Кафедра математической статистики ИВМиИТ КФУ 03 – 09.02.2020 г.

Научно-популярная статья подготовил Казанцев А.В.

Источник: **«Коммерсантъ Наука» №55, ноябрь 2019**, **«Нож», 13 ноября 2019 г.**

https://old.elementy.ru/nauchno-populyarnaya_biblioteka/435036/Kvantovye_vychisleniya

Квантовые вычисления

Существует ли квантовый компьютер на самом деле

Андрей Анненков

кандидат технических наук

В конце октября со слов *Google* (формально — материнской компании *Alphabet*), где построен 54-кубитовый квантовый вычислитель, многие вслед за WSJ опубликовали новость, что задача, для которой традиционному суперкомпьютеру потребовалось бы 10 тыс. лет, решена этим вычислителем за минуты.

Кандидат технических наук Андрей Анненков

Утверждение *Google* опротестовали конкуренты из IBM: никакие не 10 тыс. лет, суперкомпьютер справится за пару дней. WSJ добавила, опираясь на собственных экспертов, что практического значения (читай: перспективы продажи технологии) событие не имеет вне зависимости от того, правду или нет сообщает миру *Google.*

У *Google* есть оппоненты и в России. Директор по технологиям IBM в России и СНГ, кандидат технических наук Николай Марин объясняет: «Распространено мнение, будто квантовые компьютеры — новое явление в индустрии, но ученые уже более 100 лет изучают и тестируют практические свойства и принципы, лежащие в основе квантовых вычислений. IBM разрабатывает универсальный квантовый компьютер с 1981 года. Когда мы три года назад впервые предоставили открытый доступ к квантовому компьютеру через публичное облако, мы не знали точно, каких результатов ожидать. Для чего его будут использовать? Для развлечений? Для научных исследований? Возможно, для чего-то еще, о чем мы вообще не думали? Теперь мы точно знаем, что для всего сразу. Бесплатный сервис IBM *Q Experience* быстро собрал более 150 тыс. активных пользователей по всему миру, уже две сотни научных статей опубликованы благодаря его использованию. Видно, что квантовые компьютеры открывают бескрайние возможности для поиска и применения креативных решений. Человечество скоро сможет по-новому взглянуть на проблемы, которые раньше казались нам неприступными. Вот тогда и наступит время удивительных свершений».

Это тоже квантовая пропаганда. Квантовые вычисления ни в *Google*, ни в IBM не вылупились из лабораторной стадии. Теоретически ясно, что обработку данных действительно можно вести иначе, чем это происходит в обычных компьютерах, и что квантовые вычисления для нескольких — буквально нескольких — задач несопоставимо эффективнее возможностей традиционных компьютеров.

Задачи эти, однако, настолько важны для государств, что сомневаться в концентрации ресурсов, достаточных для практической реализации квантовых вычислений, не приходится. Оценить необходимое для практических результатов время, правда, нельзя. Не исключено, что они уже и достигнуты, но используются спецслужбами тайно.

Теория

Квантовый компьютер использует привычную вычислительным машинам двоичную систему счисления, «внутри» у него только нули и единицы. Однако термин «кубит» (*q-bit*, «бит» квантового компьютера) обозначает принципиальное отличие от бита: про состояние кубита в каждый момент времени нельзя сказать, что у него внутри — ноль или единица. Чтобы выяснить это, надо «снять» данные — открыть коробку с котом Шредингера и понять, жив кубит («1») или мертв («0»).

Аналогию «кубит как кот Шредингера» можно (и нужно) заменить несколько более сложной (хотя тоже примитивной) аналогией «кубит как электронное облако», то есть сфера, в каждой точке которой *может* находиться размазанный по орбите электрон. Эту сферу мысленно разрезаем (как пилой, пополам), чтобы «выловить» электрон в одной из двух получившихся полусфер. Практический смысл для конструктора квантового компьютера: если электрон в одной полусфере, значит, кубит на момент измерения находится в состоянии «1», если в другой — «0». До измерения кубит находится в так называемой суперпозиции: оба его возможных состояния смешаны (однако сумма вероятностей состояний равна 1). Едва

измерение состояние кубита произошло — все кончено, как в детской игре «Замри!». Информация о предыдущей «жизни» кубита разрушается, как коробка, в которой сидел кот.

Квантовые вычисления обеспечиваются возможностью зафиксировать взаимосвязь совокупности (регистра) кубитов, находящихся в суперпозиции. Кубиты можно ввести в так называемое запутанное (общее, единое) состояние, когда измерение одного кубита фиксирует не только его состояние, но и состояние всех N-кубитов в регистре. Если N-кубиты в регистре запутаны, тогда одной операцией квантовый компьютер может сразу, одновременно, обработать 2^N бит данных.

Это дает, во-первых, грандиозный рост размерности обрабатываемых данных: при $N = 50$ регистр запутанных кубитов эквивалентен по объему хранимых данных 10 в 18-й степени бит. Во-вторых, позволяет решать упомянутые выше задачи, недостижимые для классических компьютеров.

Практика

К числу таких задач, в частности, относятся:

- поиск в массивах неструктурированных данных (радикальное ускорение обработки больших данных);
- разложение чисел на простые множители (алгоритм Шора, важен для преодоления криптозащиты данных — квантовый компьютер за секунды способен сделать то, на что у суперкомпьютера уйдут миллиарды лет);
- быстрое генерирование последовательности подлинно случайных чисел (практическое применение — одноразовые ключи для гарантированно защищенной передачи данных по открытому каналу связи; очевидно, о решении именно этой задачи и сообщил *Google*);
- моделирование квантовых систем — молекул и материалов (практическое применение — фармакология, средства защиты от биологического оружия), причем для решения таких задач достаточен «маломощный» квантовый компьютер с регистром до 100 кубит.

Но пока это лишь теоретические возможности. Физическая реализация квантовых компьютеров находится в стадии исследований и экспериментов, а развитие алгоритмов квантовых вычислений обеспечивается имитацией квантовых компьютеров с помощью устройств, лишенных квантовой природы.

Программное обеспечение квантовых вычислений — системы программирования и отладки программ — только предстоит создать. Это нетривиальная задача. Она не решена даже для традиционных суперкомпьютеров, мощность которых эффективно используется только для ограниченного круга задач.

Квантовые коммуникации

Функция квантовых коммуникаций (технологически они совершенно самостоятельны по отношению к квантовым вычислениям, это другая предметная область) состоит в обеспечении абсолютно защищенных от хищения данных каналов связи, и в отличие

от квантовых вычислений технологии квантовых коммуникаций уже готовы к практическому применению.

В августе 2019 года в Австрии, в Университете Инсбрука и Австрийской академии наук, успешно испытана передача запутанного квантового сигнала на 50 км по обычной волоконно-оптической линии связи. Попытка перехвата данных моментально становится известной участникам обмена — прочтение сигнала разрушает передаваемые данные.

Абсолютная надежность криптозащиты квантовых коммуникаций математически доказана: определенные алгоритмы криптозащиты с использованием «шифроблокнотов», то есть одноразовых паролей (ключей), нельзя вскрыть. Условия — длина ключа не может быть меньше длины сообщения, а также абсолютная, подлинная случайность последовательности символов, составляющих пароль, — генерация псевдослучайных чисел с помощью обычных компьютеров не годится.

Проблема передачи одноразового ключа по открытому каналу связи в квантовых коммуникациях решается так: информацию об одноразовом ключе несет фотон, содержащиеся в нем данные (они записываются фазовой модуляцией, поляризацией, возможно, иными технологическими приемами) приемник и передатчик «видят» одновременно, после чего в канал поступает закодированная этим — одноразовым, напомним — ключом порция данных. Перехват фотона разрушает его и тем демаскирует внешнего наблюдателя: в этом случае участники сеанса связи немедленно узна*ю*т, что их подслушивают.

https://knife.media/quantum-supremacy/

Скотт Ааронсон Люся Ширшова Настя Травкина 13 ноября 2019

Эра квантовых вычислений началась: что означает успех эксперимента Google по достижению квантового превосходства

В конце октября компания Google официально объявила в журнале Nature о достижении квантового превосходства. Основатель Центра квантовых вычислений Техасского университета в Остине Скотт Ааронсон, разрабатывавший теорию для эксперимента, объясняет, чем квантовые вычисления отличаются от привычных двоичных, как маленький квантовый компьютер делает то же, что и суперкомпьютер размером с два баскетбольных поля, и для чего мы сможем использовать квантовые мощности.

«Квантовое превосходство» — меткое выражение физика Джона Прескилла, который в 2012 году назвал так способность квантового компьютера совершать вычисления с невиданной до сих пор для существующих суперкомпьютеров скоростью.

Вычисления при этом не должны быть полезными — они призваны лишь доказать сам факт, как в случае экспериментального самолета братьев Райт в 1903 году или первого в мире ядерного реактора Энрико Ферми в 1942-м.

Последние десять лет я занимался теоретическим обоснованием для экспериментов по достижению квантового превосходства. Работу Google я видел еще до публикации, поэтому я могу по крайней мере попытаться просто объяснить, что всё это значит.

Зачем нужен квантовый компьютер?

До недавних пор все компьютеры на планете, от больших ЭВМ 1960-х до вашего айфона или таких, на первый взгляд, экзотических изобретений, как нейроморфные компьютеры или ДНК-компьютеры, работали по одним и тем же принципам. Их сформулировал Чарльз Бэббидж в 1830-е годы и систематизировал Алан Тьюринг в 1930-е.

В ходе компьютерной революции менялись только количественные показатели: увеличивались скорость, объем оперативной и физической памяти, количество процессоров.

Но квантовые вычисления — это нечто совершенно иное. Это первая компьютерная модель со времен Тьюринга, которая изменит принципиальные основы вычислительных алгоритмов, позволяя выполнять невероятно сложные для традиционных компьютеров задачи.

Самые ожидаемые результаты квантовых вычислений — это возможность симулировать процессы химии и квантовой физики, а также разрушить большую часть систем шифрования, которые сейчас обеспечивают защиту данных в интернете.

Демонстрация компанией Google способностей квантового компьютера стала критической вехой компьютерной революции.

Квантовый компьютер: кубиты вместо битов

В лаборатории Санта-Барбары (Калифорния) команда Google под руководством Джона Мартиниса создала микрочип под названием «Сикомор». Этот квантовый чип состоит из 53 проволочных петель, вокруг которых ток может течь при двух разных энергиях, представляя собой 0 или 1. Чип располагается в криогенной холодильной машине, которая охлаждает провода почти до абсолютного нуля, делая их сверхпроводимыми. Такая температура необходима, чтобы на мгновение (точнее, на несколько десятков миллионных долей секунды) уровни энергии стали вести себя как квантовые частицы — кубиты (qubits, от quantum bits). Эти частицы могут находиться в состоянии так называемой суперпозиции — состояние 0 и 1 одновременно.

Суперпозиция печально знаменита тем, что ее очень сложно объяснить.

Многие популяризаторы используют образ, который заставляет физиков выть в муках: «Представьте, что кубит — это бит информации, который может быть сразу и 0, и 1 и исследовать эти состояния одновременно». Если бы у меня была возможность рассказать об этом подробно, я бы упомянул об амплитудах вероятности — ключевой концепции квантовой механики со времен Вернера Гейзенберга и Эрвина Шрёдингера.

Вот короткая версия: в повседневной жизни вероятность наступления какого-либо события может составлять от 0 до 100% — поэтому вы никогда не слышали о 30-процентной отрицательной вероятности дождя!

Однако первичные элементы, из которых состоит вся окружающая действительность (фотоны и электроны), подчиняются совершенно иным законам вероятности. Они измеряются амплитудами, которые могут быть положительными, отрицательными и даже комплексными (включая квадратный корень из −1).

Более того, если событие — скажем, фотон, врезающийся в какую-то точку на экране, — может произойти в одном случае с положительной амплитудой, а в другом случае с отрицательной, то обе вероятности могут взаимно уничтожиться: общая амплитуда станет равна нулю и событие никогда не произойдет. Это явление называется **квантовой интерференцией**, и именно она лежит в основе всего того, что вам кажется очень странным в квантовом мире.

Вернемся к кубитам. Кубит — это просто бит информации с двумя амплитудами вероятности: 0 и 1. Если вы наблюдаете за кубитом, вы заставляете его случайным образом принять значение либо 0, либо 1.

Однако если вы не наблюдаете за ним, то происходит интерференция амплитуд, и кубит выдает эффекты, свойственные обеим амплитудам. Вы не можете объяснить их только тем фактом, что кубит в состоянии 1 или в состоянии 0.

Один кубит соответствует двум состояниям, два кубита — уже четырем, а восемь кубитов могут принимать значения от 0 до 255.

Что происходит, если у вас не один кубит, а тысяча, и все они взаимодействуют друг с другом (в результате чего получается то самое состояние квантовой «запутанности»)? Законы квантовой механики действуют непреклонно — придется просчитывать все возможные значения всех тысяч бит. Это 2 в тысячной степени — больше, чем количество атомов в наблюдаемой Вселенной!

Если у вас 53 кубита, как в «Сикоморе» от Google, то получится 2 в степени 53, или около 9 квадриллионов значений.

В чем суть эксперимента по квантовому превосходству?

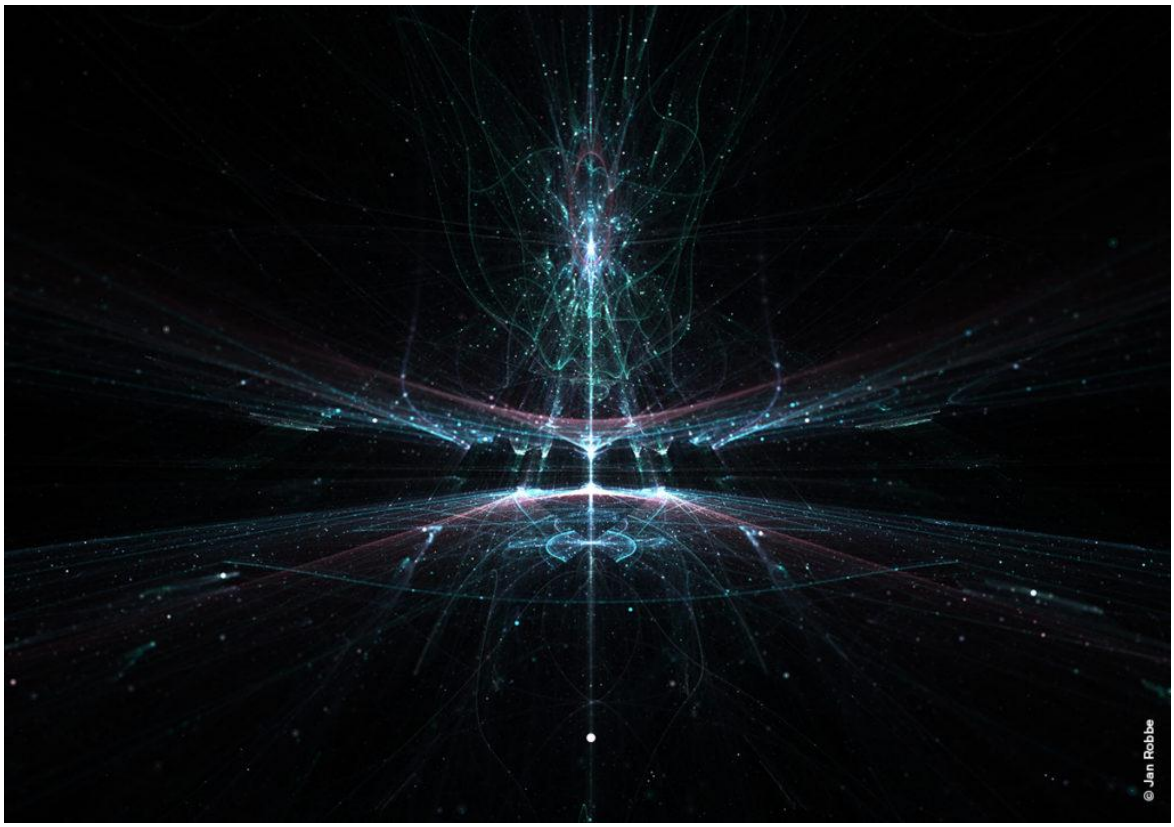
Цель эксперимента Google — с помощью 53 кубит «Сикомора» произвести вычисление, для симуляции которого обычному компьютеру действительно понадобилось бы 9 квадриллионов шагов.

Кубиты в «Сикоморе» расположены в прямоугольной сетке, которая позволяет каждому кубиту взаимодействовать с соседними. От обычного компьютера снаружи холодильной камеры к «Сикомору» идет сигнал, сообщающий каждому кубиту, как ему себя вести, с каким из соседей взаимодействовать и когда. Иначе говоря, это программируемое устройство — именно поэтому оно и называется компьютером.

В конце все кубиты измеряют, получая случайную строку из 53 битов. Какая последовательность взаимодействий используется для получения этой строки, неважно. В эксперименте Google они были случайными. Затем можно снова выполнить ту же самую последовательность, чтобы сэмплировать другую случайную 53-битную строку точно таким же образом — и так далее, так часто, как вам нужно.

По оценке Google, чтобы повторить пробное вычисление, которое заняло у «Сикомора» 3 минуты 20 секунд, понадобилось бы 10 тысяч лет и 100 тысяч традиционных компьютеров, на которых запущены самые быстрые на сегодняшний день алгоритмы.

Эта задача так сложна, что с помощью обычного компьютера оказалось невозможно даже проверить результаты вычисления! Так что для проверки работы квантового компьютера в самых сложных случаях Google полагался на аналогии с более простыми.



Почему IBM говорит, что Google ничего не достиг

Компания IBM, которая сконструировала свой собственный 53-кубитный процессор, тут же опубликовала опровержение.

Компания заявляет, что с помощью мощнейшего суперкомпьютера на планете она сможет повторить эти вычисления за 2,5 дня, а не за 10 тысяч лет. Для этого понадобится суперкомпьютер Summit в Национальной лаборатории Ок-Риджа в штате Теннесси, площадь которого занимает пару баскетбольных полей.

IBM утверждает, что может записать все 9 квадриллионов возможных состояний, используя не умещающиеся в моем воображении 250 петабайт физической памяти суперкомпьютера. Что характерно, IBM не считает, что такое моделирование будет легким: на момент написания этой статьи компания так и не провела его.

Кто и что в итоге доказал?

Сегодня мощнейшие суперкомпьютеры планеты с героическим усилием всё еще могут продемонстрировать малую долю мощности квантовых компьютеров. Но сам факт того, что в компьютерной гонке обычный и квантовый компьютер сравнялись, заставляет предположить, что очень скоро кое-кто вырвется вперед.

Будь у Google процессор не на 53 кубита, а на 60, для проверки результатов компании IBM понадобилось бы уже 30 суперкомпьютеров Summit. А на проверку 70 кубитов нужен суперкомпьютер величиной с огромный город.

Есть ли какая-то научная ценность в бодании двух технологических гигантов? Является ли формальное «квантовое превосходство», пока что не применимое к жизни, важной вехой? И когда вообще ждать от этого всего практической пользы? Предположим, Google все-таки достиг квантового превосходства — что конкретно это доказывает и кто вообще в сомневался в том, что квантовое исчисление мощнее двоичного?

Чем полезен квантовый компьютер?

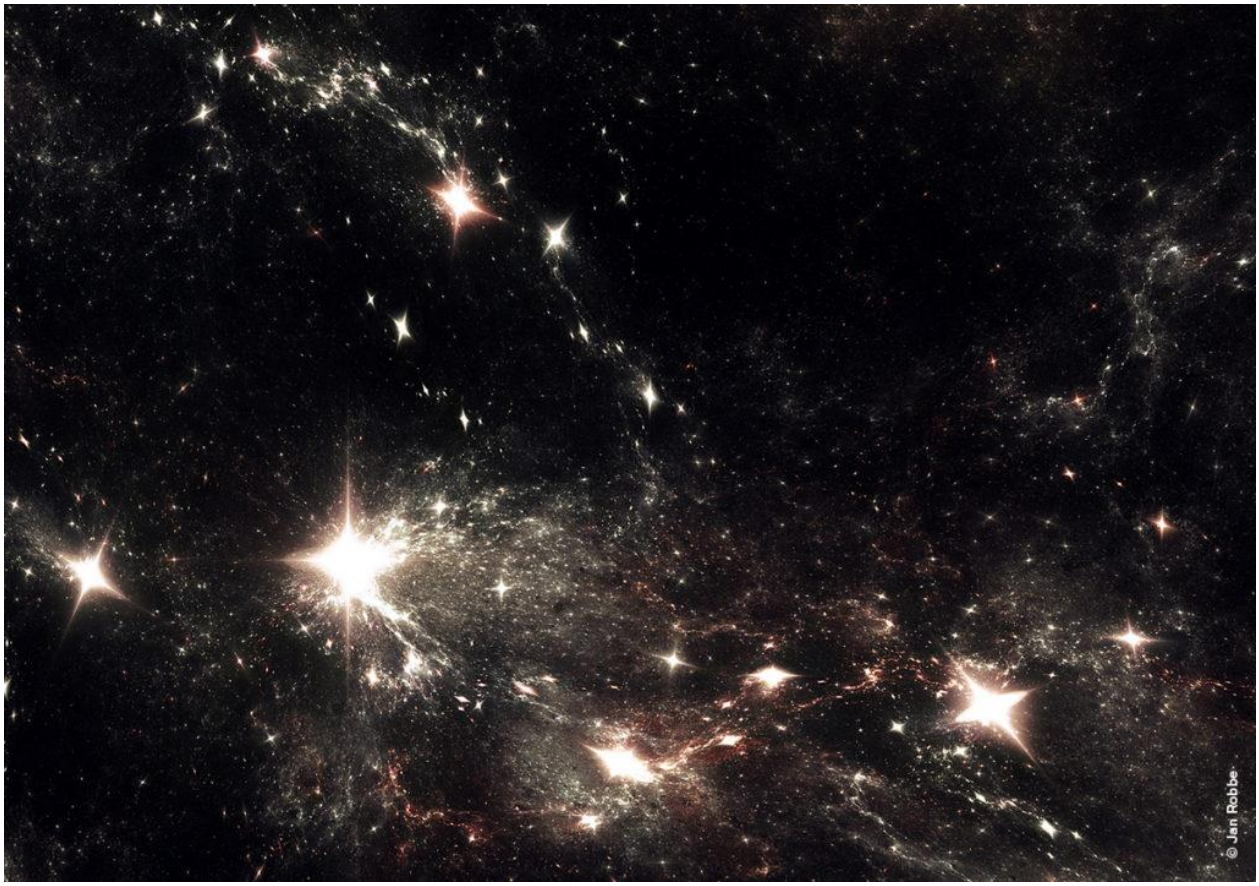
Давайте начнем с практической пользы.

Шифрование. Протокол, который я разработал пару лет назад, использует для генерации случайных битов такой же процесс выборки, как и в эксперименте Google. Сам по себе он не впечатляет, но дело в том, что даже убежденному скептику можно продемонстрировать случайность битов, обеспеченную квантовой интерференцией. Надежная случайность битов необходима для шифрования, например, в случае с криптовалютами с доказательством доли владения (Proof-of-stake, или PoS) — экологичными альтернативами биткоина. Google, кстати недавно купил права на этот протокол.

Симуляция квантовых процессов природы. Еще одно практическое применение потребует больше кубитов и более высокое качество работы — как раз сейчас техногиганты спешат обогнать друг друга в конструировании такого устройства. Это небольшие квантовые компьютеры, которые смогут симулировать квантовые процессы химических веществ и материалов, помогая ученым в их исследованиях.

Симуляция квантовой механики, превосходящая количество амплитуд в реальности за счет компьютера, равного по мощности самой природе, — о таком применении говорил Ричард Фейнман в начале 1980-х годов, когда создал концепцию квантового компьютера.

Это всё еще самое важное применение этой технологии, которое поможет в разработке чего угодно: от аккумуляторов и солнечных батарей до удобрений и лекарств.



Достижение невероятных мощностей. Еще одна веха будущего — квантовое исправление ошибок. В теории эта технология позволит удерживать кубиты в правильном состоянии без помех в течение длительного периода времени.

Исследователи полагают, что квантовое исправление ошибок в итоге позволит квантовым компьютерам вырасти от пары сотен кубитов до машин с миллионами или миллиардами кубитов, что сделает мечту Фейнмана реальностью.

Но этого пока что никто не сделал — и неизвестно, когда это станет возможным.

Google доказал, что квантовая механика работает

В то же время эксперимент Google — это решающее доказательство жизнеспособности самой идеи. Построить квантовый компьютер так трудно, что с тех пор как ученые серьезно взялись за это дело в середине 1990-х, некоторые скептики утверждали, что это попросту невыполнимая задача. Кубиты, говорили они, всегда будут слишком хрупкими, чтобы их контролировать. И если законы квантовой механики предсказывают, что количество

амплитуд вычислений растет по экспоненте — что ж, тем хуже для нашего понимания квантовой механики!

Эксперимент Google должен дать всем скептикам паузу для размышления. Очевидно, что устройство на 53 кубита действительно смогло просчитать 9 квадриллионов амплитуд, оставив позади все суперкомпьютеры на планете — пусть пока что и в совершенно бессмысленном вычислении.

Квантовая механика работает! Это вывод одновременно ожидаемый и поразительный, консервативный и радикальный.

Компьютерная революция началась с одного-единственного изобретения — транзистора. В дотранзисторную эпоху мы застряли на ненадежных электронных лампах. Но они свое дело делали — переводили абстрактную алгебру логики в электрический сигнал достаточно надежно, чтобы это было полезно практически.

У нас пока что нет квантовой версии транзистора: для этого нужно квантовое исправление ошибок. Чтобы добраться до этой точки, нам понадобятся огромные инженерные мощности, а возможно, и другие инсайты.

Но значение эксперимента Google по достижению квантового превосходства невозможно отрицать: после 25 лет попыток мы наконец оказались в «ламповой эре» квантовых вычислений.