере логические гейты рассматриваются как взаимодействия нескольких кубитов, происходящие в определенное время. При этом кубиты формируют определенную конфигурацию, в которой вариантов взаимодействия между элементами принципиально больше, чем в классическом компьютере.

Возможна проработка и других моделей квантовых вычислений, например, модели клеточного автомата [56].

Универсальный квантовый гейт

Универсальный квантовый гейт является квантовым эквивалентом классической булевой функции из универсального набора, и является гейтом, который, воздействуя на кубит или их различные комбинации, может имитировать действие любого другого квантового гейта. Однако что собой представляет множество всех возможных квантовых гейтов? Для ответа на этот вопрос нужно обратиться к уравнению Шрёдингера: поскольку квантовая эволюция унитарна, будет достаточно создать в квантовом компьютере все унитарные преобразования n кубитов. На первый взгляд это может показаться трудной задачей, поскольку имеется непрерывное, а следовательно, бесконечное множество гейтов. Однако, как показал Д. Дойч в 1985 г. [15], довольно простые квантовые гейты могут составлять универсальный набор, который будет достаточен для построения квантового компьютера. Например, пара однокубитового гейта $V(\theta, \varphi)$ и двухкубитового гейта «controlled-NOT», где $V(\theta, \varphi)$ — гейт произвольного вращения одного кубита:

$$V(\theta,\varphi) = \begin{pmatrix} cos(\theta/2) & -ie^{-i\varphi}sin(\theta/2) \\ -ie^{i\varphi}sin(\theta/2) & cos(\theta/2) \end{pmatrix}, \quad (2)$$

а *CNOT* может быть представлен матрицей

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

может считаться универсальным набором. Можно показать, что любая унитарная матрица размерности n×n может быть образована путем комбинирования двухкубитовых гейтов *CNOT* и гейтов вращений одного кубита.

Можно возразить, что гейт $V(\theta, \varphi)$ должен рассматриваться как бесконечное множество гейтов, поскольку его параметры являются непрерывными. Однако посредством выбора двух определенных иррациональных значений углов θ и φ, и многократного применения гейта с данными значениями, можно описать практически все вращения одного кубита. Но нет необходимости использовать подобные трудоемкие методы в реальной системе — путем комбинирования операций вращения и CNOT, можно описать операцию контролируемого вращения, являющуюся одиночным универсальным гейтом. Описание подобных универсальных гейтов можно найти у Д. Дойча [57], С. Ллойда [58], Д.П. ди Винченцо [59] и А. Баренцо [60]. Следует отметить, что двухкубитовые гейты достаточны для выполнения квантовых вычислений с любым количеством кубитов.

Закон Чёрча-Тьюринга

Ознакомившись с квантовым компьютером, необходимо продемонстрировать его универсальность, т.е. показать, что он функционирует в соответствии с законом Чёрча-Тьюринга (переформулированного тезиса Чёрча-

Тьюринга) [61, с.66], который гласит, что изменение любой реальной конечной физической системы может быть как угодно точно сымитировано на вычислительной машине, работающей с универсальными моделями, за конечное число шагов. Доказательство состоит из двух шагов и само по себе очень простое. Во-первых, состояние любой квантовой системы есть вектор в гильбертовом пространстве. Таким образом, оно может быть представлено как угодно точно с помощью конечного числа кубитов. Во-вторых, эволюция любой квантовой системы есть унитарное преобразование, так что она может быть сымитирована на квантовом компьютере, который способен создавать новое унитарное преобразование с произвольной точностью.

Принципиальный вопрос был затронут Д. Мейерсом [62], когда он определил, что вычислительные задачи, для которых не определено количество шагов до завершения, представляют определенные трудности. В противоположность классическому компьютеру нельзя определить остановку квантового компьютера. Однако в дальнейшем будут рассматриваться либо задачи, у которых можно прогнозировать число шагов до завершения, либо задачи, об остановке которых квантовый компьютер сообщает с помощью специально предназначенного для этого кубита, не задействованного в вычислениях [15].

Несмотря на вышеуказанные условия, остается очень широкий круг задач для исследования. М.А. Нильсен и И.Л. Чуанг рассмотрели применение массива фиксированых квантовых гейтов и показали, что если с помощью массива можно оперировать кубитами, являющимися одновременно информацией и программой, то невозможно посредством этого же массива осуществлять унитарное преобразование информации [63]. Однако существуют устройства, в которых классический компьютер управляет квантовыми гейтами, действующими на квантовый регистр. Таким образом, с помощью классической программы можно «определять» любой массив (любую последовательность) гейтов и направлять его в квантовый компьютер. Без сомнения, квантовый компьютер является познавательным теоретическим инструментом. Но рядом с ним до сих пор стоит большой знак вопроса, требующий ознакомиться с его неидеальностью. Описания квантового компьютера, указанные выше, относятся к случаю, когда при выполнении измерений или применении гейтов может быть достигнута любая точность. Данные случаи, как и четвертое требование (отсутствие эволюции извне), являются физически некорректными. Описание квантового компьютера будет реалистичным, если к каждому из четырех требований добавить положение относительно допустимой степени точности.

КВАНТОВЫЕ АЛГОРИТМЫ

Квантовый алгоритм — это физический процесс, который использует квантовые свойства объекта для процесса вычисления. Можно формализовать описание этих квантовых вычислительных процессов в терминах модели, близкой к формализму классического вычисления. Поэтому удобно логические операции над битами памяти тьюрингового компьютера классического вычисления заменить на унитарные преобразования, действующие на фиксированное конечное число кубитов. Можно аргументировать [15], что модель этого типа достаточна для описания общего квантового физического процесса. Произвольный компьютер должен работать, используя "конечный набор средств", то есть иметь возможность применения любой операции из некоторого конечного фиксированного набора основных унитарных операций. Любая другая унитарная операция, в которой мы, возможно, будем нуждаться при выполнении алгоритма, должна конструироваться из основных стандартных операций, действующих в заданной последовательности на отобранные кубиты (или скорее быть выражаемой ими с достаточной степенью точности). Можно показать [57], что различные наборы унитарных операций (так называемые "универсальные наборы") достаточны, чтобы ими аппроксимировать с произвольной точностью любую унитарную операцию, действующую на любое число кубитов. Одно из самых полезных и существенных следствий этого формализма — обеспечение способа оценки сложности вычислительной задачи (аналогично концепциям классической теории сложности вычислений).

В исследовании квантовых алгоритмов оказывается интересным нахождение полиномиально–временных алгоритмов в задачах, для которых не известно классических полиномиальных алгоритмов их решения. Так, что использование квантовых эффектов даёт экспоненциальное ускорение решения задачи по сравнению с классической обработкой информации. В этом можно убедиться на примере алгоритма Шора. Далее также опишем квантовый алгоритм поиска, который обеспечивает квадратичное ускорение по сравнению с любым классическим алгоритмом.

Алгоритм Шора

Алгоритм Шора — это квантовый алгоритм для факторизации числа N за время $O((log\ N)^3)$ и ресурсы $O(logN)$ [4]. Алгоритм подвергает ключ RSA (популярный криптографический метод) опасности быть легко взломанным, если его запустят на достаточно «большом» для этого квантовом компьютере. Алгоритм Шора может это сделать за полиномиальное время [64].

Как и многие из квантовых компьютерных алгоритмов, алгоритм Шора является вероятностным: он даёт правильный ответ с любой наперёд заданной вероятностью. Это достигается многократным повторным выполнением алгоритма. Но так как предложенное решение верифицируемо за полиномиальное время, алгоритм может быть изменен для работы за ожидаемое полиномиальное время с нулевой ошибкой.

Алгоритм Шора был разработан в 1994 г., но классическая часть была разработана прежде Дж.Л. Миллером. Семь лет спустя, в 2001 г., квантовый алгоритм Шора демонстрировался группой в *IBM*, которая осуществила факторизацию числа 15 на 3 и 5, используя квантовый компьютер с 7 кубитами (см. разд. Краткая история).

Задача, которую необходимо решить, состоит в поиске целого делителя *p* целого числа *N* в интервале между 1 и *N*. Алгоритм Шора состоит из двух частей:

1) Сведению задачи факторизации к задаче поиска порядка, которая может быть решена на классическом компьютере.

2) Выполнение квантового алгоритма для решения задачи нахождения порядка.

Классическая часть такова:

1) Выбираем случайное число $a < N$.

2) Вычисляем НОД (a, N) (НОД — наибольший общий делитель). Это может быть сделано с использованием алгоритма Евклида.

3) Если НОД $(a, N) \neq 1$, тогда есть нетривиальный делитель *N*, на чём выполнение алгоритма заканчивается.

4) В противном случае, используем подпрограмму поиска периода (ниже) чтобы найти *r*, период следующей функции: $f(x) = a^x \mod(N)$, т.е. наименьшее целое *r,* для которого $f(x + r) = f(x)$.

5) Если *r* нечётно, возвращаемся к шагу 1.

6) Если $a^{r/2} \equiv -1 \mod N$, возвращаемся к шагу 1.

7) Делителями *N* являются НОД $\left(a^{r/2} \pm 1, N\right)$.

Теперь рассмотрим квантовую часть — подпрограмму поиска периода:

1) Начнём с пары начального и выходного кубитных регистров с $log_2 N$ кубитами каждый, и инициализируем их в состоянии $N^{-1/2} \sum_x |x\rangle|0\rangle$, где *x* пробегает от 0 до *N–1*.

2) Сконструируем $f(x)$ как квантовую функцию и применим её вышеуказанному состоянию, получим

$$U_{QFT}|x\rangle = N^{-1/2} \sum_y e^{-2\pi i x y/N} |y\rangle. \tag{3}$$

Это оставляет нас в следующем состоянии:

$$N^{-1} \sum_x \sum_y e^{-2\pi i x y/N} |y\rangle\, |f(x)\rangle. \tag{4}$$

4) Произведём измерение. Получим некоторый выход *y* во вводном регистре и $f(x_0)$ в выходном регистре. Поскольку *f* периодична, вероятность получить при измерении некоторую пару *y* и $f(x_0)$ даётся выражением

$$\left| N^{-1} \sum_{x: f(x) = f(x_0)} e^{-2\pi i x y/N} \right|^2 = \left| N^{-2} \sum_b e^{-2\pi i (x_0 + rb) y/N} \right|^2. \tag{5}$$

Из анализа видно, что эта вероятность тем выше, чем ближе yr/N к целому.

5) Преобразуем y/N в несократимую дробь, и найдём знаменатель r', который является кандидатом в *r*.

6) Проверим, выполняется ли $f(x) = f(x + r')$. Если да, то задача решена.

7) В противном случае получаем больше кандидатов для *r,* используя значения близкие к y, или кратные r'. Если один из этих кандидатов подойдёт, задача решена.

8) В противном случае возвращаемся к 1 шагу подпрограммы.

Алгоритм состоит из двух частей. Первая часть алгоритма сводит задачу факторизации к проблеме обнаружения периода функции, и может быть осуществлена классически. Вторая часть находит период, используя обратное квантовое преобразование Фурье (она и порождает квантовое ускорение).

Так, в первой стадии находятся делители по периоду. Целые числа, которые меньше, чем *N* и взаимно простые с *N* формируют конечную группу по умножению по модулю *N*, которая обычно обозначается $(Z/NZ)^x$. К концу шага 3 есть целое *a* в этой группе. Так как группа конечна, *a* должно иметь конечный порядок *r*, такое наименьшее положительное целое число, что $a^r \equiv 1 \, mod N$.

Следовательно, $N \mid (a^r - 1)$. Предположим, есть возможность найти *r*, и оно чётно. Тогда

$$a^r - 1 = \left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right) \equiv 0 \, mod N, \quad \Rightarrow \quad N \mid \left(a^{r/2} - 1\right)\left(a^{r/2} + 1\right), \tag{6}$$

где *r* — наименьшее положительное целое такое, что $a^r \equiv 1$, поэтому *N* не является делителем $a^{r/2} - 1$. Если *N* также не является делителем $\left(a^{r/2} + 1\right)$, тогда *N* должно иметь нетривиальный общий делитель с каждым из $\left(a^{r/2} - 1\right)$ и $\left(a^{r/2} + 1\right)$, что приводит нас к факторизации *N*. Если *N* является произведением двух простых чисел, то это единственно возможная факторизация.

Вторая часть алгоритма посвящена нахождению периода. Здесь алгоритм Шора существенно полагается на способность квантового компьютера находиться в суперпозиции состояний. Чтобы вычислить период функции f, вычисляется функция во всех точках одновременно. Квантовая механика не позволяет получить доступ к этой информации непосредственно. Измерение приведет только к одному из всех возможных значений, разрушая все

остальные. Поэтому нужно преобразовать суперпозицию в другое состояние, которое вернёт правильный ответ с высокой вероятностью. Это достигается обратным квантовым преобразованием Фурье [65, разд. 5].

Шор должен был решить следующие три проблемы "реализации", и все они должны были быть реализованы "быстро". Это означает, что они могут быть реализованы с множеством квантовых гейтов, которые полиномиальны по $logN$. Итак необходимо:

1. Создать суперпозиции состояний. Это может быть сделано, применяя гейты Адамара [43] ко всем кубитам входного регистра. Другой подход состоял бы в том, чтобы использовать квантовое преобразование Фурье (см. ниже).

2. Применить функцию f как квантовое преобразование. Чтобы достичь этого, Шор использовал многократное возведение в квадрат для его модулярного экспоненциального преобразования. Важно отметить, что этот шаг более труден, чем квантовое преобразование Фурье, которое требует вспомогательных кубитов и существенно большего числа срабатываний гейтов.

3. Выполнить обратное квантовое преобразование Фурье. При использовании контролируемых гейтов вращения, и гейтов Адамара Шор сконструировал схему для квантового преобразования Фурье, которое использует только $O[(logN)^2]$ гейтов.

После всех этих преобразований измерение даст приближённое значение периода *r*. Для простоты предположим, что существует такое *y,* что yr/N является целым. Тогда вероятность измерить *y* равна 1. Замечаем тогда, что $e^{2\pi ibyr/N} = 1$ для всех целых *b*. Следовательно, сумма, квадрат которой даёт вероятность получить при измерении *y,* будет равна N/r, поскольку *b* грубо принимает значения N/r и таким образом вероятность равна $1/r^2$. Существуют такое yr, что yr/N — целое, и также *r* вероятности для $f(x_0)$, поэтому сумма вероятностей равна 1 [4].

Алгоритм Гровера

Рассмотрим алгоритм Гровера — квантовый алгоритм для быстрого поиска в неупорядоченной базе данных [8]. При существующих технических средствах одним из наиболее быстрых классических алгоритмов поиска является линейный поиск, требующий $O[N]$ времени. Алгоритм Гровера, использующий возможности квантовых компьютеров, позволяет решить задачу поиска в *N* записях искомой за время $O\left[\sqrt{N}\right]$ с использованием $O[logN]$ места. Доказано, что он является наиболее быстрым квантовым алгоритмом для поиска в неупорядоченной базе данных и что не существует классических алгоритмов той же эффективности. Алгоритм Гровера обеспечивает квадратичный прирост скорости, в то время как некоторые другие квантовые алгоритмы, например, алгоритм факторизации Шора, дают экспоненциальный выигрыш по сравнению с соответствующими классическими алгоритмами. Несмотря на это, квадратичный прирост значителен при достаточно больших значениях *N*.

Хотя основным назначением алгоритма Гровера принято считать поиск в базе данных, более точно его можно охарактеризовать как алгоритм «обращения функции». Грубо говоря, имея функцию $y = f(x)$, которая может быть вычислена с использованием квантового компьютера, алгоритм Гровера позволяет вычислить *x*, зная *y*. Поиск в базе данных соотносится с обращением функции, которая принимает определенное значение, если аргумент *x* соответствует искомой записи в базе данных. Алгоритм Гровера также может быть использован для нахождения медианы и среднего арифметического числового ряда. Кроме того, он может применяться для решения *NP*-полных задач путем исчерпывающего поиска среди множества возможных решений. Это может повлечь значительный прирост скорости по сравнению с классическими алгоритмами, хотя и не предоставляя «полиномиального решения» в общем виде.

Как и большинство алгоритмов квантового компьютера, алгоритм Гровера носит вероятностный характер в том смысле, что даёт правильный ответ с некоторой вероятностью (вообще говоря, с любой наперёд заданной). Вероятность неправильного ответа может быть уменьшена увеличением числа повторений выполнения алгоритма (примером детерминистического квантового алгоритма является алгоритм Дойча-Джоза [66], который всегда даёт правильный ответ с фиксированной достоверностью). В качестве примера приведем алгоритм Гровера, который выполняет поиск одной совпадающей записи.

Пусть имеется неупорядоченная база данных с *N* записями. Алгоритму требуется *N*-мерное пространство состояний *H*, которое может порождаться $log_2 N$ кубитами. Пронумеруем записи базы данных таким образом: $0, 1, \ldots, N-1$. Выберем наблюдаемую, Ω, действующую в *H* с *N* различными собственными значениями, которые все известны. Каждое из собственных состояний Ω кодирует одну из записей в базе данных таким образом, как опишем ниже. Обозначим собственные состояния (используя обозначения «bra-ket») как $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle$ и соответствующие им собственные значения $\{\lambda_0, \lambda_1, \ldots, \lambda_{N-1}\}$.

Рассмотрим унитарный оператор U_ω, который действует как подпрограмма, сравнивающая записи базы данных по некоторому поисковому критерию. Алгоритм не указывает, как работает эта подпрограмма, но она должна быть квантовой подпрограммой, которая работает с суперпозициями состояний. Далее, оператор U_ω, должен действовать только на собственное состояние $|\omega\rangle$, которое соответствует записи базы данных, подпа-

дающей под поисковый критерий. Потребуем, чтобы U_ω оказывало следующее преобразование: $U_\omega|\omega\rangle = -|\omega\rangle$ и $U_\omega|x\rangle = |x\rangle$ для всех $x \neq \omega$. Цель — идентифицировать собственное состояние $|\omega\rangle$, или, что эквивалентно, собственное значение ω, на которое действует оператор U_ω.

Алгоритм Гровера состоит из следующих шагов [8]:

1. Инициализируем систему в состоянии $|s\rangle = \frac{1}{\sqrt{N}}\sum_x|x\rangle$.

2. Выполним следующие "итерации Гровера" $r(N)$ раз. Функция $r(N)$ описана ниже.

   a) Применим оператор U_ω.

   b) Применим оператор $U_s = 2|s\rangle\langle s| - I$.

3. Проведём измерение Ω. Результатом измерения будет λ_ω с вероятностью, стремящейся к 1 при $N \gg 1$. Из λ_ω может быть получено ω.

Нашим начальным состоянием является $|s\rangle = \frac{1}{\sqrt{N}}\sum_x|x\rangle$. Рассмотрим плоскость, натянутую на вектора $|s\rangle$ и $|\omega\rangle$. Пусть $|\omega^x\rangle$ будет кет-вектором в этой плоскости, перпендикулярным вектору $|\omega\rangle$. Поскольку $|\omega\rangle$ — один из базисных векторов, перекрытие равно $\langle\omega|s\rangle = \frac{1}{\sqrt{N}}$. В геометрической интерпретации, между $|\omega\rangle$ и $|s\rangle$ угол равен $\pi/2 - \theta$, где θ определяется из $cos(\pi/2 - \theta) = \frac{1}{\sqrt{N}}$ и $sin\theta = \frac{1}{\sqrt{N}}$.

Оператор U_ω действует как отражение в гиперплоскости, ортогональной $|\omega\rangle$; для векторов в плоскости, натянутой на вектора $|s\rangle$ и $|\omega\rangle$, он действует как отражение относительно прямой, определяемой вектором $|\omega^x\rangle$. Оператор U_s — отражение относительно прямой, определяемой вектором $|s\rangle$. Следовательно, вектор состояния остаётся в плоскости, натянутой на вектора $|s\rangle$ и $|\omega\rangle$, после каждого действия оператора U_s и оператора U_ω, и можно непосредственно проверить, что оператор U_sU_ω каждого итерационного шага алгоритма Гровера вращает вектор состояния на угол 2θ в направлении $|\omega\rangle$.

Остановиться необходимо, когда вектор состояния проходит близко от вектора $|\omega\rangle$; после этого, последующие итерации поворачивают вектор состояния в направлении от $|\omega\rangle$, уменьшая вероятность получения правильного ответа. Число требуемых итераций равно r. Чтобы совместить вектор состояния в точности с $|\omega\rangle$, нужно:

$$\pi/2 - \theta = 2\theta r, \quad r = 1/4\,(\pi/\theta - 2). \tag{7}$$

Однако число r должно быть целым, поэтому, вообще, его можно выбрать только ближайшим к $1/4\,(\pi/\theta - 2)$. Угол между $|\omega\rangle$ и конечным вектором состояния равен $O(\theta)$, поэтому вероятность получения неправильного ответа равна $O(1 - cos^2\theta) = O(sin^2\theta)$. $\theta \approx N^{-1/2}$ при $N \gg 1$, поэтому $r \to \frac{\pi\sqrt{N}}{4}$. Более того, вероятность получения неправильного ответа становится $O(1/N)$, и стремится к нулю для больших N.

КВАНТОВАЯ ДЕКОГЕРЕНЦИЯ

В реальном построении квантового компьютера имеется множество практических трудностей, главная из которых — удержание элементов компьютера в когерентном состоянии, поскольку малейшее взаимодействие с внешним миром ведёт систему к потере когерентности (иначе — её декогеренции), а значит к аварийному завершению работы компьютера. Этот эффект приводит к скорому после запуска алгоритма нарушению унитарного характера (или, более точно, обратимости) квантовых шагов вычисления, следствием чего является возможность решать лишь тривиальные задачи. Поэтому становится понятно, что необходимо решить задачу построения более универсальной системы, которая изолирована от всего, кроме инструментов её управления и измерения результата вычисления, и которая способна проводить вычисления на временах, необходимых для более сложных задач.

Но дело в том, что четвертый пункт требований к квантовому компьютеру (см. выше) является в принципе физически неосуществимым. В действительности, не существует ни идеального квантового гейта, ни изолированной системы. Можно надеяться, что удастся как угодно точно приблизить реальное устройство к идеальному, но на данный момент это желание остается неосуществимой мечтой. В основе таких гейтов как XOR лежит взаимодействие двух изначально разделенных кубитов. Но если кубиты взаимодействуют друг с другом, то они неизбежно будут взаимодействовать с чем-либо еще [67]. Необходимо упомянуть о том, что чрезвычайно сложно найти систему, в которой потеря когерентности имела бы место реже одного раза на миллион применений гейта XOR. Из этого следует, что потеря когерентности требует времени примерно в 10^7 раз меньше времени разложения на множители 130-значного числа! Еще предстоит узнать, позволяют ли законы физики очертить нижний предел скорости потери когерентности, однако уже сейчас можно с уверенностью сказать, что легче увеличить скорость классических вычислений в 10^6 раз, чем во столько же раз снизить потерю когерентности в мощном квантовом компьютере. Данные красноречивые доказательства были представлены С. Гароше и Дж.М. Раймондом [68]. Его работа, как и работа Р. Ландауера [69] и других можно рассматривать как предупреждение. Серьезный численный обзор данной проблемы представлен Ц. Мигуелем [70] и А. Баренцо [71].

Классические компьютеры надежны не вследствие своей качественной разработки, а потому что они не чувствительны к помехам. Для того чтобы это понять, необходимо подробно изучить работу, например, триггера

или обычного механического переключателя. Их устойчивость определяется комбинацией процессов усиления и рассеяния: небольшое отклонение переключателя от положения «включено» или «выключено» приводит к появлению большой возвращающей силы со стороны пружины. Ее аналогом в триггере являются усилители. Однако одной лишь возвращающей силы недостаточно: при наличии консервативной силы переключатель начнет колебаться от одного положения к другому. Не менее важно и наличие затухания, в переключателе оно обеспечивается неупругими столкновениями и, как следствие, излучением тепла. В триггере затухание реализуется за счет резисторов. Однако фундаментальные законы квантовой механики исключают перенос данных методов на квантовый компьютер. Теорема клонирования не позволяет усиливать неопределенное квантовое состояние, а диссипация несовместима с унитарной эволюцией.

Такой фундаментальный подход привел к появлению широко распространенного мнения о том, что квантовая механика исключает возможность защиты квантового компьютера от случайных помех. Периодичное проецирование состояния компьютера посредством тщательно выбранных измерений само по себе не является достаточным [72]. Однако с помощью тонкого использования информационной теории можно найти выход из этого тупика. Идея заключается в применении к квантовым системам методов исправления ошибок классической теории информации.

Квантовая коррекция ошибок

Метод квантовой коррекции ошибок (ККО) [73] создан для защиты квантовой информации в квантовых вычислениях от ошибок декогеренции и другого квантового шума. Он был впервые определен Э. Стином [74] и независимо от него А.Р. Калдербанком и П.В. Шором [75] в наиболее общем виде. Они же отметили его важность. Квантовая коррекция ошибок необходима для помехоустойчивого квантового вычисления, которое предназначено не только для борьбы с шумом в хранимой квантовой информации, но и компенсации «шумных» квантовых гейтов, несовершенного квантового инструментария, и несовершенных квантовых измерений. Поскольку метод ККО включает в себя применение сетей квантовых гейтов и измерений, то изначально было не ясно, должны ли данные сети быть идеальными с целью обеспечения функционирования самого метода. Важное открытие сделал П. Шор [76]: он показал, как сделать сети исправления ошибок нечувствительными к ошибкам внутри данных сетей. Другими словами, оказалось, что подобные сети «с коррекцией ошибок» нейтрализуют помех больше, чем создают.

Квантовая коррекция ошибок использует избыточность: самый простой путь состоит в многократном дублировании информации, и — если эти копии позже обнаруживаются не совпадающими — руководствуются принципом "по большинству голосов". Например, если бит был дублирован трижды, и теперь оказывается, что один бит содержит "0", а два других — "1", то более вероятно, что первоначальное состояние содержало три единицы (произошла единственная ошибка), чем то, что первоначально было три "0", и произошло две ошибки, хотя это тоже возможно. Хотя копирование квантовой информации невозможно, что доказано теоремой о неклонируемости произвольного неизвестного квантового состояния [77], информация одного кубита может быть распространена на несколько (физических) кубитов при использовании метода квантовой коррекции ошибок. Целью метода является обеспечение сколь угодно длительного квантового вычисления при условии нахождения отношения уровня помех к элементарной операции ниже конечного предела. Однако это преимущество метода обеспечивается за счет неэффективного использования квантовой памяти (таким образом, для его реализации необходим мощный компьютер). Данное пороговое значение величины помех было получено в нескольких работах [78-80].

В классических кодах коррекции ошибок «синдромное» измерение может определить, был ли кубит разрушен, и если да, то какой именно. Что ещё важнее, результат этой операции (синдром) говорит не только, какой же кубит затронут, но также и каким из нескольких возможных путей это произошло. Последнее является алогичным лишь на первый взгляд: поскольку шум случаен, то, как эффект, от него может иметь один из немногих исходов? В большинстве кодов, эффект состоит либо в смене значения бита на противоположное, либо в смене знака (фазы), или и в том, и в другом (в соответствии с матрицами Паули σ_x, σ_z и σ_y). Дело в том, что измерение синдрома имеет проективный эффект квантового измерения. Поэтому, даже если ошибка из-за внесённого шума была случайна, она может быть выражена суперпозицией основных операций — базиса ошибок (который здесь представляется матрицами Паули и единичной матрицей). Синдромное измерение "вынуждает" кубит "решать" какая определенная "ошибка Паули" "случилась", и синдром показывает, какая, так, что можем позволить тому же самому оператору Паули действовать снова на разрушенный кубит, чтобы обратить эффект ошибки. Важным является то, что синдромное измерение указывает на случившуюся ошибку, но не позволяет установить значение, которое хранит логический кубит, в силу ограничения на измерение, которое разрушает любую квантовую суперпозицию рассматриваемого логического кубита с другими кубитами в квантовом компьютере.

Открытие метода ККО приблизительно совпало с появлением связанного с ним метода, который также обеспечивает свободную от помех передачу квантовых состояний по квантовому каналу с помехами. Речь идет об «усилении зацепления» [81, 82]. Основная идея метода заключена в том, что отправитель формирует множество зацепленных пар кубитов, а затем отправляет один кубит из каждой пары по каналу с помехами получате-

лю. Отправитель и получатель накапливают кубиты, а затем осуществляют простое измерение с контролем по четности: например, получатель осуществляет операцию XOR («исключающего – ИЛИ») для принятого и следующего за ним кубитов, а затем измеряет результирующий кубит. После того, как отправитель совершит идентичные операции над своими кубитами, они сравнивают результаты. Если результаты совпадают, то можно сказать, что состояния более половины неизмереных кубитов случайно совпадают с требуемым: $|00\rangle + |11\rangle$. Если же результаты не совпадают, кубиты отбрасываются. Посредством подобных рекурсивных проверок из множества зацепленных пар кубитов с помехами отфильтровывается несколько качественных пар. Уже обладая данным зацепленным состоянием, отправитель и получатель могут связываться посредством телепортации квантового состояния. Более подробное описание можно найти у Ч. Беннетта [81].

Альтернативный подход к проблеме "стабильность–декогеренция" состоит в том, чтобы создать топологический квантовый компьютер [83], который использует в качестве кубитов общие состояния квазичастиц двумерного электронного газа, называемых анионами, что позволяет сформировать устойчивые логические гейты, применяя теорию узлов. Этому вопросу посвящена вторая часть статьи.

ТОПОЛОГИЧЕСКИЕ КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

Существует кардинально другой метод защиты от помех, возникающих из-за взаимодействия квантового регистра с внешней средой. Для того, чтобы нейтрализовать возмущения, порождаемые внешней средой, при вычислениях можно использовать топологически–инвариантные свойства физической системы и таким образом вообще «забыть» о помехах. Топологическим инвариантом, нечувствительным по отношению к помехам внешней среды, может быть избрана структура косы, сплетённой из мировых линий частиц физической системы [84]. Перед тем, как продвигаться дальше, приведём строгое определение косы [85]. Косой из n нитей называется объект, состоящий из двух параллельных плоскостей, скажем, P_0 и P_1, в трёхмерном пространстве $\mathbb{R}^3$, содержащих упорядоченные множества точек $a_1, \dots, a_n \in P_0$ и $b_1, \dots, b_n \in P_1$, и из n простых дуг $l_1, \dots, l_n$, пересекающих каждую параллельную плоскость P_t между P_0 и P_1 однократно и соединяющих точки $\{a_i\}$ с точками $\{b_i\}$, $i=1,\dots,n$. В дальнейшем нам понадобиться также понятие группы кос. Её образуют классы эквивалентности относительно операции, определяемой конкатенацией элементов кос. Единичная коса в этой группе — класс эквивалентности, содержащий косу из n параллельных отрезков, а обратная коса определяется как отражение в плоскости $P_{1/2}$.

Процесс вычисления можно описать следующим образом. Элементы рассматриваемой физической системы выстраиваются в упорядоченный ряд. Затем начинаем менять их местами в строго определённой последовательности, запутывая тем самым их мировые линии в пространстве–времени в косу. Осуществлением той или иной геометрии сплетения, реализуется тот или иной квантовый алгоритм. Результат вычисления содержится в структуре косы, иными словами, в конечном состоянии системы, как и в случае обычного квантового компьютера [84]. Отличие состоит в том, что кубиты в обычном квантовом компьютере эволюционируют в смысле унитарного изменения своих квантовых состояний, и значительная часть квантовой информации содержится в относительных фазах этих состояний, что делает процесс вычисления уязвимым по отношению к воздействию окружающей среды. В то время, как функционирование топологического квантового компьютера уже по своей сути помехоустойчиво, поскольку «малые» смещения мировых линий не способны изменить топологию косы, порождающую фазу волновой функции. Концепцию топологической помехоустойчивости легко представить себе на примере замкнутой петли с узлом, которую невозможно преобразовать в замкнутую петлю без узла не разрезая первой. Непрерывные преобразования не избавят от узла (см. рис. 3). Под «малыми» смещениями, вызванными «малыми» возмущениями внешней средой, понимаются непрерывные деформации элементов косы, их гомеоморфизмы. Если же система подвергнется грубому вмешательству, соответствующему, например, деформациям склеивания, разрыва или «возвращения» мировых линий, изменение топологии косы приведёт к некорректному результату проводимого вычисления. Подобные деформации мировой линии трудно осуществимы при низких энергиях: тяжело себе представить частицу, то исчезающую, то появляющуюся в другой точке пространства рабочего объёма, либо встречу начального элемента системы с самим собой из будущего при замыкании его мировых линий (необходимо сильное гравитационное поле), что соответствует структуроизменяющему влиянию на косу. Единственной реальной угрозой является аннигиляция с античастицей, что, впрочем, возможно контролировать, и что, наоборот, можно использовать в своих целях на конечной стадии вычисления.

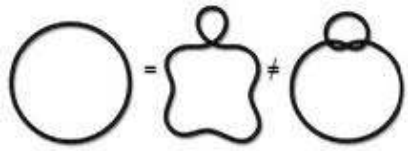

Рис. 3. Иллюстрация топологических отличий в свойствах замкнутой петли и замкнутой петли с узлом.

Топологический квантовый компьютер

Одной из центральных идей квантовой теории является концепция неразличимых (или идентичных) частиц. Например, все электроны во Вселенной в точности одинаковы. Если в системе многих тождественных частиц поменять местами любые две — физика системы не изменится. Но в результате перестановки может измениться фаза общей волновой функции системы в зависимости от типа частиц. Согласно уравнениям квантовой механики частицы в трёх и более измерениях при перестановке могут вести себя либо как бозоны, либо как фермионы, в зависимости от их статистики. Известно, что в первом случае волновая функция системы оказывается инвариантна относительно перестановки частиц, во втором — меняет знак. То же самое, хотя с некоторыми замечаниями, можно применить и к одномерному случаю. Но если рассмотреть двумерный случай, то окажется, что между двумя «стандартными» существует огромное разнообразие «нестандартных» статистик. Множитель, возникающий в общей волновой функции при перестановке в двух измерениях неразличимых частиц, может быть произвольным комплексным числом, равным по модулю 1. Такие частицы называются анионами.

Физическая реализация анионов может быть следующей. В трех измерениях необходимо реализовать двумерный электронный газ, запирая электроны в тонком слое между двумя полупроводниковыми пластинами так, что при низких энергиях движение электронов в направлении перпендикулярном слою будет заморожено. При достаточно больших магнитных полях (~150кГ) и достаточно низких температурах (~1К) [86], если электроны в применяемом материале достаточно подвижны, двумерный электронный газ конденсируется в сильносвязанное основное состояние, отделённое от вышележащих возбуждённых уровней ненулевой энергетической шириной. Кроме того, низкоэнергетические возбуждения частиц этого газа не обладают квантовыми числами электронов. Они несут электрический заряд, равный дробной части от заряда электрона. Благодаря им наблюдается удивительный эффект, касающийся свойств проводимости двумерного слоя, который получил название дробного квантового эффекта Холла. В 1998 году Цуи, Штормер и Лаффлин получили Нобелевскую премию за открытие и объяснение этого явления [87]. В. Голдман, Ф. Камино и В. Чжоу (Wei Zhou) из университета Stony Brook (Нью-Йорк) заявили, что им удалось получить прямое экспериментальное подтверждение того, что эти квазичастицы имеют свойства абелевых анионов [88]. Однако, как будет видно ниже, для осуществления квантовых вычислений особенно интересны неабелевы анионы, и есть все основания полагать, что определенные квазичастицы в дробном квантовом эффекте Холла действительно неабелевы. Чтобы это проверить, необходимо провести новые эксперименты. Один из них был предложен Фридманом и Санкаром Дас Сармой из Университета штата Мэриленд в Колледж Парке и Четаном Найяком из Майкрософт. Важные уточнения по его постановке высказали Эдди Штерн из Института Вейцмана в Израиле и Бертран Гальперин из Гарвардского университета. Ещё один эксперимент был разработан Алексеем Китаевым и Парсой Бондерсоном из Калифорнийского технологического института, а также Кириллом Штенгелем. И, наконец, в 1997 году Алексей Китаев обосновал идею использования неабелевых анионов для реализации помехоустойчивого квантового вычисления [84]. Но стоит заметить, что сама идея на то время была уже не новой. В конце 1988 г. Майкл Фридман читал в Гарвардском университете лекции о возможности использования квантовой топологии для вычислений. Его расчеты, опубликованные в 1998 г. [89], основаны на открытии связи инвариантов узлов с квантовой физикой двумерной поверхности, изменяющейся во времени. Если создать такую систему и выполнить соответствующее измерение, можно автоматически вычислить приближенное значение инварианта узла, не прибегая к длительным вычислениям на обычном компьютере. Такие же простые решения существуют и для других трудных задач, имеющих большое практическое значение. Впоследствии схема, предложенная Китаевым, была значительно доработана Джоном Прескиллом [90], и обобщена Карлосом Мочоном [91]. Так был сделан первый шаг к осознанию важности концепции топологического квантового вычисления. В дальнейшем сконцентрируемся на этих результатах, и не будем обсуждать столь же важный вопрос о том, каким образом системы анионов, обладающие нужными свойствами, могут быть реализованы на практике [92–95].

Составляющие поток-заряд и их статистика

Начнём исследование теории анионов с эффекта Ааронова-Бома (или эффекта Эренберга-Сидая-Ааронова-Бома) [96]. Он является квантово-механическим явлением, в котором на заряженную частицу влияет электромагнитное поле в областях, где частица не может находиться. Самая ранняя форма этого эффекта была предсказана В. Эренбергом и Р.Е. Сидаем в 1949 г. [97], и подобный эффект был позже вновь открыт Й. Аароновым и Д.Ж. Бомом в 1959 г. [98]. Этот эффект предсказан для магнитного и электрического полей, но влияние магнитного поля легче наблюдать. Глубокое следствие эффекта Ааронова-Бома заключается в том, что знание классического локального действия электромагнитного поля на частицу не достаточно, чтобы предсказать ее квантово-механическое поведение.

Рассмотрим электромагнетизм в двумерном мире, где «потоковая трубка» представляет собой локализованный «точечный» объект (в трёхмерном мире, можно представить плоскость, пересекающую магнитный соленоид, направленный перпендикулярно плоскости). Пусть поток будет заключён внутри трубки, так что частица никогда не сможет оказаться в области с ненулевым магнитным полем. Эффект состоит в воздействии изме-

римого влияния магнитного поля на заряженную частицу, находящуюся вне потоковой трубки. Если электрический заряд q будет адиабатически перемещён (против часовой стрелки) вокруг потока Φ, волновая функция получит топологическую фазу $e^{iq\Phi}$ (мы используем единицы $\hbar = \mathrm{c} = 1$). Здесь слово «топологический» означает, что фаза Ааронова-Бома нечувствительна к деформациям траектории нашей частицы, а важным является «число витков» заряда вокруг потока.

Концепция топологической инвариантности возникает естественным образом при изучении проблемы помехоустойчивости. При этом очевидным образом можно определить помехоустойчивость квантового гейта: таковым является тот, действие которого на защищённую информацию остаётся инвариантным (или приблизительно таковым), когда добавлением в него «шума» деформируется сама его реализация. Топологическая инвариантность явления Ааронова-Бома — важнейшее свойство, которое ниже попытаемся использовать в построении модели квантовых гейтов, обладающих естественной помехоустойчивостью.

Обычно считают, что эффект Ааронова-Бома связан с безмассовостью электромагнитного поля [96]. Однако явление Ааронова-Бома может также проявляться и в массивных теориях [96]. Например, можно рассмотреть сверхпроводящую систему, состоящую из частиц заряда e, такую, что составные объекты с зарядом ne образуют конденсат (где n — чётное). В этом сверхпроводнике может быть определён минимальный ненулевой квант потока $\Phi_0 = 2\pi/ne$ такой, что перемещение частицы с зарядом ne в этом конденсате вокруг него приведёт к получению волновой функцией частицы тривиальной фазы Ааронова-Бома. Изолированная область, которая содержит квант потока — это островок обычного вещества, окружённого не распространяющимся сверхпроводящим конденсатом, поскольку магнитный поток не может проникнуть в сверхпроводник. То есть это стабильная частица, будем называть её «флаксоном». Когда одна из частиц с зарядом e перемещается вокруг флаксона, её волновая функция получает нетривиальную топологическую фазу $e^{iq\Phi_0} = e^{\frac{2\pi i}{n}}$. Но в сверхпроводнике масса фотона обусловлена механизмом Хиггса, и безмассовых частиц нет. То, что топологические фазы совместимы с массивными теориями очень важно, потому что безмассовые частицы легко возбуждаемы, и это было бы огромным источником декогеренции.

Пусть в двумерном мире, флаксон и электрический заряд находятся в связанном состоянии. Можно себе представить флаксон как поток Φ, замкнутый внутри непроницаемой стенки-окружности, а электрический заряд q — «прилипшим» к этой стенке. Каков угловой момент этого потоко-зарядовой структуры? Предположим, что можно осуществить поворот ее против часовой стрелки на угол 2π, возвращая при этом к начальной ориентации. В результате, заряд q перемещается вокруг потока Φ, генерируя топологическую фазу $e^{iq\Phi}$. Это вращение на угол 2π может быть представлено в гильбертовом пространстве унитарным преобразованием

$$U(2\pi) = e^{-i2\pi \boldsymbol{J}} = e^{iq\Phi}, \tag{8}$$

где $\boldsymbol{J}$ — оператор углового момента. Далее становится понятно, что возможными собственными значениями оператора углового момента будут

$$J = m - \frac{q\Phi}{2\pi} \ (m - \text{целое}). \tag{9}$$

Этот спектр можно характеризовать по угловой переменной $\theta \in [0, 2\pi)$, определяемой как $\theta = q\Phi \ (mod\ 2\pi)$. Будем называть фазу $e^{i\theta}$, которая представляет вращение на 2π против часовой стрелки, *топологическим спином* составного объекта. Для системы с фермионным числом F имеем

$$e^{-i2\pi \boldsymbol{J}} = (-1)^F. \tag{10}$$

Если F — нечётно, собственные значения J смещены от целого на 1/2. Этот сдвиг физически допустим, поскольку есть правила суперотбора по $(-1)^F$: нет такого наблюдаемого локального оператора, который мог бы изменить значение $(-1)^F$ (нет такого физического процесса, который мог бы родить или уничтожить изолированный фермион). Действуя на когерентную суперпозицию состояний, имеющих разные значения $(-1)^F$, оператором $e^{-i2\pi \boldsymbol{J}}$, имеем

$$e^{-i2\pi \boldsymbol{J}}(a|even\ F\rangle + b|odd\ F\rangle) = a|even\ F\rangle - b|odd\ F\rangle. \tag{11}$$

Относительный знак в суперпозиции поменялся, но это не ведёт к изменению наблюдаемой физики.

Аналогично в двух измерениях смещение в спектре углового момента $e^{-i2\pi \boldsymbol{J}} = e^{i\theta}$ не приводит к нефизическим последствиям, если установлено правило суперотбора по θ, которое утверждает, что относительная фаза в суперпозиции состояний с различными θ физически ненаблюдаема. То есть, как и для фермионов, нет разрешённого физического процесса, который привёл бы к рождению или уничтожению изолированного аниона.

С топологической точки зрения в трёх измерениях разрешены только $\theta = 0, \pi$ из-за топологического свойства группы вращения SO(3): замкнутая кривая в SO(3), начинающаяся в единице и заканчивающаяся оборотом в 4π, может быть непрерывно деформирована в точку. То есть, вращение на 4π действительно соответствует тривиальному преобразованию, а значит собственные значения вращения на 2π равны ±1. Но группа вращения SO(2) не обладает этим топологическим свойством, что ведёт к любому значению θ. Таким образом, спин в двух измерениях может быть любым вещественным числом и статистика тоже может быть «дробной». Если переставить потоко-зарядовые составные объекты местами по направлению против часовой стрелки, каждый из них получит фазу $e^{iq\Phi/2}$, что изменит фазу общей волновой функции на $e^{i\theta}$. Таким образом, связь спина и статисти-

ки продолжается в форме, которая является естественным обобщением случая с фермионами и бозонами. Происхождение этой связи совершенно ясно в изложенной модели потоко-зарядовых составных объектов.

Системы анионов

Известно, что сложный объект, состоящий из двух фермионов, является бозоном. К чему приведёт составление сложного объекта из двух анионов? Предположим, что a — анион с обменной фазой $e^{i\theta}$, и построена «молекула» из n числа анионов a. Можно легко проверить, что в соответствии с нашей составной моделью, фаза, получаемая общей волновой функцией двух молекул при их перестановке равна $e^{in^2\theta}$. Аналогичный результат можно получить, вращая одну молекулу, состоящую из n анионов, на угол 2π.

Причина того, что угловой момент в анионной молекуле не комбинируется аддитивно, в следующем. Полный угловой момент молекулы состоит из двух частей: спинового углового момента S каждого из двух анионов (который аддитивен) и орбитального углового момента L анионной пары. Вращение одного аниона вокруг другого против часовой стрелки генерирует нетривиальную фазу $e^{i2\theta}$, поэтому зависимость двух-анионной волновой функции ψ от относительного азимутального угла φ неоднозначна, а именно,

$$\psi(\varphi + 2\pi) = e^{-i2\theta}\psi(\varphi). \tag{12}$$

Так, что спектр орбитального углового момента L смещён от целых значений:

$$e^{-i2\pi L} = e^{i2\theta}, \tag{13}$$

и этот орбитальный угловой момент комбинируется аддитивно со спином S, формируя полный угловой момент

$$-2\pi J = -2\pi L - 2\pi S = 2\theta + 2\theta + 2\pi(\text{целое}) = 4\theta + 2\pi(\text{целое}). \tag{14}$$

Но что если, с другой стороны, составить молекулу из частицы и античастицы? Тогда, спин S молекулы $\bar{a}a$ будет тот же, что и спин молекулы aa. Но обменная фаза имеет противоположный знак в аргументе, так что нецелая часть орбитального углового момента равна $-2\pi L = -2\theta$ вместо $-2\pi L = 2\theta$, и полный угловой момент $J = L + S$ — целый. Это свойство необходимо, если пара $\bar{a}a$ должна иметь возможность аннигилировать без продуктов, несущих нетривиальный угловой момент.

Унитарные представления группы кос

Как уже отмечалось, спектр углового момента имеет различные свойства в дву- и трёхмерном пространствах, потому что группа SO(2) имеет топологические свойства, отличные от топологических свойств группы SO(3) (группа SO(3) имеет компактную односвязную накрывающую группу SU(2), в то время как SO(2) не имеет). Это отличие позволяет понять, почему анионы возможны в двух измерениях, но не в трёх.

Рассмотрим систему n неразличимых точечных частиц, заключённых в двумерной пространственной поверхности (которую сейчас можно представлять плоскостью), и предположим, что две частицы не могут занимать одно и то же пространственное состояние. Конкретную конфигурацию частиц в фиксированное время можно представлять себе в виде плоскости с n «проколами» в заданных положениях — то есть с каждой частицей ассоциируется дырка на поверхности плоскости с бесконечно-малым радиусом. Условие того, что частицам запрещено в одно и то же время занимать одно и то же пространственное состояние, автоматически выполняется, если потребовать, чтобы в конкретный момент времени на плоскости находилось в точности n дырок. В силу идентичности всех n частиц их перестановка не даст никакого физического эффекта, важным является — n различных положений на плоскости.

Чтобы вычислить квантовую амплитуду перехода из одной конфигурации n частиц в момент времени $t = 0$ в другую в момент времени $t = T$ нужно провести суммирование по всем классическим историям n частиц, которые происходили на данном промежутке времени, взвесив фазой e^{iS}, где S — классическое действие. Если представить каждую мировую линию частицы в виде нити, то каждая история n частиц предстанет в виде косы. Далее, поскольку мировым линиям частиц запрещено пересекаться, множество кос распадается на различные топологические классы, которые не могут быть непрерывно деформированы один в другой, и тогда интеграл по траектории может быть вычислен суммированием вкладов, каждый из которых соответствует отдельному топологическому классу историй.

Нетривиальные операции обмена частиц местами на конечном промежутке времени меняют топологический класс косы. Таким образом, видим, что элементы группы симметрии, генерируемые обменами, находятся во взаимно-однозначном соответствии с топологическими классами. Эта (бесконечная) группа носит название B_n: группа кос на n нитях; закон композиции группы соответствует конкатенации кос (то есть последовательному сцеплению одной косы с другой). В квантовой теории квантовое состояние n неразличимых частиц принадлежит гильбертовому пространству, которое преобразуется как унитарное представление группы кос B_n.

Группа может быть представлена как множество генераторов, которые подчиняются специальным определяющим соотношениям. Представим n частиц, занимающих n упорядоченных позиций (пронумерованных как 1, 2, 3, …, n), и выстроенных в линию. Пусть σ_1 обозначает обмен против часовой стрелки частиц, изначально занимающих положения 1 и 2, σ_2 — частиц 2 и 3, и так далее. Любая коса может быть сплетена последовательными перестановками соседних частиц; следовательно, $\sigma_1, \sigma_2, \ldots, \sigma_{n-1}$ — генераторы группы. Есть два типа определяющих соотношений, которым подчиняются эти генераторы. Первое из них

$$\sigma_j\sigma_k = \sigma_k\sigma_j, \quad |j-k| \geq 2, \tag{15}$$

которое означает, что перестановка частиц не из пересекающихся пар коммутативна. Вторым соотношением является

$$\sigma_j\sigma_{j+1}\sigma_j = \sigma_{j+1}\sigma_j\sigma_{j+1}, \qquad j = 1, 2, \dots, n-2, \tag{16}$$

которое называется соотношением Янга-Бакстера. На рис. 4 можно видеть простую иллюстрацию этого соотношения, показывающего, что эти косы топологически эквивалентны.

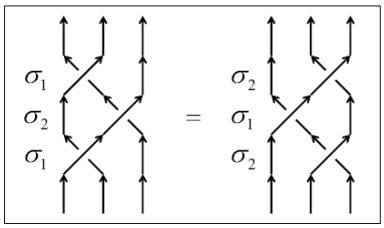

Рис.4. Иллюстрация соотношения Янга-Бакстера (16)

Поскольку группа кос бесконечна, она имеет бесконечное число унитарных неприводимых представлений, и более того, она имеет бесконечное число одномерных представлений. Неразличимые частицы, которые преобразуются как одномерное представление группы кос, называются абелевыми анионами. В одномерных представлениях каждый генератор σ_j из B_n представляется фазой $\sigma_j = e^{i\theta_j}$. Тогда соотношение Янга-Бакстера принимает вид $e^{i\theta_j}e^{i\theta_{j+1}}e^{i\theta_j} = e^{i\theta_{j+1}}e^{i\theta_j}e^{i\theta_{j+1}}$, откуда следует, что $e^{i\theta_j} = e^{i\theta_{j+1}} \equiv e^{i\theta}$ — все перестановки представлены *одной и той же* фазой, что имеет смысл только для неразличимых частиц.

Группа кос также имеет множество неабелевых представлений, размерность которых больше единицы. Неразличимые частицы, волновые функции которых преобразуются таким представлением, называются неабелевыми (или, иногда, неабелионами).

Для неабелевых анионов неприводимое представление группы B_n, реализуемое n анионами, действует на «топологическое векторное пространство» V_n, размерность D_n которого возрастает экспоненциально с n. И для анионов с подходящими свойствами, образ представления может быть плотным в SU(D_n). Осуществляя сплетение необходимой косы, можно промоделировать квантовое вычисление — любое (специальное) унитарное преобразование, действующее на экспоненциально большое векторное пространство V_n, которое может быть реализовано с любой наперёд заданной статистической доверительностью.

Вернёмся к составной модели абелевых анионов, в которой описаны не только эффекты перестановок анионов, но и также типов частиц, являющихся системами анионов. Подобным же образом, в общей анионной модели анионы имеют различные типы, и модель содержит в себе «синтезирующие правила», которые определяют, какие именно типы анионов могут быть получены при слиянии двух определённых типов анионов. Нетривиальные правила соответствия возникают потому, что слияние ассоциативно (*(ab)c = a(bc),* где *a*, *b*, *c* — анионы), и потому, что синтезирующие правила должны находиться в соответствии с правилами сплетения. Хотя условия этого соответствия являются сильно ограничивающими, существует много решений, и, следовательно, много разных моделей неабелевых анионов в принципе реализуемы.

Неабелев эффект Ааронова-Бома

Рассмотрим построение теории неабелевых анионов, которая обладает некоторыми свойствами хромодинамики, и будем опираться на составную модель абелевых анионов. Пусть имеется неабелев сверхпроводник в двух измерениях. Этот мир содержит частицы, которые несут «магнитный поток» (похожий на цветовой магнитный поток в хромодинамике) и частицы, которые несут заряд (подобно цветным кваркам в хромодинамике). Поток принимает значения в неабелевой конечной группе G, а зарядами являются унитарные неприводимые представления группы G. В этой постановке можно сформулировать различные модели неабелевых анионов. Остановимся на одной из них [99].

Пусть R обозначает конкретное неприводимое представление группы G, размерность которого обозначим как $|R|$. Выберем произвольно ортонормированный базис для $|R|$ — мерного векторного пространства, на которое действует R:

$$|R, i\rangle, \quad i = 1, 2, \dots, |R|. \tag{17}$$

Когда заряд R перемещается вдоль замкнутой траектории вокруг потока $a \in G$, возникает эффект Ааронова-Бома: базис R поворачивается унитарной матрицей $D^R(a)$, который представляет a:

$$|R, j\rangle \mapsto \sum_{i=1}^{|R|} |R, i\rangle\, D^R_{ij}(a). \tag{18}$$

Элементы матрицы $D^R_{ij}(a)$ в принципе измеряемы. Например, проводя интерференционные эксперименты, в которых пучок откалиброванных зарядов мог бы проходить с любой стороны от потока (фаза комплексных чисел $D^R_{ij}(a)$ определяет величину смещения интерференционных полос, а их модуль — контрастность полос). Таким образом, поскольку определён стандартный базис для частиц, можно использовать заряды, чтобы сопоставить «метки» (элементы группы G) всем потокам. Это соответствие однозначно, если представление R точное и запрещает любые автоморфизмы группы (которые создают неоднозначности).

Однако элементы группы, которые сопоставляются потокам, зависят от соглашения. Предположим имеется k флаксонов (частиц, несущих поток). Тогда, используя стандартные заряды, померяем поток каждой из этих частиц. Групповые элементы $a_1, a_2, \dots, a_k \in G$ каждому из k флаксонов. И теперь попросим вас померять поток,

проверить наши сопоставления. Но ваши стандартные заряды отличаются от наших, потому что они перемещались вокруг другого потока (обозначим его $g \in G$). Следовательно, k флаксонам вы сопоставите групповые элементы $ga_1g^{-1}, ga_2g^{-1}, \ldots, ga_kg^{-1} \in G$, и следовательно наши сопоставления будут отличаться общим сопряжением по элементу g.

Таким образом, сопоставление групповых элементов флаксонам неоднозначно и не имеет инвариантного смысла. Но из-за того, что «правильное» сопоставление групповых элементов флаксонам разнится только сопряжением по некоторому элементу $g \in G$, класс сопряжённости потока в G имеет инвариантный смысл, с которым согласятся все наблюдатели. Действительно, если определить соглашение, то групповой элемент, сопоставленный конкретному флаксону, может меняться, если этот флаксон принимает участие в физическом процессе, в котором он заплетается с другими флаксонами. По этой причине флаксоны, принадлежащие одному и тому же классу сопряжённости, должны рассматриваться как неразличимые частицы, даже если они встречаются во многих типах (от разных классов), которые могут быть определены во время нашего измерения в конкретный момент времени и конкретном месте. Таким образом, становится ясно, что флаксоны — это неабелевы анионы.

Сплетение неабелевых флаксонов

Покажем, что, используя неабелев сверхпроводник с подходящими свойствами, можно осуществлять обработку квантовой информации помехозащищённым универсальным квантовым компьютером, манипулируя флаксонами. Ключевым здесь есть понимание того, что происходит, когда два флаксона меняются местами.

Для этой цели представим, что откалиброваны два флаксона, и им сопоставлены элементы из группы G. Это сопоставление осуществляется при создании стандартного базиса для заряженных частиц в начальной точке x_0. Затем выберем стандартную траекторию (которую обозначим через α), что берет своё начало в точке x_0, обходит против часовой стрелки флаксон, и возвращается в точку x_0 (см. рис. 5). И наконец, заряженные частицы перемещаются вдоль замкнутой траектории α, и наблюдается, что во время этого параллельного переноса на состояние частиц действует $D(a)$, где D — представление группы G, и $a \in G$ — выбранный нами групповой элемент, соответствующий первому флаксону. То же самое происходит и со вторым флаксоном, соответствующим групповому элементу b, обход против часовой стрелки вокруг которого по траектории β приводит к преобразованию частиц представлением $D(b)$ (см. рис. 5).

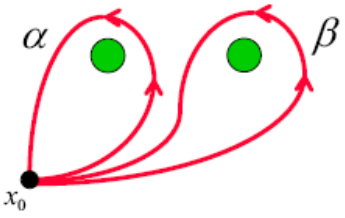

Рис. 5. Стандартные траектории α и β обхода пары флаксонов против часовой стрелки.

Теперь представим, что осуществлён обмен флаксонов местами против часовой стрелки, после чего выполнена перекалибровка. Чтобы определить, каким групповым элементам будут соответствовать теперь флаксоны, рассмотрим траекторию $\alpha\beta\alpha^{-1}$ (см. рис. 6), где под α^{-1} подразумевается прохождение траектории α в обратном направлении, а все траектории в комбинации проходятся в операторном порядке — справа налево. Если в то время, когда два флаксона обмениваются местами против часовой стрелки, траектории деформируются так, что они ни разу не пересекутся флаксонами, траектория $\alpha\beta\alpha^{-1}$ деформируется в траекторию α, в то время как α деформируется в β

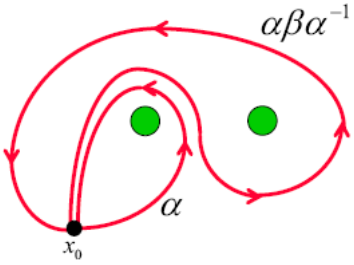

Рис. 6. Новая траектория обхода после обмена флаксонов местами и перекалибровки.

$$\alpha\beta\alpha^{-1} \mapsto \alpha, \quad \alpha \mapsto \beta. \tag{19}$$

Отсюда следует вывод, что оператор сплетения R, представляющий обмен против часовой стрелки, действует на флаксоны как

$$R\colon |a,b\rangle \mapsto |aba^{-1}, a\rangle. \tag{20}$$

Конечно, если флаксоны a и b коммутируют в G, то всё, что делает сплетение, это изменение порядка a и b. Но если a и b не коммутируют, эффект, порождаемый обменом, более интересен. Ассиметричная форма действия оператора R является следствием наших соглашений и смысла обмена (против часовой стрелки). Обратный оператор R^{-1}, осуществляющий обмен по часовой стрелке, действует как

Заметим, что полный поток пары флаксонов может быть детектирован заряженной частицей, которая проходит траекторию $\alpha\beta$, обходящую оба флаксона в паре. Поскольку этот заряд может быть очень далеко от флак-

$$R^{-1}\colon |a,b\rangle \mapsto |b, b^{-1}ab\rangle \tag{21}$$

сонной пары, обмен в ней не изменит полного потока. Действительно, можно убедиться, что поток ab сохраняется под действием и R, и R^{-1}.

Эффект двух последовательных обменов против часовой стрелки соответствует действию «монодромного» оператора R^2, и соответствует следующему:

$$R^2\colon |a,b\rangle \mapsto |(ab)a(ab)^{-1}, (ab)b(ab)^{-1}\rangle, \tag{21}$$

где оба потока сопряжены полным потоком ab. Нетривиальная монодромия означает, что если в плоскости распределено много флаксонов, и один из них «забирается» для анализа, групповой элемент, поставленный в соот-

ветствие ему, может зависеть от траектории, по которой он забирается. Если в одном случае флаксону соответствует элемент $a \in G$, тогда для других вариантов траекторий любой другой элемент bab^{-1} в принципе может быть поставлен в соответствие. Таким образом, класс сопряжённости в G, который представляет флаксон, инвариантен, но конкретный представитель этого класса не определяется однозначно.

Например, предположим, что группа G совпадает с группой перестановок трёх объектов S_3. Один из её классов сопряжённости содержит все двойные перестановки (перестановки двух объектов): $\{(12), (23), (31)\}$. Когда два таких двойных флаксона комбинируются, существует три варианта для их полного потока — тривиальный поток e, и один из тройных потоков: или (123), или (132). Если полный поток тривиален, сплетение двух потоков тоже тривиально (a и $b = a^{-1}$ коммутируют). Но если полный поток нетривиален, то оператор сплетения R имеет орбиту длиной 3

$$\begin{aligned} R\colon |(12),(23)\rangle &\mapsto |(31),(12)\rangle \mapsto |(23),(31)\rangle \mapsto |(12),(23)\rangle, \\ R\colon |(23),(12)\rangle &\mapsto |(31),(23)\rangle \mapsto |(12),(31)\rangle \mapsto |(23),(12)\rangle. \end{aligned} \tag{22}$$

Таким образом, если два флаксона обмениваются местами три раза — они меняются местами, но, несмотря на это, обозначение состояния остаётся прежним. Это означает, что может существовать квантовая интерференция между «прямым» и «обменным» рассеянием двух флаксонов, которым сопоставлены разные элементы одного и того же класса сопряжённости, укрепляя ещё больше идею о том, что потоки с разными «метками» в классе сопряжённости должны рассматриваться как неразличимые частицы.

Поскольку оператор сплетения, действующий на пары двойных потоков, удовлетворяет требованию $R^3 = I$, то его собственные значения равны корню третей степени из единицы. Например, выбирая линейные комбинации трёх состояний с общим потоковым состоянием (123), получаем такие собственные функции оператора R

$$\begin{aligned} R = 1\colon &\quad |(12),(23)\rangle + |(31),(12)\rangle + |(23),(31)\rangle, \\ R = \omega\colon &\quad |(12),(23)\rangle + \bar{\omega}|(31),(12)\rangle + \omega|(23),(31)\rangle, \\ R = \bar{\omega}\colon &\quad |(12),(23)\rangle + \omega|(31),(12)\rangle + \bar{\omega}|(23),(31)\rangle, \end{aligned} \tag{23}$$

где $\omega = e^{2\pi i/3}$.

Хотя пара $|a, a^{-1}\rangle$ с тривиальным общим потоком имеет тривиальные свойства косы, она интересна по другой причине — ее полный заряд отличен от нуля. Чтобы померять заряд объекта надо переместить вокруг этого объекта поток b (против часовой стрелки). Это изменит объект действием на него оператора $D^R(b)$ некоторого представления R группы G. Если заряд равен нулю, тогда представление тривиально — $D(b) = I$ для всех $b \in G$. Но если переместить поток b против часовой стрелки вокруг состояния $|a, a^{-1}\rangle$, состояние трансформируется так

$$|a, a^{-1}\rangle \mapsto |bab^{-1}, ba^{-1}b^{-1}\rangle. \tag{24}$$

Это — нетривиальное преобразование (по крайней мере, для некоторого b) в том случае, если a принадлежит классу сопряжённости, содержащего более чем один элемент. На самом деле, для каждого класса сопряжённости α существует единственное состояние $|0, \alpha\rangle$ с нулевым зарядом, которое можно представить унифицированной суперпозицией представителей класса:

$$|0, \alpha\rangle = \frac{1}{\sqrt{|\alpha|}} \sum_{a \in \alpha} |a, a^{-1}\rangle, \tag{25}$$

где $|\alpha|$ обозначает порядок α. Пара флаксонов в классе α, которые могут родиться в локальном процессе, не должны нести какие-либо сохраняющиеся заряды и следовательно должны быть в состоянии $|0, \alpha\rangle$. Другие линейные комбинации, ортогональные $|0, \alpha\rangle$, несут ненулевой заряд. Этот заряд, который несёт пара флаксонов, может быть измерен другими флаксонами, хотя странно, что заряд не может быть локализован в одной частице пары. Скорее это коллективное свойство пары целиком. Если два флаксона с ненулевым общим зарядом сталкиваются, аннигиляция пары будет запрещена законом сохранения заряда, даже если полный поток равен нулю.

В случае пары флаксонов из двойного класса группы $G = S_3$, например, существует двумерное подпространство с тривиальным полным потоком и нетривиальным зарядом, для которого можно выбрать базис

$$\begin{aligned} |0\rangle &= |(12),(12)\rangle + \bar{\omega}|(23),(23)\rangle + \omega|(31),(31)\rangle, \\ |1\rangle &= |(12),(12)\rangle + \omega|(23),(23)\rangle + \bar{\omega}|(31),(31)\rangle. \end{aligned} \tag{26}$$

Если поток b перемещается вокруг пары, оба потока сопрягаются по b. Следовательно преобразование (посредством сопряжения) этих состояний будет

$$\begin{aligned} D(12) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad D(23) = \begin{pmatrix} 0 & \bar{\omega} \\ \omega & 0 \end{pmatrix}, \quad D(31) = \begin{pmatrix} 0 & \omega \\ \bar{\omega} & 0 \end{pmatrix}, \\ D(123) &= \begin{pmatrix} \omega & 0 \\ 0 & \bar{\omega} \end{pmatrix}, \quad D(132) = \begin{pmatrix} \bar{\omega} & 0 \\ 0 & \omega \end{pmatrix}. \end{aligned} \tag{27}$$

Это преобразование, соответствующее двумерному неприводимому представлению $R = \{2\}$ группы S_3, отсюда заключаем, что заряд пары флаксонов равен $\{2\}$.

Более того, с помощью сплетений этот заряд, который несёт пара флаксонов, может быть перенесён другим частицам. К примеру, рассмотрим пару частиц, каждая из которых несёт заряд, но не поток (будем называть их чарджионом), так что полный заряд пары тривиален. Если один из чарджионов преобразуется как унитарное

неприводимое представление R группы G, существует единственное сопряжённое представление $\bar{R}$, которое может быть объединено с представлением R, результатом чего стало бы тривиальное представление. Если $\{|R,i\rangle\}$ — базис в R, тогда базис $\{|\bar{R},i\rangle\}$ может быть выбран для $\bar{R}$ так, что чарджионная пара с тривиальным зарядом может быть представлена в виде

$$|0,R\rangle = \frac{1}{\sqrt{|R|}}\sum_i |R,i\rangle\otimes|\bar{R},i\rangle. \tag{28}$$

Пусть созданы — пара флаксонов в состоянии $|0;\alpha\rangle$ и пара чарджионов в состоянии $|0;R\rangle$. Затем чарджион с зарядом R перемещается вокруг флаксона с потоком в классе α против часовой стрелки, и два чарджиона опять сталкиваются, чтобы увидеть, аннигилируют ли они.

Для выбранного значения потока $a \in \alpha$ эффектом обхода состояния двух чарджионов будет

$$|0;R\rangle = \frac{1}{\sqrt{|R|}}\sum_{i,j} |R,j\rangle\otimes|\bar{R},i\rangle D^R_{ji}(a). \tag{29}$$

Если теперь будет измерен заряд пары, то вероятность того, что заряд окажется нулевым, равна квадрату перекрытия этого состояния с состоянием $|0;R\rangle$, т. е.

$$Prob(0) = \left|\frac{\chi^R(a)}{|R|}\right|^2, \tag{30}$$

где

$$\chi^R(a) = \sum_i D^R_{ii}(a) = tr\, D^R(a) \tag{31}$$

есть характер представления R, вычисленного в a. Вообще-то, характер (след) инвариантен по отношению к сопряжению — он имеет одно и то же значение для всех $a \in \alpha$. Следовательно, вероятность обнаружить нулевой заряд пары чарджионов после вращения одного из них вокруг флаксона равна таковой при обороте одного чарджиона вокруг пары флаксонов. Конечно, поскольку полный заряд всех четырёх частиц равен нулю, и заряд сохраняется, то после вращения две пары имеют противоположные заряды: если пара чарджионов имеет полный заряд R', тогда пара флаксонов должна иметь заряд $\overline{R'}$ такой, что в комбинации с R' дало бы тривиальный полный заряд. Пара частиц с нулевым полным зарядом и потоком могут аннигилировать не оставляя после этого никакой стабильной частицы, в то время как пара с ненулевым зарядом не сможет аннигилировать «полностью». Из этого становится ясно, что если мировые линии флаксонной и чарджионной пар зацепятся один раз, то вероятность того, что обе пары смогут аннигилировать даётся формулой (30). Эта вероятность меньше, чем единица, гарантируя при этом то, что представление R не одномерное и класс α не представлен тривиально. Таким образом, зацепление мировых линий приводит к обмену зарядом между двумя парами.

К примеру, в случае, когда α двойной класс группы $G = S_3$ и $R = \{2\}$ (двумерное неприводимое представление S_3), видим из выражений (27), что $\chi^{\{2\}}(\alpha) = 0$. Следовательно, обмен зарядом достоверно происходит: после обхода и флаксонная пара, и чарджионная пара преобразовываются как $R' = \{2\}$.

Суперотборный сектор неабелевого сверхпроводника

При рассмотрении неабелевого сверхпроводника до сих пор рассматривались два типа частиц: флаксоны, которые несут поток, но не заряд, и чарджионы, которые несут заряд, но не поток. Но, вообще говоря, они не являются наиболее общими возможными частицами. Каков заряд частицы, составленной из флаксона и чарджиона? В принципе, заряд может быть измерен в интерференционном эксперименте Ааронова-Бома. Можно спрятать объект, заряд которого должен быть найден, за экраном между двумя щелями, запустить пучок точно откалиброванных флаксонов на экран, и детектировать их за экраном. По смещению и интенсивности интерференционной схемы положений флаксонов в пространстве можно определить $D^R(b)$ для каждого $b \in G$, что позволит установить R. Однако есть некоторая неопределенность, так как исследуемый объект несёт нетривиальный поток $a \in G$ вместе с зарядом. Поскольку оборот потока b вокруг потока a меняет a на bab^{-1}, то две возможных траектории, по которой следует поток b, не взаимодействуют, если a и b не коммутируют. После того, как поток b зарегистрирован, можем проверить, изменился ли поток a, и определить, прошёл ли поток через одну, или другую щель экрана. Из-за того, что поток (a или bab^{-1}) связан с вариантом траектории (левая или правая щель), интерференция разрушается. Следовательно, эксперимент даёт информацию о заряде, но только в случае, если a и b коммутируют. Значит заряд, прикреплённый к потоку a, не описывается как неприводимое представление группы G. Вместо этого он описывается как неприводимое представление подгруппы группы G, нормализатора $N(a)$ по элементу a группы G, которая определяется как

$$N(a) = \{b \in G | ab = ba\}. \tag{32}$$

Нормализаторы $N(a)$ и $N(bab^{-1})$ изоморфны, поэтому можно ассоциировать нормализатор с классом сопряжённости α группы G, а не с конкретным элементом. Следовательно, каждый тип частицы, который может возникать в нашем неабелевом сверхпроводнике, имеет в действительности две метки: класс сопряжённости α, описывающий поток, и неприводимое представление $R^{(\alpha)}$ нормализатора $N(\alpha)$, который описывает заряд. Ут-

верждается, что α и $R^{(\alpha)}$ категоризируют суперотборный сектор теории, поскольку они являются свойствами локализованного объекта, которые должны сохраняться во всех локальных физических процессах. Для частиц, которые несут метки (α, $R^{(\alpha)}$), введем $|\alpha| \cdot |R^{(\alpha)}| \equiv d_{(\alpha,R^{(\alpha)})}$ — это величина называется размерностью сектора. Но если эти частицы заплетены с другими частицами, то вид частиц может поменяться, в то время как метки (α, $R^{(\alpha)}$) остаются инвариантными.

В любой теории анионов, размерность может быть поставлена в соответствие любому типу частицы, хотя размерность не обязана быть целой, и может не иметь прямой интерпретации в терминах подсчёта различных видов одного типа. Полная размерность D может быть определена суммированием по всем типам, и в случае неабелевого сверхпроводника имеем

$$D^2 = \sum_{\alpha} \sum_{R^{(\alpha)}} d^2_{(\alpha,R^{(\alpha)})} = \sum_{\alpha} |\alpha|^2 \sum_{R^{(\alpha)}} |R^{(\alpha)}|^2. \tag{33}$$

Поскольку сумма квадратов размерностей по всем неприводимым представлениям конечной группы является порядком группы, а порядок нормализатора $N(\alpha)$ равен $|G|/|\alpha|$, имеем

$$D^2 = \sum_{\alpha} |\alpha| \cdot |G| = |G|^2, \tag{34}$$

а полная размерность $D = |G|$. Для случая $G = S_3$ есть 8 типов частиц, перечисленных в таблице:

Таблица. 8 типов частиц для случая $G = S_3$.

Тип	Поток	Заряд	Размерность
A	e	{+}	1
B	e	{-}	1
C	e	{2}	2
D	(12)	{+}	3
E	(12)	{-}	3
F	(123)	{1}	2
G	(123)	{ω}	2
H	(123)	{$\bar{\omega}$}	2

Если поток тривиален (обозначено e), тогда заряд может быть любым из трёх неприводимых представлений группы S_3: тривиальным одномерным представлением {+}, нетривиальным одномерным представлением {-}, или двумерным представлением {2}. Если поток двойной, тогда нормализатором является Z_2, и зарядом может быть либо тривиальное представление {+}, либо нетривиальное представление {-}. И если поток тройной, то нормализатором будет Z_3, и заряд — может быть либо тривиальным представлением {1}, либо нетривиальным представлением {ω}, либо его сопряжённым представлением {$\bar{\omega}$}. Вы можете проверить, что полной размерностью будет $D = |S_3| = 6$, как это и должно быть.

Поскольку a коммутирует со всеми элементами $N(a)$ по определению, то матрица $D^{R^{(a)}}(a)$, которая представляет a в неприводимом представлении $R^{(a)}$, коммутирует со всеми матрицами в представлении. Следовательно, по лемме Шура она кратна единице

$$D^{R^{(a)}}(a) = exp\left(i\theta_{R^{(a)}}\right)I. \tag{35}$$

Чтобы оценить важность фазы $exp\left(i\theta_{R^{(a)}}\right)$, рассмотрим композит поток-заряд, в котором чарджион в представлении $R^{(\alpha)}$ скреплён с потоком a, и представим вращение этого композитного объекта на 2π против часовой стрелки. Это вращение перемещает заряд вокруг потока, порождая фазу

$$e^{-i2\pi J} = e^{i\theta_{R^{(a)}}}. \tag{36}$$

Значит каждый суперотборный сектор имеет определённое значение топологического спина, определяемого по $\theta_{R^{(a)}}$.

Поток составного объекта может принадлежать к любому классу сопряжённости, который может быть получен произведением представителей классов, соответствующих двум составляющим объекта. Нахождение заряда составной системы особенно утончено, поскольку нужно разложить тензорное произведение представлений двух разных нормализаторных групп на сумму представлений нормализатора полного потока. В случае, когда $G = S_3$, правило, указывающее путь слияния двух частиц типа D, будет таким

$$D \times D = A + C + F + G + H. \tag{37}$$

Отмечалось, что слияние двух двойных потоков может привести либо к тривиальному полному потоку, либо к тройному потоку, и что заряд композита с тривиальным полным потоком может быть либо {+} или {2}. Если полный поток тройной, тогда собственными состояниями заряда являются собственные состояния оператора сплетения, который был сконструирован в (30).

Почему для системы из двух анионов собственные состояния полного заряда должны быть также собственными состояниями оператора сплетения? Можно понять эту связь, думая об угловом моменте двух-

анионного составного объекта. Оператор монодромии R^2 инкапсулирует в себе эффект обхода одной частицей против часовой стрелки вокруг другой. Этот обход — то же самое, что и вращение составной системы против часовой стрелки на 2π, кроме того, что вращение последней поворачивает обе компоненты. Можно компенсировать вращение этих компонент последующим за вращением составной системы против часовой стрелки вращением компонент по часовой стрелке. Следовательно, оператор монодромии может быть представлен как

$$(R_{ab}^{c})^2 = e^{-i2\pi J_c} e^{i2\pi J_a} e^{i2\pi J_b} = e^{i(\theta_c - \theta_a - \theta_b)}. \quad (38)$$

Здесь R_{ab}^{c} обозначает оператор сплетения для обмена местами частиц типов *a* и *b* против часовой стрелки, которые объединены вместе в композит типа *c*, и используя более лаконичное, чем прежде, обозначение, в котором *a*, *b*, *c* являются обобщёнными метками суперотборного сектора (указывающими, в модели неабелевого сверхпроводника, и заряд, и спин). Поскольку каждый суперотборный сектор имеет определённый топологический спин, и монодромный оператор диагонален в базисе топологического спина, видно, что собственные состояния оператора сплетения совпадают с собственными состояниями заряда. Заметим, что (38) обобщает первоначальные исследования абелевых анионов, когда было видно, что композит двух идентичных анионов имеет топологический спин $e^{i4\theta}$, и что обменная фаза анионной-антианионной пары (с тривиальным полным спином) равна $e^{-i\theta}$.

Квантовые вычисления на неабелевых анионах

Модель анионов характеризуется ответами на два основных вопроса:

1) Что происходит, когда два аниона объединяются вместе (каковы *правила слияния*)?
2) Что происходит, когда два аниона обмениваются местами (каковы *правила сплетения*)?

Выше было описано, как ответить на эти вопросы в специальном случае модели неабелевого сверхпроводника, где использовалась связь с неабелевой конечной группой *G*. Сейчас надо понять как эти правила слияния и сплетения могут быть использованы в моделировании квантового тока.

Разрабатывая принципы моделирования, будем основываться на следующих физических возможностях:

Рождение и идентификация пар. Можно создавать пары частиц, и определить тип каждой частицы (класс сопряжённости α потока каждой из частиц пары, и заряд частицы — неприводимое представление $R^{(\alpha)}$ нормализаторной группы потока N(α)). Это предположение разумно, поскольку нет частиц различных типов, подчиняющихся отношению симметрии; у них различимые физические свойства: например, разные ширины запрещённых энергетических зон и разные эффективные массы. На практике, единственными типами частиц, которые понадобятся, будут флаксоны, которые не несут заряд, и чарджионы, которые не несут поток.

Аннигиляция пар. Можно объединить две частицы, и наблюдать за тем, аннигилировала ли пара полностью. Таким образом, получаем ответ на вопрос: Имеет ли данная пара частиц тривиальный поток и заряд, или нет? Это предположение тоже разумно, поскольку если пара несёт нетривиальное значение некоторой сохраняющейся величины, то должно остаться локализованное возбуждение, когда пара аннигилирует, и эта остаточная частица, в принципе, детектируема.

Сплетение. Можно вести частицы вдоль указанных траекторий, и так осуществлять обмены частиц. Выбирая мировые линии частиц, которые реализуют нужную косу, получаем возможность моделировать квантовые гейты.

Эти операции будут основой для осуществления более сложных операций в циклическом режиме. Во-первых, можно использовать чарджионы для калибровки флаксонов и установлению некоторого стандарта. Предположим, есть две пары флаксонов в состояниях $|a, a^{-1}\rangle$ и $|b, b^{-1}\rangle$, и надо определить, одинаковы ли флаксоны *a* и *b*. Создадим чарджион-античарджионную пару, где заряд чарджиона является неприводимым представлением *R* в *G*. Затем переместим чарджион по замкнутой траектории, которая окружает первый компонент первой флаксонной пары и второй компонент второй флаксонной пары, переобъединим чарджион с античарджионом, и посмотрим аннигилирует ли чарджион-античарджионная пара или нет. Поскольку полный поток, охватываемый чарджионной траекторией, равен ab^{-1}, чарджионная пара аннигилирует с вероятностью

$$Prob(0) = \left| \frac{\chi^R(\mathrm{ab}^{-1})}{|R|} \right|^2, \quad (39)$$

которая меньше единицы, если поток ab^{-1} не равен единице (предполагая, что представление *R* не одномерное и представляет ab^{-1} нетривиально). Таким образом, если аннигиляции пары не произойдёт, то известно наверняка, что *a* и *b* — разные потоки, а в обратном случае — вероятность их совпадения растёт. Повторяя эту процедуру конечное число раз, с высокой статистической достоверностью можно сделать вывод о том, одинаковы ли *a* и *b*.

Эта процедура позволяет отсортировать флаксонные пары в множества с одинаковым потоком. Если множество содержит *n* пар, то его общее состояние является смесью состояний вида

$$\sum_{a\in G}\psi_a|a,a^{-1}\rangle^{\otimes n}. \tag{40}$$

Избавляясь от одной пары в множестве, каждое такое состояние становится смесью вида

$$\sum_{a\in G}\rho_a(|a\rangle\langle a|)^{\otimes(n-1)}. \tag{41}$$

Можно рассматривать каждое множество как содержащее $(n-1)$ пару, имеющую определённый поток, но где этот поток пока ещё не известно.

Чтобы идентифицировать множества, пометим множества элементами из группы *G*. Для достижения непротиворечивого соответствия элементам группы, будем «извлекать» пары флаксонов из трёх различных множеств. Допустим, тремя парами будут $|a,a^{-1}\rangle$, $|b,b^{-1}\rangle$ и $|c,c^{-1}\rangle$, и надо проверить равенство $c=ab$. Создаём чарджион-античарджионную пару, перемещаем чарджион по замкнутой траектории, охватывающей первый компонент первой пары флаксонов, первый компонент второй пары, и второй компонент третьей пары, наблюдаем, аннигилирует ли вновь объединённая чарджионная пара или нет. Поскольку полный поток, охватываемый чарджионной траекторией равен abc^{-1}, повторяя процедуру можно определить с высокой статистической доверительностью, одинаковы ли ab и c. Такие наблюдения позволяют пометить множества так, чтобы это соответствовало правилу композиции группы. Это соответствие однозначно, не считая групповых автоморфизмов (и неоднозначности, возникающие в автоморфизмах, могут быть разрешены произвольным образом). Как только установлены стандарты для потоков, можно использовать их для измерения неизвестного потока непомеченной пары. Если состояние пары, которая должна подвергнуться измерению, равно $|d,d^{-1}\rangle$, можно извлечь помеченную пару $|a,a^{-1}\rangle$ из множества и использовать чарджионные пары для измерения потока ad^{-1}. Повторяя эту процедуру с другими помеченными потоками, можно, в итоге, определить значение потока *d*, осуществляя проективное измерение потока.

Для моделирования квантовых вычислений с помощью флаксонов понадобится выполнение логического гейта, действующего на значение потока. Основной гейт, который будем использовать, реализуется перемещением флаксонной пары, находящейся в состоянии $|a,a^{-1}\rangle$, против часовой стрелки вокруг первого компонента другой флаксонной пары, находящейся в состоянии $|b,b^{-1}\rangle$. Поскольку пара $|a,a^{-1}\rangle$ имеет тривиальный полный поток, пара $|b,b^{-1}\rangle$ не подвергается никакому влиянию в результате процедуры перемещения. Но ввиду того эффекта, когда поток b перемещается против часовой стрелки вокруг обоих компонентов пары, чьё начальное состояние было $|a,a^{-1}\rangle$, эта пара преобразуется как

$$|a,a^{-1}\rangle\longmapsto|bab^{-1},ba^{-1}b^{-1}\rangle. \tag{42}$$

Условимся называть эту операцию действием сопрягающего гейта на флаксонную пару. Далее необходимо решить, как кодировать кубиты используя флаксоны. Подходящие кодировки могут быть выбраны различными способами. Воспользуемся одним конкретным выбором, который иллюстрирует ключевые идеи [99]. А именно, кодируем кубит, используя пару флаксонов, где полный поток пары тривиален. Выберем два некоммутирующих элемента $a,b\in G$, где $b^2=e$, и выберем расчётный базис для кубита:

$$|\bar{0}\rangle=|a,a^{-1}\rangle,\qquad |\bar{1}\rangle=|bab^{-1},ba^{-1}b^{-1}\rangle. \tag{43}$$

Важным является то, что один изолированный флаксон с потоком a «выглядит» идентичным флаксону с сопряжённым потоком bab^{-1}. Следовательно, если два флаксона пары удерживаются далеко друг от друга, локальные взаимодействия со средой не приведут к декогеренции суперпозиции состояний $|\bar{0}\rangle$ и $|\bar{1}\rangle$. Квантовая информация защищена от повреждения (поскольку она хранится нелокально), используя топологическое вырождение состояний, в которых флаксон и антифлаксон «закреплены» в фиксированных и пространственно разделённых положениях.

В отличие от топологического вырождения, которое возникает в системах абелевых анионов, этот защищённый кубит может быть померен относительно легко, без обращения к интерферометрическим процедурам, которые извлекают фазы Ааронова-Бома. Уже было описано, как измерить поток, используя предварительно откалиброванные флаксоны. Следовательно, можно осуществить проективное измерение оператора Паули $\bar{\sigma}_z$ (проекцию на базис $\{|\bar{0}\rangle,|\bar{1}\rangle\}$). Также можно померять дополняющий оператор Паули $\bar{\sigma}_x$, хотя деструктивно и неточно. Собственными состояниями $\bar{\sigma}_x$ являются

$$|\pm\rangle=\frac{1}{\sqrt{2}}(|\bar{0}\rangle\pm|\bar{1}\rangle)\equiv\frac{1}{\sqrt{2}}(|a,a^{-1}\rangle\pm|bab^{-1},ba^{-1}b^{-1}\rangle). \tag{44}$$

Следовательно, состояние $|-\rangle$ ортогонально состоянию с нулевым зарядом

$$|0;\alpha\rangle=\frac{1}{\sqrt{|\alpha|}}\left(\sum_{c\in\alpha}|c,c^{-1}\rangle\right), \tag{45}$$

где α — класс сопряжённости, который содержит *a*. С другой стороны, состояние $|+\rangle$ имеет ненулевое перекрытие с $|0;\alpha\rangle$

$$\langle+|0;\alpha\rangle=\sqrt{2/|\alpha|}. \tag{46}$$

Следовательно, если два компонента флаксонной пары сводятся вместе, то полная аннигиляция невозможна, если пара находится в состоянии $|-\rangle$, и возникает с вероятностью $Prob(0) = 2/|\alpha|$, если состоянием пары есть $|+\rangle$.

Заметим, что есть также возможность приготовить флаксонную пару в состоянии $|+\rangle$. Для этого можно создать пару в состоянии $|0;\alpha\rangle$. Если α содержит только два элемента a и bab^{-1}, то всё готово. Иначе, — сравниваем вновь созданную пару с откалиброванными парами в каждом из состояний $|c, c^{-1}\rangle$, где $c \in \alpha$ и c отличается и от a, и от bab^{-1}. Если пара не будет совпадать ни с одной из пар $|c, c^{-1}\rangle$, его состояние должно быть $|+\rangle$.

Чтобы продвигаться дальше, нужно определить вычислительную мощность гейта сопряжения. Используем для этого более компактное обозначение, в котором состояние $|x, x^{-1}\rangle$ флаксонной пары обозначается просто $|x\rangle$, и рассмотрим преобразования состояния $|x, y, z\rangle$, которые могут быть построены из гейтов сопряжения. Перемещая третью пару вокруг первой, либо по часовой стрелке, либо против, можно реализовать выполнение гейтов

$$|x, y, z\rangle \mapsto |x, y, xzx^{-1}\rangle, \qquad |x, y, z\rangle \mapsto |x, y, x^{-1}zx\rangle, \tag{47}$$

а перемещая третью пару вокруг второй, либо по часовой стрелке, либо против, можем реализовать выполнение гейтов

$$|x, y, z\rangle \mapsto |x, y, yzy^{-1}\rangle, \qquad |x, y, z\rangle \mapsto |x, y, y^{-1}zy\rangle. \tag{48}$$

Кроме того, используя дополнительную пару с потоком $|c\rangle$, имеем

$$|x, y, z\rangle \mapsto |x, y, czc^{-1}\rangle \tag{49}$$

для любого постоянного $c \in G$. Составляя эти элементарные операции, можно выполнить любой гейт вида

$$|x, y, z\rangle \mapsto |x, y, fzf^{-1}\rangle, \tag{50}$$

где функция $f(x, y)$ может быть выражена в мультипликативной форме, т.е. как конечное произведение групповых элементов, где элементы, возникающие в произведении, могут быть входными x и y, их обратными x^{-1} и y^{-1}, или постоянными элементами из G, каждый из которых может участвовать в произведении любое число раз.

Найдем функции $f(x, y)$, которые могут быть представлены в этой форме. Напомним, что подгруппа H конечной группы G является нормальной, если для любого $h \in H$ и любого $g \in G$, $ghg^{-1} \in H$, и что конечная группа G называется простой, если G не имеет нормальных подгрупп, кроме самой G и тривиальной группы $\{e\}$. Если группа G является простой неабелевой конечной группой, то любая функция $f(x, y)$ может быть представлена в мультипликативной форме. В частности, если группа G неабелева и проста, то существует функция f, которая может быть представлена так

$$f(a, a) = f(a, bab^{-1}) = f(bab^{-1}, a) = e, \qquad f(bab^{-1}, bab^{-1}) = b. \tag{51}$$

Таким образом, для $x, y, z \in \{a, bab^{-1}\}$, действие $|x, y, z\rangle \mapsto |x, y, fzf^{-1}\rangle$ приводит к «переворачиванию» потока третьей пары тогда, и только тогда, когда $x = y = bab^{-1}$. То есть, из элементарных операций теперь сконструирован гейт Тоффоли в расчётном базисе. Следовательно, гейтов сопряжения, действующих на стандартные базисные состояния, оказывается достаточно для осуществления универсального обратимого классического вычисления.

Неабелевой простой группой минимального порядка является A_5, группа чётных перестановок пяти объектов ($|A_5| = 60$). Конкретная реализация универсального классического вычисления с использованием гейтов сопряжения выполняется выбором a, являющегося тройным элементом $a = (345) \in A_5$, и b, произведения двух двойных элементов $b = (12)(34) \in A_5$, так что $bab^{-1} = (435)$.

В теории квантовой помехоустойчивости, если можно осуществить классические гейты Тоффоли и *CNOT* (контролируемого «NOT»), для универсального квантового вычисления будет достаточно иметь возможность выполнять каждый из операторов Паули σ_x, σ_y и σ_z, и иметь возможность выполнить проективное измерение каждого из σ_x, σ_y и σ_z. Но, проективное измерение σ_x и σ_y, и выполнение σ_z отсутствуют среди допустимых операций. Посмотрим, как можно улучшить несовершенное деструктивное измерение σ_x до надёжного проективного измерения σ_x. Вспомним действие сопряжения *CNOT* на операторы Паули:

$$CNOT\colon \sigma_x I \mapsto \sigma_x \sigma_x, \tag{52}$$

где первый кубит — контрольный, а второй — целевой для *CNOT*. Следовательно, гейтов *CNOT* вместе с возможностью готовить собственные состояния $X = 1$ и выполнять деструктивные измерения σ_x оказывается достаточно для выполнения проективных измерений σ_x. Можно приготовить вспомогательный кубит в собственном состоянии $\sigma_x = 1$, выполнить *CNOT* со вспомогательным кубитом в качестве контрольного и информацией, которая должна быть измерена, в качестве целевой, и затем деструктивно померять вспомогателный кубит. Измерение приготовит информацию в собственном состоянии σ_x, собственные значения которого совпадают с выходом измерения вспомогательного кубита. В нашем случае, деструктивное измерение не вполне надёжно, но можно повторить измерение несколько раз. Каждый раз готовится и измеряется новый вспомогательный кубит, и после нескольких повторений измерений будем иметь приемлемую статистическую доверительность.

Когда же можно измерять σ_x проективно, то есть возможность приготовить как собственные состояния $\sigma_x = -1$, так и собственные состояния $\sigma_x = 1$ (например, за измерением σ_z проводим измерение σ_x, пока в итоге ни получим выход $\sigma_x = -1$). Затем, выполняя гейт *CNOT*, целевым состоянием которого является собствен-

ное состояние $\sigma_x = -1$, можем выполнить оператор Паули, действующий на контрольный кубит. Остаётся только показать, что может быть осуществлено измерение σ_y. Это измерение кажется проблематичным, поскольку наши физические возможности не содержат способов различать собственные состояния $\sigma_y = 1$ и $\sigma_y = -1$ (то есть состояния ψ и его комплексно сопряжённое ψ^*). Однако эта неоднозначность не вызывает серьёзных сложностей, поскольку не важно, как эта неопределённость разрешается. Если бы нужно было заменить измерение σ_y измерением $-\sigma_y$ в нашем моделировании унитарного преобразования U, то несмотря на это эффект моделирования U^* всё равно сохранился бы. Эта замена не изменила бы распределение вероятностей выходов для измерений в стандартном расчётном базисе.

Теперь можно сформулировать протокол для измерения σ_y, отмечая при этом, что применение гейта Тоффоли, чьим целевым кубитом является собственное состояние $\sigma_x = -1$, осуществляет гейт контролируемой фазы $\Lambda(Z)$, действующего на два контрольных кубита. Компонуя этот гейт с гейтом CNOT $\Lambda(\sigma_x)$, получаем гейт $\Lambda(i\sigma_y)$, действующий следующим образом:

$$\begin{aligned}\Lambda(i\sigma_y)\colon\quad & |\sigma_x = +1\rangle \otimes |\sigma_y = +1\rangle \mapsto |\sigma_y = +1\rangle \otimes |\sigma_y = +1\rangle,\\ & |\sigma_x = +1\rangle \otimes |\sigma_y = -1\rangle \mapsto |\sigma_y = -1\rangle \otimes |\sigma_y = -1\rangle,\\ & |\sigma_x = -1\rangle \otimes |\sigma_y = +1\rangle \mapsto |\sigma_y = -1\rangle \otimes |\sigma_y = +1\rangle,\\ & |\sigma_x = -1\rangle \otimes |\sigma_y = -1\rangle \mapsto |\sigma_y = +1\rangle \otimes |\sigma_y = -1\rangle,\end{aligned} \tag{53}$$

где первый кубит — контрольный, а второй — целевой. Теперь предположим, что у нас есть начальный кубит в состоянии $|\sigma_y = 1\rangle$. Известно, как можно приготовить состояния $|\sigma_x = 1\rangle$ и как выполнить гейты $\Lambda(i\sigma_y)$. Следовательно, поскольку гейт $\Lambda(i\sigma_y)$ с целевым $|\sigma_y = 1\rangle$ преобразует $|\sigma_x = 1\rangle$ в $|\sigma_y = 1\rangle$, можно сделать много копий первоначального состояния $|\sigma_y = 1\rangle$. Для того, чтобы измерить σ_y, необходимо применить обратный гейт $\Lambda(i\sigma_y)$, целевым кубитом которого является измеряемый кубит, а контролируемым — одно из скопированных состояний $\sigma_y = 1$. Затем производим измерение σ_x вспомогательного кубита для считывания результата измерения σ_y другого кубита. Если первоначальный кубит находился не в состоянии $|\sigma_y = 1\rangle$, а в состоянии $|\sigma_y = -1\rangle$, то будут сделаны копии состояния $|\sigma_y = -1\rangle$, и проводиться измерения $-\sigma_y$ вместо σ_y. По сути, будет проводиться моделирование комплексного сопряжения идеальной схемы, но это не изменит конечного результата квантового вычисления. Аналогично равновероятная смесь состояний $|\sigma_y = 1\rangle$ и $|\sigma_y = -1\rangle$ в начальном кубите не повлияет на правильность моделирования. То есть в качестве начального состояния можно использовать равновероятную суперпозицию с $\rho = I/2$, которую известно, как приготовить.

Это завершает демонстрацию возможности эффективного и помехоустойчивого моделирования квантового вычисления, используя флаксоны и чарджионы неабелевого сверхпроводника, по крайней мере в случае, когда группа G является простой неабелевой конечной группой (Мочон показал, что универсальное квантовое вычисление возможно и для более широкого класса групп [100]). В целом, включая приготовления всех состояний и калибровку флаксонов, это моделирование может быть представлено так:

1) Приготавливается много пар анионов (флаксонов и чарджионов).

2) Мировые линии анионов сплетаются в выбранную структуру косы.

3) Пары анионов снова объединяются для верификации их аннигиляции.

Моделирование является недетерминистическим в том смысле, что реальная коса, осуществляемая анионами, зависит от результатов измерений, проводимых (с помощью объединений в пары) в ходе моделирования. Оно устойчиво к ошибкам, если температура мала по сравнению с шириной запретной зоны, и если частицы находятся достаточно далеко друг от друга (кроме моментов, когда пары создаются и объединяются), чтобы подавить обмен виртуальными анионами. Небольшие деформации мировых линий частиц не оказывают никакого эффекта на результат вычисления, поскольку сплетение частиц находится в правильном топологическом классе.

ЗАКЛЮЧЕНИЕ

Таким образом, в работе рассмотрены основные концепции квантовых вычислений, приведены наиболее разработанные квантовые алгоритмы и некоторые схемы помехоустойчивого кодирования, основанных на топологических свойствах рассматриваемых систем.

Вводное описание концепции топологического квантового вычисления и доказательство её принципиальной реализуемости использует модель неабелевого сверхпроводника, отличительной характеристикой которой является близость к практической реализации. Это позволяет интуитивно сформировать понимание свойств неабелевых анионов. Однако такая модель не единственна. Существуют более элегантные и простые модели, которые избавлены от некоторых усложнений (различия между флаксонами и чарджионами, калибровки потоков, и измерений, требуемых для моделирования неклассических гейтов), лишающих теорию абстрактной красоты. Кратко рассмотрим пути построения обобщённой теории анионов.

Обобщённая анионная модель — это теория частиц дробной статистики с локально сохраняющимися зарядами на двумерной поверхности. Теория не предполагает дальнодействия между частицами, и характеризуется тремя определяющими свойствами:

1) Набором типов частиц. Типы — это метки, устанавливающие возможные значения сохраняющегося заряда, который может нести частица.

2) Правила слияния и деления, указывающие возможные значения заряда, которые могут быть получены, когда две частицы с известными зарядами объединяются, либо возможные варианты деления одной частицы с известным зарядом на две других.

3) Правила сплетения, указывающие исход обмена частиц местами.

На основе этих трёх отправных пунктов конструируется математический объект, называемый унитарным топологическим модулярным функтором [99, 101]. Он тесно связан с двумя другими объектами, которые сейчас интенсивно исследуются: топологической квантовой теорией поля в 2+1-мерном пространстве-времени [102–104], и конформной теорией поля в 1+1–мерном пространстве–времени [105–108]. Большинство известных моделей анионов конструируются с использованием более эффективных методов и являются частными случаями теории Черна–Саймонса [99].

Существует доказательство того, что вычислительная мощность топологического квантового компьютера не превышает мощности обычного квантового компьютера и равна ей для неабелевых анионов со специальными свойствами (например, для анионов Фибоначчи) [109]. Однако важнейшим преимуществом первого является естественная топологическая помехоустойчивость, что определяет предпочтительность использования топологических моделей квантовых компьютеров.

Несмотря на то, что состояния квантовых кос по своей природе более устойчивы, чем состояния, удерживаемых в ловушке квантовых частиц, существует потребность в контроле ошибок, возникающих в результате тепловых колебаний, рождающих случайные блуждающие пары анионов, которые вплетаются в близлежащие косы. Решение задачи контроля тепловых ошибок осуществляется при помощи пространственного разделения анионов на расстояния, где уровень посторонних вплетений не превышает допустимого значения. Оценка частоты ошибок, например, для логической операции NOT, действующей на состояние кубита, оказывается равной 10^{-30} или даже меньше. Хотя эта оценка поддавалась некоторой критике о значительном завышении, есть основания полагать, что в то время, как в других схемах квантовой обработки информации коррекция ошибок трудноосуществима, либо вообще непригодна, топологически защищенные системы будут особенно устойчивы к возникновению источников ошибок, а значит и обладать повышенной надёжностью.

Авторы выражают благодарность В.В. Калашникову за многочисленные и ценные обсуждения, а также В.Е. Корепину за прочтение рукописи и полезные замечания.

СПИСОК ЛИТЕРАТУРЫ

1. Feynman R. Simulating physics with computers // Int. J. Theoret. Phys. –1982. –Vol.21. –P.467-488.
2. Odiyzko A.M. The future of integer factorization // Preprint AT&T Bell Laboratories. –1995. –16p.
3. A discussion of RSA-129 activity // http://www.math.okstate.edu/~wrightd/numthry/rsa129.html
4. Shor P.W. Polynomial-time algorithms for prime factorization and discrete logs on a quantum computer // SIAM J. Comput. –1997. –Vol.26. –P.1484-1509.
5. Feynman R. Simulating physics with computers // Physics of computation, Part II (Dedham, Mass., 1981). Internat. J. Theoret. Phys. –1981/82. –Vol.21, №6-7. –P.467-488.
6. Casati G., Zoller P., Shepelyansky D.L. Quantum computers, algorithms and chaos // Proceedings of the International school of physics “Enrico Fermi”. –Bologna. –2006. –620p.
7. Song P.H., Shepelyansky D.L. Quantum computing of quantum chaos and imperfection effects // Phys. Rev. Lett. –2001. –Vol.86. –P.2162-2165.
8. Grover L.K. A fast quantum mechanical algorithm for database search // Proc. 28th Annual ACM Symposium on the Theory of Computing. –1996. –P.212-219.
9. Wiesner S. Conjugate coding // Sigact News. –1983. –Vol.15, №1. –P.78-88.
10. Holevo A. Some estimates of the information transmitted by quantum communication channels // Probl. Inform. Trans. –1973. –Vol.9, №3. –P.177-183.
11. Поплавский Р.П. Термодинамические модели обработки информации // Успехи физических наук. –1975. –Т.115, В.3. –С.465-501.
12. Ingarden R.S. Quantum information theory // Reports in Mathematical Physics. –1976. –Vol.10. –P.43–72.
13. Toffoli T. Reversible Computing. –Massachusetts, 1980. –36p.
14. Bennett C.H., Brassard G. An Update on Quantum Cryptography // Advances in Cryptology: Proceedings of CRYPTO 84. –1985. –Vol.196. –P.475-480.
15. Deutsch D. Quantum theory, the Church-Turing principle, and the universal quantum computer // Proc. Roy. Soc. of Lond. A, Mathematical and Physical Sciences. –1985. –Vol.400, №1818. –P.97-117.
16. Ekert A. La mecanique quantique au secours des agents secrets // La Recherche. –1991. –Vol.22. –P.790-791.
17. Monroe C., Meekhof D. M., King B. E., Itano W. M., Wineland D. J. Demonstration of a Fundamental Quantum Logic Gate // Phys. Rev. Let. –1995. –Vol.75, №25. –P.4714-4717.
18. Shor P.W. Scheme for reducing decoherence in quantum computer memory // Phys. Rev. A. –1995. –Vol.52. –P.2493-2496.
19. Monroe C., Meekhof D. M., King B. E., Itano W. M., Wineland D. J. Demonstration of a Fundamental Quantum Logic Gate // Phys. Rev. Let. –1995. –Vol.75, №25. –P.4714-4717.
20. Cory D.G., Fahmy A.F., Havel T.F. Ensemble quantum computing by NMR spectroscopy // Proc. Natl. Acad. Sci. USA. –1997. –Vol.94. –P.1634–1639.
21. Gershenfeld N.A., Chuang I.L. Bulk spin-resonance quantum computation // Science. –1997. –Vol.275. –P.350-356.

22. Jones J.A., Mosca M. Implementation of a quantum algorithm on a nuclear magnetic resonance quantum computer // J. Chem. Phys. –1998. –Vol.109. –P.1648-1653.
23. Chuang I., Gershenfeld N., Kubinec M. Experimental implementation of fast quantum searching // Phys. Rev. Let. –1998. –Vol.80, №15. –P.3408-3411.
24. Jones J. A., Mosca M., Hansen R. H. Implementation of a quantum search algorithm on a quantum computer // Nature. –1998. –Vol.393. –P.344-346.
25. Quantum Computation Roadmap // http://qist.lanl.gov/qcomp_map.shtml.
26. Anwar M. S., Blazina D., Carteret H., Duckett S. B., Jones J. A. Implementing Grover's quantum search on a parahydrogen based pure state NMR quantum computer // Chem. Phys. Lett. –2004. –Vol.400. –P.94-97.
27. Longdell J. J., Fraval E., Sellars M. J., Manson N. B. Stopped light with storage times greater than one second using electromagnetically induced transparency in a solid // Phys. Rev. Lett. –2005. –Vol.95. –№063601.
28. Sillanpää M. A., Lehtinen T., Paila A. et al. Direct observation of Josephson capacitance // Phys. Rev. Lett. –2005. –Vol.95. –№206806.
29. Häffner H., Hänsel W., Roos C.F., Benhelm J. et al. Scalable multiparticle entanglement of trapped ions // Nature. –2005. –Vol.438. –P.643-646.
30. Rabl P., Demille D., Doyle J., Lukin M., Schoelkopf R., Zoller P. Hybrid quantum processors: molecular ensembles as quantum memory for solid state circuits // Phys. Rev. Lett. –2006. –Vol.97. –№033003.
31. Morton J.J.L., Tyryshkin A.M., Ardavan A. et al. Bang–bang control of fullerene qubits using ultrafast phase gates // Nature Physics. –2006. –Vol.2. –P.40-43.
32. Misra B., Sudarshan E.C.G. Quantum Zenon effect // J. Math. Phys. –1977. –Vol.18. –P.756-763.
33. Koike S., Takahashi H., Yonezawa H., Takei N., Braunstein S.L., Aoki T., Furusawa A. Demonstration of quantum telecloning of optical coherent states // Phys. Rev. Lett. –2006. –Vol.96. –№060504.
34. Katz N., Ansmann M., Bialczak R.C. et al. Coherent state evolution in a superconducting qubit from partial-collapse measurement // Science. –2006. –Vol.312, №5779. –P.1498-1500.
35. Fujisawa T., Hayashi T., Tomita R., Hirayama Y. Bidirectional counting of single electrons // Science. –2006. –Vol.312. –P.1634-1636.
36. Negrevergne C., Mahesh T. S., Ryan C. A., Ditty M. et al. Benchmarking quantum control methods on a 12-qubit system // Phys. Rev. Let. –2006. –Vol.96. –№170501.
37. Seidelin S., Chiaverini J., Reichle R., Bollinger J. J. et al. Microfabricated Surface-Electrode Ion Trap for Scalable Quantum Information Processing // Phys. Rev. Lett. –2006. –Vol.96. –№253003.
38. Miroshnychenko Y., Alt W., Dotsenko I., Fυrster L., Khudaverdyan M., Meschede D., Schrader D., Rauschenbeutel A. An atom-sorting machine // Nature. –2006. –Vol.442. –№7099. –P.151-154.
39. Koppens F. H. L., Buizert C., Tielrooij K. J., Vink I. T. et al. Driven coherent oscillations of a single electron spin in a quantum dot // Nature. –2006. –Vol.442. –P.766-771.
40. Culcer D., Lechner C., Winkler R. Spin Precession and Alternating Spin Polarization in Spin-3/2 Hole Systems // Phys. Rev. Lett. –2006. –Vol.97. –№106601.
41. Brun T., Devetak I., Hsieh M.-H. Correcting Quantum Errors with Entanglement // Science. –2006. –Vol.314. –P.436-439.
42. Pirandola S., Vitali D., Tombesi P., Lloyd S. Macroscopic Entanglement by Entanglement Swapping // Phys. Rev. Let. –2006. –Vol.97. –№150403.
43. Speer N. J., Tang S.-J., Miller T., Chiang T.-C. Coherent electronic fringe structure in incommensurate silver-silicon quantum wells // Science. –2006. –Vol.314. –P.804-806.
44. Stegner A.R., Boehme C., Huebl H., Stutzmann M., Lips K., Brandt M.S. Electrical detection of coherent 31P spin quantum states // Nature Physics. –2006. –Vol.2. –P.835-838.
45. Tame M.S., Prevedel R., Paternostro M. et al. Experimental realization of Deutsch's algorithm in a one-way quantum computer // Phys. Rev. Let. –2007. –Vol.98. –№140501.
46. Gurudev Dutt M.V., Childress L., Jiang L., Togan E. et al. Quantum register based on individual electronic and nuclear spin qubits in diamond // Science. –2007. –Vol.316, №5829. –P.1312-1316.
47. Plantenberg J.H., Groot P.C., C.J.P.M. Harmans, J.E. Mooij. Demonstration of controlled-NOT quantum gates on a pair of superconducting quantum bits // Nature. –2007. –Vol.447. –P.836-839.
48. Morley G.W., Tol J., Ardavan A., Porfyrakis K., Zhang J., Briggs G.A.D. Efficient dynamic nuclear polarization at high magnetic fields // Phys. Rev. Lett. –2007. –Vol.98. –№220501.
49. Weber F.M., Karl M., Lupaca-Schomber J., Löffler W. et al. Optical modes in pyramidal GaAs microcavities // Appl. Phys. Lett. –2007. –Vol.90. –№161104.
50. Majer J. et al. Coupling superconducting qubits via a cavity bus // Nature . –2007. –Vol.449. –P.443-447.
51. Sillanpää M.A. et al. Coherent quantum state storage and transfer between two phase qubits via a resonant cavity // Nature. –2007. –Vol.449. –P.438-442.
52. Langford N.K., Dalton R.B., Harvey M.D. et al. Measuring Entangled Qutrits and Their Use for Quantum Bit Commitment // Phys. Rev. Let. –2004. –Vol.93. –№053601.
53. Monroe C. et al. Demonstration of a fundamental quantum logic gate // Phys. Rev. Let. –1995. –Vol.75. –P.4714-4717.
54. Barenco A. et al. Elementary gates for quantum computation // Phys. Rev. A. –1995. –Vol.52. –P.3457-3488.
55. Duplij S.A, Kalashnikov V.V., Maslov E.A. Quantum information, qubits and quantum algorithms // Journal of Kharkiv National University. Ser. Nuclei, Particles and Fields. –2005. –№657, Issue 1(26). –P.103-108.
56. Margolus N. Parallel Quantum computation // Complexity, entropy and the physics of information. Santa Fe Institute Studies in the Sciences of Complexity. –1990. –Vol.8. –P.273-281.
57. Deutsch D., Barenco A., Ekert A. Universality in quantum computation // Proc. Roy. Soc. A. –1995. –Vol.449. –P.669-677.
58. Lloyd S. Almost any quantum logic gate is universal // Phys. Rev. Lett. –1995. –Vol.75. –P.346-349.
59. Di Vincenzo D.P. Two-bit gates are universal for quantum computation // Phys. Rev. A. –1995. –Vol.51. –P.1015-1022.
60. Barenco A. A universal two-bit gate for quantum computation // Proc. R. Soc. Lond. A –1995. –Vol.449. –P.679-683.
61. Стин Э. Квантовые вычисления. –Ижевск: НИЦ «Регулярная и хаотическая динамика», 2000. –112с.
62. Mayers D. Unconditionally secure quantum bit commitment is impossible // Phys. Rev. Lett. –1997. –Vol.78. –P.3414-3417.
63. Nielsen M.A., Chuang I.L. Programmable quantum gate arrays // Phys. Rev. Lett. –1997. –Vol.79. –P.321-324.
64. Rabin M.O. On digital signatures and public-key cryptosystems. –Massachusetts, 1979. –20p.
65. Nielsen M.A., Chuang I.L. Quantum Computation and Quantum Information. –Cambridge: Cambridge University Press, 2000. –665p.
66. D. Deutsch, R. Jozsa. Rapid solutions of problems by quantum computation // Proc. Roy. Soc. of Lond. A. –1992. –Vol.439. –P. 553-558.
67. Plenio M. B., Knight P. L. Realisitic lower bounds for the factorisation time of large numbers on a quantum computer // Phys. Rev. A. –1996. –Vol.53. –P.2986-2990.
68. Haroche S., Raimond J.-M. Quantum computing: dream or nightmare? // Phys. Today. –1996. –Vol.16. –P.51-52.
69. Landauer R. Is quantum mechanics useful? // Philos. Trans. R. Soc. London Ser. A. –1995. –Vol.353. –P.367-376.
70. Miquel C. et al. Factoring in a dissipative quantum computer // Phys. Rev. A. –1996. –Vol.54. –P.2605-2613.

71. Barenco A. et al. Effects of noise on quantum error correction algorithms // Phys. Rev. A. –1997. –Vol.56. –P.1177-1188.
72. Berthiaume A., Deutsch D., Jozsa R. The stabilisation of quantum computation // Proceedings of the Workshop on Physics and Computation, Phys. Comp. –Los Alamitos: IEEE Computer Society Press, –1994. –P.60-62.
73. Shor P.W. Scheme for reducing decoherence in quantum computer memory // Phys. Rev. A. –1995. –Vol.52. –P.2493–2496.
74. Steane A.M. Error correcting codes in quantum theory // Phys. Rev. Lett. –1996. –Vol.77. –P.793-797.
75. Calderbank A. R., Shor P. W. Good quantum error-correcting codes exist // Phys. Rev. A. –1996. –Vol.54. –P.1098-1105.
76. Dass T. Measurements and Decoherence // arXiv: quant-ph/0505070v1.
76. Shor P.W. Fault, tolerant quantum computation // arXiv: quant-ph/9605011.
77. Wootters W.K., Zurek W.H. A single quantum cannot be cloned // Nature. –1982. –Vol.299. –P.802-803.
78. Knill E., Laflamme R., Zurek W.H. Accuracy threshold for quantum computation // arXiv: quant-ph/9610011.
79. Aharonov D., Ben-Or M. Fault-tolerant quantum computation with constant error // arXiv: quant-ph/9611025.
80. Gottesman D. Class of quantum error-correcting codes saturating the quantum Hamming bound // Phys. Rev. A. –1996. –Vol.54. –P.1862-1868.
81. Bennett C. H. et al. Purification of noisy entanglement and faithful teleportation via noisy channels // Phys. Rev. Lett. –1996. –Vol.76. –P.722-725.
82. Deutsch D., Ekert A., Jozsa R. et al. Quantum privacy amplification and the security of quantum cryptography over noisy channels // Phys. Rev. Lett. –1996. –Vol.77. –P.2818-2823.
83. Collins G.P. Computing with quantum knots // Scientific American. –2006. –№4. –P.57-63.
84. Kitaev A.Yu. Fault-tolerant quantum computation by anyons // Annals Phys. –2003. –Vol.303. –P.2-30 // arXiv: quant-ph/9707021.
85. Фукс Д.Б. Когомологии группы кос mod 2 // Функциональный анализ и его приложение. –1970. –Т.4, №2. –С.62-73.
86. Laughlin R.B. Anomalous quantum Hall effect: An incompressible quantum fluid with fractionally charged excitations // Phys. Rev. Let. –1983. –Vol.50, №18. –P.1395-1398.
87. Laughling R.B. Anomalous Quantum hall effect: an incompressible quantum fluid with fractionally charged excitations // Phys. Rev. Let. –1983. –Vol.50, №18. –P.1395-1398.
88. Camino F.E., Zhou W., Goldman V.J. Direct observation of fractional statistics in two dimensions // arXiv: cond-mat/0502406v1.
89. Freedman M.H. Topological views on computational complexity // Proceedings of the international congress of mathematicians. –Berlin. –1998. Vol.II // Doc. Math. –1998. –Extra Vol.II. –P.453-464.
90. Preskill J. Fault-tolerant quantum computation // arXiv: quant-ph/9712048.
91. Mochon C. Anyons from non-solvable finite groups are sufficient for universal quantum computation // Phys. Rev. A. –2003. –Vol.67. –№022315. // arXiv: quant-ph/0206128.
92. Doucot B., Ioffe L. B., Vidal J. Discrete non-abelian gauge theories in two-dimensional lattices and their realizations in Josephson-junction arrays // Phys. Rev. B –2004. –Vol.69. –№214501. // arXiv: cond-mat/0302104.
93. Kitaev A. Anyons in a spin model on the honeycomb lattice // http://online.kitp.ucsb.edu/online/glasses_c03/kitaev.
94. Duan L.-M., Demler E., Lukin M.D. Controlling spin exchange interactions of ultracold atoms in optical lattices // Phys. Rev. Lett. –2003. –Vol.91. –№090402 // arXiv: cond-mat/0210564.
95. Freedman M., Nayak C., Shtengel K., Walker K., Wang Z. A class of P, T — invariant topological phases of interacting electrons // arXiv: cond-mat/0307511.
96. Peshkin M., Tonomura A. The Aharonov-Bohm effect. –Berlin: Springer-Verlag, 1989. –152p.
97. Ehrenberg W., Siday R. E. The refractive index in electron optics and the principles of dynamics // Proc. Phys. Soc. B. –1949. –Vol.62. –P.8-21.
98. Aharonov Y., Bohm D. Significance of electromagnetic potentials in the quantum theory // Phys. Rev. D. –1959. –Vol.115. –P.485-491.
99. Sarma S.D., Freedman M., Nayak C., Simon S.H., Stern A. Non-abelian anyons and topological quantum computation // arXiv: 0707.1889v1.
100. Mochon C. Anyons from non-solvable finite groups are sufficient for universal quantum computation // Phys. Rev. A. –2003. –Vol.67. –№022315 // arXiv: quant-ph/0206128v2.
101. Freedman M.H. Quantum computation and the localization of Modular Functors // arXiv: quant-ph/0003128
102. Labastida J. M. F., Lozano C. Lectures in topological quantum field theory // arXiv: hep-th/9709192v1.
103. Lawrence R.J. Introduction to topological quantum field theory // Proc. Symp. Appl. Math. –1996. –Vol.51. –40p.
104. Witten E. Topological quantum field theory // Comm. Math. Phys. –1988. –Vol.117, №3. –P.353-386.
105. Schottenloher M. A mathematical introduction to conformal field theory. –Berlin Heidelberg: Springer-Verlag, 1997. –142p.
106. Ginsparg P. Applied conformal field theory // arXiv: hep-th/9108028.
107. Ketov S.V. Conformal field theory. –Hannover, 1995. –500p.
108. Schellekens A.N. Introduction to conformal field theory. –Amsterdam, 1996. –125p.
109. Freedman M.H., Kitaev A., Wang Z. Simulation of topological field theories by quantum computers // Commun. Math. Phys. –2002. –Vol.227. –P.587-603 // arXiv: quant-ph/0001071.
110. DiVincenzo D.P. Quantum computation // Science. –1995. –Vol.270, №5234. –P.255-261.

TOPOLOGICAL METHODS IN QUANTUM COMPUTATIONS

S.A. Duplij[1], I.I. Shapoval[2]
[1]Kharkiv national university
4, Svobody sq., Kharkiv, 61077, Ukraine
e-mail: sduplij@gmail.com
[2] National science center "Kharkiv Institute of Physics and Technology"
1, Akademichna str., Kharkiv, 61108, Ukraine
e-mail: ishapoval@kipt.kharkov.ua

Basic concepts of quantum information theory, principles of quantum calculations and the possibility of creation on this basis unique on calculation power and functioning principle device, named quantum computer, are concerned. The main blocks of quantum logic, schemes of quantum calculations implementation, as well as some known today effective quantum algorithms, called to realize advantages of quantum calculations upon classical, are presented here. Among them special place is taken by Shor's algorithm of number factorization and Grover's algorithm of unsorted database search. Phenomena of decoherence, its influence on quantum computer stability and methods of quantum errors correction are described. Topological quantum computation conception is stated. It hasn't more computational power than the conventional quantum computation has, but is noiseless by its nature. Anyon statistics necessity for qubits is shown and representative anyon model of topological quantum information processing is presented.
KEY WORDS: quantum calculations, quantum algorithms, noise stability, decoherence, topological quantum calculations, theory of braids, anyons.