УДК 519.688, 681.3, 519.7

ЗАКАТ КРЕМНИЕВЫХ ТЕХНОЛОГИЙ И КВАНТОВАЯ РЕВОЛЮЦИЯ В ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКЕ

П.А. Правильщиков
Институт проблем управления им. В.А. Трапезникова РАН
Россия, 117997, Москва, Профсоюзная ул., 65
E-mail: pavelp@ipu.ru

Ключевые слова: квантовые алгоритмы, квантовые компьютеры, квантовая революция, квантовый параллелизм, квантовый регистр, новые модели вычислений, кубиты, кутриты и куниты.

Аннотация. Кратко рассмотрены причины заката классических кремниевых технологий. Поясняется понятие «*квантовое превосходство*» в условиях квантовой революции в вычислительной технике (ВТ) и причины возникновения компьютерной гонки по созданию полноценного универсального квантового компьютера (КК). Показано, что закон сохранения перебора (ЗСП), выведенный из дискретного аналога «*физической*» теоремы Нетер [1-4], выполняется и для проблемно-ориентированного КК, (т.е. для специализированного квантового ускорителя - КвУ). Для КвУ предложена новая модель вычислений с новым механизмом квантового параллелизма.

1. Введение

Многие современные системы управления, системы САПР и технической диагностики работают на платформе тех или иных компьютеров, созданных с помощью кремниевых технологий. Однако теперь на закате кремниевых технологий в ВТ происходит очередная революция и эта революция квантовая. «*Кремниевый закат*» ощутили многие компании. Сегодня они откладывают сроки введения новых техпроцессов или прекращают инвестиции в них. Отчасти это связано с удорожанием технологического оборудования и низким процентом выхода годных. К тому же объемы производства и продаж растут медленнее, чем планировалось. О массовом производстве новых чипов говорить не приходится. Реализация 7-, 5-, 3- и 2-*нм* техпроцессов требует больших инвестиций и может оказаться невыгодной: для того, чтобы окупить инвестиции, нужно выпускать не менее 150 млн чипов в год, а объемы продаж падают. Но, несмотря на это, корпорация IBM недавно представила первый в мире 5-нанометровый чип. Однако сроков начала промышленного производства новых процессоров в IBM не назвали. Возможно, в связи с этим наблюдается определенная стагнация суперкомпьютерной отрасли и стагнация в рейтинге Top-500. Уже сегодня инвестиции в разработку КК у некоторых компаний превосходят инвестиции в разработку экзафлопсных суперкомпьютеров. Это связано с *компьютерной гонкой* за *квантовым превосходством*, которая в наши дни развернулась в мире. Под *квантовым превосходством* понимается абстрактный порог, пройдя который КК будут способны решать задачи, недоступные ни одному из существующих классических суперкомпьютеров. Целью гонки является создание полноценного универсального КК.

Квантовая революция и появление первых коммерчески доступных КК открывает новые невиданные горизонты в *computer* и *control science*, связанные с использованием

КК в управлении, в криптографии, в области ИИ, в области САПР и технической диагностике, а также в материаловедении (компьютерный дизайн материалов), в разработке новых лекарств для ранее неизлечимых болезней. Появление КК создает потребность в квантовых алгоритмах, гарантирующих квантовое превосходство. В компьютерной гонке участвуют такие страны, как Канада, США, страны ЕС, Англия. Участвуют и Австралия, и Китай, и Сингапур, и Япония. Участвует и РФ. Внутри США конкурируют IBM, HP, Microsoft, Google, Intel и многие университеты: МТИ, Гарвард, Принстон, Калтех, университет Мериленда и др. Учитывая проблемы кибербезопасности, в США проект создания КК иногда сравнивают с проектом по созданию атомной бомбы, и денег на него не жалеют. Так, в частности, корпорация IBM в 2014 получила на 5 лет от разведывательного сообщества США 3 млрд. долл. Эти средства выделены IBM на создание универсального КК. Сегодня разработчики IBM добились больших успехов (создан прототип КК с регистром в 50 запутанных кубитов, т.е. $L = 50$), а также организован облачный доступ с помощью средств IBM Cloud, что позволило уже 60 тысячам пользователей поставить около 1,7 миллионов вычислительных экспериментов на платформе КК. Корпорация Google также разработала собственный прототип квантового процессора Бристлекон (*Bristlecone*), у которого $L = 72$ [5].

Здесь уместно упомянуть разработки КК в компании Intel, которая несколько задержалась на старте, но в 2017 Intel представила прототип КК Tangle Lake с регистром в 49 кубитов ($L = 49$). Разработки в Intel вызывают особый интерес. В Intel регистр КК может быть построен на двух типах запутанных кубитов. Первый — *сверхпроводящие* кубиты. Такие кубиты делают и конкуренты Intel. Второй тип кубитов называют *спиновыми* [6]. Как утверждают инженеры Intel, они похожи на обычные транзисторы, которых на серверных процессорах Intel миллиарды. Разработчики КК в Intel надеются, что смогут модифицировать эти транзисторы так, чтобы они работали как *спиновые* кубиты. Тогда *кремниевая* технология поможет создать мощнейший КК. Однако сегодня регистр КК Intel содержит только 3 *спиновых* кубита, но не смотря на это, представители Intel уже говорят о создании КК с 1 млн. кубитов. В Intel считают, что вторая технология на основе *спиновых* кубитов на данном этапе уникальна. Но, похоже, по тому же пути идут и разработчики КК в Австрийской АН в Вене, в Австралии [7], да и наш соотечественник М. Лукин – профессор Гарвардского университета – предполагает разработать КК на алмазах с присадками. Его регистр будет построен на *спиновых* кубитах. В будущем *спиновые* кубиты можно превратить в кутриты или куквадриты [7].

Больших успехов достигли и в Канаде: компания D-wave systems в недавно презентовала коммерчески доступный КК, у которого квантовый регистр содержит 2000 кубитов. Регистр КК с $L = 2000$ может хранить 2^{2000} больших двоичных чисел: их разрядность равна 2000. Подчеркнем, что 2^{2000} много больше оценки числа атомов в наблюдаемой Вселенной: $2^{2000} >> 10^{78}$. Однако не все кубиты этого КК находятся в запутанном состоянии, и поэтому некоторые физики не считают КК D-wave systems полноценными. Однако в США КК канадской компании уже приобрела корпорация Локхид Мартин. Такой же КК приобрела и компания Google, а также ЦРУ и ФБР (США). Компания D-wave systems, как и IBM, начала использовать облачный доступ для вычислений на КК.

Недавно в ЕС опубликовали «*квантовый манифест*» европейских ученых о необходимости разработки КК, чтобы не отстать в конкурентоспособности от США. После этого Еврокомиссия выделила на разработки КК более 1 млрд. евро [8]. Также в [8] утверждается, что в ЕС исследования в области квантовых вычислений поддерживаются на протяжении почти 20 лет (инвестиции в проекты КК уже составили около 550 млн евро). Сегодня у Евросоюза есть план на много миллиардов долларов по финансированию квантовых вычислений по всей Европе.

Китай под эгидой Академии наук разрабатывает собственный КК, который, как пишут китайские специалисты, станет самым мощным КК в мире. Президент Китайской АН Бай Чунли пояснил, что набор уравнений, который китайский суперкомпьютер «Тяньхэ-2» (2-е место в списке TOP500) сможет решить за сто лет, разрабатываемый КК решит за сотую долю секунды. Так Бай Чунли приводит пример квантового превосходства будущего китайского КК [9].

В Англии так же создается КК размером с футбольное поле. Его стоимость составит, не менее 125 млн. долларов. Английские ученые, как и китайские, утверждают, что их КК станет самым мощным в мире [10].

В РФ для Института физики твердого тела РАН в 2015 был выделен ≈1 млрд. руб. на создание КК. Работами руководит В. Рязанов. Основным потребителем результатов проекта станет «Росатом». В октябре 2016 Президент РФ В.В. Путин распорядился выделить дополнительно 3,5 млрд. руб. на три направления перспективных исследований в нашей науке [11]: 1) генетические исследования в интересах медицины и сельского хозяйства; 2) информационные технологии в части квантовых вычислений; 3) исследования для создания заделов в области природоподобных технологий[1].

2. Закон сохранения перебора

Еще на заре кибернетики в 60-е годы XX века многие ученые в СССР предлагали решать задачи с помощь перебора, так как «*перебор универсален*». Однако тогда традиционные классические компьютеры не справлялись с полным перебором за приемлемое время. Напротив, КК, используя квантовый параллелизм, быстро справляются с перебором в процессе решения сложных задач, что показали работы П. Шора (*P. Shor*), разработавшего квантовый алгоритм факторизации. При наличии КК с регистром, содержащим 1000 запутанных кубитов, используя алгоритм Шора можно «*взломать*» любой документ, зашифрованный алгоритмом RSA (приблизительно за 80 *сек*). Для решения других задач можно выполнить перебор с помощью, например, QD-алгоритмов [12-14].

Ранее в ИПУ РАН из дискретного аналога известной теоремы Нетер был выведен закон сохранения перебора (ЗСП) [1-4], который служит основой механизма гипермассового параллелизма, подогнанного для выполнения параллельно-последовательных и квантовых D-алгоритмов, эффективно выполняющих полный перебор при решении некоторых задач, например, при решении булевых и алгебраических уравнений [12, 17]. Заметим, что квантовый параллелизм является частным случаем механизма гипермассового параллелизма [2, 14-16]. Он позволяет решать *NP*-полные задачи за полиномиальное время. ЗСП характеризует такую форму движения, как движение в дискретном лабиринте Λ. Лабиринт Λ служить моделью процесс решения переборных задач [1-4]. Примерами таких задач могут служить прямая и обратная задача диагностирования (задача $\check{D}$ и задача $\check{I}$) [2], либо прямая и обратная задачи $\check{D}$ и $\check{I}$ в случае решения булевых и других уравнений [12, 17]. ЗСП ломает стереотипы многих современных математиков, считающих, что в случае решения, например, булевых уравнений время $\Delta t_{\check{D}}$ решения задачи $\check{D}$ меньше времени $\Delta t_{\check{I}}$ решения задачи $\check{I}$. Заметим, что при использовании компьютеров величина перебора определяется как временная сложность (т.е. как время $\Delta t_{\check{D}}$ или время $\Delta t_{\check{I}}$). Иными словами, величина $Pr_{\check{\text{D}}}$ перебора при решении задачи $\check{D}$ меньше, чем величина $Pr_{\check{\text{I}}}$ перебора при решении задачи $\check{I}$. При использовании клас-

[1] Более полный список литературы, используемой во введении, приведен в работах [12,13].

сических или квантовых D-алгоритмов с учетом принятых обозначений выражение для ЗСП достаточно просто:

(1) $$Pr_{\text{Ď}} = Pr_{\text{Ĭ}} = Pr = \Delta t_{\check{D}} = \Delta t_{\check{I}} = \Delta t = R \ (\textit{вдеп}).$$

В (1) *вдеп* обозначает *внесистемную* временную дискретную единицу перебора: 1 *вдеп* равна времени выполнения одной элементарной операции пересечения (операции α_j) в D-алгоритмах [1-4]. Символ *R* обозначает, что число рангов в булевом уравнении или число рангов в эквивалентном комбинационном устройстве (КУ).

3. Об основах двух новых моделей вычислений

С появлением КК известная модель вычислений в виде машины Тьюринга подвергается жесткой критике. Так в [18] Д. Дойч утверждает: «*Квантовое вычисление – это нечто большее, чем просто более быстрая и миниатюрная технология реализации машин Тьюринга. Квантовый компьютер – это машина, использующая уникальные квантовомеханические эффекты, в особенности, интерференцию, для выполнения совершенно новых видов вычислений, которые, даже в принципе, невозможно выполнить ни на одной машине Тьюринга, а, следовательно, ни на каком классическом компьютере. Таким образом, квантовое вычисление – это ни что иное, как принципиально новый способ использования природы*». Далее в [18] он пишет: «*Теория вычислений традиционно изучалась абстрактно, как раздел чистой математики. При этом теряется ее суть. Компьютеры — это реальные физические объекты, а вычисления — это реальные физические процессы. Поэтому то, что могут вычислить компьютеры, и то, что они не могут вычислить, определяется исключительно законами физики, а не чистой математикой*». Затем Д. Дойч добавляет: «*Тьюринг надеялся, что его абстрактная бумажная модель настолько проста, открыта, четко определена и понятна, что не зависит ни от каких допущений относительно физики, без которых ее можно было бы исказить постижимым образом, и, следовательно, она может стать основой абстрактной теории вычисления, независимо от лежащей в ее основе физики. «Он считал, – как однажды выразился Фейнман, – что он понял бумагу». Но он* (*Тьюринг*) *ошибался. Реальная, квантово-механическая бумага очень отличается от абстрактного материала, используемого машиной Тьюринга*».

В том же духе высказался и другой специалист в области КК Дж. Прескилл [19]: «*Результаты тридцатилетних исследований в теории сложности вычислений так и останутся математическими истинами, как, например, теоремы, характеризующие возможности классических компьютеров. Но они не устоят как физические истины, поскольку классическая машина Тьюринга – неподходящая модель вычислений, которые могут быть реально выполнены в физическом мире. Если квантовая классификация сложности действительно отличается от классической* (*как подозревается, но пока не доказано*)*, тогда этот результат перевернет основы computer science. В долгосрочной перспективе этот результат также может сильно повлиять на технологию*».

Квантовая машина Тьюринга и попытки ее использования также оказались не популярными, так как в ее основе лежат кубиты, а в настоящее время уже известны прототипы КК, у которых регистр построен на кутритах. Поэтому в условиях квантовой революции в ВТ возникла потребность в новых моделях вычислений [14-17]. Основой моделей является ЗСП и регистр КК, построенный из таких разрядов как куниты (англ. эквивалент *qudit*). Здесь кунит рассматривается как некоторый абстрактный математический объект, свойства которого описываются вектором состояния – вектором $|\psi\rangle_{\nu}$. Физической основой кунита ℓ_{ℓ} могут быть атомные ядра, каждое состояние которых может быть описано такой квантовой характеристикой, как, например, их спины. Здесь

они не рассматриваются. Символ ν – это размерность гильбертова пространства H_ℓ кунита ℓ_ℓ: ν = Dim $H_\ell(\ell = \overline{1,L})$; ν также определяет количество чисел, которое может одновременно хранится в одном разряде регистра КК. Для кунита суперпозиция вектора $|\psi\rangle_\nu$ имеет вид:

(2) $$|\psi\rangle_\nu = a_1 \cdot |0\rangle + a_2 \cdot |1\rangle + \ldots + a_\xi \cdot |\xi - 1\rangle + \ldots + a_\zeta \cdot |\zeta - 1\rangle + \ldots + a_\nu \cdot |\nu - 1\rangle. \quad \sum_{\xi=1}^{\nu} |a_\xi|^2 = 1.$$

В (2) справа – условие нормировки. Кунит вводится для того, чтобы не изменять каждый раз исчисления и алгоритмы в зависимости от развития квантовых технологий КК и КвУ и, следовательно, в зависимости от увеличения числа ν. Частными случаями кунита являются кубиты (ν=2), кутриты (ν=3) и куквадриты (ν=4). Их суперпозиции имеют вид:

(3) $$|\psi\rangle_\nu = |\psi\rangle_2 = a_1|0\rangle + a_2|1\rangle \quad | \quad |a_1|^2 + |a_2|^2 = 1.$$

(4) $$|\psi\rangle_\nu = |\psi\rangle_3 = a_1|0\rangle + a_2|1\rangle + a_3|3\rangle \quad | \quad |a_1|^2 + |a_2|^2 + |a_3|^2 = 1.$$

(5) $$|\psi\rangle_\nu = |\psi\rangle_4 = a_1|0\rangle + a_2|1\rangle + a_3|3\rangle + a_4|4\rangle \quad | \quad |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 = 1.$$

Схемы одной из двух моделей представлены в докладе «Новые модели вычислений и квантовые D-алгоритмы» автора и его соавтора на этом совещании (ВСПУ-2019).

Список литературы

1. Правильщиков П.А. Симметрия диагностического лабиринта и закон сохранения перебора // Оборонный комплекс — научно-техническому прогрессу России. М.: НТЦ «Информтехника2, 1996. № 3. С. 38-52.
2. Правильщиков П.А. Закон сохранения перебора и естественный параллелизм **D**-алгоритмов для построения тестов и моделирования в технической диагностике // Автоматика и телемеханика. 2004. № 7. С. 156-199.
3. Правильщиков П.А. «Физическая теорема» Нетер в фотонике и computer science (Часть I) // Прикладная физика. 2005. № 6. С. 144-154.
4. Правильщиков П.А. «Физическая» теорема Нетер в фотонике и computer science (Часть II) // Прикладная физика. 2006. № 1. С. 95-109.
5. Jones B. Google Just Unveiled The World's Most Advanced Quantum Processor by Far. URL: https://www.sciencealert.com/google-bristlecone-quantum-computing-72-qubits-chip
6. Шаг к квантовому превосходству: 49-кубитный квантовый компьютер от Intel. URL:https://habr.com/company/it-grad/blog/347044/ (27.08.2018)
7. Hsu J. Flip-Flop Qubit Could Make Silicon the King of Quantum Computing. // IEEE SPECTRUM. 13.09.2017. URL: https://spectrum.ieee.org/nanoclast/computing/hardware/flipflop-qubit-could-make-silicon-king-the-of-quantum-computing
8. Binosi D. Quantum Manifesto endorsement. URL: http://qurope.eu/manifesto
9. Ларионов В.В Китае начали разработку квантового компьютера. URL: https://hi-news.ru/technology/v-kitae-nachali-razrabotku-kvantovogo-kompyutera.html (11.05.2017)
10. Lekitsch B., Weidt S., Fowler A.G., Devitt S.J. et al. Blueprint for a microwave trapped ion quantum computer // Science Advances. 2017. Vol. 3. No. 2. e1601540.
11. Перспективные исследования в России дополнительно профинансируют на 3,5 млрд. рублей. URL: https://rns.online/science/Perspektivnie-issledovaniya-v-Rossii-dopolnitelno-profinansiruyut-na-35-mlrd-rublei-2016-10-17/ (10.11.2016)
12. Правильщиков П.А. Квантовое превосходство и решение алгебраических уравнений // Информационные технологии в проектировании и производстве. 2018. № 3. С. 49-60.

13. Правильщиков П.А. Новая квантовая логика: новые однородные и неоднородные квантовые логические элементы // Информационные технологии в проектировании и производстве. 2019. № 1. С. 37-50.
14. Правильщиков П.А. Новая квантовая математика: матричное исчисление кубических комплексов и квантовые D-алгоритмы // Информационные технологии в проектировании и производстве. 2017. № 2. С. 21-32.
15. Правильщиков П.А. Теоретико-множественные основания новой модели вычислений – квантового генератора тестов // Информационные технологии в проектировании и производстве. 2017. № 3, С. 20-28.
16. Правильщиков П.А. Новый механизм квантового параллелизма и его физические и математические основания //Информационные технологии в проектировании и производстве. 2017. № 4. С. 15-26.
17. Правильщиков П.А. Квантовое решение булевых уравнений и проблема P =? NP // Информационные технологии в проектировании и производстве. 2018. № 1, С. 50-64.
18. Дойч Д. Структура реальности. (The Fabric of Reality). РХД. Москва-Ижевск, 2001.