Программа на пятилетку

А. ГОЛЫШКО, канд. техн. наук, г. Москва

"Если кто-то ежедневно зажигает звёзды, значит, ему за это вовремя платят".

(Никита Богословский)

На ежегодной конференции Think-2018 в Лас-Вегасе компания IBM выступила с очередным прогнозом о том, какие пять технологий в ближайшие пять лет изменят наш мир. Среди них оказались квантовые вычисления, блокчейн, криптография на решётках, искусственный интеллект (ИИ) и специальные устройства — микроскопические роботы (ИИ-микроскопы), использующие в своей работе принципы ИИ. Все эти технологии уже существуют, но их ждёт и изменение, и популяризация.

Но сначала о квантовых компьютерах, которые сделают проще многие вычисления. Идее использования квантовой механики для обработки информации уже десятки лет. Одно из ключевых событий произошло в 1981 г., когда IBM и MIT (Massachusetts Institute of Technology — Массачусетский технологический институт) совместно организовали конференцию по физике вычислений. Знаменитый физик Ричард Фейнман предложил тогда построить квантовый компьютер. По его словам, для моделирования следует воспользоваться средствами квантовой механики. И это прекрасная задача, поскольку не выглядит такой простой. У квантового процессора принцип действия основан на нескольких странных свойствах атомов — суперпозиции и запутанности. Частица может находиться в двух состояниях одновременно. Однако при проведении измерений она окажется только в одном их них. И невозможно предугадать в каком, кроме как с позиции теории вероятности. Этот эффект лежит в основе мысленного эксперимента с котом Шредингера, который находится в коробке одновременно живым и мёртвым до тех пор, пока наблюдатель украдкой туда не заглянет. Ничто в повседневной жизни не работает подобным образом. Тем не менее около 1 млн экспериментов, проведённых с начала XX века, показывают, что суперпозиция действительно существует. И следующим шагом будет выяснение того, как использовать эту концепцию.

Классические биты могут принимать значение 0 или 1. Квантовые компьютеры оперируют кубитами, которые могут иметь логическое значение 0, 1, 0 и 1 сразу. Для решения определённых задач они будут иметь преимущество по сравнению с традиционными вычислительными машинами. Сегодня уже есть десятки описаний алгоритмов работы. Программисты создают особый программный код, который сможет работать по новым принципам вычислений. Принцип работы квантового процессора таков, что выполнение логической операции даёт возможность работать со всеми положениями сразу. И число доступных состояний равно двум в степени числа кубитов. Так что, если сделать 50-кубитный универсальный квантовый компьютер, теоретически можно исследовать все 1,125 квадриллиона комбинаций одновременно.

Благодаря свойству квантовых объектов под названием "суперпозиция" кубит может принимать все значения, которые являются комбинацией основных. При этом его квантовая природа позволяет ему находиться во всех этих состояниях одновременно. В этом и заключается параллельность квантовых вычислений с кубитами. Всё случается сразу — уже не нужно перебирать все возможные варианты состояний системы, а это именно то, чем занимается обычный компьютер. Поиск по большим базам данных, составление оптимального маршрута, разработка новых лекарств — лишь несколько примеров задач, решение которых способно ускорить во множество раз квантовые алгоритмы. Это те задачи, где для поиска правильного ответа нужно перебрать огромное число вариантов.

Кроме того, для описания точного состояния системы теперь не нужны огромные вычислительные мощности и объёмы оперативной памяти, ведь для расчёта системы из 100 частиц достаточно 100 кубитов, а не триллионов бит. Более того, с ростом числа частиц (как в реальных сложных системах) эта разница становится ещё существеннее.

Наиболее известным квантовым алгоритмом является алгоритм Шора (его придумал в 1997 г. английский математик Питер Шор), который нацелен на решение задачи разложения чисел на простые множители (задача факторизации, дискретного логарифма). Казалось бы, что в этом сложного и зачем для решения такой задачи нужен квантовый компьютер? Мы все без труда раскладываем на простые множители числа вида: $15 = 3\times5$; $55 = 5\times11$; $91 = 13\times7$ и т. д. Но можете ли вы разложить на два простых множителя число 853 или 13297, или 99487? Уже не так просто, правда? Но если написать программу для компьютера, то он довольно быстро найдёт исходные множители простым перебором (или с помощью другого, более сложного алгоритма). А если в числе будет не пять знаков, а хотя бы 100? С такой задачей не могут справиться и самые современные компьютеры, на это у них уйдёт от нескольких десятков тысяч до нескольких миллионов лет в зависимости от числа знаков.

А вот квантовые компьютеры, исполняя алгоритм Шора, должны справляться с этой задачей за считанные секунды. По крайней мере, в теории. На практике это удастся проверить только тогда, когда будет создан первый полноценный квантовый компьютер, оперирующий парой тысяч кубитов. Кстати, не так давно учёные реализовали алгоритм Шора на квантовом процессоре из трёх кубитов.

Почему же задача факторизации чисел так важна? Дело в том, что многие из современных протоколов, обеспечивающих защищённую передачу данных (например, при совершении банковских операций), используют вычислительную сложность этой задачи для генерации секретного ключа, который применяется для шифрации и дешифрации сообщений. С созданием квантового компьютера эти системы в мгновение ока перестанут быть скольлибо секретными и безопасными. То есть отличительной особенностью, которой обладают квантовые компьютеры, является способность быстро подобрать нужный код или шифр. Собственно, квантовые компьютеры попросту "убивают" существующие сегодня системы шифрования. Обычный компьютер выполняет решение математической оптимизации последовательно, перебирая один вариант за другим. Квантовый конкурент работает сразу со всем массивом данных, молниеносно выбирая наиболее подходящие варианты за беспрецедентно короткое время. Банковские операции будут расшифрованы в мгновение ока, что современным вычислительным машинам недоступно. Нельзя утверждать, что современные компьютеры не могут справиться с подобной задачей, но затраченное на решение значительное время попросту обесценит расшифрованную информацию.

Есть, правда, и проблемы. В частности, сложность заключается в создании условий, при которых квантовый бит сможет бесконечно долго находиться в состоянии суперпозиции. Каждый кубит представляет собой микропроцессор, который работает на принципах сверхпроводимости и законах квантовой механики. Вокруг микроскопических элементов логической машины создаётся целый ряд уникальных условий окружающей среды, и даже небольшое отклонение от этих условий вызывает мгновенную потерю кубитами состояния суперпозиции, что приводит к сбою в работе. Впрочем, технологии развиваются, и, хотя настольной версии квантового компьютера в ближайшую пятилетку явно не появится, создание нечто для коммерческого использования где-то в "облаках" вполне возможно.

Новый подход в процессе вычислений позволяет работать с огромными массивами данных и выполнять вычислительные операции моментально. Новый способ вычислений создаст предпосылки для грандиозных научных открытий во всех отраслях путём обработки колоссальных массивов данных,

чтобы выявить скрытые в них закономерности. Быть может, стоит говорить о "втором дыхании" такой технологии, как Big Data.

По мысли аналитиков американской компании, через пять лет квантовые вычисления вскоре будут использоваться повсеместно. С их помощью можно будет решать проблемы, которые до этого считались неразрешимыми. Медицина решит многие проблемные вопросы, которых накопилось в последнее время довольно много. Станет возможной диагностика самых серьёзных заболеваний на более раннем этапе заболевания, чем сейчас. Станет проще разработка новых видов лекарств. Химическая промышленность сможет синтезировать продукты с уникальными свойствами. Расчёты полётов к другим планетам помогут космонавтике. Потенциал, который заложен в квантовых вычислениях, безусловно, преобразит нашу планету до неузнаваемости.

Не обязательно работать в IBM, чтобы предсказывать набор оборотов киберкриминальной индустрии, когда она обзаведётся квантовыми компьютерами и станет творить невиданные по масштабам DDoS-атаки, с которыми будет крайне сложно справиться, а также взламывать приложения с помощью ИИ. "Квантовые компьютеры с вычислительной силой в миллионы кубитов позволят быстро перебрать все возможные варианты и взломать даже самый сложный шифр из существующих", — говорится в официальных документах IBM. Что нужно делать в такой ситуации? Например, придумывать лучший способ защиты.

В этом случае в IBM делают ставку на так называемый метод криптографии на решётках — Lattice-based Cryptography. Это следующий шаг эволюции алгоритмов шифрования после алгоритма эллиптических кривых. Глава данного проекта, математик Сецилия Бочини, объяснила, что взлом любой криптографической защиты сводится к решению определённой математической задачи. Чем сложнее эта задача, тем дольше её решать и тем надёжнее защита. Нынешние методы шифрования устроены так, что пришлось бы потратить десятилетия на то, чтобы взломать код. Но, как указывалось выше, очень мощные вычислители в теории могли бы справиться с этой задачей гораздо быстрее. Если верить словам аналитиков IBM, криптография на решётках, представляющая собой новый подход к построению алгоритмов шифрования, обеспечит поистине "непробиваемую" защиту ценной личной информации от атак хакеров. Собственно, важнейшая сфера применения криптографии — защита личных данных пользователей.

Представим себе воображаемую решётку, скажем, тюремную (будущим хакерам это вообще было бы полезно). В точках пересечения прутьев располагаются узлы с определёнными координатами. Каждый из узлов может быть соединён с любым другим с помощью вектора. Поиск длины самого короткого ненулевого вектора в такой системе представляет собой сложную математическую проблему, которая так и называется Shortest vector problem (SVP) — проблема самого короткого вектора. Казалось бы, что тут сложного — нужно просто посмотреть на решётку и станет ясно, какая точка ближе всего к заданному узлу. Но если таких решёток много и они распределены, скажем, по сотне измерений, то даже квантовый компьютер будет не в состоянии решить эту математическую задачу. Собственно, по этой причине данный метод считается одним из самых многообещающих способов так называемого постквантового шифрования.

Постквантовая криптография — это часть криптографии, которая остаётся актуальной и при появлении квантовых компьютеров и квантовых атак. Построенные на её основе системы независимы от квантовых вычислений, и, следовательно, их считают квантово-устойчивыми (quantum-resistant) или постквантовыми криптосистемами. Постквантовая криптография, в свою очередь, отличается от квантовой криптографии, которая занимается методами защиты коммуникаций, основанных на принципах квантовой физики.

Большинство традиционных криптосистем опираются на проблемы факторизации целых чисел или задачи дискретного логарифмирования, которые будут легко разрешимы на достаточно больших квантовых компьютерах, использующих алгоритм Шора. Многие криптографы в настоящее время ведут разработку алгоритмов, независимых от квантовых вычислений, т. е. устойчивых к квантовым атакам.

IBM уже начала готовиться к переходу на протоколы, использующие данную защиту. Правда, быть может, преждевременно. Ведь до создания квантового компьютера с миллионами кубитов на самом деле ещё очень далеко. IBM в прошлом году анонсировала, что работает над 50-кубитной машиной, в этом году Google похвасталась 72 кубитами. В целом же за последние 20 лет, начиная с 1998 г., когда было объявлено о первом двухкубитовом квантовом вычислителе, число кубит увеличивалось примерно вдвое ежегодно. И всё это время хакеры взламывали криптографические системы из-за ошибок в реализации даже очень стойких, можно сказать, безупречных алгоритмов. Собственно, математическая теория зачастую сильно отличается от практики, и эксперты IBM несколько поторопились с пятилетними планами.

Из последних трендов наиболее знакомым, помимо криптографии для современного продвинутого пользователя, является блокчейн, с которым уже знакомы читатели журнала. Кроме того, как отмечают в IBM, совсем скоро во все товары в обязательном порядке будут встраиваться специальные криптографические метки. Размер данных меток будет не больше, чем чернильная точка, а крошечные компьютеры меньше, чем кристалл соли. Кстати, в рамках конференции IBM Think-2018 американская корпорация представила то, что назвала самым миниатюрным в мире компьютером. При этом, по словам самих разработчиков, его вычислительная мощность находится на уровне производительности процессора x86 1990 г.

Такая кроха состоит из нескольких сотен тысяч транзисторов и может контролировать, анализировать и даже обрабатывать данные. В случае запуска массового производства один чип будет стоить менее десяти центов. Компьютер работает с блокчейном и может стать источником данных для блоков приложений. Также устройство способно справиться с базовыми задачами систем ИИ, такими как сортировка данных.

IBM предлагает для своих клиентов приватный блокчейн, который отличается, например, от блокчейна биткоина. Пока что блокчейн от IBM доступен компаниям для коммерческого использования в тестовой версии. Пока неизвестно, сколько будет стоить это решение от IBM после официального запуска.

Криптографические метки, наряду с блокчейном, радикально изменят ситуацию во многих сферах. Например, в сфере торговли пользователи получат возможность легко проконтролировать путь товара от производителя к потребителю. Всё это позволит практически исключить подделки в сфере торговли пищевыми продуктами, на рынке генномодифицированных продуктов и среди предметов роскоши. Таким образом, эта технология изменит области бизнеса, которые тесно связаны с безопасностью пищевых продуктов, идентификацией подделок и рынком предметов роскоши. Если, конечно, эти метки не начнёт производить тот, кто кровно заинтересован в распространении ГМО и различных подделок.

А вот сфера интересов микроскопических роботов, действующих на основе принципов ИИ, — вода. Аналитики IBM предполагают, что они смогут отслеживать состояние планктона в естественной среде обитания в режиме реального времени. В перспективе всё это позволит предотвращать (скорее, правда, осуществлять мониторинг) такие ситуации, как разливы нефти и стоки от источников загрязнения на суше, а также прогнозировать такие угрозы, как красные приливы. Крошечные микророботы смогут собирать информацию о передвижении планктона, что поможет делать прогнозы на основе его поведения, справляться с загрязнением океана, например от разливов нефти. Впрочем, как они будут именно справляться, хотелось бы узнать поподробнее, если это не банальная подача сигнала тревоги специальным службам ликвидаторов.

И последнее. В IBM, понимая значимость ИИ для развития человеческой цивилизации, акцентируют внимание на особых алгоритмах его работы. Специалисты корпорации намерены поработать над объективностью ИИ. Это может звучать странно, но здесь кроется действительно серьёзная научная, социальная и технологическая проблема. Дело в том, что нейронные сети обучаются людьми с помощью наборов данных, в которые уже "зашита" предвзятость. К примеру, в наборе данных с фотографиями знаменитостей, который некоторые приложения могут использовать для обучения алгоритмов распознавания лиц, есть перекос в сторону представителей светлокожей расы.

Обученная на таких данных нейронная сеть будет хуже распознавать людей с другим цветом кожи или каким-нибудь нетрадиционным поведением. Не исключено, что такая предвзятость может привести к дискриминации, некорректным решениям и т. д. Поэтому IBM разработала и продолжает совершенствовать методику для проверки наборов данных для выявления таких предубеждений. Специалисты IBM уже сейчас работают над тем, чтобы исключить из алгоритмов обучения ИИ данные, которые не свободны от расовых, гендерных и идеологических предубеждений. Использование этого подхода позволит создать "объективный" ИИ, который не будет способствовать распространению неравенства. Его появление приведёт к качественному рывку в области обучения других систем ИИ, уверены в IBM.

Учёные компании уверены, что в ближайшие пять лет эта проблема исчезнет или перестанет быть существенной. Более интересен побочный эффект этого исследования. Франческа Росси, которая руководит данным проектом, сообщила, что чем больше учёные работают над выявлением таких отклонений в наборах данных, тем больше они понимают свои собственные предвзятые убеждения. Что ж, это нам уже показала нейронная сеть Microsoft, которая обучалась на сообщениях в Твиттере и подхватила от людей все возможные ментальные болезни, вроде сексизма, расизма и любви к нецензурному грубому самовыражению.

Над избавлением ИИ от субъективных предвзятых оценок работают сегодня специалисты из множества различных областей, включая людей искусства, философов, юристов. Есть надежда, что избавленный от человеческих слабостей ИИ в будущем станет подсказывать людям, если они их проявляют.

А вы готовы к такому будущему, в котором машины нас учат, как нужно жить? IBM предсказывает, что оно наступит уже через пять лет. Вдруг ИИ, избавленный от таких человеческих слабостей, как сопереживание, доброта и забота, решит, что во имя гендерного, расового и пр. равенства, заботливо подсказанного какими-нибудь закулисными политиканами, целесообразно перевести всех граждан в какое-нибудь стандартное сертифицированное состояние и уложить их ровными рядами в каком-нибудь красивом месте, чтобы никому не было обидно? Впрочем, как свидетельствует мировой опыт, избавленные с помощью ИИ от своих слабостей люди, пожалуй, станут опаснее любого ИИ.

Возможно, их попробует исправить государство. В частности, недавно комиссия по национальному развитию и реформам КНР объявила о намерении ввести запрет на пользование поездами и самолётами для лиц с пониженным "социальным кредитом". Согласно анонсированному плану, возможности пользоваться транспортом дальнего сообщения с 1 мая лишаются лица, уличённые в безбилетном проезде, курении в поездах или самолётах, дебоширстве на транспорте. Кроме того, новые правила будут действовать в отношении тех, кто занимался перепродажей билетов или продавал фальшивки, а также использовал поддельные документы для покупки билетов. Наконец, путешествовать не смогут неплательщики налогов, должники перед государством или частными структурами, а также те, кто не выполнил предписания судебных органов.

Напомним, так называемая система социального кредита представляет собой общенациональную систему автоматизированной слежки за жителями Поднебесной. Система включает в себя элементы ИИ и занимается анализом больших данных. Запуск этой системы начался в Китае около двух лет назад, и в настоящее время она следит за жителями страны в Интернете и за его пределами, фиксируя допущенные ими нарушения. Люди с низким "социальным кредитом" (или набравшие много отрицательных очков) сталкиваются с трудностями при получении различных социальных благ. Некоторые СМИ уже сравнили систему "социального кредита" с "Большим братом" и называют её "цифровой диктатурой".

Как утверждают в IBM, технологический прогресс в следующие пять лет позволит радикально изменить мир. Мол, к 2023 г. станут обыденными и будут применяться повсеместно такие вещи, которые сейчас воспринимаются исключительно в качестве фантазий (например, "цифровая диктатура"). Должен состояться мощный рывок, который, как ожидается в IBM, превзойдёт всё, что мы видели ранее. Если, конечно, не случится какой-нибудь традиционный планетарный форс-мажор. И только от человека, его способностей и желаний применить данные технологии на благо всего человечества зависит, насколько радикально и справедливо изменится всё вокруг нас.

Кстати, крайне интересно, что этот самый человек будет считать благом?

По материалам ***hi-news.ru, apple-iphone.ru, mirtesen.sputnik.ru, weekend.rambler.ru, fb.ru, syl.ru, cnews.ru***