

УДК 004.383.4

UDC 004.383.4

05.00.00 Технические науки

Technical Sciences

**МОДЕЛИРОВАНИЕ КВАНТОВЫХ
ВЫЧИСЛЕНИЙ С ИСПОЛЬЗОВАНИЕМ
АППАРАТНОГО ВЫЧИСЛИТЕЛЬНОГО
ЯДРА****SIMULATION OF QUANTUM COMPUTING
USING HARDWARE CORES**

Гушанский Сергей Михайлович
к.т.н., доцент
РИНЦ SPIN: 1556-5238, Scopus ID: 56225520500
e-mail: kron@pbox.ttn.ru

Gushanskiy Sergey Michaylovich
Cand.Tech.Sci., associate professor
RSCI SPIN: 1556-5238, Scopus ID: 56225520500
e-mail: kron@pbox.ttn.ru

Переверзев Владимир Андреевич
РИНЦ SPIN-код: 8154-1309
e-mail: pereverzevva@mail.ru
*Южный федеральный университет, г. Таганрог,
Россия*

Pereverzev Vladimir Andreevich
RSCI SPIN-code: 8154-1309
e-mail: pereverzevva@mail.ru
*South Federal University,
Taganrog, Russia*

В данной статье рассмотрены принципы моделирования квантовых вычислений с использованием аппаратного подхода. Описана общая математическая модель квантового компьютера, приведена методика математического моделирования квантовых вычислений с оптимизацией и схема аппаратного вычислительного ядра ускорителя квантовых вычислений. Предложена методика оценки увеличения производительности при моделировании квантовых вычислений с использованием аппаратного вычислительного ядра. Рассмотрены вопросы, связанные с распараллеливанием вычислений на аппаратном ускорителе, моделирующем квантовые вычисления. Приведены результаты сравнения программного и аппаратного моделирования, а также зависимость временной оценки от количества кубитов и параллельных АЛУ в вычислительном ядре аппаратного ускорителя

This article discusses the principles of quantum computing simulation using hardware approach. We describe a general mathematical model of a quantum computer; we show the method of mathematical modeling of quantum computation with optimization and a scheme of a hardware processing core in a quantum computing accelerator. The article gives a method of assessment of increasing productivity in the simulation of quantum computations using computing hardware core. The problems associated with the parallelization of computations on a hardware accelerator, simulating quantum computing were analyzed. The work lists the results of comparison of software and hardware simulation, as well as the dependence of the temporal evaluation of the number of qubits and parallel ALU in the computer-hardware accelerator

Ключевые слова: КВАНТОВЫЙ КОМПЬЮТЕР;
МОДЕЛИРОВАНИЕ КВАНТОВЫХ
ВЫЧИСЛЕНИЙ; АППАРАТНЫЙ УСКОРИТЕЛЬ;
ОЦЕНКА ПРОИЗВОДИТЕЛЬНОСТИ

Keywords: QUANTUM COMPUTER;
SIMULATION OF QUANTUM COMPUTING;
HARDWARE ACCELERATOR; PERFORMANCE
EVALUATION

Doi: 10.21515/1990-4665-123-019

В настоящее время наибольшую перспективу в сверхбыстрых параллельных вычислениях представляет собой квантовый компьютер. Идея создание такого типа устройства, осуществляющего обработку информации при помощи механизмов квантовой механики, впервые была высказана американским физиком Р. Фейнманом ещё в 1982 г. [1].

Хотя на данный момент уже существуют работающие прототипы квантового компьютера (на ионных ловушках, ядерные магнитно-резонансные квантовые компьютеры, твердотельные квантовые компьютеры на квантовых точках и т.п.), однако невозможность широкого доступа к ним, а также ограничения связанные с особенностями архитектуры и невозможностью реализации и проверки части квантовых алгоритмов приводят к необходимости моделирования таких вычислений на ЭВМ с классической архитектурой.

Как известно, основным преимуществом квантового компьютера является способность эффективно решать задачи невыполнимые за приемлемое время на классической ЭВМ, поэтому необходимость моделирования таких алгоритмов с использованием стандартных вычислительных средств требует дополнительных усилий, так как эффективное моделирование квантовых вычислений не представляется возможным на классических ЭВМ ввиду того, что сам процесс математического моделирования носит экспоненциальный рост, при увеличении квантовой системы, для которой это моделирование производится.

В то же время моделирование квантовых вычислений представляет огромное поле исследований, так как новые квантовые алгоритмы нуждаются в проверке их эффективной работы на квантовом компьютере. Для этой цели создаются симуляторы квантового вычислителя (jQuantum – Quantum Computer Simulator, QuIDDPro: High-Performance Quantum Circuit Simulator и др.), однако не все из моделей получают эффективными с точки зрения производительности и объема используемой памяти на классических ЭВМ.

Одним из наиболее приемлемых вариантов достижения наибольшей эффективности работы при симуляции процессов квантовых вычислений можно считать разработку ускорителя на основе аппаратного

вычислительного ядра на базе ПЛИС. Поэтому разработка методики создания аппаратного ускорителя для моделирования квантовых вычислений носит актуальный и перспективный характер, так как заведомо понятно, что при использовании проблемно-ориентированного вычислительного ядра, задача, для которой он создается, решается в разы быстрее.

Единицей информации в квантовом компьютере является кубит [2]. Физически кубит может быть реализован, используя электроны, ионные ловушки или молекулы. Информация хранится с использованием спина или поляризации данных частиц.

При моделировании квантовых вычислений используются такие понятия как квантовый регистр и квантовые вентиль. Квантовый регистр является абстракцией структуры, хранящей квантовые состояния. При симуляции квантовый регистр представляют в виде вектора столбца, причем отношение

$$\mathit{quantum_states} = 2^n, \quad (1)$$

где n – количество кубитов, определяет размерность данного вектора состояний. Квантовые вентили являются обратимыми преобразованиями, которые воздействуют на квантовый регистр и изменяют его.

Общая методика моделирования квантовых вычислений представлена в [3,6,7]. Под квантовым регистром здесь понимается ОЗУ для хранения амплитуд и фаз состояний. При моделировании создается матрица преобразования, соответствующую воздействию на квантовый регистр. Такие воздействия называются квантовыми вентилями или гейтами. Вентили разделяются на однокубитовые, двухкубитовые, трехкубитовые и гейты, применяющиеся ко всему регистру. После ряда таких воздействий нам необходимо произвести измерение квантового регистра. В случае с реальным квантовым вычислением при измерении происходит коллапс волновой функции. Это означает, что квантовый

регистр переходит в одно единственное состояние со 100% вероятностью. Данная операция является необратимой, в отличие от воздействий на регистр при помощи квантовых гейтов. Реализовано это так, что при измерении, вначале амплитуды возводятся в квадрат для получения вероятностей состояний. Далее мы считаем, что число с наибольшей вероятностью является истинным результатом.

Очевидно, что данный участок вычислений является наиболее ресурсоемким и необходимо оптимизировать работу по вычислению матрицы преобразования. Для этого можно использовать предложенный в [8] алгоритм, который также используется в качестве оптимизации в программных моделях.

Дело в том, что при тензорном произведении в матрице имеется огромное количество нулевых элементов, которые не несут никакой информационной составляющей. Поэтому цель данного алгоритма выделение матрицы для однокубитовых вентилей – перемножение её с вектором состояния по определенной последовательности. Схему для трех кубитов можно представить, как:

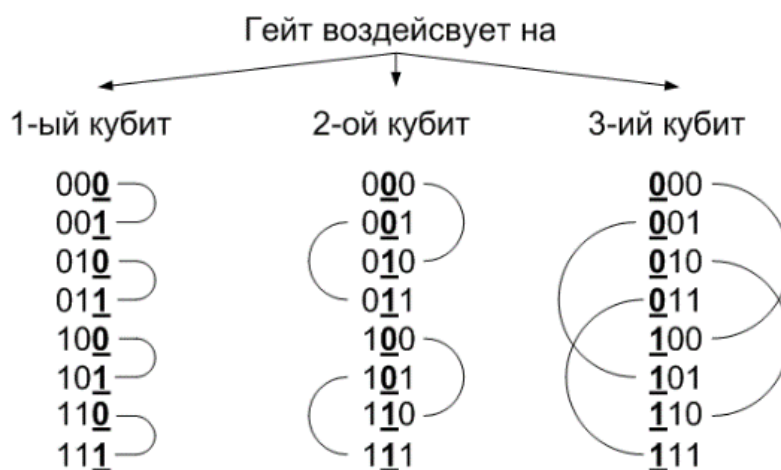


Рисунок 1 – Последовательность выбора состояний в зависимости от кубита

Вначале алгоритма воздействия однокубитового вентиля с оптимизацией, представленного на рисунке 2, производится

инициализация модели квантового регистра, что представляет собой установку амплитуды со значением 1 для одного из состояний регистра. Далее происходит вычисление бинарного индекса кубита (`qubit_binary_index`), который представляет число с установленной единицей в разряде, соответствующем номеру кубита, на который производится воздействие. Затем в цикле происходит обход состояний модели квантового регистра и выборка пары состояний для осуществления воздействия вентиля. Для правильной выборки используется переменная маска (`qubit_mask`), которая при помощи операции конъюнкции фильтрует значения (индексы состояний) таким образом, чтобы соблюдалась последовательность выборки пар состояний, обозначенная соединительными линиями на рисунке 1. После обхода всех состояний, алгоритм завершается. [8]

Без оптимизации мы вынуждены производить одно воздействие на квантовый регистр за время $O(2^{4n} + 2^{2n})$ и использовать $O(2^{2n} + 2^n)$ ячеек памяти, n – количество кубит. С оптимизацией количество операций является равным $O(2^{n-1})$, а объем памяти составляет $O(2^n)$. [9, 10]

Если рассматривать общую методику моделирования квантовых вычислений с позиции аппаратного ускорителя [5, 6], то можно сразу использовать те преимущества, которые даёт аппаратура.

Совмещая вычислительные возможности проблемно-ориентированной аппаратной части и алгоритмы оптимизации представленного в [8], которые позволяют минимизировать количество обрабатываемых состояний модели квантового регистра предлагается методика, которая позволяет учитывать такие особенности модели квантового компьютера как:

- работа с комплексными числами;
- матричные и векторные операции;
- параллелизм вычислений.

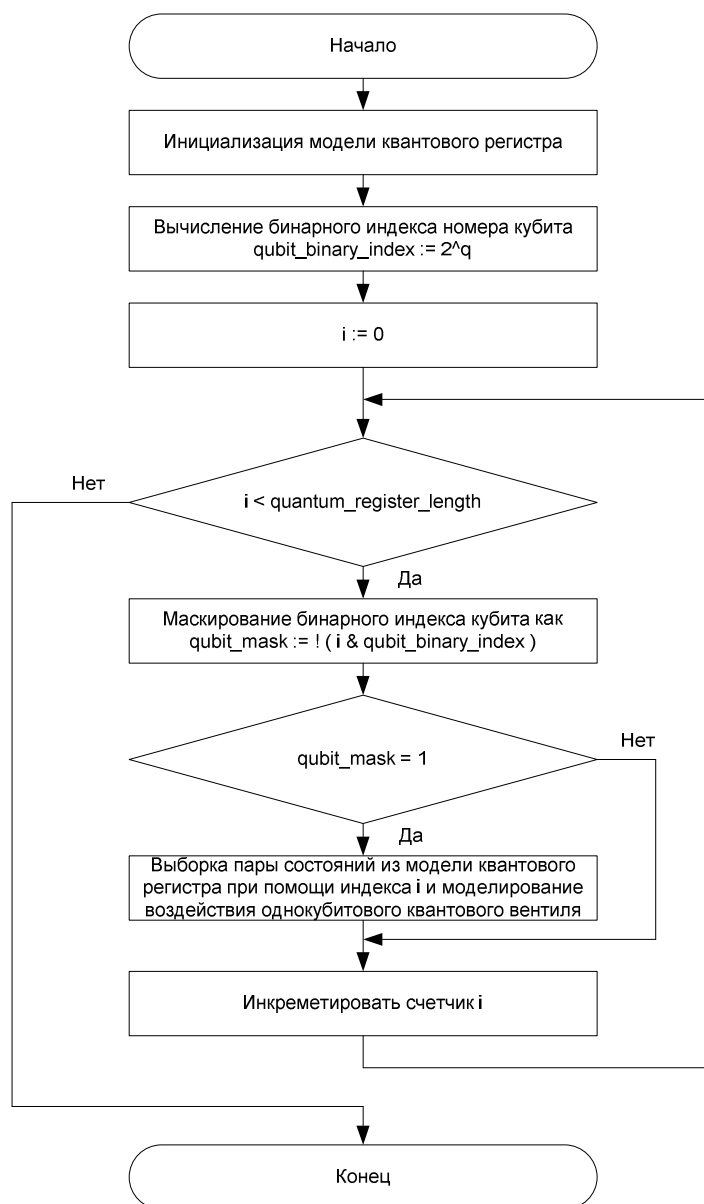


Рисунок 2 – Блок-схема алгоритма воздействия однокубитового вентиля, используя оптимизацию

Общая схема аппаратного ускорителя изображена на рисунке 3. Блоки «Устройство управления» (УУ) и «Память микропрограммы» (ПМ) являются стандартными при реализации ускорителей. Главными функциями УУ являются осуществление инициализации данных, организация выборки и исполнение команды из ПМ. Также УУ необходимо получать данные извне и правильно их обрабатывать. Однако

поскольку существует большое количество интерфейсов, то схема контроллера интерфейса здесь не рассматривается и будем условно предполагать, что данные поступают с шины X, данные на которой формируются контроллером интерфейса ускорителя.

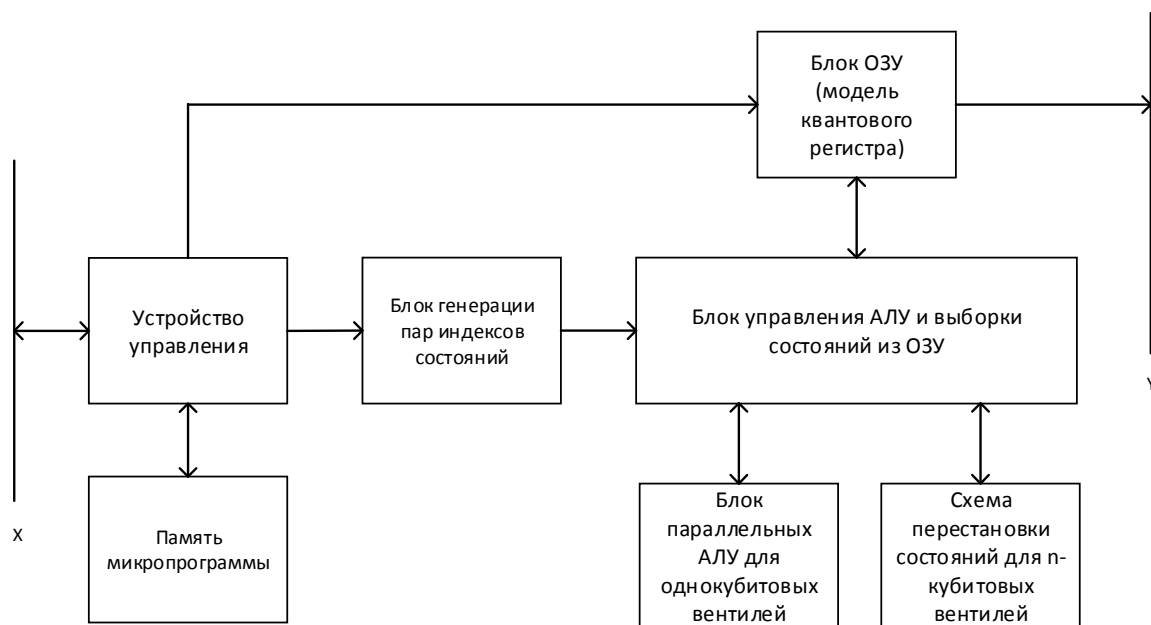


Рисунок 3 – Общая схема аппаратного ускорителя квантовых вычислений

Далее следуют блоки специфичные для ускорителя квантовых вычислений, а именно «Блок генерации пар индексов состояний» (БГИС) и «Блок управления АЛУ и выборки состояний из ОЗУ» (БУАиВС).

БГИС реализует алгоритм, который ищет последовательность состояний, в зависимости от операции (однокубитовая или многокубитовая) и кубита(ов) на который будет применяться данное воздействие. Сигналы выборки с БГИС поступают на вход БУАиВС, который определяет, как наиболее эффективно извлечь данные из «блока ОЗУ» (БО), так как ОЗУ может быть несколько для увеличения производительности и организации параллелизма вычислений.

«Блок параллельных АЛУ» (БПА) и «Схема перестановки состояний» (СПС) осуществляют непосредственно операции над данными

извлеченными из ОЗУ. По окончании вычислений УУ посылает сигнал в блок ОЗУ для выдачи результата на шину Y.

Методика построения такого рода ускорителя состоит из следующих пунктов:

а) Создание формата данных, который позволит уменьшить количество действий, затрачиваемых на арифметические операции [6].

б) Применение алгоритма оптимизации для уменьшения действий, связанных с конструированием матрицы преобразования квантового вентиля. Алгоритм был использован в [7] с целью уменьшения требуемых операций при вычислении на суперкомпьютерах (реализуется в БГИС).

в) Создание блоков БПА и СПС, которые являются основными вычисляющими схемами в структуре ускорителя.

г) Создание схемы управления АЛУ и выборки состояний из ОЗУ, которая позволит делать парную выборку состояний из блока ОЗУ.

д) Блоки УУ и ПМ являются общими для различных типов ускорителей. Создание данных блоков является типовым, а именно: при запуске вычислений УУ начинает считывать микрокоманду из ПМ и затем, дешифровав её, передаёт управляющие сигналы на БГИС.

е) Осуществление инициализации модели квантового регистра. В качестве начальных данных, которые необходимы для запуска вычислений, следует передать через интерфейс (шина X на рисунке 3) номер состояния, который будет равен 1. Остальные состояния следует проинициализировать нулями.

ж) Реализация считывания информации может происходить как на самом ускорителе, так и вне его. При считывании, согласно физике процесса квантовых вычислений, происходит коллапс волновой функции.

Разработка аппаратного вычислительного ядра проводилась в САПР Quartus II. На рисунке 4 представлена схема вычислений для однокубитовых вентилях. В качестве базовой ПЛИС использовалась

микросхема Stratix III EP3S3E50F780C4L (130МГц). Результаты сравнения программного и аппаратного моделирования показаны на рисунке 5.

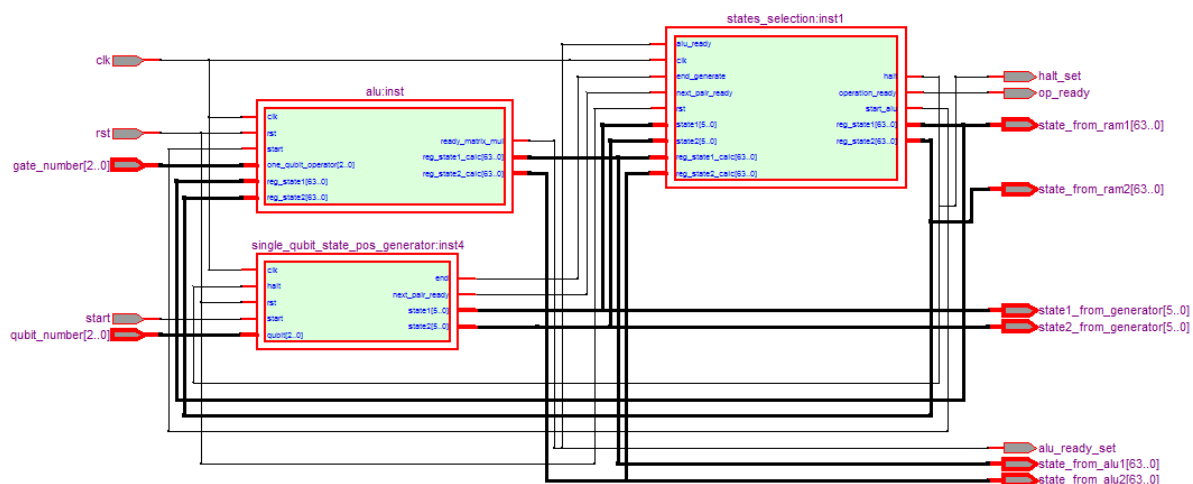


Рисунок 4 – Схема вычислений для однокубитовых вентилей

Выигрыш аппаратной реализации обеспечивается главным образом реализацией схемы АЛУ (матричного умножителя). При количестве кубитов больше 5 аппаратная реализация начинает уступать программной реализации. Однако данный результат показан без учета возможности параллельного и конвейерного выполнения операций и в сравнении с процессором, заметно превосходящим по частоте используемую ПЛИС.

В результате количество тактов блока ГСОВ составляет

$$GSOV = q + 2^{n-1} * 5, \tag{2}$$

где q тактов тратятся на сдвиги при инициализации (в зависимости от номера

кубита на который воздействует данное преобразование) и тактов на генерацию пар состояний, q – номер кубита, n – количество кубитов в квантовом регистре, 5 тактов тратятся на вычисление следующего индекса состояния.

Количество тактов блока АЛУОКВ является постоянным

$$ALUOKV = 24, \tag{3}$$

Данное количество тактов получается ввиду перемножения матрицы однокубитового квантового вентиля на пару значений из вектора состояний модели квантового регистра.

Количество тактов блока УАЛУиВС составляет постоянное число 5. При чтении из ОЗУ тратится 3 такта, а при записи 2

$$UALUaSS = 5. \tag{4}$$

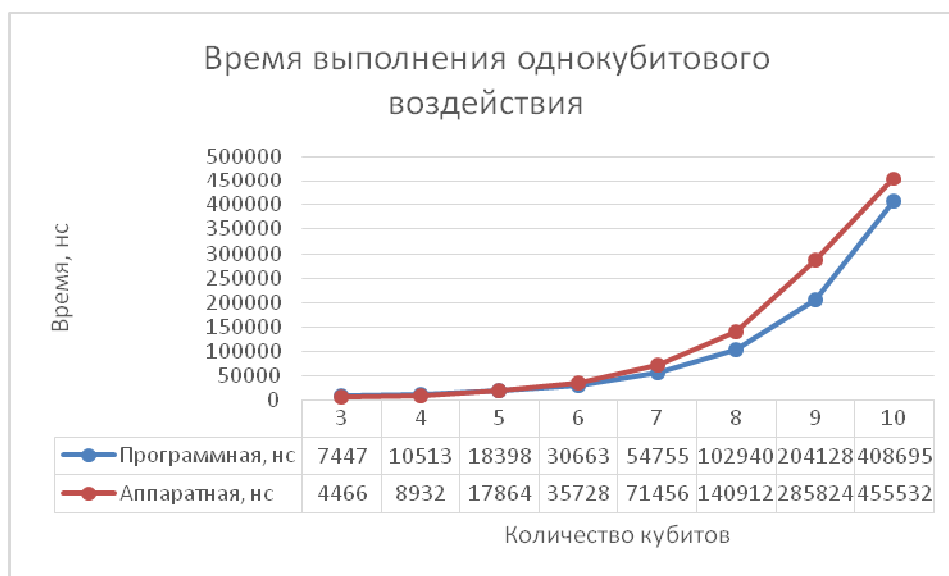


Рисунок 5 – Результаты сравнения программного и аппаратного моделирования в случае однокубитовых вентилях (1 АЛУ)

Таким образом, суммарное количество тактов, необходимых для воздействия однокубитового квантового вентиля на квантовый регистр вычисляется по формуле:

$$TotalTime = GSOV + ALUOKV * 2^{n-1} + UALUaSS * 2^{n-1}. \tag{5}$$

С целью увеличения производительности в дальнейшем планируется использовать несколько аппаратных блоков АЛУ, что усложнит блок управления арифметико-логическим устройством и выборки состояний из ОЗУ, за счет необходимости параллельного считывания и записи

состояний нескольких кубитов благодаря использованию многопортовой ОЗУ.

В этом случае зависимость временной оценки от количества кубитов при использовании распараллеливания благодаря возможности размещения в ПЛИС нескольких АЛУ, работающих параллельно, показана на рисунке 6.

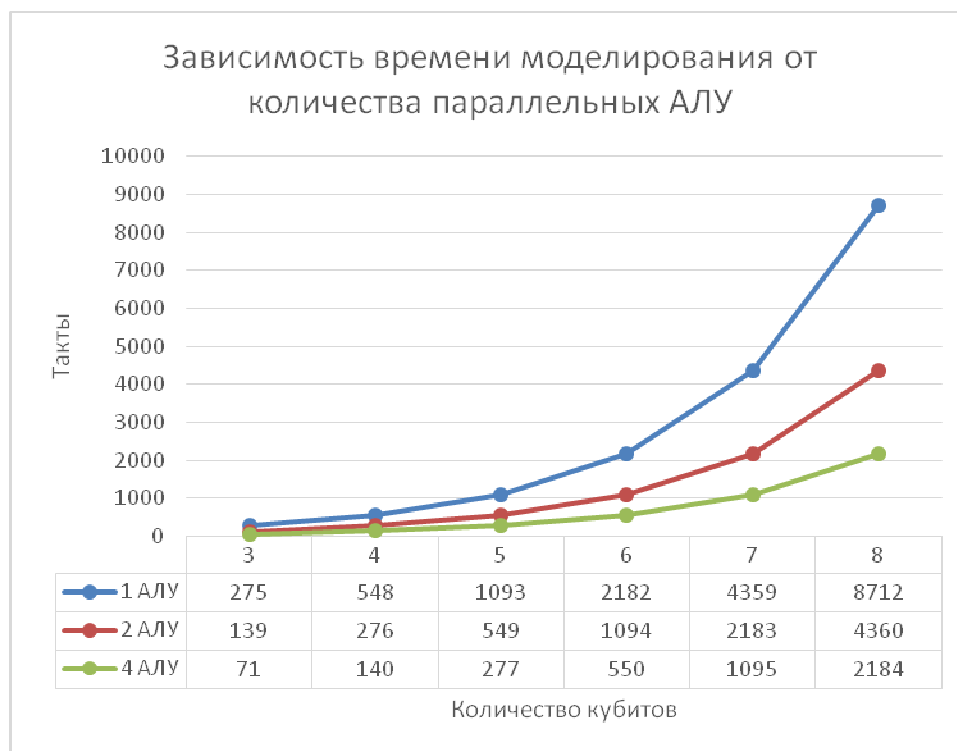


Рисунок 6 – Зависимость временной оценки от количества кубитов и параллельных АЛУ

К преимуществам использования аппаратного вычислительного ядра стоит отнести и возможность создания спецопераций, которые превышают по производительности операции стандартных универсальных процессоров. Дополнительный прирост производительности следует ожидать и от использования более мощной и скоростной ПЛИС.

Работа выполнена при финансовой поддержке РФФИ, грант № 15-01-01270.

Литература

1. Feynman, R.P. Simulating physics with computers // International Journal of Theoretical Physics. – 1982. – V. 21. – № 6. – P. 467-488.
2. Shor P. Algorithms for quantum computation: discrete logarithms and factoring. // Foundations of Computer Science: Conference Publications, 1994, pp. 124-134.
3. Schumacher B. Quantum coding. // Phys. Rev., 1995, v. A51 (4), pp. 2738 –2747.
4. Валиев К., Кокин А. Квантовые компьютеры: надежды и реальность. // Ижевск: РХД, 2004, 320 с.
5. Richter M., Arnold G., Trieu B., Lippert T. Massively Parallel Quantum Computer Simulations: Towards Realistic Systems. // John von Neumann Institute for Computing, NIC series v. 38, 2007, pp. 61-68.
6. Гузик В.Ф., Гушанский С.М., Кубраков Е.С. Аппаратный подход для моделирования квантовых вычислений // Известия ТТИ ЮФУ – ДонНТУ материалы тринадцатого международного научно-практического семинара «Практика и перспективы развития партнерства в сфере высшей школы». В 3-х кН. – Таганрог: Изд-во ТТИ ЮФУ. Кн. 2. 2012, № 12. С.49-57.
7. Гузик В.Ф., Гушанский С.М., Кубраков Е.С. Ускорение моделирования квантовых вычислений с помощью алгоритма оптимизации // Информационные технологии, системный анализ и управление – ИТСАиУ-2013/ Сборник трудов XI Всероссийской научной конференции молодых ученых аспирантов и студентов. – Таганрог: Изд-во Южного федерального университета, 2013 –Т.1. – с.15-20.
8. Khalid, A.U. FPGA Emulation of Quantum Circuits: master of Computer Engineering thesis: 31.10.2005 / Khalid Ahmed Usman; McGill University. – 2005. – 73 p.
9. Кубраков Е.С. Аппаратные стратегии моделирования квантового компьютера. // X Ежегодная научная конференция студентов и аспирантов базовых кафедр Южного научного центра РАН: тезисы докладов (г. Ростов-на-Дону, 14–29 апреля 2014 г.). Ростов н/Д: Изд-во ЮНЦ РАН, 2014. – с. 71-72.
10. Гузик В.Ф., Гушанский С. М., Кубраков Е.С. Алгоритм для оптимизации воздействий квантовых вентилях при моделировании работы квантового компьютера // Информатизация и связь. – 2014. № 2. – с. 39-42.

References

1. Feynman, R.P. Simulating physics with computers // International Journal of Theoretical Physics. – 1982. – V. 21. – № 6. – P. 467-488.
2. Shor P. Algorithms for quantum computation: discrete logarithms and factoring. // Foundations of Computer Science: Conference Publications, 1994, pp. 124-134.
3. Schumacher B. Quantum coding. // Phys. Rev., 1995, v. A51 (4), pp. 2738 –2747.
4. Valiev K., Kokin A. Kvantovye komp'yutery: nadezhdy i real'nost'. // Izhevsk: RHD, 2004, 320 s.
5. Richter M., Arnold G., Trieu B., Lippert T. Massively Parallel Quantum Computer Simulations: Towards Realistic Systems. // John von Neumann Institute for Computing, NIC series v. 38, 2007, pp. 61-68.
6. Guzik V.F., Gushanskij S.M., Kubrakov E.S. Apparatnyj podhod dlja modelirovaniya kvantovyh vychislenij // Izvestija TTI JuFU – DonNTU materialy trinadcatogo mezhdunarodnogo nauchno-prakticheskogo seminar «Praktika i perspektivy razvitija partnerstva v sfere vysshej shkoly». V 3-h kN. – Taganrog: Izd-vo TTI JuFU. Kn. 2. 2012, № 12. S.49-57.
7. Guzik V.F., Gushanskij S.M., Kubrakov E.S. Uskorenie modelirovaniya kvantovyh vychislenij s pomoshh'ju algoritma optimizacii // Informacionnye tehnologii, sistemnyj analiz i upravlenie – ITSAiU-2013/ Sbornik trudov XI Vserossijskoj nauchnoj konferencii molodyh

uchenyh aspirantov i studentov. – Taganrog: Izd-vo Juzhnogo federal'nogo universiteta, 2013 –Т.1. – s.15-20.

8. Khalid, A.U. FPGA Emulation of Quantum Circuits: master of Computer Engineering thesis: 31.10.2005 / Khalid Ahmed Usman; McGill University. – 2005. – 73 p.

9. Kubrakov E.S. Apparatnye strategii modelirovanija kvantovogo komp'jutera. // X Ezhegodnaja nauchnaja konferencija studentov i aspirantov bazovyh kafedr Juzhnogo nauchnogo centra RAN: tezisy dokladov (g. Rostov-na-Donu, 14–29 aprelja 2014 g.). Rostov n/D: Izd-vo JuNC RAN, 2014. – s. 71-72.

10. Guzik V.F., Gushanskij S. M., Kubrakov E.S. Algoritm dlja optimizacii vozdejsvij kvantovyh ventilej pri modelirovanii raboty kvantovogo komp'jutera // Informatizacija i svjaz'. – 2014. № 2. – s. 39-42.