

ФИЗИЧЕСКИЕ ОСНОВЫ И ПРОБЛЕМЫ ТЕХНИЧЕСКОЙ РЕАЛИЗАЦИИ КВАНТОВОГО КОМПЬЮТЕРА

Т. В. Вахний, А. К. Гуц

Даётся обзор различных подходов к созданию квантового компьютера. Обсуждаются основные проблемы технической реализации и перспективы каждого из подходов. Обращено внимание на исследования поведения квантовых компьютеров с помощью симуляторов, базирующихся на классических компьютерах.

Введение

Развитие технологий высокого уровня контроля над объектами наноразмеров могут открыть новые возможности по созданию не только более миниатюрных и быстродействующих микропроцессоров, но и принципиально иных способов вычислений, которые не могут быть реализованы в нынешних классических компьютерах. Компьютеры, существенно использующие в своей работе квантовые эффекты путём выполнения квантовых алгоритмов, получили название *квантовых* [1, 3, 6–8].

Перспективы проведения вычислений на квантовых компьютерах обычно связывают с ожидаемым экспоненциальным уменьшением времени решения сложных задач [1, 3, 5–8]. К таким задачам можно отнести разложение больших чисел на множители, теоретико-числовые задачи, связанные с абелевыми группами, поиск нужной записи в неупорядоченной базе данных и другие. Задачи такого типа не могут быть решены на классических компьютерах за время, полиномиально зависящее от числа битов, используемых для представления этих задач в памяти компьютеров.

Возможно, одним из важных приложений квантовых вычислений окажется моделирование поведения широкого класса многочастичных квантовых систем [6]. Это позволит предсказывать свойства молекул и кристаллов, а также проектировать микроскопические электронные устройства размером в несколько десятков ангстрем. Актуальность решения задач такого рода связана не только с быстрым продвижением современной нанотехнологии всё глубже в область

нанометровых масштабов, но и с необходимостью прямого моделирования электронных процессов в приборах наноэлектроники, в том числе и в многокубитовых квантовых устройствах. Кроме того, представляет огромный интерес возможность моделирования физических свойств различных сложных органических молекулярных и биологических систем, искусственных полупроводниковых и магнитных материалов и структур.

1. Основные идеи и принципы, лежащие в основе квантового компьютера

1.1. Элементная база

Наименьшим элементом для хранения информации в квантовом компьютере является *кубит*. В качестве кубитов могут быть использованы различные квантовые двухуровневые системы, в частности [1]:

- ионы или нейтральные атомы с двумя низколежащими колебательными или сверхтонкими уровнями, удерживаемые в силовых ловушках, созданных в вакууме с помощью электрических и магнитных полей, при лазерном охлаждении до микрокельвиновых температур;
- сверхпроводниковые структуры с переходами Джозефсона;
- отдельные электронные и ядерные спины в магнитном поле;
- квантовые точки с двумя электронными орбитальными и спиновыми состояниями;
- определённые состояния квантованного электромагнитного поля в электродинамических резонаторах и фотонных кристаллах.

1.2. Кубиты и запутанные состояния

В отличие от единицы классической информации бита, который принимает только два возможных значения (0 и 1), квантовый бит может находиться в суперпозиции этих состояний [1, 3, 6–8]. Как и бит, кубит допускает два собственных состояния, обозначаемых $|0\rangle$ и $|1\rangle$, но при этом может находиться и в их суперпозиции, т. е. в состоянии $\alpha|0\rangle + \beta|1\rangle$, где α и β — любые комплексные числа, удовлетворяющие условию $|\alpha|^2 + |\beta|^2 = 1$. При любом измерении состояния кубита он случайно переходит в одно из своих собственных состояний $|0\rangle$ или $|1\rangle$. Вероятности перехода в эти состояния равны, соответственно, $|\alpha|^2$ и $|\beta|^2$.

Преимущество работы квантового компьютера над классическим основывается на наличии *запутанных (сцепленных) состояний* между кубитами. Запутанность выражается в том, что при всяком изменении состояния одного из кубитов остальные меняют своё состояние согласованно с ним. Причём это происходит не посредством обычных классических взаимодействий (классических корреляций), ограниченных, например, скоростью света, а посредством *нелокальных квантовых корреляций*, когда изменение сказывается в тот же самый момент времени независимо от расстояния между сцепленными кубитами [3].

Если до измерения, т. е. операции вывода данных, m -разрядный квантовый регистр находится в состоянии

$$\sum_{n_{m-1}=0}^1 \sum_{n_{m-2}=0}^1 \dots \sum_{n_0=0}^1 c_{n_{m-1}n_{m-2}\dots n_0} |n_{m-1}n_{m-2}\dots n_0\rangle, \quad (1)$$

$$c_{n_{m-1}n_{m-2}\dots n_0} \in \mathbb{C},$$

являющемся суперпозицией базовых состояний $|n_{m-1}\rangle|n_{m-2}\rangle\dots|n_0\rangle$ ¹, где каждое $|n_j\rangle = |0\rangle$ или $|1\rangle$, то при невозможности быть представленным в виде

$$|x_1\rangle\dots|x_m\rangle, \quad (2)$$

где $|x_j\rangle = \alpha_j|0\rangle + \beta_j|1\rangle$ ($j = 1, \dots, m$), состояние (1) называется *сцепленным*.

Совокупность сцепленных между собой кубитов может интерпретироваться как заполненный квантовый регистр. Как и отдельный кубит, квантовый регистр (1) гораздо более информативен, чем классический. Он может находиться не только во всевозможных комбинациях составляющих его битов, но и реализовывать различные тонкие зависимости между ними.

1.3. Квантовый параллелизм

Наличие запутанных состояний между кубитами является основным фактором, отвечающим за *квантовый параллелизм*. Этот эффект не имеет аналога при работе классических компьютеров. Если в классическом компьютере вычисляется единственное выходное значение для одного входного, то в квантовом компьютере вычисляются выходные значения сразу для всех входных состояний. Таким образом, благодаря квантовому параллелизму, квантовый компьютер на каждом такте своей работы преобразует **сразу все** базовые состояния. В результате этого квантовые вычисления являются параллельными, что должно позволить получить значительное увеличение скорости и эффективности вычислений квантовых компьютеров по сравнению с классическими.

2. Варианты исполнения квантовых компьютеров

В настоящее время наиболее широко обсуждаются следующие основные направления в развитии элементной базы квантовых компьютеров [1, 6].

2.1. Квантовый компьютер на ионах в ловушках

Для реализации таких квантовых компьютеров в качестве кубитов используются уровни энергии ионов (основное и возбуждённое состояние ионов соответствуют значениям $|0\rangle$ и $|1\rangle$), захваченных ионными ловушками, создаваемыми в вакууме определённой конфигурацией электрического поля в условиях

¹Обозначение $|n_{m-1}\rangle|n_{m-2}\rangle\dots|n_0\rangle$ для состояния m -разрядного регистра — это сокращение записи $|n_{m-1}\rangle \otimes |n_{m-2}\rangle \otimes \dots \otimes |n_0\rangle$. Другая используемая запись, причём самая простая, — $|n_{m-1}n_{m-2}\dots n_0\rangle$.

лазерного охлаждения их до микрокельвиновых температур. Взаимодействие между заряженными ионами в одномерной цепочке этих ловушек осуществляется посредством возбуждения их коллективного движения, а индивидуальное управление ими — с помощью лазеров инфракрасного диапазона.

Преимущество такого подхода состоит в сравнительно простом индивидуальном управлении отдельными кубитами. Основными недостатками этого типа квантовых компьютеров являются [1]:

- необходимость создания сверхнизких температур;
- обеспечение устойчивости состояний ионов в цепочке;
- решение проблемы декогерентизации квантовых состояний, определяемой сильным взаимодействием заряженных частиц с окружением;
- ограниченность возможного числа кубитов значением 40 (реально достигнутое число кубитов в таких системах, по-видимому, не может в ближайшее время быть существенно увеличено).

В результате системы из ионов на ловушках без дальнейшего развития принципов работы кубитов на ионах не могут рассматриваться в качестве аппаратного средства для квантового суперкомпьютера, хотя в качестве модельных структур они несомненно имеют определённые перспективы [1].

2.2. Квантовый ЯМР-компьютер на органической жидкости

Эти квантовые компьютеры базируются на использовании в качестве кубитов спинов ядра (состояниям $|0\rangle$ и $|1\rangle$ могут соответствовать направления спина атомного ядра вверх и вниз) атомов, принадлежащих молекулам органических жидкостей, с косвенным скалярным взаимодействием между ними, и методов ядерного магнитного резонанса (ЯМР) для управления кубитами.

В области квантовых ЯМР-компьютеров на органических жидкостях к настоящему времени достигнуты наибольшие успехи, на этом пути удалось реализовать простейшие квантовые компьютеры [1, 6]. Экспериментально на них были осуществлены алгоритм Гровера поиска данных, квантовое фурье-преобразование, квантовая коррекция ошибок, квантовая телепортация, квантовое моделирование и другие операции.

Квантовый компьютер на органической жидкости имеет ряд значительных преимуществ [1]:

- компьютер может работать при комнатной температуре;
- для управления кубитами и измерения их состояний может быть использована хорошо развитая техника ЯМР;
- физической системой, представляющей кубиты, является макроскопический объем органических практически независимых молекул жидкости, содержащих атомы с ядерными спинами, различающимися по резонансной частоте;
- время декогерентизации квантовых состояний ядерных спинов в жидкости достаточно велико (может составлять несколько секунд).

Основными ограничениями для этого направления являются [1]:

- смешанный характер исходного квантового состояния кубитов при температурах жидкого состояния, что требует разработки специальных методов;

— для жидкостных квантовых ЯМР-компьютеров на сегодняшний день число кубитов не может превышать двух десятков из-за экспоненциального уменьшения интенсивности измеряемого сигнала с ростом числа кубитов (это требует экспоненциального роста чувствительности измеряющего оборудования);

— число различающихся по резонансной частоте ядерных спинов-кубитов в отдельной молекуле не может быть произвольно большим;

— однокубитовые и двухкубитовые квантовые операции являются относительно медленными.

Таким образом, этот вариант не может лечь в основу для создания квантового суперкомпьютера, превосходящего возможности современного классического компьютера [1].

2.3. Полупроводниковый квантовый ЯМР-компьютер с индивидуальным обращением к кубитам при низких температурах

В этих квантовых компьютерах роль кубитов играют ядерные спины одинаковых донорных атомов в полупроводниковой структуре, для электрического управления которыми и измерения их состояний должна быть создана структура из затворов нанометрового масштаба. Учитывая достижения современной нанотехнологии, в этом варианте можно создать систему из многих тысяч кубитов [1]. Кроме того, полупроводниковые квантовые ЯМР-компьютеры с индивидуальным обращением к кубитам при работе в условиях низких температур способны решить проблемы инициализации и экспоненциального уменьшения интенсивности сигнала с ростом числа кубитов [1].

Основной проблемой полупроводникового варианта является необходимость измерения состояния отдельного кубита. Для решения этой проблемы предложен ряд способов, однако ни один из них пока ещё не реализован. Другая трудность связана с наличием управляющих затворов, шумовое напряжение на которых является существенным источником декогерентизации. Этот вариант квантового компьютера, несмотря на имеющиеся трудности, несомненно заслуживает дальнейшей разработки [1].

2.4. Твердотельный квантовый ЯМР-компьютер с ансамблевым обращением к кубитам

Является более перспективным, чем предыдущая модель [1]. Появляется возможность существенно упростить управление кубитами и измерения их состояний. Кроме того, при использовании в ансамблевых вариантах принципов квантового клеточного автомата можно в значительной степени упростить и систему управляющих затворов и даже, возможно, отказаться от них совсем. Это позволило бы исключить связанные с ними существенные механизмы декогерентизации.

2.5. Полупроводниковый квантовый ЯМР-компьютер с использованием СВЧ и лазерных импульсов

Полупроводниковый квантовый ЯМР-компьютер, в котором для управления кубитами и измерения их состояний, наряду с электрическими, используются СВЧ и лазерные импульсы, является альтернативой по отношению к модели полупроводникового квантового ЯМР-компьютера с индивидуальным обращением к кубитам. Этот вариант облегчает решение задач, связанных с измерениями состояний отдельных кубитов, но при этом сохраняются недостатки, связанные с наличием системы затворов. Здесь также является перспективным использование ансамблевого подхода [1].

2.6. Квантовые компьютеры на квантовых точках с электронными орбитальными и спиновыми состояниями

Эти компьютеры имеют ряд преимуществ перед квантовыми ЯМР-компьютерами [1]:

- они способны работать при более высоких температурах, чем полупроводниковые ЯМР-квантовые компьютеры;
- имеют значительно более высокие тактовую частоту и величину измеряемого сигнала;
- современная нанотехнология позволяет создавать квантовые структуры с практически неограниченным числом квантовых точек.

Основной трудностью для них является относительно быстрая декогерентизация квантовых состояний, связанная с электрическим зарядом электрона и электрическими методами управления кубитами, для подавления которой нет хорошо разработанных методов. Выходом может быть использование для этого не электрических, а оптических ультраскоростных методов [1].

2.7. Квантовые компьютеры на переходах Джозефсона

В таких компьютерах в качестве кубитов используются зарядовые состояния куперовских пар в квантовых точках, связанных переходами Джозефсона. Перспективность этого направления состоит в возможности создания электронных квантовых устройств высокой степени интеграции на одном кристалле, при этом для управления кубитами не требуются громоздкие лазерные или ЯМР-установки [1].

Сверхпроводниковый вариант квантового компьютера, несмотря на уже имеющиеся достижения в реализации отдельного кубита, имеет ряд трудностей [1]. Они связаны с необходимостью жёсткого контроля за совершенством изготовления туннельных джозефсоновских переходов, за временными характеристиками импульсных воздействий, с использованием для управления отдельными кубитами электрических схем, флуктуации напряжений, которые являются основной причиной декогерентизации. Система большого числа кубитов, связанная с электромагнитным окружением, представляет собой сложную

нелинейную систему, в которой могут проявляться многие нежелательные нелинейные эффекты.

2.8. «Необычные» квантовые компьютеры

Рассмотренные выше варианты квантовых компьютеров относятся к группе обычных квантовых компьютеров. Они предполагают использование достаточно изученных квантовых явлений. В последнее время обсуждаются так называемые необычные квантовые компьютеры [1], в которых в качестве базовых носителей информации — кубитов — рассматриваются частицы, подчиняющиеся фермиевской статистике — фермионы. Это могут быть, например, электроны и дырки в полупроводнике. Состояние, занятое фермионом в таких системах, может представлять состояние $|1\rangle$, а незанятое — состояние $|0\rangle$.

В качестве другого варианта необычных квантовых компьютеров рассматриваются также бозонные компьютеры, использующие свойства бозе-конденсата с нелинейным взаимодействием между бозонами, проявляющиеся, например, в фотонных кристаллах, в системах из нейтральных атомов в оптических ловушках [1].

Интересны квантовые компьютеры, использующие экзотические частицы, не подчиняющиеся ни фермиевской, ни бозоновской статистике. Был предложен компьютер на анионах [1,6] — квазичастицах, отличающихся тем, что волновая функция аниона при обходе другого аниона приобретает произвольную фазу. Примером анионов являются элементарные возбуждения в двумерном электронном газе в условиях квантового эффекта Холла. Привлекательным свойством анионных квантовых систем является возможность при использовании нелокальной природы аниона обеспечить защиту квантовых операций от влияния случайных помех.

Возможно, в будущем появятся новые идеи для физической реализации квантового суперкомпьютера или комбинации уже известных вариантов, в которых будут одновременно учитываться их преимущества.

3. Наиболее перспективные направления конструирования квантового компьютера

Из всех известных направлений в развитии элементной базы квантовых компьютеров наиболее привлекательными с точки зрения создания суперкомпьютеров в настоящее время представляются следующие [1]:

- полупроводниковые ЯМР-квантовые компьютеры,
- квантовые компьютеры на переходах Джозефсона,
- квантовые компьютеры на квантовых точках.

Указанные перспективные направления конструирования квантового компьютера допускают произвольно большое число кубитов и для них существует множество наработанных приёмов микро- и нанотехнологий создания полупроводниковых и сверхпроводниковых интегральных схем.

Наиболее важными преимуществами обладает твердотельный ЯМР-квантовый компьютер. Основные из них следующие [1]:

- ядерные спины сами по себе являются кубитами;
- при низких температурах они характеризуются очень большими временами релаксации (и, соответственно, временами декогерентизации) по сравнению с электронными спинами;
- технологические структуры нанометрового масштаба в полупроводниковых квантовых ЯМР-компьютерах предназначаются не для создания самих кубитов, как в случае сверхпроводниковых устройств, а лишь для задач управления кубитами и измерения их состояний.

В настоящее время состояние современной высокоточной технологии и технологии высокочистых материалов уже сейчас позволяют экспериментально создавать простейшие варианты квантовых компьютеров. Создание же многокубитовых образцов пока находится в далёкой перспективе. Для преодоления существующих трудностей физической реализации квантового суперкомпьютера потребуются привлечение технологических и схемотехнических достижений современной микро- и нанoeлектроники, а также разработка программ математического моделирования физических процессов, и в частности процессов декогерентизации в многокубитовых квантовых системах [1].

4. Общие требования к элементной базе квантового компьютера

Считается, что для реализации полномасштабного квантового компьютера, превосходящего по производительности любой классический компьютер, на каких бы физических принципах он не работал, необходимо выполнение следующих основных требований [1]. Квантовый компьютер должен:

1. Содержать более 10^3 хорошо различаемых кубитов;
2. Обеспечить условия для приведения входного регистра в исходное основное базисное состояние, т. е. возможность процесса инициализации;
3. Обеспечить максимальное подавление эффектов декогерентизации квантовых состояний, обусловленных взаимодействием системы кубитов с окружающей средой, что приводит к разрушению суперпозиций квантовых состояний и может сделать невозможной выполнение квантовых алгоритмов. Время декогерентизации должно существенно превышать (более чем в 10^4 раз) время выполнения основных квантовых операций (времени такта). Для этого система кубитов должна быть достаточно слабо связана с окружением;
4. Обеспечить выполнение за время такта требуемой совокупности квантовых логических операций, определяющей унитарное преобразование [3, 4];
5. Обеспечить с достаточно высокой надёжностью измерение состояния квантовой системы на выходе. Проблема измерения конечного квантового состояния является одной из основных проблем квантовых вычислений.

5. Методы построения симуляторов квантового компьютера

Помимо технологической сложности устройства квантового компьютера перед разработчиками стоит также проблема, заключающаяся в невозможности просчитать поведение квантовой системы при помощи классических компьютеров. Для решения этой проблемы строятся модели квантовых вычислителей [2].

При моделировании статистики системы обычно используется матричное представление операторов и векторов квантовых состояний. Для реализации таких моделей чаще всего используются языки высокого уровня (Delphi, C++) и квантовые подключаемые библиотеки, например QDD [10]. Также создаются специальные языки программного описания квантовых процессов, такие как QASM — квантовый ассемблер, созданный как простое средство описания действия квантовых цепочек, состоящих из кубитов и однокубитных вентилях, или Qgol [9]. Существуют подключаемые библиотеки для классических моделирующих программ типа Matlab и Maple [11], которые содержат набор интуитивно понятных квантовых операторов.

Ещё одним направлением является использование стандартных языков аппаратного описания (*HDL) за их возможность компактно раскрыть структурную и функциональную составляющие архитектуры систем [2]. Здесь же предложена технология ухода от необходимости дополнительно описывать квантовую сцепленность кубитов. Для снижения временных затрат и необходимого объёма памяти при моделировании применяется методика QuIDD, которая рассматривает новый класс матриц и векторов, специально разработанных и используемых для описания состояний и поведения квантовых информационных систем [2].

Заключение

Появление полноценных квантовых компьютеров даст мощный толчок не только развитию вычислительной техники, но и техники передачи информации, организации принципиально новых систем связи типа квантового Интернета и может оказаться началом развития новых, пока ещё неизвестных областей науки и техники. Кроме того, исключительные возможности квантовых суперкомпьютеров, несомненно, будут способствовать более глубокому пониманию физических законов.

ЛИТЕРАТУРА

1. Валиев К. А., Кокин А. А. Квантовые компьютеры: надежды и реальность. Ижевск: РХД, 2001. 352 с.
2. Гузик В. Ф., Гушанский С. М. Методы построения симуляторов квантового компьютера // Изв. ТРТУ. 2006. Т. 64. № 9–1. С. 92.

-
3. Гуц А. К. Основы квантовой кибернетики: учеб. пособие. Омск: КАН, 2008. 204 с.
 4. Дуприй С. А., Калашников В. В., Маслов Е. А. Квантовая информация, кубиты и квантовые алгоритмы. 2005. URL: homepages.spa.umn.edu/~duplij/publications/Duplij_vest_sd-kal-mas.pdf (дата обращения: 30.03.2010).
 5. Ежов А. А. Некоторые проблемы квантовой нейротехнологии // Научная сессия МИФИ–2003. V Всероссийская научно-техническая конференция «Нейроинформатика–2003»: лекции по нейроинформатике. Часть 2. М.: МИФИ, 2003. С. 3–79.
 6. Китаев А., Шень А., Вялый М. Классические и квантовые вычисления. М.: МЦНМО, ЧеРо, 1999. 192 с.
 7. Кокин А. А. Твердотельные ядерные магнито-резонансные (ЯМР) ансамблевые квантовые компьютеры (исследования физических основ и проблем реализации): дис. . . . д-ра физ.-мат. наук. М., 2003. 187 с.
 8. Ожигов Ю. И. Квантовые вычисления / ВМиК. М.: МГУ, 2003. 104 с.
 9. Baker G. Qgol. A system for simulating quantum computations: Theory, Implementation and Insights. 1996. 62 p. URL: <http://ifost.org.au/~gregb/q-gol/index.html> (дата обращения: 30.03.2010).
 10. Greve D. QDD: A quantum computer emulation library. URL: <http://thegreves.com/david/QDD/qdd.html> (дата обращения: 30.03.2010).
 11. OpenQUACS — Open-source Quantum Computer Simulation. URL: <http://userpages.umbc.edu/~gcmccub1/quacs/quacs.html> (дата обращения: 30.03.2010).