Сентябрь 2024 г. *Том 194, № 9*

УСПЕХИ ФИЗИЧЕСКИХ НАУК

К 90-ЛЕТИЮ ФИЗИЧЕСКОГО ИНСТИТУТА им. П.Н. ЛЕБЕДЕВА РАН (ФИАН)

ФИЗИКА НАШИХ ДНЕЙ

Вычислимое и невычислимое в квантовом мире: утверждения и гипотезы

А.К. Федоров, Е.О. Киктенко, Н.Н. Колачевский

Значительные успехи в разработке вычислительных устройств, использующих квантовые эффекты, и демонстрация решения с их помощью различных задач стимулировали новую волну интереса к вопросу о природе "квантового вычислительного преимущества" (quantum computational advantage). Хотя различные попытки количественно оценить и охарактеризовать природу квантового вычислительного преимущества предпринимались и раньше, в широком контексте данный вопрос остаётся открытым. В самом деле, не существует универсального подхода, помогающего определить круг задач, решение которых квантовые компьютеры способны ускорить, теоретически и на практике. В настоящей работе мы рассмотрим подход к этому вопросу, основанный на концепции сложности и достижимости квантовых состояний. С одной стороны, класс квантовых состояний, представляющий интерес для квантовых вычислений, должен быть сложным, т.е. не поддающимся моделированию с помощью классических компьютеров с менее чем экспоненциальными ресурсами. С другой стороны, такие квантовые состояния должны быть достижимы на практическом квантовом компьютере. Последнее означает, что унитарная операция, соответствующая преобразованию квантовых состояний от исходного к желаемому, может быть декомпозирована в не более чем полиномиальную по числу кубитов последовательность одно- и двухкубитных вентилей. Формулируя ряд утверждений и гипотез, мы рассматриваем вопрос об описании класса задач, решение которых может быть ускорено с помощью квантового компьютера.

Ключевые слова: квантовые вычисления, квантовая сложность, квантовые алгоритмы

PACS numbers: 03.67.Ac, 03.67.Lx, 42.50.Dv DOI: https://doi.org/10.3367/UFNr.2024.07.039721

Содержание

1. **Введение (960).**
2. **Картина квантовых состояний и универсальная вентильная модель квантовых вычислений (962).**
3. **Классификация состояний (962).**
4. **Соотношения между классами состояний (963).**
5. **Заключение (965).**

Список литературы (965).

А.К. Федоров [1,2,3,a], **Е.О. Киктенко** [2,3,b], **Н.Н. Колачевский** [1,2,c]
[1] Физический институт им. П.Н. Лебедева РАН,
Ленинский просп. 53, 119991 Москва, Российская Федерация
[2] Российский квантовый центр, Инновационный центр "Сколково",
Большой бульвар 30, стр. 1, 121205 Москва,
Российская Федерация
[3] Национальный исследовательский технологический университет "МИСиС",
Ленинский просп. 4, 119049 Москва, Российская Федерация
E-mail: [a] lex1026@gmail.com, [b] evgeniy.kiktenko@gmail.com,
[c] kolachevsky@lebedev.ru

*Статья поступила 17 мая 2024 г.,
после доработки 19 июля 2024 г.*

1. Введение

Развитие технологии производства процессоров на основе полупроводниковой микроэлектроники [1] позволило в течение последних десятилетий постоянно наращивать вычислительную мощность и привело к тому, что вычислительные устройства используются практически повсеместно и ежедневно. Однако некоторые вычислительные задачи по-прежнему представляют исключительно высокую вычислительную сложность для имеющихся в нашем распоряжении вычислительных устройств. Примеры таких задач — это, во-первых, разложение целых чисел на простые множители (так называемая факторизация), при которой для заданного составного числа N необходимо найти его нетривиальные множители p и q (такие, что $N = p \times q$). Такая задача имеет непосредственные приложения в криптографии, поскольку на предположении о сложности решения задачи факторизации для больших N строится анализ стойкости алгоритмов криптографии с открытым ключом [2]. Во-вторых, это моделирование сложных квантовых систем, в частности, вычисление энергетических состояний "больших" молекул. Изучение свойств молекул и химических реакций важно для различных приложений, например, создания материалов с заданными

свойствами и разработки лекарств. Наконец, в-третьих, интерес представляют задачи комбинаторной оптимизации, где нужно найти лучшее решение среди большого набора возможных кандидатов, что актуально, например, для логистики и составления расписаний. Хотя классические алгоритмы и вычислительные устройства продолжают развиваться, а "смерть закона Мура" [3] — это значительное преувеличение [4], указанные выше вычислительные задачи, по всей видимости, не могут быть эффективно решены с помощью существующих устройств и известных алгоритмических методов, даже с учётом прогнозируемого роста их возможностей.

Одним из подходов к расширению возможностей является построение принципиально других типов вычислительных устройств — *квантовых компьютеров*, которые используют явления, проявляющиеся на уровне индивидуальных квантовых объектов, таких как индивидуальные атомы, ионы, фотоны, а также макроскопические нелинейные сверхпроводящие контуры, проявляющие свойства одиночных атомов [5]. Квантовые компьютеры, также часто называемые *квантовыми процессорами* или *квантовыми со-процессорами* (что, пожалуй, наиболее точно отражает их суть, так как квантовые устройства работают совместно с классическими, а также имеют классические интерфейсы ввода и вывода), рассматриваются как способ решать классически-сложные вычислительные задачи. Например, для уже упомянутых задач факторизации [6] и моделирования сложных квантовых систем [7] известны квантовые алгоритмы, показывающие разрешимость такой задачи за полиномиальное время.

Исторически к появлению квантовых компьютеров привело несколько концепций. Фейнман предложил квантовый компьютер как инструмент для моделирования других квантовых систем [8, 9], которые, как предполагается, трудно моделировать с помощью классических методов [10]. Более точно, предполагается, что для класса многочастичных и взаимодействующих квантовых систем ресурсы для моделирования, т.е. вычисления вероятностей измерений ("сильное моделирование") или генерации конечной выборки результатов измерений ("слабое моделирование"), растут экспоненциально с увеличением размерности системы. Такое явление известно как "рубеж квантовой запутанности" [11]. Тогда, в самом деле, начиная с какого-то размера системы её становится невозможно моделировать классически, поэтому нужны альтернативные подходы, а квантовая запутанность играет при этом ключевую роль.

Для примера рассмотрим состояние n кубитов (двухуровневых квантовых систем)

$$|\psi\rangle = \bigotimes_i \left(\alpha_i|0\rangle + \beta_i|1\rangle\right), \qquad (1)$$

где α_i и β_i — комплексные числа с условием нормировки $|\alpha_i|^2 + |\beta_i|^2 = 1$ для $i = 1, \ldots, n$. Описание такого состояния требует до $2n$ действительных чисел, например, если для параметризации используются углы на сфере Блоха. Однако если мы применяем к квантовому состоянию достаточно длинную последовательность однокубитных операций и двухкубитную запутывающую операцию, например, вентиль контролируемого отрицания CNOT [12], между разными парами кубитов, то состояние становится запутанным, т.е. не представимым в виде произведения состояния подсистем. В таком случае, кажется, нет очевидного способа промоделировать такое состояние с использованием линейных ресурсов. Можно предположить, что тогда нам потребуются ресурсы, растущие как 2^n, т.е. экспоненциально, с увеличением размерности системы. Для случая $n = 100$ прямая симуляция потребует хранения в памяти комплексного вектора размерности 2^{100} и вычисления результатов вращений в пространстве размерности 2^{100}, что выглядит невозможным с помощью любых вычислительных устройств. Так что наличие любого суперпозиционного запутанного состояния может быть рассмотрено как условие для квантового вычислительного преимущества.

Однако теорема Готтсмана – Нилла [13 – 15] демонстрирует, что в ряде случаев это не так. Многочастичное запутанное состояние, приготовленное только с помощью множества вентилей из группы Клиффорда, применённое к состоянию в вычислительном базисе (так называемое стабилизаторное состояние), может быть промоделировано за полиномиальные ресурсы в отношение любых паулевских измерений, включая измерения в вычислительном базисе. К клиффордовским операциям относится, например, вентиль CNOT. Примером многочастичного запутанного квантового состояния, принадлежащего данному классу, является состояние Гринбергера – Хорна – Цайлингера (ГХЦ) [16] и графовые состояния [17]. Это демонстрирует наивность рассуждения о квантовых компьютерах как устройствах, вычислительное преимущество которых исключительно связано с суперпозиционным и запутанным характером обрабатываемых квантовых состояний. Другим примером являются квантовые цепочки, состоящие из матч-вентилей (match-gates), которые, как известно, тоже можно эффективно моделировать на классическом компьютере [18].

Вопрос о классической моделируемости тех или иных классов квантовых состояний играет важную роль для достижения квантового вычислительного преимущества — демонстрации квантовым компьютером решения какой-либо задачи быстрее, чем с помощью классических вычислительных устройств. Однако данный вопрос связан не только со степенью запутанности, но также и с типом измерений и применяемых операций. В самом деле, применение слоя неклиффордовских операций на запутанное стабилизаторное состояние прямо перед измерениями в вычислительном базисе (что эквивалентно реализации некоторого общего локального измерения) делает теорему Готтсмана – Нилла неприменимой, а соответствующее состояние — сложным для классического моделирования. Также добавление неклиффордовских операций, таких как Т-вентиль, в квантовую цепочку делает её немоделируемой с помощью классических ресурсов. Эти примеры показывают, что пространство возможных состояний квантовой системы — её гильбертово пространство — неоднородно с точки зрения сложности моделирования (по отношению к измерениям в вычислительном базисе): n-кубитное сепарабельное состояние требует линейных ресурсов, n-кубитное запутанное состояние, приготовленное только с помощью клиффордовских операций, моделируется полиномиально-сложно, тогда как нам известны n-кубитные запутанные состояния, например, приготовленные с помощью неклиффордовских операций, которые могут требовать экспоненциальных ресурсов для моделирования.

С другой стороны, хотя квантовый процессор и рассматривается как универсальное квантовое устройство, т.е. в принципе возможна реализация любой унитарной операции (с указанной точностью), не все унитарные операции могут быть эффективно декомпозированы на последовательности одно- и двухкубитных квантовых операций (вентилей), которые реализуются практическими квантовыми процессорами. В самом деле, если рассмотреть произвольную $2^n \times 2^n$ унитарную матрицу, то её декомпозиция на унитарные матрицы размерностей 2×2 и 4×4 (т.е. матриц одно- и двухкубитных операций соответственно) будет экспоненциально длинной по n. Для ряда исключительных случаев такие последовательности могут быть линейными или полиномиальными (как в случае алгоритма Шора для факторизации [6]). Наблюдение Манина [19] о "большей ёмкости квантового пространства состояний" опирается на предположение о том, что такие состояния *достижимы* при использовании практического квантового компьютера.

Таким образом, квантовые компьютеры полезны для анализа классически-немоделируемых и квантово-достижимых состояний. Насколько большой класс таких состояний? Какой структурой в гильберотовом пространстве этот класс обладает? Подобные вопросы мотивируют нас сделать первые попытки к классификации квантовых состояний с вышеупомянутой точки зрения. Нахождение соотношений между разными классами состояний может пролить новый свет на природу квантового вычислительного преимущества, в данном контексте вытекающего из размера и структуры множества сложных квантовых состояний, которые не могут быть промоделированы классически с менее чем экспоненциальными ресурсами. Мы представляем первый вариант диаграммы сложности квантовых состояний, в которой пока не точно установлены границы между определёнными классами. Предлагаемая классификация принимает во внимание существующие подходы к оценке сложности квантовых состояний с точки зрения физики многих тел, физики конденсированного состояния и квантовой теории информации.

Стоит отметить, что в данном случае мы работаем с идеальными кубитами, которые также называют логическими. В реальных физических системах значительный эффект на вычислительный процесс оказывают шумы. Эти шумы, однако, могут быть либо подавлены до приемлемых значений, либо эффект может быть устранён с помощью кодов коррекции ошибок. Сегодня экспериментальная демонстрация возможности коррекции ошибок является одним из ключевых направлений развития квантовых вычислений. Среди наиболее ярких результатов — реализация "логического квантового алгоритма", т.е. действия логических (скорректированных на ошибки) операций над логическими кубитами с помощью ионного квантового процессора Quantinuum H1-1 [20].

Сегодня вопросы реализации квантовых вычислительных устройств стали предметом работы широкого научного сообщества. В России это направление развивается в рамках Дорожной карты по квантовым вычислениям, координируемой Госкорпорацией "Росатом"; обзор развития квантовых технологий в России по состоянию на 2019 г. (момент начала работ по Дорожной карте) представлен в работе [21]. Одной из наиболее динамично развивающихся платформ для квантовых вычислений являются ионы в ловушках. Создание квантовых вычислительных устройств на данной платформе подразумевает как развитие традиционно сильных для ФИАН им. П.Н. Лебедева научных тематик [22], таких как лазерное охлаждение, ультрастабильные лазеры и развитие стандартов частоты [23], так и создание новых направлений, например, в области многоуровневой квантовой логики для реализации квантовых алгоритмов [24]. В период с 2020 по 2024 гг. это позволило разработать квантовые вычислительные устройства с несколькими десятками кубитов, а также продемонстрировать работу квантовых алгоритмов [24–26], в том числе для моделирования фазовых переходов [27]. Разрабатываемые квантовые вычислительные устройства позволяют на практике тестировать гипотезы относительно соотношения классов сложности квантовых состояний.

2. Картина квантовых состояний и универсальная вентильная модель квантовых вычислений

Главный объект нашего интереса — n-кубитное квантовое состояние $|\Psi_n\rangle$, возникающее после выполнения в квантовой цепочке всех унитарных операций U_n к состоянию $|0\rangle^{\otimes n}$, т.е. квантовое состояние, появляющееся перед измерениями в вычислительном базисе: $|\Psi_n\rangle = U|0\rangle^{\otimes n}$. Почему нас интересуют именно состояния, хотя можно думать не только о сложных квантовых состояниях, но также и о сложных квантовых процессах U, сложных гамильтонианах H, которые задают нетривиальную квантовую динамику $U = \exp(-\mathrm{i}Ht)$ в зависимости от времени t или задают сложное основное состояние, или о сложных измерениях?

В первом случае изоморфизм Чоя–Ямилковского позволяет рассматривать все квантовые процессы (такие как U), соответствующие квантовым цепочкам, как квантовые состояния в расширенном гильбертовом пространстве $\mathcal{H}_{\text{in}} \otimes \mathcal{H}_{\text{out}}$ (где $\mathcal{H}_{\text{in}}$ и $\mathcal{H}_{\text{out}}$ — гильбертовы пространства входных и выходных состояний соответственно). В случае рассмотрения гамильтонианов и измерений эквивалентность адиабатической [28], основанной на измерениях [17] и вентильной [12] моделей квантовых вычислений без потери общности позволяет рассматривать всю возникающую сложность с использованием квантовых состояний. Отметим, что произвольные выходные измерения всегда могут быть сведены к измерениям в вычислительном базисе путём добавления соответствующих унитарных операций в квантовую цепочку. Схожий приём может быть применён при рассмотрении операций, построенных на прямой обратной связи от результатов промежуточных измерений, которые могут быть заменены контролирующими унитарными операциями и отложенными измерениями. Таким образом, наш подход к рассмотрению сложности квантовых состояний универсален ввиду универсальности вентильной модели квантовых вычислений.

3. Классификация состояний

Напомним, что для достижения квантового вычислительного преимущества мы рассматриваем квантовые состояния, которые экспоненциально сложно моделировать, т.е. предсказывать вероятности реализации исходов измерений или, по крайней мере, имитировать

соответствующую процедуру их случайного разыгрывания. Если состояния, которыми мы оперируем, поддаются классическому моделированию, кажется нереалистичным ожидать в этом случае преимущества квантовых вычислений. Ниже мы вводим определённые классы состояний, для которых далее будет сформулирован набор утверждений и предположений.

Рассмотрим следующий набор n-кубитных квантовых состояний:

• Stab — набор стабилизаторных ("клиффордовских") состояний, т.е. квантовых состояний, полученных применением квантовых цепочек из клиффордовских вентилей на состояние из вычислительного базиса;

• ClassSimMeas — множество состояний, для которых существует классический алгоритм, имеющий сложность не выше полиномиальной по n и способный воспроизводить результаты измерения таких состояний в вычислительном базисе, хотя бы в слабом смысле;

• ClassNonSimMeas — множество состояний, для которых не существует классического алгоритма, имеющего сложность не выше полиномиальной по n и способного воспроизводить результаты измерения таких состояний в вычислительном базисе, хотя бы в слабом смысле;

• $\mathrm{QuantPrep}_{1,2}$ — множество состояний, которые можно подготовить на квантовом компьютере, используя квантовую цепочку, состоящую не более чем из полиномиального по n количества одно- и двухкубитных вентилей, применённых к некоторому начальному состоянию из вычислительного базиса;

• $\mathrm{NotQuantPrep}_{1,2}$ — множество состояний, которые невозможно подготовить на квантовом компьютере, используя квантовую цепочку, состоящую не более чем из полиномиального по n количества одно- и двухкубитных вентилей, применённых к некоторому начальному состоянию из вычислительного базиса;

• AreaLaw (VolLaw) — множество состояний, для которых энтропия запутанности области пространства имеет тенденцию расти для достаточно больших областей как размер границы (объёма) области;

• QuantCompAdv — набор состояний, возникающих перед измерением в вычислительном базисе, квантовых алгоритмов с явными схемами (в частности, без оракулов как "чёрных ящиков"), имеющих более чем полиномиальное по n преимущество по сравнению с лучшим (известным или теоретически возможным) классическим алгоритмом.

Заметим, что ClassNonSimMeas является дополнением к ClassSimMeas, а также $\mathrm{QuantPrep}_{1,2}$ является дополнением к $\mathrm{NotQuantPrep}_{1,2}$. Также дополнительно прокомментируем класс $\mathrm{QuantPrep}_{1,2}$. В его определении подчёркивается возможность выразить общее унитарное преобразование через доступные на практике одно- и двухкубитные вентили. Этот класс соответствует множеству квантовых состояний, которые можно получить с помощью реалистичного квантового компьютера, между тем, как известно, для разложения произвольного n-кубитного унитарного U_n на последовательность одно- и двухкубитных вентилей обычно требуется последовательность экспоненциального размера. Данный класс можно расширить, скажем, до $\mathrm{QuantPrep}_{1,2,\ldots,m}$ в случае, если квантовое оборудование будет поддерживать до m-кубитных вентилей, что на практике пока обычно не доступно. Однако даже если такие вентили существуют при некотором фиксированном m, это не влияет на асимптотическое поведение длины последовательности вентилей. То же самое справедливо и для $\mathrm{NotQuantPrep}_{1,2}$.

Недавние исследования в области квантовой физики многих тел и физики конденсированного состояния, в которых активно используют концепцию моделирования квантовых систем с помощью классических подходов, показали, что поведение запутанности с разбиением всей системы на две части играет решающую роль. Заметим, что такое разбиение обычно реализуется относительно топологии соответствующей физической системы, например, в рамках одномерной цепи или двухмерного или трёхмерного массива квантовых объектов. Например, речь может идти о спиновых системах. Существуют эффективные классические инструменты для моделирования запутанных квантовых систем многих тел, в которых запутанность области пространства имеет тенденцию масштабироваться (для достаточно больших областей) как размер границы области. Однако если запутанность растёт как объём одной из областей, такие методы больше не могут работать эффективно. Согласно нашему определению, мы называем эти классы AreaLaw и VolLaw соответственно. В частности, тензорные сети, например, типа состояний матричного произведения (СМП), хороши для аппроксимации квантовых состояний класса AreaLaw [29], тогда как нейросетевые квантовые состояния (НСКС) считаются полезными для описания определённых состояний из класса VolLaw [30 – 32]. Также отметим, что AreaLaw и VolLaw не являются дополнениями друг друга, поскольку могут существовать состояния, запутанность которых не масштабируется ни как объём, ни как площадь (например, быть постоянной или масштабироваться как некоторая нетривиальная степень от площади).

4. Соотношения между классами состояний

Рассмотрим набор утверждений и гипотез, касающихся взаимоотношений между введёнными классами квантовых состояний.

По определению:

Утверждение 1. QuantCompAdv принадлежит $\mathrm{QuantPrep}_{1,2}$ и ClassNonSimMeas.

Только такие состояния могут давать квантовое вычислительное преимущество с помощью реалистичных квантовых вычислительных устройств.

Утверждение 2. Согласно теореме Готтсмана – Нилла [13 – 15], Stab принадлежит ClassSimMeas.

Данное утверждение очевидно вследствие возможности моделировать квантовые стабилизаторные состояния с использованием полиномиальных ресурсов [13 – 15].

Утверждение 3. Вследствие [15, 33, 34] Stab принадлежит $\mathrm{QuantPrep}_{1,2}$. Конкретно сложность приготовления заданного стабилизаторного состояния $|\Psi_n\rangle$ масштабируется как $\mathcal{O}(n^2/\log n)$.

Это связано с тем, что стабилизаторные состояния можно эффективно готовить с помощью одно- и двухкубитных вентилей, например через набор поворотов Паули и вентилей CNOT. Примером такого состояния является многокубитное ГХЦ состояние вида:

$$|\mathrm{GHZ}_n\rangle = \frac{|0\rangle^{\otimes n} + |1\rangle^{\otimes n}}{\sqrt{2}}\,, \tag{2}$$

где n — число кубитов.

Утверждение 4. Stab пересекает AreaLaw и VolLaw.

Примерами состояний на пересечении этих классов являются кластерные состояния, использующиеся в квантовых вычислениях на основе измерений [17].

Утверждение 5. AreaLaw пересекает ClassSimMeas.

Данное утверждение основано на том факте, что тензорные сети в СМП-форме состояния могут эффективно описывать запутанные квантовые состояния, запутанность которых растёт по закону площади [29]. СМП особенно хорошо подходят для описания одномерных систем квантовой решётки со щелью и локальными взаимодействиями [35].

Гипотеза 1. AreaLaw принадлежит ClassSimMeas.

Данная гипотеза является усилением утверждения 1. Здесь мы предполагаем, что *все квантовые состояния, запутанность которых растёт как площадь разбиения подсистем*, можно моделировать, используя не более чем полиномиальные ресурсы на классическом компьютере (например, с помощью СМП или обобщений).

Утверждение 6. ClassSimMeas пересекает VolLaw.

Это связано с тем, что некоторые состояния из VolLaw можно эффективно описать с помощью НСКС [30–32]; например, существуют состояния одномерных систем, не поддающихся эффективному описанию с помощью СМП, но описываемых с помощью НСКС [30, 32].

Утверждение 7. QuantPrep пересекает AreaLaw и VolLaw.

Состояние из AreaLaw можно приготовить путём применения $\sim n$ случайных двухкубитных вентилей, действующих между соседними (в рамках данной геометрической топологии) кубитами. Состояние из VolLaw, соответственно, можно приготовить путём применения $\sim n^2$ случайных двухкубитных вентилей ко всем возможными парам кубитов. Отметим, что произвольный двухкубитный вентиль может быть реализован с помощью не более чем трёх вентилей CNOT [36].

Гипотеза 2. Существуют состояния VolLaw, выходящие за пределы ClassSimMeas.

Примерами таких состояний предположительно являются квантовые состояния, создаваемые случайными схемами (в отсутствие шумов), использовавшиеся для демонстрации квантового вычислительного преимущества (это было сделано для зашумлённых схем в работах [37, 38]). По сути, выбор квантовых цепочек для подобных демонстраций осуществлялся таким образом, чтобы обеспечить приготовление состояний из VolLaw и тем самым нивелировать возможность их симуляции тензорно-сетевыми анзацами и другими известными классическими методами. Тем не менее строгое обоснование данного интуитивно ожидаемого предположения авторам неизвестно. Также отметим, что в шумном случае предложен классический полиномиальный алгоритм [39] (который, однако, не касается вышеупомянутых экспериментов по квантовому преимуществу схемы конечного размера).

Гипотеза 3. ClassSimMeas пересекает $\mathrm{NotQuantPrep}_{1,2}$.

Данная гипотеза связана с тем, что все известные алгоритмы приготовления произвольного состояния

$$|\Psi_n\rangle = \sum_{\mathbf{x}\in\{0,1\}^n} C_{\mathbf{x}}|\mathbf{x}\rangle \tag{3}$$

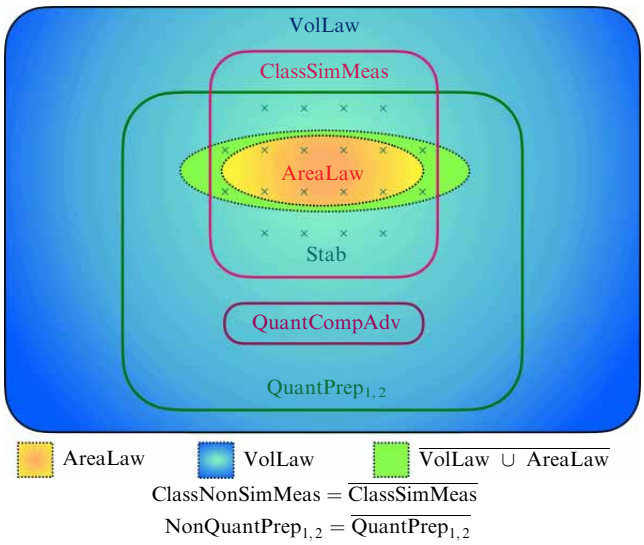

Рис. 1. Схематичная иллюстрация представленных отношений между классами состояний. $\overline{\text{Class}}$ обозначает дополнение множества Class. Символы × в обозначении класса Stab (принадлежащего пересечению ClassSimMeas и $\mathrm{QuantPrep}_{1,2}$, но не покрывающего его полностью) используются, чтобы подчеркнуть конечность этого класса для фиксированного n.

по амплитудам вероятности $\{C_{\mathbf{x}}\}$ имеют экспоненциальную сложность по количеству требуемых операций (см. свежий обзор результатов в работе [40]). С другой стороны, можно представить ситуацию, когда функция $\mathbf{x}\mapsto|C_{\mathbf{x}}|^2$ устроена так, что может быть эффективно вычислена на классическом компьютере, но при этом никак не согласуется со структурой тензорного произведения физического пространства кубитов. Подобная ситуация реализуется, в частности, в НСКС, в которых величины $C_{\mathbf{x}}$ по сути являются выходными сигналами из нейросети для заданного входа $\mathbf{x}$.

Итоговое предполагаемое соотношение между классами состояний представлено на рис. 1. Рассмотрим дополнительно вопрос о размере классов состояний для фиксированного значения n. Известно, что множество стабилизаторных состояний Stab содержит

$$2^n\prod_{i=1}^{n}(2^i+1) \tag{4}$$

состояний [41]. В то же время $\mathrm{QuantPrep}_{1,2}$, AreaLaw, VolLaw, $\mathrm{NotQuantPrep}_{1,2}$ содержат бесконечное число состояний, поскольку добавление произвольных непрерывных локальных операций к схемам их приготовления оставляет состояния внутри этих классов. ClassSimMeas содержит бесконечное число состояний вследствие пересечения AreaLaw и $\mathrm{QuantPrep}_{1,2}$. Бесконечное подмножество внутри QuantCompAdv содержит состояния, возникающие в случайных схемах, например, с однокубитными вентилями, распределёнными равномерно случайно по мере Хаара. Представляется интересным вопрос о том, можно ли специфицировать класс задач в определении квантового вычислительного преимущества в рамках QuantCompAdv так, чтобы соответствующий набор состояний или, точнее, набор соответствующих считываемых распределений вероятностей, стал конечным.

5. Заключение

В настоящей работе мы предложили подход к установлению связей между различными классами квантовых состояний. Отметим, что "простота" состояний не означает их непрактичность в целом для квантовых информационных технологий. Показательным примером является протокол квантового распределения ключей BB84 (для обзора см. [42]), в котором стабилизаторные состояния и Паули измерения используются для решения проблемы информационно-теоретически стойкого наращивания криптографических ключей.

Другая интересная область — это алгоритмы на основе оракулов, которые могут обеспечить доказуемое преимущество (см., например, алгоритм Бернштейна – Вазирани с одиночным запуском [43]). Тем не менее, с нашей точки зрения, потенциальное ускорение в подобного рода алгоритмах может быть отнесено, скорее, к области квантовой коммуникации, а не квантовых вычислений, по крайней мере с практической точки зрения.

В-третьих, актуальный вопрос — это построение классов сложности с учётом влияния ошибок на процессы квантовых вычислений.

Наконец, можно отметить конкретные попытки предложить классы квантовых состояний для изучения "переходов сложности" [44, 45], т.е. наборы квантовых состояний, изменяя параметры которых, можно делать их менее или более сложными (при этом они являются достижимыми). Примерами таких состояний является класс состояний Дике со знакопеременной структурой, в которых наблюдается переход в класс VolLaw при определённом наборе параметров [45]. Подобные состояния могут служить основой для экспериментальной проверки сформулированных выше гипотез.

Благодарности. Авторы выражают благодарность Б.И. Бантышу и И.В. Ермакову за плодотворные обсуждения. Работа поддержана программой Приоритет 2030 в Национальном университете науки и технологий "МИСиС" (проект К1-2022-027).

Список литературы

1. Moore G E *Electronics* **38** (8) 114 (1965); reprinted: *IEEE Solid-State Circuits Soc. Newslett.* **11** (3) 33 (1965) https://doi.org/10.1109/N-SSC.2006.4785860
2. Rivest R L, Shamir A, Adleman L *Commun. ACM* **21** (2) 120 (1978)
3. Waldrop M M *Nature* **530** 144 (2016)
4. Fedorov A K, Gisin N, Beloussov S M, Lvovsky A I, arXiv:2203.17181
5. Brassard G, Chuang I, Lloyd S, Monroe C *Proc. Natl. Acad. Sci. USA* **95** 11032 (1998)
6. Shor P, in *Proc. 35th Annual Symp. on Foundations of Computer Science, 20–22 November 1994, Santa Fe, NM, USA* (Piscataway, NJ: IEEE, 1994) pp. 124–134, https://doi.org/10.1109/SFCS.1994.365700
7. Lloyd S *Science* **273** 1073 (1996)
8. Feynman R P *Int. J. Theor. Phys.* **21** 467 (1982)
9. Feynman R P *Found. Phys.* **16** 507 (1986)
10. Поплавский Р П *УФН* **115** 465 (1975); Poplavskii R P *Sov. Phys. Usp.* **18** 222 (1975)
11. Preskill J "Quantum computing and the entanglement frontier", arXiv:1203.5813
12. Ladd T D, Jelezko F, Laflamme R, Nakamura Y, Monroe C, O'Brien J L *Nature* **464** 45 (2010)
13. Gottesman D "The Heisenberg representation of quantum computers", quant-ph/9807006; in *Group 22: Proc. of the 12th Intern. Colloquium on Group Theoretical Methods in Physics* (Eds S P Corney, R Delbourgo, P D Jarvis) (Cambridge, MA: Intern. Press, 1999) p. 32
14. Nielsen M A, Chuang I L *Quantum Computation and Quantum Information* (Cambridge: Cambridge Univ. Press, 2000)
15. Aaronson S, Gottesman D *Phys. Rev. A* **70** 052328 (2004)
16. Федоров А К, Киктенко Е О, Хабарова К Ю, Колачевский Н Н *УФН* **193** 1162 (2023); Fedorov A K, Kiktenko E O, Khabarova K Yu, Kolachevsky N N *Phys. Usp.* **66** 1095 (2023)
17. Raussendorf R, Briegel H J *Phys. Rev. Lett.* **86** 5188 (2001)
18. Ermakov I, Lychkovskiy O, Byrnes T "Unified framework for efficiently computable quantum circuits", arXiv:2401.08187
19. Манин Ю И *Вычислимое и невычислимое* (М.: Советское радио, 1980)
20. Wang Y et al. "Fault-tolerant one-bit addition with the smallest interesting colour code", arXiv:2309.09893; *Sci. Adv.* **10** eado9024 (2024)
21. Fedorov A K, Akimov A V, Biamonte J D, Kavokin A V, Khalili F Ya, Kiktenko E O, Kolachevsky N N, Kurochkin Y V, Lvovsky A I, Rubtsov A N, Shlyapnikov G V, Straupe S S, Ustinov A V, Zheltikov A M *Quantum Sci. Technol.* **4** 040501 (2019)
22. Беляев А А, Воронцов В Г, Демидов Н А, Хабарова К Ю, Колачевский Н Н *УФН* **193** 1091 (2023); Belyaev A A, Voronzov V G, Demidov N A, Khabarova K Yu, Kolachevsky N N *Phys. Usp.* **66** 1026 (2023)
23. Хабарова К Ю, Заливако И В, Колачевский Н Н *УФН* **192** 1305 (2022); Khabarova K Yu, Zalivako I V, Kolachevsky N N *Phys. Usp.* **65** 1217 (2022)
24. Aksenov M A, Zalivako I V, Semerikov I A, Borisenko A S, Semenin N V, Sidorov P L, Fedorov A K, Khabarova K Yu, Kolachevsky N N *Phys. Rev. A* **107** 052612 (2023)
25. Zalivako I V, Borisenko A S, Semerikov I A, Korolkov A E, Sidorov P L, Galstyan K P, Semenin N V, Smirnov V N, Aksenov M D, Fedorov A K, Khabarova K Yu, Kolachevsky N N *Front. Quantum Sci. Technol.* **2** 1228208 (2023) https://doi.org/10.3389/frqst.2023.1228208
26. Zalivako I V, Nikolaeva A S, Borisenko A S, Korolkov A E, Sidorov P L, Galstyan K P, Semenin N V, Smirnov V N, Aksenov M A, Makushin K M, Kiktenko E O, Fedorov A K, Semerikov I A, Khabarova K Yu, Kolachevsky N N "Towards multiqudit quantum processor based on a $^{171}Yb^{+}$ ion string: Realizing basic quantum algorithms", arXiv:2402.03121
27. Kazmina A S, Zalivako I V, Borisenko A S, Nemkov N A, Nikolaeva A S, Simakov I A, Kuznetsova A V, Egorova E Yu, Galstyan K P, Semenin N V, Korolkov A E, Moskalenko I N, Abramov N N, Besedin I S, Kalacheva D A, Lubsanov V B, Bolgar A N, Kiktenko E O, Khabarova K Yu, Galda A, Semerikov I A, Kolachevsky N N, Maleeva N, Fedorov A K *Phys. Rev. A* **109** 032619 (2024)
28. Aharonov D, van Dam W, Kempe J, Landau Z, Lloyd S, Regev O *SIAM J. Comput.* **37** 166 (2007)
29. Orús R *Nat. Rev. Phys.* **1** 538 (2019)
30. Deng D-L, Li X, Das Sarma S *Phys. Rev. X* **7** 021021 (2017)
31. Sharir O, Shashua A, Carleo G *Phys. Rev. B* **106** 205136 (2022)
32. Kurmapu M K, Tiunova V V, Tiunov E S, Ringbauer M, Maier C, Blatt R, Monz T, Fedorov A K, Lvovsky A I *PRX Quantum* **4** 040345 (2023)
33. Patel K N, Markov I L, Hayes J P, quant-ph/0302002
34. Bravyi S, Maslov D *IEEE Trans. Inform. Theory* **67** 4546 (2021)
35. Hastings M B *Phys. Rev. B* **73** 085115 (2006)
36. Vatan F, Williams C *Phys. Rev. A* **69** 032315 (2004)
37. Arute F et al. *Nature* **574** 505 (2019)
38. Wu Y et al. *Phys. Rev. Lett.* **127** 180501 (2021)
39. Aharonov D, Gao X, Landau Z, Liu Y, Vazirani U, in *STOC 2023. Proc. of the 55th Annual ACM Symp. on Theory of Computing* (Eds B Saha, R A Servedio) (New York: Association for Computing Machinery, 2023) pp. 945–957
40. Sun X, Tian G, Yang S, Yuan P, Zhang S *IEEE Trans. Computer-Aided Design Integr. Circuits Syst.* **42** 3301 (2023)
41. Gross D *J. Math. Phys.* **47** 122107 (2006)
42. Трушечкин А С, Киктенко Е О, Кронберг Д А, Федоров А К *УФН* **191** 93 (2021); Trushechkin A S, Kiktenko E O, Kronberg D A, Fedorov A K *Phys. Usp.* **64** 88 (2021)

43. Pokharel B, Lidar D A *Phys. Rev. Lett.* **130** 210602 (2023)
44. Ghosh S, Deshpande A, Hangleiter D, Gorshkov A V, Fefferman B *Phys. Rev. Lett.* **131** 030601 (2023)
45. Sotnikov O M, Iakovlev I A, Kiktenko E O, Fedorov A K, Mazurenko V V "Achieving the volume-law entropy regime with random-sign Dicke states", arXiv:2404.15050

Computable and noncomputable in the quantum domain: statements and conjectures

A.K. Fedorov [1,2,3,a], **E.O. Kiktenko** [2,3,b], **N.N. Kolachevsky** [1,2,c]
[1] *Lebedev Physical Institute, Russian Academy of Sciences, Leninskii prosp. 53, 119991 Moscow, Russian Federation*
[2] *Russian Quantum Center, Innovation Center Skolkovo, Bol'shoi bul'var 30, str. 1, 121205 Moscow, Russian Federation*
[3] *National University of Science and Technology MISIS, Leninskii prosp. 4, 119049 Moscow, Russian Federation*
E-mail: [a] *lex1026@gmail.com*, [b] *evgeniy.kiktenko@gmail.com*, [c] *kolachevsky@lebedev.ru*

Significant advances in the development of computing devices based on quantum effects and the demonstration of their use to solve various problems have rekindled interest in the nature of the "quantum computational advantage." Although various attempts to quantify and characterize the nature of the quantum computational advantage have previously been made, this question largely remains open. Indeed, there is no universal approach that allows determining the scope of problems whose solution can be accelerated by quantum computers, in theory of in practice. In this paper, we consider an approach to this question based on the concept of complexity and reachability of quantum states. On the one hand, the class of quantum states that are of interest for quantum computing must be complex, i.e., not amenable to simulation by classical computers with less than exponential resources. On the other hand, such quantum states must be reachable on a practically feasible quantum computer. This means that the unitary operation that transforms the initial quantum state into the desired one must be decomposable into a sequence of one- and two-qubit gates of a length that is at most polynomial in the number of qubits. By formulating several statements and conjectures, we discuss the question of describing a class of problems whose solution can be accelerated by a quantum computer.

Keywords: quantum computing, quantum complexity, quantum algorithms

PACS numbers: 03.67.Ac, 03.67.Lx, 42.50.Dv

Bibliography — 45 references

Received 17 May 2024, revised 19 July 2024

Uspekhi Fizicheskikh Nauk **194** (9) 960 – 966 (2024)

Physics – Uspekhi **67** (9) (2024)

DOI: https://doi.org/10.3367/UFNr.2024.07.039721

DOI: https://doi.org/10.3367/UFNe.2024.07.039721