Необходимость и обоснование нового механизма квантового параллелизма

П.А. Правильщиков,
в.н.с, к.т.н, с.н.с, pavelp@ipu.ru
ИПУ РАН, г. Москва

Показаны преимущества нового механизма квантового параллелизма, основанного на использовании в квантовых компьютерах (КК) и квантовых процессорах-ускорителях (КвУ) регистра, которых построен не из кубитов, а из кунитов (англ. эквивалент «*qudit*»). Приводится формула для количественного определения увеличения ёмкости регистра КК, построенного из кунитов по сравнению с регистром, построенным из кубитов. Приводятся унитарные блочно-диагональные матрицы, определяющие степень квантового параллелизма в новом механизме. Указано, что более подробное и детальное математическое и физическое обоснование нового механизма квантового параллелизма приведено в [1].

The advantages of a new mechanism of quantum parallelism based on the use of a register in quantum computers (QCs) and quantum accelerator processors (QAs), which is built not from qubits, but from qudits are shown. A quantitative increase in the capacitance of the QC register, built from the qudits, is shown in comparison with the register built from qubits. Unitary block-diagonal matrices that determine the degree of quantum parallelism in the new mechanism are given. It is indicated that a more detailed mathematical and physical justification for the new mechanism of quantum parallelism is given in Сингапур [1].

Введение

Некоторые горячие головы среди энтузиастов квантового компьютеростроения считают, что создание универсального полноценного квантового компьютера (КК) эквивалентно освоению огня первобытными людьми. По их мнению, в XXI веке вычисления на традиционных классических компьютерах сменятся на вычисления на КК, т.е. основным способом вычислений станут вычисления на КК. И эти суждения в настоящее время находят подтверждение в той компьютерной гонке за *квантовым превосходством*, которая развернулась в мире. Известно, что в этой гонке участвуют такие страны, как Канада, США, страны ЕС, Англия, Австралия, Китай, Сингапур, Япония и Россия. Внутри США конкурируют IBM, HP, Microsoft, Google. Intel и многие американские университеты, например, МТИ, Гарвард Принстон и др. Иногда в США проект создания КК сравнивают с атомным проектом – проектом по созданию атомной бомбы, и денег на этот проект не жалеют.

Так, в частности, IBM в 2014 получила от разведывательного сообщества США на 5 лет 3 млрд долларов на создание универсального КК. Если судить по открытым публикациям разработчиков IBM, то они в настоящее время уже достигла больших успехов (в настоящее время создан КК с регистром в 17 запутанных кубитов) и скоро презентуют КК с регистром в 50 запутанных кубитов. Канадская компания D-wave systems в 2017 презентовала КК, у которого квантовый регистр содержит 4000 кубитов, хотя не все кубиты этого КК находятся в запутанном состоянии. Регистр КК, содержащий 4000 куби-тов, может хранить 2^{4000} очень больших двоичных чисел**:** их разрядность равна 4000. Здесь для сравнения можно привести число 10^{78} – число элементарных частиц в нашей наблюдаемой Вселенной **10^{78}** (**$10^{78} \approx 2^{259,5} << 2^{4000}$**)**.** Многие физики не считают КК компании D-wave systems полноценными КК. Однако эти КК в США уже купили корпорации Локхид Мартин, Google, а также ЦРУ и ФБР (США). Иногда функционирование первых коммерчески доступных КК канадской компании сравнивают с первым полётом самолётов братьев Райт.

Недавно в ЕС был опубликован «*квантовый манифест*» европейских учёных о необходимости разработки универсального КК, чтобы не отстать в конкурентоспособности от США. После этого Еврокомиссия выделила на разработку европейского КК 1,6 млрд. евро. В Китае под эгидой Академии наук также разрабатывается КК, который, как утверждают китайские специалисты станет самым мощным КК в мире. Президент Китайской академии наук Бай Чунли пояснил, что набор уравнений, который китайский суперкомпьютер «Тяньхэ-2» (в списке TOP500 «Тяньхэ-2» занимает 2 место) сможет решить за сто лет, КК решит за сотую долю секунды. В Англии создаётся КК размером с футбольное поле. Английские специалисты, как и китайские, утверждают, что их КК станет самым мощным в мире.

В 2015 в РФ был выделен ≈1 млрд. руб. на создание собственного КК. Работами руководит заведующий лабораторией сверхпроводимости Института физики твёрдого тела РАН Валерий Рязанов. Основным потребителем результатов проекта станет «Росатом». Несколько позднее в октябре 2016 в ходе совещания по вопросам финансирования фундаментальной науки Президент РФ В.В. Путин распорядился найти и выделить дополнительно 3,5 млрд. руб. на три направления перспективных исследований в отечественной науке. В качестве таких направлений были определены: 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, то есть создание минимально потребляющих энергию устройств.

О разработке КвУ в ИПУ РАН

В ИПУ РАН предполагается создать проблемно-ориентированный КК, т.е. специализированный КвУ для решения уравнений и, прежде всего, логических. Квантовый регистр КвУ будет построен с использованием кунитов. Если для кубита размерность dim H гильбертова пространства H равна 2 (Dim $H = \nu = 2$), то для кунита Dim $H = \nu$, где ν может быть больше любого наперёд заданного числа $\tilde{N}$. Заметим, что неравенство $\nu > \tilde{N}$ является некоторой идеализацией. Одно из направлений развития КК состоит в увеличении числа ν для разрядов квантового регистра КК и КвУ. При переходе от такого разряда регистра как кубит (ν =2) к кутриту (ν =3) и далее к куквадриту (ν =4) приращение $\Delta\nu$ чис-

ла ν равно 1. Чтобы не изменять каждый раз алгоритмы и исчисления в зависимости от развития КК и КвУ и, следовательно, в зависимости от числа ν или приращения $\Delta\nu$ в общем случае $\nu > \tilde{N}$. Исходя из этого, кубит можно рассматривать в качестве частного случая кунита, содержащего только два состояния, которые могут быть закодированы двумя числами. Это означает, что кубит может хранить одновременно два числа. Здесь уместно привести *суперпозицию* вектора состояния (вектора $|\psi\rangle_{\nu=2}$) для кубита, кутрита, куквадрита и в общем случае для кунита, а также условия (правила) нормировки для них.

$$|\psi\rangle_{\nu=2} = a_1|0\rangle + a_2|1\rangle; \qquad |a_1|^2 + |a_2|^2 = 1. \tag{1}$$

В (1) коэффициенты a_1 и a_2, называются амплитудами и справа приведено условие нормировки для кубита.

Для кутрита:

$$|\psi\rangle_3 = a_1|0\rangle + a_2|1\rangle + a_3|2\rangle \mid |a_1|^2 + |a_2|^2 + |a_3|^2 = 1. \tag{2}$$

Заметим, что одна из австралийских исследовательских групп уже создана КК, у которого регистр построен на кутритах.

Для куквадрита :

$$|\psi\rangle_4 = a_1\cdot|0\rangle + a_2\cdot|1\rangle + a_3\cdot|2\rangle + a_4\cdot|3\rangle. \mid |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 = 1. \tag{3}$$

Для кунита вектор $|\psi\rangle_\nu$ имеет вид:

$$|\psi\rangle_\nu = a_1|0\rangle + a_2|1\rangle + \ldots + a_\xi|\xi-1\rangle + \ldots + a_\zeta|\zeta-1\rangle + \ldots + a_\nu|(\nu-1)\rangle \tag{4}$$

Правило нормировки для кунита имеет вид:

$$\sum_{\xi}^{\nu}|a_\xi|^2 = 1. \tag{5}$$

С появлением кунитов в регистре КК в ВТ и в *computer science* появляется бесконечность. Таким образом, можно повторить утверждение, что в «*гильбертовом пространстве много места*». Отсюда можно сделать вывод, что одной из основ создания нового механизма квантового параллелизма является использование не кубитов, кутритов или куквадритов, которые являются частными случаями, а кунитов. Здесь уместно привести коэффициент *k*, показывающий увеличение ёмкости квантового регистра с ростом числа ν по сравнению с ёмкостью регистра, построенного на кубитах. Пусть QR_1 – регистр, построенный на кубитах. Регистр QR_2 построен на кунитах, у которых ν = 16. Длина *L* квантовых регистров (т.е. число квантовых разрядов в регистре) QR_1 и QR_2 одинакова: $L = L_1 = L_2 = 3$. Тогда

$$k = 16^3 : 2^3 = 4096 : 8 = 512.$$

Общая формула для вычисления *k* , т.е. количественного сравнения емкости квантовых регистров, у которых числа ν разрядов различны, приведены в [3-5]. Выражение для числа *k* выведено из логарифмического уравнения [5].

Другой основой нового механизма, используемого в КвУ, предназначенном для решения уравнений, является закон сохранения перебора (ЗСП [2]). Этот закон обосновывает механизм гипермассового параллелизма для классических и квантовых ускорителей и имеет вид:

$$Pr = Pr_{пз} = Pr_{оз} = \Delta t_{пз} = \Delta t_{оз} = \Delta t = R\ (\textit{вдеп}) \tag{6}$$

Так как величина *Pr* перебора часто определяется как временная сложность решения задачи, то в (6) символ $r_{пз}$ определяет время решения прямой задачи для заданного уравнения, $Pr_{оз}$ – время. То же самое обозначают символы $\Delta t_{пз}$ и $\Delta t_{оз}$ (в общем случае Δt). В (6) символ *R* обозначает число рангов в уравнении или число рангов в эквивалентном устройстве (см. [2]). В (6) *вдеп* обозначает временную дискретную единицу перебора. Одна *вдеп равна времени выполнения одной элементарной операции пересечения в* D-алгоритмах и классическом или матричном исчислении кубических комплексов [3-7].

Сегодня для кунита практически достижимым считается число $\nu \le 10^7$. Однако в недалёком будущем практически достижимым может стать число $\nu \le 10^{1000}$, либо ещё большее число. Поэтому скоро можно будет поставить под вопрос утверждение академика А.Н. Колмогорова. Он, как математик, в 1968 не предполагал возможности создания КК. Сегодня мы знаем, что КК хорошо справляется с перебором больших размерностей**.** Колмогоров наоборот утверждал, что большой перебор в $10^{10^{10}}$ невозможно будет выполнить «*ни на какой ступени развития техники и культуры*». На следующей конференции мы покажем, что это не так. Сегодня мы знаем, что КК хорошо выполняют полный перебор. Примером может служить известный алгоритм факторизации американского математика П. Шора. При наличии КК с 1000 кубитов алгоритм Шора сможет взломать любой зашифрованный с помощью алгоритма RSA документ. По некоторым оценкам время взлома с помощью перебора, выполненного алгоритмом Шора, - 80 сек. Публикация алгоритма Шора взволновала банковское сообщество и сообщество спецслужб. Сегодня перед специалистами по кибербезопасности стоит задача создать квантовостойкие шифры (коды).

Третьей основой нового механизма квантового параллелизма является использование квантовых элементов (вентилей), реализующие унитарные блочно-диагональные матрицы вида:

$$A_{Б\text{-}Д,\boldsymbol{\omega}} = \begin{bmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_{\boldsymbol{\omega}} \end{bmatrix} \tag{6}$$

Четвёртой основой механизма квантового параллелизма являются схемы подготовки кунитов к измерению. Действие этих схем равносильно перекрашиванию кубика игральной кости так, чтобы на каждой грани было выписана одна и та же цифра (например, цифра 6). Описание этих схем приведено в [5] Кроме этого на эту тему я выступал с докладом на прошлогодней конференции «CAD/CAM/PDM – 2016».

Заключение

В заключении следует привести исследовательскую программу в области квантовых вычислений до 2025.
2018. Универсальные и проблемно-ориентированные КК в САПР, технической диагностике и компьютерной графике (обзор).
2019. Решение алгебраических уравнений с использованием КвУ и D-алгоритмов.
2020. Теоретико-множественные основания новой модели вычислений – квантового генератора тестов.
2021. Новая квантовая математика: матричное исчисление кубических комплексов и квантовые *D*-алгоритмы (*QD*-алгоритмы).
2022. Решение дифференциальных уравнений с использованием *QD*-алгоритмов на платформе КГТ.
2023. Использование *QD*-алгоритмов на платформе КГТ для решения задач ИИ (задач типа «*крепкий орешек*») и некоторых задач криптографии
2024. Решение *нечётких* уравнений на платформе квантового генератора тестов (КГТ) с использованием *QD*-алгоритмов.
2025. КГТ и решение сложных задач компьютерной графики (задач функционально-воксельного моделирования)
2026. КГТ и решение центральной проблемы современной дискретной математики (*P* = ? *NP*)

Литература

1. Правильщиков П.А. Новый механизм квантового параллелизма и его физические и математические основания //Информационные технологии в проектировании и производстве. 2017. № 4. С. 7 – 28.
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. Использование квантовых компьютеров и квантовых ускорителей в информационных технологиях // «Информационные технологии в проектировании и производстве». 2016. № 2. С. 3-12.
4. Правильщиков П.А. Использование квантовых алгоритмов в информационных технологиях и задачах управления // «Информационные технологии в проектировании и производстве». 2016. № 2. С. 13-22.
5. Правильщиков П.А. О решении проблемы подготовки к измерению кунитов в регистре квантового компьютера // Информационные технологии в проектировании и производстве. 2016. № 3. С. 34-41.
6. 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.
7. Правильщиков П.А. Теоретико-множественные основания новой модели вычислений – квантового генератора тестов // Информационные технологии в проектировании и производстве. 2017. № 3. С. 20-27.