О. Н. ГРАНИЧИН, С. Л. МОЛОДЦОВ

СОЗДАНИЕ ГИБРИДНЫХ СВЕРХБЫСТРЫХ КОМПЬЮТЕРОВ И СИСТЕМНОЕ ПРОГРАММИРОВАНИЕ

Санкт-Петербург
2 0 0 6

УДК 519.712
ББК 32.973.3
Г77

Р е ц е н з е н т ы: д-р техн. наук *С. Н. Турусов*
(Комитет по науке и высшей школе Правительства СПб)
д-р физ.–мат. наук *П. С. Щербаков*
(Институт проблем управления РАН)

Граничин О. Н., Молодцов С. Л.

Г 77 **Создание гибридных сверхбыстрых компьютеров и системное программирование.** — СПб., 2006. — 108 с.

ISBN 5-288-03919-4

В книге дается описание некоторых физических основ развития и миниатюризации вычислительных устройств вместе с теоретическими принципами работы квантовых компьютеров. Кроме того, приводится возможный вариант обобщения концепции классической схемы машины Тьюринга. В новой концепции переосмысливаются традиционные понятия “лента” и “ячейка памяти”. В частности, считается, что “ячейка памяти” представляет собой постоянно функционирующую модель некой динамической системы. “Естественная” эволюция ячеек в некоторые моменты времени прерывается программой (происходят “скачки”).

Книга предназначена для специалистов, занимающихся разработками в области создания новой вычислительной техники, а также для студентов старших курсов и аспирантов, обучающихся на кафедре системного программирования СПбГУ по курсу “Квантовые компьютеры”.

Библиогр. 71 назв.

ББК 32.973.3

ISBN 5-288-03919-4

© О. Н. Граничин,
С. Л. Молодцов, 2006

Оглавление

1 Введение 5

1 Создание новой элементной базы СВУ 9
1.1 Миниатюризация элементной базы 9
1.2 Математическая модель квантового компьютера 12
1.3 Основные направления экспериментальных исследований 16
1.4 Гибридные металло-биологические наноструктуры 21
1.5 Гибридные металло-биологические вычислительные устройства . 30
1.5.1 Основа работы 30
1.5.2 Формирование квантового регистра 31
1.5.3 Операции с квантовым регистром 33
1.5.4 Функциализация биологических элементов 36

2 Программирование гибридных СВУ 37
2.1 Вычислимость и вычислимый объект 37
2.2 Разработка теоретических принципов работы новых гибридных вычислительных устройств 43
2.2.1 Описания процесса работы ВУ как гибридной системы . . 44
2.2.2 Разработка модели макета ВУ нового типа 45
2.2.3 Разработка языка и архитектуры СВУ нового типа 47
2.3 Концепция обобщенной машины Тьюринга 50

3 Квантовые вычисления 53
3.1 Примеры квантовых алгоритмов 53
3.1.1 Задача Дойча 53
3.1.2 Задача Бернштейна-Вазирани 57
3.1.3 Задача Саймона 58
3.1.4 Поиск в квантовой базе данных 60
3.1.5 Периодичность, квантовое преобразование Фурье 66
3.2 Решение диофантовых уравнений 75
3.2.1 Квантовый гармонический осциллятор 76
3.2.2 Квантовые адиабатические вычисления 79
3.3 Минимизация функционала среднего риска 94
3.3.1 Процедура Кифера–Вольфовица 95

3.3.2 Рандомизированные алгоритмы стохастической аппроксимации 97
3.3.3 Квантовый компьютер и вычисление оценки вектора-градиента функции 100

4 Заключение 102

5 УКАЗАТЕЛЬ ЛИТЕРАТУРЫ 103

Глава 1

ВВЕДЕНИЕ

В настоящее время существующие вычислительные устройства не позволяют быстро и эффективно решать ряд сложных многомерных задач, связанных с быстроизменяющимися динамическими процессами, имеющими большое экономическое, государственное и оборонное значение (распознавание изображений и речи, поиск целей, динамика иерархий структур в живых системах, кластеризация в потоках концентрированных дисперсных смесей, образование многомасштабных вихревых структур в турбулентных течениях жидкости и пластических течениях твердых материалов при импульсном нагружении (ударе) и т. п.).

Основная цель этой книги — описать возможные физические и теоретические принципы создания принципиально нового сверхбыстрого гибридного вычислительного устройства (СВУ), основу которого составляли бы упорядоченные гибридные наноэлементы, включающие компоненты со сложной молекулярной структурой — металлизированные сверхрешетки квантовых точек с участием белков (протеинов), ДНК, РНК и других биологических макромолекул. Практическая реализация таких СВУ могла бы дать эффективные решения для некоторых из перечисленных выше задач.

В 1936 г. английским математиком А. Тьюрингом [65] в качестве математической модели для описания алгоритмов было предложено абстрактное вычислительное устройство, которое впоследствии было названо машина Тьюринга (МТ).

Первоначально концепция МТ развивалась с целью ответа на вопрос: можно ли для любого математического утверждения указать конечную последовательность инструкций, которые могли бы выполняться механически одна за другой человеком или вычислительным устройством, и в итоге выяснить, истинно это утверждение или ложно. При этом машина Тьюринга — дискретные вычислительное устройство, изменяющее свои характеристики в определенные моменты времени. Хотя и доказано, что поставленная проблема в общем случае неразрешима, применение машины Тьюринга вышло далеко за пределы первоначальной постановки задачи. По существу, именно работы Тьюринга положили начало математической теории вычислений. Машина Тьюринга сыграла и продолжает играть важную роль в теории информатики, а вычислимость при помощи МТ стала признанным определением процедуры.

В том же самом 1936 г. А. Черчем [28] была высказана гипотеза, что любой процесс, который естественным образом мог бы быть назван процедурой, реализуем машиной Тьюринга. Впоследствии эту гипотезу стали называть тезисом Черча-Тьюринга [11, 30]. Более точно тезис Черча-Тьюринга обычно формулируют так:

• любое эффективное вычисление может быть проведено с помощью МТ.

Традиционно понятие эффективного или механического метода (М) в логике и математике означает одно из следующих утверждений:

◇ М — конечный набор точных правил, каждое из которых выражается конечным набором символов;

◇ будучи выполненным без ошибок, М дает желаемый результат за конечное число шагов;

◇ М может быть, в принципе, выполнен человеком без использования вычислительного устройства;

◇ М не требует от человека, его выполняющего, никакой

интуиции или изобретательности.

Физическая формулировка принципа Черча-Тьюринга:

• любая конечно реализуемая физическая система может быть достаточно точно смоделирована с помощью универсальной модели компьютера, оперирующего конечными средствами.

На практике этот набор конечных средств сводится, как правило, к множеству двоичных символов {0,1}, а конечная реализуемость оказывается эквивалентной конечному числу тактов (моментов переключений).

Одним из основных понятий дискретной схемы машины Тьюринга является "такт". Его глубоко противоречивый смысл был замечен еще древними греками. Одна из возможных эквивалентных его формулировок представляет собой знаменитый парадокс Зенона об Ахиллесе и черепахе. В рамках классической теории множеств он выступает в качестве неразрешимости проблемы континуума в рамках аксиоматики Френкеля–Цермело. По мнению современных толкователей, Зенон, на самом деле, стремился доказать, что "логика и здравый смысл несовместимы" и что строгие логические умозаключения неприменимы в реальной жизни.

Одним из вариантов расширения тезиса Черча-Тьюринга является введение нового понятия вычислительного устройства, в котором вычисления строятся не на традиционных алгоритмах, а на моделях. Такой подход уже использовался в [9], опираясь на модели параллельных высокоэффективных вычислений. Следующий естественный шаг — обобщение на модели динамических систем.

В книге излагается новая абстрактная концепция вычислительного устройства, предложенная и обоснованная в [2, 3, 7]. Новая концепция принципиально отличается от классической включением "непрерывности" эволюции и переосмыслением понятий "лента" и "ячейка памяти". Если в классическом подходе ячейки памяти используются для хранения дискретной

информации и их изменение возможно только в тех случаях, когда указатель ленты показывает на нее, то в новой концепции “ячейка памяти” представляет собой постоянно функционирующую модель некой, вполне возможно, достаточно сложной динамической системы, а “лента” — некоторый “мостик” для задания или переопределения параметров эволюции состояния “ячейки”. Очевидно, что классическая ячейка памяти для хранения “бита” является частным случаем такого обобщения.

При написании книги С. Л. Молодцовым были составлены пункты 1.3–1.5, а остальной текст — О. Н. Граничиным. При этом пункт 2.1 составлен по работам И. А. Жувикиной, пункт 3.1 является кратким конспектом шестой главы лекций Дж. Прескилла [56], а пункт 3.2 написан по результатам дипломной работы А. А. Макарова [10], опиравшейся на статьи Т. Д. Кью [44].

Книга издана при финансовой поддержке целевой программы “Исследования и разработки по приоритетным направлениям развития науки и техники” на 2002-2006 годы, государственный контракт №02.442.11.7300.

Глава 1

Создание новой элементной базы СВУ

1.1. Миниатюризация элементной базы

Размеры вычислительных устройств постоянно уменьшаются. Когда-то предполагалось, что более мощные машины будут требовать больше места для периферийных устройств, памяти и т. д. Это предположение оказалось неверным. В 1965 г. Г. Мур [51] сформулировал действующее и сейчас правило (позже названное законом Мура), согласно которому производительность вычислительных систем удваивается каждые восемнадцать месяцев. Г. Мур вывел свой эмпирический закон, построив зависимость числа транзисторов в интегральной микросхеме от времени. Как следствие из этого закона можно вывести темпы миниатюризации отдельного транзистора.

Сейчас в мире построено несколько заводов, производящих

микросхемы с линейными размерами менее 0,1 мкм [=100 нм= 1000 Ангстрем (Å), 1Å$\sim$ размер атома водорода]. Корпорация Intel объявила о готовности в ближайшем будущем перейти к технологиям 0,06 мкм.

Таким образом развитие цифровых электронных технологий приводит к тому, что размер элементарного вычислительного устройства приближается к размеру молекулы или даже атома. На таком уровне законы классической физики перестают работать и начинают действовать квантовые законы, которые для многих важных динамических задач еще не описаны теоретически. Р. Фейнман [36] обосновал невозможность представления результатов квантовой механики на классическом универсальном вычислительном устройстве даже с использованием вероятностных алгоритмов. Это связано с тем, что число элементарных операций такого вычислительного устройства будет расти экспоненциально с ростом числа степеней свободы системы. Именно поэтому для точного моделирования квантовых систем Фейнман предложил теоретическую модель квантового компьютера и обосновал ее "экспоненциальное" преимущество над классической. Д. Дойч [31] построил модель такого универсального компьютера, основанную на идее квантовых вычислений, и показал, как квантовый компьютер может моделировать физические системы, которые находятся за пределами области, доступной универсальной МТ. Модель Дойча представляет собой новый подход к проблеме создания современных вычислительных устройств, но, по своей сути, она остается дискретной.

Стремление к увеличению быстродействия вычислительных устройств и уменьшению их геометрических размеров с неизбежностью приводит к необходимости рассмотрения операций с переходными процессами. Вместо примитивных операций с классическими битами в будущем было бы естественно перейти к операциям, задаваемым теми или иными динамическими моделями микромира. Под примитивной "моде-

лью" вычислений можно, в частности, понимать и выполнение классических операций с битами. Конечно же введение более широкого класса примитивных моделей было бы более обоснованным, если бы удалось для функции, значения которой записаны в регистре квантовых битов, определить операцию, эффективно выполняющую, например, преобразование Фурье. Причем может оказаться реальным предположение о том, что время на ее выполнение будет вполне соизмеримым с временем выполнения одной классической операции, так как операции типа "свертки" функций вполне могут быть обнаружены "в природе". Последние исследования похожих моделей показывают, что их выполнение за счет присущей природе способности к самоорганизации не обязательно "раскладывается" на более простые составляющие, т. е. не всегда может быть записано в виде классического алгоритма.

В некотором смысле переход к разработке и созданию моделей сложных вычислений — закономерный этап развития микропрограммирования. Понимание возможных преимуществ работы устройств с эффективным микрокодом отмечалось еще в 50-е гг. прошлого века. Во втором ряду серии ЕС ЭВМ в конструкцию была заложена возможность динамического микропрограммирования. Хорошо известен целый ряд ЭВМ от "Мир-1" до "Эльбрус", использующих языки высокого уровня (HLL) как машинные. На кафедре системного программирования СПбГУ широко известен стал компьютер "САМСОН", при создании которого удалось разработать эффективную технологию микропрограммирования [13, 64]. В настоящее время *технологии микропрограммирования естественным образом сдвигаются в сторону физических процессов.*

1.2. Математическая модель квантового компьютера

В качестве нового поколения вычислительных устройств, как правило, рассматриваются, так называемые, квантовые компьютеры, использующие квантомеханические алгоритмы решения задач.

Опишем кратко математическую модель квантового компьютера. Состояния в квантовой механике часто обозначают как вектора единичной длины в гильбертовом пространстве над полем комплексных чисел. Наблюдаемые представляются как самосопряженные операторы в рассматриваемом гильбертовом пространстве. Наблюдаемая — это способ получения информации о состоянии. Измерение квантовой системы изменяет ее. В результате измерения исследователь получает одно из собственных чисел оператора наблюдаемой, а сама система переходит в состояние, соответствующее этому собственному числу. Реализация того или иного собственного числа при измерении происходит случайно, с вероятностью, равной квадрату проекции изучаемого состояния на соответствующий собственный вектор. Измерение квантовой системы дает нам полную информацию о ней только в том случае, когда ее состояние совпадает с одним из собственных векторов выбранной наблюдаемой.

Квантовый компьютер обрабатывает “кубиты” (“квантовые биты”), представляющие собой квантовую систему двух состояний (микроскопическая система, соответствующая описанию, например, возбужденного иона или поляризованного фотона, или спина ядра атома, или магнитного момента кластера атомов). Базис пространства состояний кубита обычно обозначается как $|0\rangle$ и $|1\rangle$ (Рис. 1.1, [63]), по аналогии с $\{0, 1\}$ в классической теории информации. Такая система может принимать не только базисные состояния и, следовательно, способна хранить больше информации, нежели соответствующая

Рис. 1.1: Классический и квантовый биты [63].

классическая:

$$W = \sum_s \Psi_s |s\rangle.$$

Состояние W называется суперпозицией векторов $|s\rangle$,

$$\Psi_s \in \mathbb{C},\ \sum_s |\Psi_s|^2 = 1,$$

$|\Psi_s|$ — вероятностными амплитудами.

Тем не менее при измерении такой системы она переходит в одно из базисных состояний (в случае правильно выбранной наблюдаемой), и информация, хранимая в ней, будет соответствовать некоторой классической информации.

Регистр квантовых битов, являющийся квантовой системой из нескольких, например, n кубитов, математически представляется как их тензорное произведение. Набор базисных векторов пространства состояний такого регистра квантовых битов можно параметризовать строками битов длины n. Например, при $n = 3$ для базисного вектора $|0\rangle \otimes |0\rangle \otimes |0\rangle$ можно использовать обозначение $|000\rangle$. Иногда для удобства используются и другие формы записи: $|0\rangle|0\rangle|0\rangle$ или $|00\rangle|0\rangle$. Таким образом размерность пространства состояний, с которым оперирует квантовый компьютер, растет экспоненциально с ростом числа кубитов. Это свойство лежит в основе феномена квантового параллелизма. С экспериментальной точки зрения для достижения этого эффекта при создании квантовых

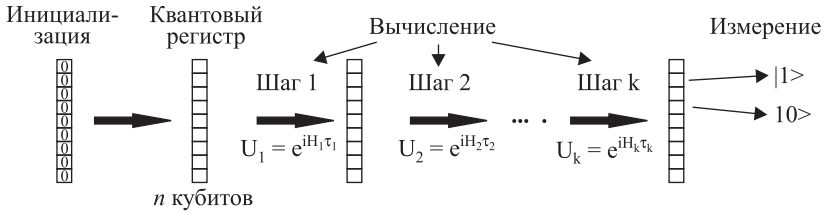


Рис. 1.2: Процесс квантового преобразования информации.

регистров необходимо обеспечить когерентность корреляций между отдельными квантовыми битами. Достаточно строгие и более подробные обоснования математической модели квантовых вычислений можно найти, например, в [17, 63, 56].

При проектировании вычислительных устройств регистр квантовых битов целесообразно рассматривать как единое целое (а не набор изолированных битов) по двум причинам:

• во-первых, сокращение длины такта и расстояний между битами с определенного уровня делает невозможным рассматривать их изолированно в силу законов квантовой механики;

• во-вторых, отказ от "скалярных битов" позволяет говорить о принципиальной возможности выполнения многомерных (векторных) операций за один "такт" (Рис. 1.2, [63]). Например, П. Шор [59] (см. п. 3.1.5) предложил алгоритм квантового преобразования Фурье, которое может выполняться за время пропорциональное $(\log_2 N)^2$, а не за $N \log_2 N$ как классическое быстрое преобразование Фурье. В [10] (см. п. 3.2.2) обсуждается опирающийся на квантовую адиабатическую теорему гипотетически возможный "физический" способ решения за конечное время 10-ой проблемы Гильберта, неразрешимость которой на классической МТ была показана Ю.В. Матиясевичем в 1970 г. [12]. В работе [6] (см. п. 3.3.3) предложен эффективный квантовый алгоритм вычисления "за такт" оценки вектора-градиента многомерной функции.

Еще одним важным свойством квантовых состояний явля-

ется то, что их эволюция должна быть унитарной. Иными словами, любое преобразование кубитов в квантовом компьютере является унитарным оператором в соответствующем гильбертовом комплексном пространстве. Отсюда следует, что все преобразования информации (кроме измерения) в квантовом компьютере должны быть обратимы.

Для реального применения основных квантовых алгоритмов, описанных далее в третье главе, необходимо порядка 1000 или более квантовых битов. До настоящего времени, однако, практическая реализация квантового регистра подобной емкости остается нерешенной. Увеличение количества квантовых битов приводит к серьезным проблемам адресации каждого конкретного элементарного носителя информации.

На наш взгляд, серьезные проблемы возникают у создателей новых вычислительных устройств и из-за попыток построить модель квантовых вычислений по прямой аналогии с классическими. Следуя логике развития классической цифровой вычислительной техники, в настоящее время в обычно рассматриваемой модели квантовых вычислений предполагается возможность выделения простой базовой вычислительной структуры (чаще всего системы из двух кубитов), которая рассматривается как элемент (некий “кирпичик”) для строительства любого более сложного устройства. Основной недостаток такой модели организации вычислений заключается в чрезмерном увеличении сложности получающейся системы за счет необходимости использования средств автоматической корректировки ошибок, которые могут возникнуть при каждом элементарном преобразовании информации. Эти трудности конкретной модели представления квантовых вычислений часто приводят к дискредитации общей идеи о возможной эффективности использования квантовых компьютеров в будущем.

1.3. Основные направления экспериментальных исследований

Задача создания элементной базы принципиально нового поколения вычислительных устройств, способных быстро и эффективно решать перечисленные во введении трудные проблемы, до настоящего времени остается нерешенной, хотя в этой области работает большое количество исследовательских лабораторий, специализирующихся в основном в сфере использования неорганических материалов. В значительной степени причина неудач заключается в использовании слишком простых базовых структур, отвечающих требованиям традиционной машины Тьюринга и неадекватных уровню сложности современных нерешенных задач.

В мировой практике рассматриваются несколько возможных основных направлений создания элементной базы СВУ нового поколения, компьютеры, работающие:

— на принципе ядерного магнитного резонанса в жидкостной молекулярной фазе (“Liquid state molecular NMR quantum computer”) [66],

— на атомных ионах, помещенных в ловушки Пауля (Paul) или Пеннинга (Penning) (“Ion trap quantum computer”) [29],

— с использованием ядерного магнитного резонанса или электронного парамагнитного резонанса в твердом теле (“Solid state NMR/EPR quantum computer”) [46],

— с использованием явления сверхпроводимости (“Superconducting systems”) [50],

— на квантовых точках в полупроводниковых неорганических системах (“Quantum dot computer”) [23, 53],

— на основе оптической симуляции квантовой логики (“Optical computer”) [27],

— или на металло-биологической гибридной основе (“Hybrid quantum computer”) [61, 67, 68].

Перечислим ведущие организации, *основных исследовате-*

лей и направления исследований по всем указанным выше принципам:

◇ IBM/MIT/Berkeley/Stanford, *Isaac Chuang (IBM), Neil Gershenfeld (MIT)*, разработка технологий для NMR компьютеров; количество квантовых битов до 10-40;

◇ Harvard/MIT/Los Alamos, *David Cory (Harvard)*, квантовые алгоритмы и NMR компьютеры;

◇ NIST, *Christopher R. Monroe*, Ion-trap квантовые компьютеры; создан прототип устройства с двумя квантовыми битами, работающий на основе ионов бария;

◇ Caltech/MIT/USC, *Seth Lloyd (MIT), M. Despain (USC), H. Jeff Kimble, John Preskill, and Steven Koonin (Caltech)*, квантовые алгоритмы и коррекция квантовых ошибок;

◇ Oxford University, *David Deutsch, Jonathan Jones*, Ion-trap и NMR реализации компьютеров; теория квантовой информации;

◇ Lucent Technologies, *Lov Grover*, исследование параметров работы квантовых компьютеров различных типов;

◇ Michigan State University/Bell Laboratories, *Mark Dykman (MSU), Phil M. Platzman (BL)*, исследования в области движения электронов на поверхности гелия;

◇ IBM, *David P. DiVincenzo*, квантовые расчеты с использованием квантовых точек;

◇ U. California at Santa Barbara, *Mark Sherwin, David D. Awschalom*, квантовые расчеты с использованием квантовых точек;

◇ CREST-JST, Keo University, Japan, *Kohei M. Itoh*, квантовые проволоки (Si^{29} на ступенчатом Si^{28}), NMR компьютеры;

◇ U. de los Andes, Colombia/U. Oxford, UK, *Luis Quiroga (U. de los Andes), Neil F. Johnson (U. Oxford)*, экситоны в когерентных квантовых точках;

◇ NEC, Tsukuba, Japan, *Y. Nakamura, J. S. Tsai, Yu. A. Pashkin*, квантовые компьютеры на куперовских парах (сверхпроводящие системы);

◇ Rutgers U./ETH, Zurich/Landau Institute, Moscow, *Lev B. Ioffe, Vadim B. Geshkenbein, Mikhail V. Feigelman, Alban L. Fauchere, Gianni Blatter*, квантовые компьютеры на переходах Джосефсона (Josephson junctions);

◇ University of Barcelona/Xerox, Spain, *Javier Tejada Palacios, Ron Ziolo*, молекулярные магниты;

◇ U. Geneva, Switzerland/Hewlett Packard Labs, UK, *Nicolas Gisin (Geneva), Sandu Popescu (HP)*, спиновые переходы и квантовая информация для антипараллельных спинов;

◇ U. Vienna, AT, *Anton Zeilinger*, эксперименты в области основ квантовой механики;

◇ MagiQ Technologies, *Hoi-Kwong Lo*, исследования и разработки по использованию технологий квантовой информации; квантовые алгоритмы; масштаб до 10-40 квантовых битов;

◇ Los Alamos, *P. G. Kwiat*, симуляция оптических компьютеров;

◇ U. of Technology Dresden/MBZ of Biomaterials Dresden, *Serguei Molodtsov (UTD), Michael Mertig (MBZ)*, квантовые точки в биологических наноструктурах;

◇ U. of Technology Dresden/U. of Technology Berlin, *Serguei Molodtsov (UTD), Mario Dahne (UTB)*, квантовые проволоки.

Многие из рассмотренных направлений имеет существенные недостатки, которые в некоторых случаях приводят к принципиальной невозможности создания конкурентоспособного вычислительного устройства.

Характерным примером являются устройства, работающие на принципе ядерного магнитного резонанса в жидкостной молекулярной фазе [66]. Корпорация IBM только на первый этап разработки молекулярной элементной базы новых СВУ - создание макета, реализующего алгоритм П. Шора [59], основанный на квантовом преобразовании Фурье, выделила в 1999 г. 17 млрд USD на 5 лет. В результате был создан NMR макет, оперирующий с 5 или 7 квантовыми битами и весом около 7 тонн, способный решать только примитивные задачи

типа факторизации двухзначных чисел.

Компьютеры на атомных ионах, помещенных в ловушки Пауля или Пеннинга, подвержены сильному влиянию паразитных полей, которые могут приводить, например, к нагреванию ионов. С увеличением числа ионов в ловушке возникают проблемы, связанные с ограничением частоты или разогревом системы, поэтому представляется маловероятным, что каждая отдельная ловушка будет способна надежно работать с достаточным числом (порядка 1000) ионов.

Твердотельные системы, работающие на основе магнитных резонансов, являясь естественным развитием жидкофазных систем, обладают очевидными недостатком последних — трудностью имплементации устройств с более чем 100 квантовыми битами.

Компьютеры, использующие явление сверхпроводимости, требуют для проведения вычислений экстремально низких рабочих температур.

Оптические реализации сталкиваются с проблемой индивидуальной адресации носителей информации — фотонов.

В настоящее время наиболее перспективным направлением разработки элементной базы компьютеров нового поколения представляется использование самоорганизующихся квантовых точек в твердотельных системах, которые могут выполнять функции квантовых битов и быть связанными в квантовый регистр на основе, например, электростатического или магнитного типа взаимодействия. Инициированная основополагающими работами в этом направлении, выполненными под руководством академика Ж. И. Алферова (лауреат Нобелевской премии в области физики полупроводников), процедура приготовления квантовых точек в полупроводниковых неорганических системах известна и всесторонне изучена. Однако, прямое применение этих ведущихся разработок для изготовления элементов квантовых компьютеров представляется по ряду причин проблематичным. Так, для надежной рабо-

ты квантовых устройств необходима высокая степень квантовой когерентности отдельных квантовых битов, которая может быть обеспечено только в идеально упорядоченной системе (сверхрешетке) квантовых точек строго одинакового размера. Воспроизводимое приготовление подобных систем, содержащих 1000 и более квантовых точек, в рамках существующих методик является в высшей степени затруднительной задачей. Нерешенной проблемой является также обеспечение возможности индивидуальной адресации каждой квантовой точки (квантового бита) как это необходимо для работы квантового вычислительного устройства.

Предварительные исследования, проведенные С. Л. Молодцовым с коллегами (см. [67, 68]), в развитии направления применения твердотельных упорядоченных систем квантовых точек для создания нового поколения вычислительных устройств, показали, что решающим элементом успеха может оказаться использование высокоупорядоченных биологических (бактериальных) масок, позволяющих приготавливать упорядоченные сверхрешетки магнитных монодисперсных кластеров контролируемых размеров со строго определенными межкластерными расстояниями. Предполагается, что применение биологических компонент, пространственно связывающих отдельные квантовые точки (сами бактериальные маски или, например, нити ДНК), позволит обеспечить необходимую индивидуальную адресацию квантовых битов квантового регистра. Сочетание неорганических и специальным образом синтезированных биологических элементов заданной структуры, несущих собственную функциональную нагрузку (гибридный характер элементной базы), может принципиально расширить возможности новых гибридных вычислительных устройств по сравнению с традиционно рассматриваемыми квантовыми компьютерами.

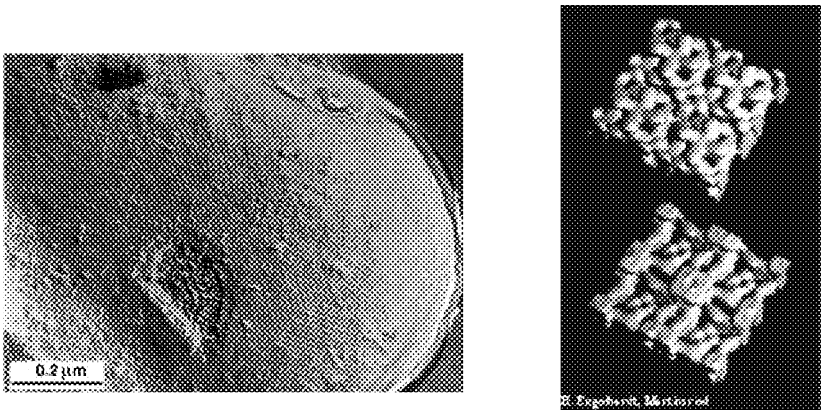


Рис. 1.3: (слева) Изображение *S layer* бактерий *Sporosarcina ureae*, полученное TEM [33]; (справа) Трехмерная реконструкция TEM результатов [34], вид *S layer* сверху и снизу. Видна элементарная ячейка с симметрией $p4$, состоящая из отдельных протеинов (мономеров) и структура упорядоченных пор между протеинами.

1.4. Гибридные металло-биологические наноструктуры

Одному из авторов книги, С. Л. Молодцову, совместно с другими экспериментаторами (см. [67, 68]) удалось разработать методику выращивания сверхрешеток гибридных биологических наноструктур на основе кластеров (квантовых точек) магнитных металлов, внедренных в упорядоченные матрицы протеинов, входящих в состав различных культур бактерий, с характерными размерами порядка 10 нм (=0,01 мкм= 100Å). Такие магнитные квантовые точки могут рассматриваться как квантовые биты квантовых компьютеров. При этом можно говорить о возможности создания устройств с характерными линейными размерами в пять-десять раз меньше существующих и содержащих несколько тысяч квантовых битов

в одном регистре. Принципиально новые возможности связаны с тем, что квантовые точки соединяются протеинами, которые можно функциализировать в зависимости от конкретных задач вычислительного процесса. В качестве функциализированных элементов вместо протеинов могут быть использованы ДНК (или металлизированные ДНК).

Обычно культуры бактерий покрыты поверхностным слоем протеинов (*"bacterial surface layer"* или *"S layer"*, Рис. 1.3) [60], который предохраняет бактерии от неблагоприятных внешних воздействий. *S layer* представляют собой упорядоченные двумерные протеиновые кристаллы различной точечной симметрии ($p1$, $p2$, $p3$, $p4$ и $p6$) с расстояниями между отдельными морфологически эквивалентными элементами (постоянными решетки) от 3 до 30 нанометров. Поверхностные слои протеинов имеют толщину от 5 до 15 нанометров и упорядоченную структуру сквозных отверстий (пор) диаметром от 2 до 6 нанометров, которые могут быть заполнены, например, кластерами различных металлов.

Способность к самоорганизации (упорядоченной сборке) отдельных протеиновых мономеров в двумерные массивы большой площади на поверхности гладких твердотельных подложек [55] позволяет рассматривать *S layer* в качестве идеальных масок для выращивания наноструктур (квантовых точек) с заданными физическими, электрическими или магнитными свойствами. Следует особо отметить возможность выращивания упорядоченных структур металлических кластеров с латеральными плотностями, намного превышающими структурные плотности, доступные в современных приборах микроэлектроники [47]. Мономеры поверхностного бактериального слоя протеинов были выделены из культуры бактерий *Bacillus sphaericus* NCTC 9602. Условия для культивации и очистки ячеек *S layer* описаны в работах [67, 68], а также в статьях, ссылки на которые приведенны в этих работах. В качестве подложек для приготовления опытных образ-

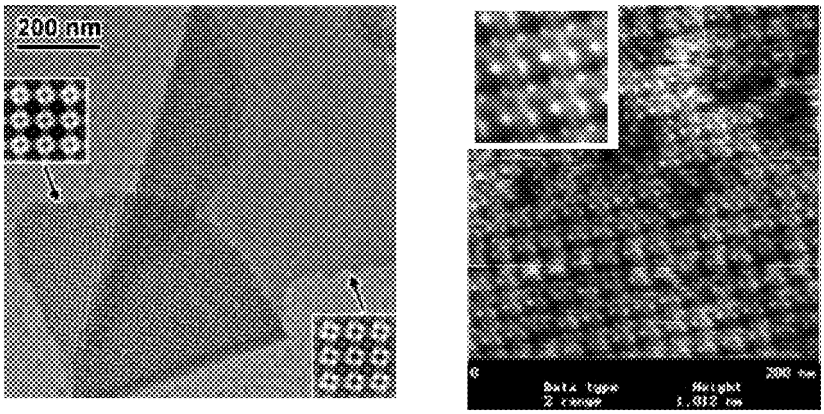


Рис. 1.4: (слева) TEM изображение отдельного монослойного листа *S layer* бактерий *Bacillus sphaericus* NCTC 9602. В нижней и левой частях рисунка лист сложен в два монослоя; (справа) AFM изображение, видны отдельные мономеры, формирующие структуру с $p4$ симметрией.

цов использовались обработанные в плазме остаточных атмосферных газов n-типа дотированные кремниевые пластинки $SiO_x/Si(100)$. Поверхностные слои протеинов наносились из капель суспензии протеиновых мономеров на предварительно подготовленную поверхность кремния. В результате процесса биологической самоорганизации в течение непродолжительного времени (порядка 30 мин.) мономеры формировали монослой поверхностных протеинов, осажденных на поверхность подложки, остаток суспензии удалялся с поверхности образца.

Полученные образцы характеризовались с помощью следующих методик:

— сканирующей электронной микроскопии (“scanning electron microscope”, SEM),

— электронной микроскопии, работающей “напросвет” (“transmission electron microscope”, TEM),

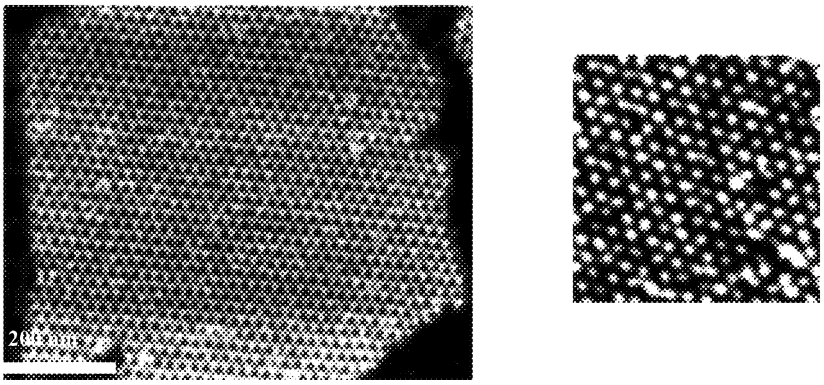


Рис. 1.5: AFM изображения (слева) листа *S layer* с нанесенными вакуумным путем кластерами Cr; (справа) та же структура после вакуумного ионного травления [52].

— и микроскопии атомных сил ("atomic force microscope", AFM).

На Рис. 1.4 приведены результаты TEM и AFM экспериментов, которые демонстрируют высокое качество полученных пленок. Размеры полученных листов протеинов и их строго упорядоченная структура позволяют говорить о возможности приготовления на их основе метало-биологических гибридных систем, содержащих несколько тысяч квантовых точек строго определенного размера. Величина кластеров, расстояние между ними, а также симметрия их взаимного расположения может варьироваться выбором определенного типа *S layer*. Гибридные кластерные наноструктуры можно приготавливать путем нанесения адсорбатов в условиях сверхвысокого вакуума или из химического раствора.

Результаты вакуумного напыления 0,6 нм Cr на поверхность *S layer*, нанесенного на кремний, показаны на Рис. 1.5 (левая часть), где хорошо виден массив нанокластеров (темные точки) упорядоченный структурой подложки. В случае необходимости более легкие атомы элементов, входящих в со-

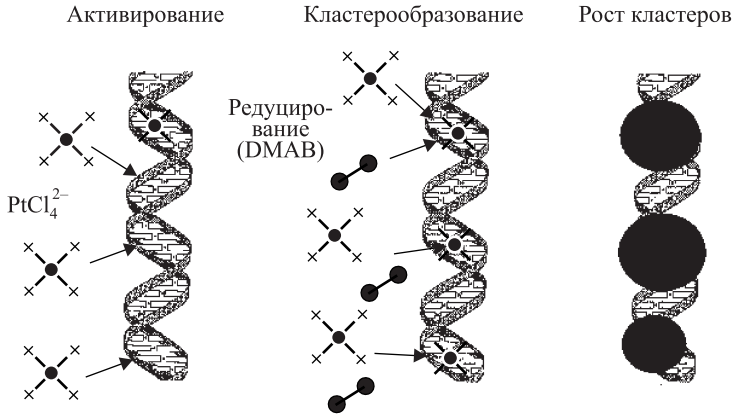


Рис. 1.6: Иллюстрация процесса приготовления образцов из химического раствора.

став протеинов, могут быть удалены с помощью высоковакуумного ионного травления. Результаты травления в атмосфере аргона показаны на правой части Рис. 1.5, где белым цветом представлены кластеры Cr.

В качестве альтернативного способа выращивания нанокластеров на биологических объектах (например, *S layer* или ДНК) можно использовать осаждение из химического раствора, которое проводится в два этапа, как это продемонстрировано на Рис. 1.6 (слева) для случая нанесения Pt на ДНК. На первом этапе (активирование) биологический объект помещается в раствор K_2PtCl_4. При этом радикалы $PtCl_4^{2-}$ оказываются связанными с определенными группами, входящими в состав ДНК. Кластерообразование достигается путем редуцирования $PtCl_4$ в растворе Dimethylaminobenzaldehyd (DMAB) или атмосфере водорода.

После того как морфология выращиваемых структур была полностью охарактеризована микроскопическими методами, исследовательской группе С. Л. Молодцова удалось провести всестороннее исследование электронной структуры образцов.

Информация об электронной структуре, прежде всего в области энергий вблизи уровня Ферми (E_F), необходима для описания электронных и транспортных свойств гибридных наноструктур, оценки возможности их использования в той или иной области наноэлектроники. Важными являются, например, такие вопросы как:

• обладают ли применяемые биологические структуры проводящими свойствами,

• являются ли образовавшиеся кластеры металлическими или наносимые металлы находятся в химической реакции с матрицей.

Как правило, электронная структура исследуется с помощью спектроскопических методик: заполненные электронные состояния — методом фотоэлектронной спектроскопии (ФЭС или "photoemission", PE), в то время как незаполненные состояния — методом спектроскопии квантового выхода вблизи порогов возбуждения внутренних уровней ("near-edge x-ray absorption fine structure", NEXAFS). Для использования NEXAFS необходимо перестраиваемое по энергии синхротронное излучение. В обоих случаях, PE и NEXAFS, облучение структур светом может приводить к деградации биологических компонент. Поэтому проведение спектроскопических исследований с биологическими образцами является очень трудной задачей.

Впервые в мировой практике методом фотоэлектронной спектроскопии группе С. Л. Молодцова удалось получить надежную информацию об электронной структуре валентной зоны биологического объекта (поверхностного слоя протеинов *Bacillus sphaericus* NCTC 9602). Фотоэмиссионные исследования были выполнены в лабораторных условиях кафедры физики поверхности и микроструктур Технического университета Дрездена и в рамках билатеральной программы "Российско-Германская лаборатория" на российско-германском канале вывода синхротронного излучения BESSY/Берлин, по-

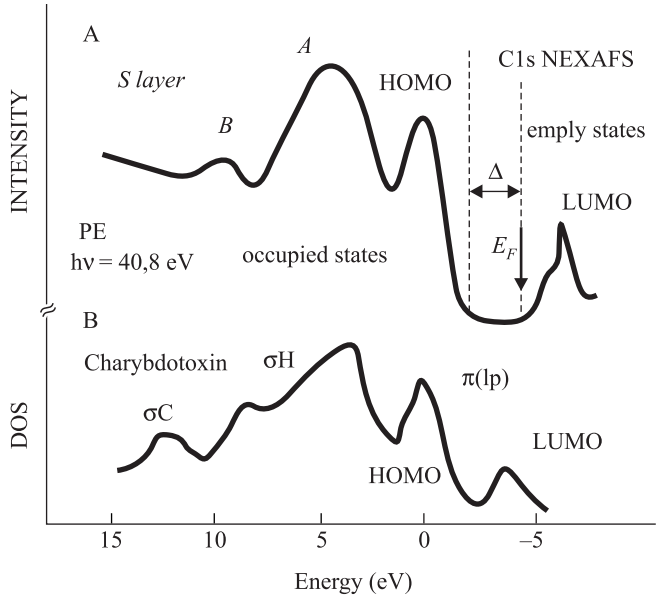


Рис. 1.7: Электронная структура заполненных (PE) и свободных (NEXAFS) состояний *S layer Bacillus sphaericus* NCTC 9602 в сравнении с результатами расчетов [41].

строенном при непосредственном участии С.-Петербургского госуниверситета. Все NEXAFS эксперименты были проведены на российско-германском канале, спроектированном специальным образом для исследования биологических образцов. Этот дипольный канал обладает сверхвысоким энергетическим разрешением (разрешающая сила - 100000 в области энергий фотонов до 100 эВ) и характеризуется оптимальной плотностью потока фотонов, чтобы не разрушать биологические объекты.

Результаты спектроскопических исследований электронной структуры поверхностного слоя протеинов *Bacillus sphaericus* NCTC 9602 [67, 68] представлены на Рис. 1.7. Видно, что *S layer* является полупроводником с шириной запрещенной зоны около 3 эВ (расстояние между "highest occupied molecular orbital", HOMO, и "lowest unoccupied molecular orbital", LUMO) и уровнем Ферми, находящимся вблизи края LUMO.

Как высоковакуумное напыление, так и нанесение металлов из раствора существенным образом не изменяют электронную структуру биологической матрицы, что свидетельствует об отсутствии химической реакции в гибридной системе. Аналогичная информация была получена при анализе фотоэлектронных спектров внутренних уровней образцов. Изменение фотоэмиссионных спектров валентной зоны *S layer Bacillus sphaericus* NCTC 9602 после активации и редуцирования показаны на Рис. 1.8. Важным результатом является появление электронных состояний на уровне Ферми после проведения редуцирования. Соответствующий сигнал подавляется при использовании фотонов с энергией вблизи куперовского минимума для $5d$ состояний Pt, что подтверждает металлические свойства выращенных кластеров. Результаты спектроскопических исследований показывают, что изучавшиеся образцы представляют собой металлические кластеры внедренные в полупроводниковую биологическую матрицу.

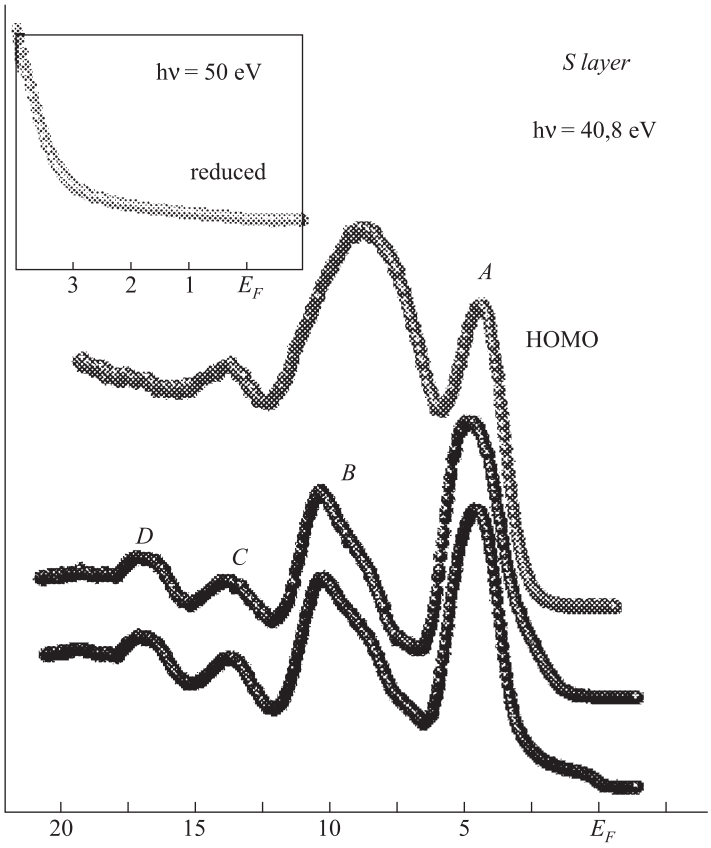


Рис. 1.8: Фотоэмиссионные спектры валентной зоны *S layer Bacillus sphaericus* NCTC 9602 до активации K_2PtCl_4 (верхний), после активации (средний) и редуцирования (нижний). Структура на уровне Ферми редуцированного образца подавляется при возбуждении фотонами с энергиями в области куперовского минимума $5d$ состояний Pt (вставка).

1.5. Гибридные металло-биологические вычислительные устройства

Как уже отмечалось в пункте 1.2 элементная база компьютеров нового поколения должна отвечать целому ряду требований. В частности, для эффективной работы количество кубитов (носителей информации) должно быть порядка или более 1000. Предварительные исследования показывают, что описанные гибридные наноструктуры могут обеспечивать необходимое количество элементарных носителей информации. Наиболее важным шагом является выбор физического явления (например, электрическое или магнитное взаимодействие), лежащего в основе работы нового вычислительного устройства. В соответствии с выбранным явлением должен быть решен вопрос обеспечения необходимых квантовых корреляций между элементарными носителями информации (квантовыми точками). Кроме того, должны быть решены технические проблемы инициализации квантового регистра, записи и считывания информации.

1.5.1. Основа работы

Окончательное решение о выборе наиболее оптимального фундаментального физического явления для работы вычислительного устройства нового поколения может быть принято после всестороннего исследования электронной структуры квантовых точек внедренных в биологические матрицы. Подобные исследования должны быть проведены спектроскопическими методами (PE и NEXAFS) со сверхвысоким энергетическим разрешением порядка 1 мэВ, равным энергетическому расстоянию между соседними электронными уровнями квантовых точек, которые могут быть использованы для имплементации взаимно ортогональных состояний квантовых битов.

Экспериментаторам удалось установить металлический ха-

рактер электронной структуры получаемых нанокластеров. Более подробная информация об отдельных электронных уровнях требует сверхвысокого энергетического разрешения (около 1 мэВ).

Необходимо провести дополнительные фотоэмиссионные исследования со сверхвысоким энергетическим разрешением электронной структуры валентной зоны кластеров различных металлов (благородных: Au, Ag, Pt, и металлов, обладающих магнитными свойствами: Fe, Co, пермаллоя), внедренных в биологические матрицы поверхностных слоев протеинов различных бактерий. Величина квантовых точек может варьироваться выбором *S layer*, обладающих разными размерами пор.

В отсутствии детальных данных об электронной структуре, полученных со сверхвысоким энергетическим разрешением, анализ зарубежного опыта позволяет сделать заключение о наиболее перспективном использовании магнитных явлений для работы вычислительных устройств нового поколения.

1.5.2. Формирование квантового регистра

Квантовый регистр может быть сформирован на основе магнитных корреляций между отдельными магнитными нанокластерами. При этом отдельные нанокластеры должны обладать магнитными моментами, то есть быть приготовленными из магнитных металлов, например: Fe, Co или пермаллоя. Эти металлы могут внедряться в протеиновые матрицы поверхностных слоев различных культур бактерий, обладающих порами разных размеров, расположенными на разном расстоянии друг от друга. Гибридные структуры могут выращиваться на подложках, обладающих проводящими (напр., Au) или изолирующими (напр., SiO_x/Si) свойствами. Предполагается, что, изменяя тип подложки, можно будет оказывать влияние на характер и силу корреляций между отдельными неорганическими кластерами. Химическое взаимодей-

ствие между всеми тремя компонентами выращиваемых гибридных наноструктур (матрицей, кластерами и подложкой) может исследоваться с помощью фотоэмиссионной спектроскопии валентной зоны и внутренних уровней (сверхвысокое энергетическое разрешение необязательно).

Магнитные свойства отдельной квантовой точки могут быть локально исследованы с помощью спин-поляризованного сканирующего туннельного микроскопа ("spin-polarized scanning tunneling microscope", STM) и микроскопа магнитных сил ("magnetic force microscope", MFM). Эксперименты должны проводиться при разных температурах, включая температуры жидкого гелия. При этом возможно варьирование размеров квантовой точки путем выбора определенной биологической матрицы.

Магнитные свойства всего ансамбля выращенных квантовых точек должны исследоваться с применением целого ряда комплиментарных экспериментальных методик. В области низких энергий электронных возбуждений — с использованием сверхпроводящих квантовых интерферометров ("superconducting quantum interference device", SQUID). В области более высоких энергий — фотоэлектронной спектроскопией со спиновым разрешением ("spin-resolved photoemission") и NEXAFS с использованием явления линейного или циркулярного магнитного дихроизма ("linear magnetic dichroism", LMD или "circular magnetic dichroism", CMD). Проведение экспериментов по исследованию электронной структуры кластеров со спиновым разрешением может быть осуществлено с помощью фотоэлектронного анализатора, оснащенного спиновым детектором.

Функционирование квантового регистра предполагает наличие определенной силы квантовых корреляций между отдельными нанокластерами. Корреляции необходимы для обеспечения квантовой когерентности кубитов в течение всего процесса вычислений. В то же время корреляции не должны быть

слишком сильными: для проведения вычислений необходимо иметь возможность быстрого изменения состояния каждого отдельного кубита (запись информации) без того, чтобы влиять на состояние остальных кубитов квантового регистра.

Силу локальных магнитных корреляции между отдельными квантовыми точками можно исследовать с помощью следующих экспериментальных методик: спин-поляризованного сканирующего туннельного микроскопа, микроскопа магнитных сил и фотоэмиссионного электронного микроскопа с использованием явления магнитного дихроизма (LMD/CMD - "photoemission electron microscope", LMD/CMD - PEEM). Фотоэлектронная спектроскопия со спиновым разрешением и эксперименты по магнитной рентгеновской дифракции могут использоваться для получения информации о степени магнитных корреляций во всем массиве магнитных нанокластеров.

1.5.3. Операции с квантовым регистром

Выбранные оптимальным образом на основании результатов вышеописанных исследований структуры нужно исследовать на предмет возможности их конкретного использования для проведения квантовых вычислений. При этом особое внимание должно быть уделено разработке процессов инициализации, записи и считывания информации.

Инициализация квантового регистра. Являясь принципиально неунитарной операцией, инициализация (приведение в устойчивое основное состояние) магнитного квантового регистра может быть осуществлена приложением достаточно сильного магнитного макрополя одновременно ко всем квантовым битам.

Запись и считывание информации. Оба процесса предполагают необходимость адресации каждого отдельного кубита. Локальная адресация теоретически возможна при использовании, например, MFM или спин-поляризованного STM приборов. Но эффективность подобной адресации ограничена ис-

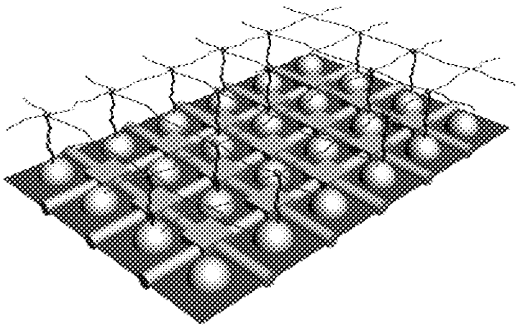


Рис. 1.9: Упорядоченная система нанокластеров ($p4$) с фиксированной на их поверхности решеткой из проводящих квантовых нанопроволок.

пользованием сложного микроскопического оборудования.

Альтернативный подход может быть основан на использовании проводящих двумерных наносеточных структур, фиксированных на поверхности упорядоченных массивов квантовых нанокластеров с четырехкратной точечной симметрией ($p4$, Рис. 1.9). При этом, по необходимости, биологическая матрица может быть оставлена или удалена ионным травлением.

Двумерная проводящая решетка, собранная из тонких проводящих квантовых нанопроволок, должна быть закреплена каждым своим узлом на одном нанокластере. Тогда каждый отдельный нанокластер может быть адресован пропусканием тока через две нанопроволоки, пересекающиеся на этом нанокластере. Адресация может осуществляться, например, соответствующим пропускаемому току магнитным полем, значение которого оказывается больше установленного порога срабатывания переключения состояния магнитного момента квантового бита. В свою очередь, проводящая нанорешетка может быть использована для считывания информации с квантового регистра, поскольку магнитное состояние нанокласте-

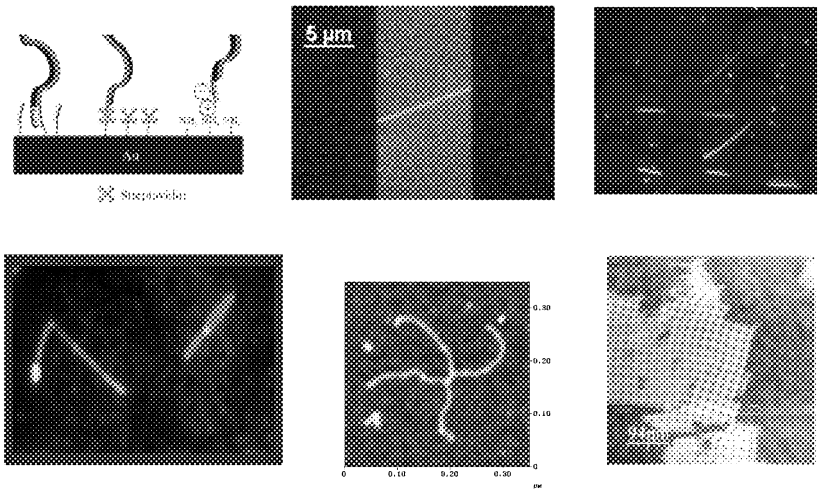


Рис. 1.10: Манипуляции с молекулами ДНК (верхний ряд слева направо): нанесение ДНК на подложку из золота; растяжка ДНК между двумя контактами; синтез структур с участием ДНК; (нижний ряд слева направо) ДНК манипуляции с молекулярными моторами; сращивание ДНК; синтез двумерных решеток из ДНК [32, 48, 49, 57, 58].

ра влияет на электрические свойства прикрепленной к нему пары нанопроволок.

В качестве описанных выше нанопроволок можно использовать, например, ДНК, обладающие необходимыми для этих целей геометрическими размерами, с нанесенными на их поверхности различными металлами (например, Pt). В свою очередь, молекулы ДНК могут быть нанесены на поверхности нанокластеров с помощью иголок сканирующих туннельных микроскопов, упомянутых выше, или с использованием методики молекулярного упорядочения ("molecular combing") [22, 24, 25]. Примеры различных манипуляций с молекулами ДНК приведены на Рис. 1.10.

1.5.4. Функциализация биологических элементов

Основу элементной базы рассматриваемого сверхбыстрого гибридного вычислительного устройства могут составлять упорядоченные наноэлементы, соединенные между собой биомолекулярными структурами (например, ДНК, РНК, протеинами поверхностных слоев бактериальной клетки или другими биологическими макромолекулами). Подобно ситуации, используемой в, так называемых, ДНК компьютерах [21], биологические составляющие новых гибридных вычислительных устройств могут быть специальным образом функциализированы для сверхбыстрого решения определенного класса специфических задач (например, проведения преобразования Фурье), используя структурные особенности биологических макромолекул.

Молекулярная сборка нанопроволок. Биологические структуры позволяют моделировать базисный набор при решении задачи о разложении функции, к которой сводится ряд практических проблемы шифрования, распознавания и т. п.

Одной из возможностей подобного моделирования является молекулярная сборка биологических нанопроволок со строго определенной последовательностью повторяющихся базовых (основных) элементов: в случае ДНК — нуклеотидов, в случае протеинов - аминокислот. Собранная контролируемым образом система нанопроволок закрепляется на поверхности нанокластеров. Исходная функция в форме электрического сигнала подается одновременно на всю систему базисных элементов. Имея разную структуру, отдельные базисные элементы по-разному преобразуют подаваемый сигнал. Процедура преобразования сигнала каждой отдельной нанопроволокой может быть математически описана как проекция исходной функции на определенную базисную. Преобразованный каждой из проволок сигнал считывается и может обрабатываться с помощью особых алгоритмов, адаптированных для конкретной молекулярной сборки базисных биоэлементов.

Глава 2

Программирование гибридных СВУ

2.1. Вычислимость и вычислимый объект

К настоящему времени накоплено достаточное количество примеров, доказывающих иллюзорность убеждения в том, что решение сложной динамической задачи можно получить с любой наперед заданной точностью, используя классическую МТ. В астрономии законы, управляющие движением небесных тел хорошо известны — это закон тяготения Ньютона или уточняющие его уравнения Эйнштейна. Казалось бы, чем более точно заданы начальные условия - положения и скорости небесных тел в начальный момент времени, и чем мельче делаем шаг по времени при машинном интегрировании уравнений движений, тем точнее можно предсказывать поведение системы в будущем. Однако, на этом пути до сих пор не удается ответить даже на фундаментальный вопрос об устойчивости Солнечной системы на больших временах. Это означает, что даже малая неизбежная неточность начальных данных делает поведение системы непредсказуемым: видимая простота уравнений движения, тем не менее, скрывает их неинтегриру-

емость, любая малая неточность в начальных условиях очень сильно влияет на последующую эволюцию.

Другой пример показывает, что даже точное задание начальных условий отнюдь не гарантирует решения динамической задачи. Это пример из биологии. Как известно, экспоненциальный характер изменения численности популяции какого-либо биологического вида при постоянном коэффициенте ее прироста справедлив лишь при отсутствии пределов роста популяции (например, при неограниченном запасе пищи и отсутствии внешних врагов). При наличии пределов роста численность популяции x_n через n лет при начальном значении x_0 удовлетворяет следующему уравнению (процесс Ферхюльста)

$$x_n = (1 + r)x_{n-1} - rx_{n-1}^2,$$

где r — константа, связанная с коэффициентом прироста популяции за год. Оказывается, что поведение системы, подчиняющейся такому уравнению, предсказуемо лишь при малых значениях величины r. При $r = 2,3$ численность популяции начинает периодически осциллировать между двумя значениями 0 и 1. При дальнейшем росте величины r характер поведения численности популяции усложняется. Сначала начинаются колебания численности между четырьмя характерными значениями с удвоенным периодом, далее — количество значений, между которыми происходят колебания численности популяции, удваивается вместе с удвоением периода колебания. Наконец, при $r = 2,570$ процесс перестает быть периодическим — происходят перескоки численности между бесконечно большим количеством значений. Таким образом, предсказание поведения системы оказывается невозможным, несмотря на полную ее детерминированность и определенность начальных условий. Поведение носит хаотический характер, т. е. не существует способа предсказать развитие системы на длительное время. Причиной этого является нелинейность уравнения, описывающего процесс Ферхюльста.

Понятие вычислимости предполагает требование найти приближение для рассматриваемого объекта с любой наперед заданной точностью в классе вычислимых объектов. Вычислимым объектом в смысле классической МТ является множество конечных двоичных дробей. При этом происходит редукция сложности изучаемого объекта — например, иррациональные или трансцендентные числа заменяются существенно более простыми вычислимыми объектами — конечными двоичными дробями.

В последние десятилетия этот подход вызвал непреодолимые трудности при описании конкретных природных систем, а именно, т. н. "сложных систем". К ним относятся, в частности, материальные среды, имеющие сложную, в некотором смысле патологическую, морфологию — пористые, ветвящиеся, чешуйчатые, коллоидные среды и т. п. В качестве конкретных принципиальных трудностей, возникающих при их описании, упомянем расходимость термодинамического давления в очень мелких порах, невозможность найти площадь сильно развитой поверхности геля: чем мельче берется масштаб измерения, тем больше получается искомая величина. Аналогичные трудности возникают при измерении длины береговой линии или определении объема облака. Такие системы получили названия фракталов [15], они являются промежуточными объектами между точкой и линией, линией и поверхностью, поверхностью и объемом.

В [38] обсуждаются трудности формального описания динамических "переходных" процессов в системах, возникающих при быстром изменении "внешних" условий. Обычные подходы к описанию таких неравновесных процессов неэффективны, поскольку сама структура пространства состояний зависит от времени. Многие экспериментальные наблюдения за протеканием неравновесных процессов подтверждает зарождение в системе новых структур мезоскопического (промежуточного между микро и макро) масштаба, которые в значи-

тельной степени и определяют динамическое изменение типа формальной модели. В настоящее время известно, что синергетические процессы формирования динамических структур мезоскопического масштаба в открытых термодинамических системах связаны с возникновением информационно-управленческой обратной связи, внутреннего управления, которое вместе с внешним управлением через наложенные на систему граничные условия и приводит к дискретизации пространства и времени неравновесной системы. При этом физическими носителями информации являются элементы динамических структур.

При описании физических процессов эволюции в сложных материальных системах традиционный подход редукции сложности к конечным двоичным дробям оказывается эквивалентным использованию двух моделей материальной среды — материальной точки и жордановой области в евклидовом пространстве. Эти модели являются отражением математического определения аддитивных физических величин (массы, энергии, электрического заряда) только как чисто атомистических или непрерывно распределенных мер. Неразрешимость проблемы континуума в классической теории множеств является, в конечном итоге, причиной, не позволяющей дать замкнутое описание свойств реальных физических систем, связанных с изменением формы и диссипации энергии в рамках традиционного подхода к понятиям вычислимости и вычислимого объекта, используемыми в классической машине Тьюринга.

В излагаемом далее новом подходе считается, что сложность вычислимого объекта должна быть эквивалентна сложности изучаемого реального объекта и адекватно отражать его свойства. В частности, для материальных сред, имеющих сложную морфологию необходимо использовать математические модели материальной среды, основанные на более слабых требованиях, по сравнению с условием быть си-

стемой изолированных точек или жордановой областью. А именно, моделирующее множество должно быть замкнутым (т. е. содержать все свои предельные точки) и плотным в себе (т. е. каждая его точка должна быть предельной). Совместное выполнение этих свойств эквивалентно требованию быть совершенным множеством. Существует много типов совершенных множеств, среди которых есть регулярные, поддающиеся формальному построению и описанию, [8]. Некоторые из совершенных множеств имеют свойства в строго определенном смысле близкие к свойствам множеств изолированных точек, а некоторые — к свойствам жордановых областей. В промежуточных случаях они хорошо отражают свойства фракталов и являются измеримыми в смысле p-меры Хаусдорфа [39]. Перспективность применения понятия размерности Хаусдорфа обусловлена тем, что эта размерность, рассматриваемая как текущая непрерывная переменная, может быть характеристикой, описывающей эволюцию сложной системы как целого, включая диссипацию энергии [69, 70, 71], в то время как топологическая размерность Урысона-Менгера в процессе изменения реальной системы, как правило, остается постоянной [18, 19, 39, 40].

Требует обобщения и само понятие вычислимости. Проиллюстрируем это рядом примеров.

Пример 1. *Корень квадратный из* 2. *По определению,* $\sqrt{2}$ *равен длине диагонали единичного квадрата.*

Считаем, что это число вычислено, если построен единичный квадрат. Будем говорить, что сложность числа $\sqrt{2}$ равна сложности единичного квадрата. Диагональ единичного квадрата назовем вычислительным примитивом для $\sqrt{2}$ и арифметически связанных с ним иррациональных чисел.

Пример 2. *Число* π. *По определению равно отношению длины любой окружности к ее диаметру.*

Будем считать, что число π вычислено, если построена единичная окружность. Сложность числа π равна сложности единичной окружности. Единичная окружность есть вычислительный примитив для чисел, арифметически связанных с числом π.

Пример 3. *Измерение снежинки. Снежинка представляет собой вписанный в окружность радиуса* 1 *сантиметр фрактал с заданной морфологией и хаусдорфовой размерности* $3/2$ *с шестью лучами.*

В качестве размера снежинки принимаем величину 6 $\text{см}^{3/2}$. Фрактал данной размерности и морфологии является вычислительным примитивом для измерения снежинки.

Пример 4. *Для диофантового уравнения с целыми рациональными числовыми коэффициентами указать способ, при помощи которого возможно после конечного числа операций установить, разрешимо ли это уравнение в целых рациональных числах.*

Неразрешимость этой проблемы на классической МТ была показана Ю. В. Матиясевичем в 1970 г. [12]. В [44] обсуждается гипотетически возможный "физический" способ решения, опирающийся на квантовую адиабатическую теорему. Подробное описание этого способа приведено в п. 3.2.2.

Таким образом объект считаем (когнитивно) вычислимым определенным вычислительным устройством, если он арифметически связан с присутствующим в составе устройства соответствующим вычислительным примитивом. Вычислительный примитив является одним из основных понятий предлагаемого нового подхода к построению обобщенной модели МТ.

2.2. Разработка теоретических принципов работы новых гибридных вычислительных устройств

Для формального описания ряда сложных многомерных задач, связанных с быстроизменяющимися сложными динамическими процессами, такими как распознавание изображений и речи, поиск целей, динамика иерархий структур в живых системах, кластеризация в потоках концентрированных дисперсных смесей или образование многомасштабных вихревых структур в турбулентных течениях жидкости и пластических течениях твердых материалов при импульсном нагружении (ударе), применение математических моделей (изолированных точек или континуумов) на сепарабельных функциональных пространствах, лежащих в основе использования современных вычислительных устройств, не дает удовлетворительных результатов. Физической причиной этого является тот факт, что свойства многих реальных материальных сред (дробление - слияние, сжатие - растяжение, текучесть, диссипация энергии), могут быть адекватно описаны только на множествах более сложной структуры, например, на упомянутых выше совершенных множествах. Постановка и решение вычислительных задач на таких множествах требует отказа от использования основного принципа современных вычислительных устройств: фиксирование определенного такта времени и предположение о том, что информация, хранящаяся в ячейке памяти, не изменяется на протяжении одного такта.

В практике автоматического управления оказалась плодотворной идея релейного регулирования, заключающаяся в (дискретном) переключении системы управления с одного "скользящего режима" (непрерывного процесса) на другой. Один из возможных способов обобщения дискретной классической модели вычислений — это использование так называемых "гибридных систем", свойства которых активно изучаются в по-

следнее время в рамках теории автоматического управления. В последнее десятилетие в информатике и системах управления активно внедряется нейросетевой подход, часто говорят об использовании в управляющих контурах нейрокомпьютеров.

Новые возможные принципы функционирования вычислительных устройств могут основываться на идее комбинирования асинхронных сложных динамических моделей (например, описывающих эволюцию комбинации предлагаемых гибридных наноэлементов). Наверное необходимо пересмотреть традиционные понятия "лента" и "ячейка памяти". В частности, целесообразно рассматривать "ячейку памяти" как постоянно функционирующую модель некой динамической системы. "Естественная" эволюция ячеек в некоторые моменты времени будет прерывается "скачками", способ задания которых будет рассматриваться как программа. Для организации эффективного взаимодействия между разными моделями можно использовать рандомизированные алгоритмы стохастической оптимизации (см. п. 3.3.2, [5, 37]), которые работоспособны в условиях почти произвольных помех, естественно "вписываются" и удобно могут быть реализованы в новых вычислительных устройствах.

2.2.1. Описания процесса работы СВУ как гибридной системы

Гибридный характер СВУ нового типа будет проявляться не только на уровне разработки элементной базы при соединении биологических и неорганических элементов, но и при описании процессов его функционирования. Упрощенно можно говорить о соединении в одном устройстве цифровых и аналоговых вычислительных блоков или процессов.

Рассматриваемая выше концепция выбора элементной базы нового СВУ предполагает,

- во-первых, невозможность во многих случаях точного

определения значений состояния и памяти

• и, во-вторых, недетерминированность переходов из одного положения состояния-памяти в другое. Кроме того, необходимо иметь ввиду большое количество ограничений по таким переходам.

Для адекватного описания динамических процессов, которые будут происходить в новых гибридных СВУ, необходимо выбрать определенный способ описания гибридных динамических систем со стохастическими свойствами, описать и строго сформулировать понятия наблюдаемости, управляемости, области достижимости и т. п.

2.2.2. Разработка модели макета СВУ нового типа

Возможные области применения даже одной упорядоченной системы нанокластеров ($p4$) с фиксированной на их поверхности решеткой из проводящих квантовых биологических нанопроволок (см. Рис. 1.9) достаточно широки, и это может привести к обеспечению более быстрого выполнения некоторых весьма полезных операций, так как природа такого вычислительного устройства отличается от классической и более естественна для задач, встречающихся в физике.

Первое возможное применение — выполнение аналогов классических операций. Ввиду квантовых эффектов будет происходить "сглаживание" данных, что приведет к весьма интересным результатам. Например, зачастую в задачах требуется непрерывным образом приблизить имеющуюся функцию, известную только по конечному числу наблюдений. Кластеры квантовых точек могли бы дать способ быстрого решения такой задачи. Кроме того, прямоугольная сетка с непрерывным распределением внутри нее некоторой функции играет важную роль в задачах математической физики. Например, задача Дирихле или задача о распределении тепла могут быть представлены на конечной сетке, и в этом случае после большого количества итераций на классическом вычислительном

устройстве можно получить приближение к реальному ответу (метод сеток). В случае квантового вычислителя, количество итераций может резко сократиться из-за того, что не нужно будет постоянно выполнять операцию усреднения, которая уже лежит в природе квантового микромира. После получения схемы для решения этих двух базовых задач математической физики можно будет перейти и к решению более сложных дифференциальных уравнений.

Многие другие операции, работающие с аналоговыми данными, также могут быть представлены более естественным образом в квантовой модели, в силу того, что непрерывность пространства состояний заложена в основе квантового микромира. Одной из перспективных возможностей представляется реализация свертки функций и квантового преобразования Фурье [59].

Если, например, на всю упорядоченную систему нанокластеров ($p4$) с фиксированной на их поверхности решеткой из проводящих квантовых биологических нанопроволок одновременно подать два разных электрических сигнала, отражающих две исходные функции, то можно ожидать, что при определенных условиях на выходе системы может быть получен результирующий сигнал, определяемый сверткой изначальных функций. Альтернативной возможностью может являться раздельная подача двух исходных сигналов, каждого на свою подсистему, состоящую из параллельных друг другу нанопроволок. Для эффективной реализации свертки функций необходимо исследовать возможность такого теоретического описания модели системы нанокластеров с нанопроволоками, в котором можно было бы подтвердить эту гипотезу.

Для эффективного решения задачи о разложении исходной функции по некоторой системе базисных функций в пункте 1.5.4 предлагается использовать дополнительные возможности молекулярной сборки биологических нанопроволок со строго определенной последовательностью повторяющихся ба-

зовых (основных) элементов. Собранная контролируемым образом система индивидуальных нанопроволок закрепляется на поверхности нанокластеров. Исходная функция в форме электрического сигнала подается одновременно на всю систему базисных элементов. Имея разную структуру, отдельные базисные элементы по-разному преобразуют подаваемый сигнал. Необходимо разработать математическую модель процесса такого типа, в которой процедура преобразования сигнала каждой отдельной базисной нанопроволокой может быть математически описана как проекция исходной функции на определенную базисную функцию. Кроме того, необходимо разработать алгоритмы для обработки считываемых с нанопроволок сигналов, адаптированные для конкретной молекулярной сборки базовых биоэлементов.

После предварительного выбора набора операций и функций макета необходимо разработать его общую математическую модель как сложной гибридной самоорганизующейся системы, в которой детально описать возможные "входы" и "выходы", управляющие воздействия, внутренние связи и возможности самоорганизации.

2.2.3. Разработка языка и архитектуры СВУ нового типа

Естественно, что для СВУ нового типа потребуется разработка нового языка программирования, который мог бы использовать возможности СВУ эффективным образом. Среди требований к новому языку следует отметить:

• возможность работы непосредственно с объектами, используемыми при расчетах (например, функция, вектор, матрица), наличие операций над этими объектами (сложение и умножение векторов и матриц, свертка функций и т. п.);

• возможность задавать процессы, которые создают программу в процессе ее выполнения;

• эффективный общий параллелизм. Классические опера-

ции должны устойчиво выполняться параллельно с квантовыми вычислениями.

Следует отметить, что существуют специальные языки программирования, частично отвечающие указанным выше требованиям. Но реализация программ на таких языках очень затруднена. Из-за этого они не получают широкого распространения, и часто интересны только узкому кругу теоретиков.

Наивысшая производительность работы системы может быть достигнута, если язык будет разрабатываться параллельно с архитектурой СВУ. Архитектура должна опираться на классические разработки, однако, иметь особенности, связанные с уникальностью используемой технологии. При разработке архитектуры макета СВУ, наверное, целесообразно использовать элементы теории гетерогенных нейронных сетей с самоорганизующейся архитектурой [1].

В настоящее время наиболее эффективной представляется разработка языка функционального типа, в котором вышеперечисленные требования предусмотрены с самого начала.

В случае выбора языка функционального типа, как правило, не возникает проблем с эффективным параллелизмом, а также достаточно эффективно задаются операции над данными векторного типа. Функции как объекты вычислений можно задавать несколькими способами: сумма ряда или предел, подстановка и/или композиция, “черный ящик”. Модификация программы может обеспечиваться концепцией “черного ящика”.

Существенно, что в связи с недетерминированностью СВУ, результаты вычисления будут носить стохастический характер. Возможность операций с неточными данными, а также со случайными величинами и помехами должна быть предусмотрена в общей концепции.

В отличие от классических устройств, СВУ нового типа допускает “непрерывные” операции. Однако концепция непре-

рывных операций предполагает (и современная теоретическая и практическая база подтверждает эти сведения), что процесс, единожды инициированный, какое-то время работает сам по себе. Это придает специфический характер языку описания таких процессов — в отличие от обычных языков программирования, в основе которых лежит классическое утверждение о достижимости любого состояния. Очевидно, что в случае непрерывного процесса сфера нашего влияния на процесс ограничена, так как, например, мы не можем до бесконечности уменьшать интервалы между внешними вмешательствами. Это свидетельствует о том, что непрерывные процессы могут, вообще говоря, породить большее множество состояний, чем классические дискретные процессы.

Ограниченность внешних влияний влечет за собой необходимость совершенствования наших знаний о понятии алгоритма. В этом плане очень полезным представляется использование концепции обобщенной машины Тьюринга, описанной далее в следующем пункте. Кроме того, следует иметь в виду, что проверка дискретными методами допустимости данной конструкции или набора конструкций для непрерывной части представляется малореальной. Следовательно, необходимо разработать специальный "компилятор", одной из задач которого являлась бы проверка исходного текста "программы", написанной для "непрерывной" части.

Довольно интересной представляется также возможность отказаться от традиционной фон-Неймановской концепции, неестественной для квантового мира. Наиболее естественной представляется концепция двойственности, столь распространенная в природе, и открывающая новые горизонты. Действительно, в эту концепцию вписываются даже такие невероятные сегодня, но вполне возможные уже в недалеком будущем процессы, как программная генерация аппаратной части компьютера.

2.3 Концепция обобщенной МТ

Определим новое понятие "обобщенная машина Тьюринга" как следующую структуру

$$\langle S, X, Y, s, s_0, y, y_0, E, P, J, F\rangle,$$

в которой множества состояний S, памяти X и состояний памяти Y могут быть произвольными, т. е. не обязательно конечными и даже счетными;
s — текущее состояние машины;
$s_0 = s(0)$ — состояние в начальный момент времени;
y — текущее содержимое памяти;
y_0 — начальное содержимое памяти;
E — терминальное множество: $E \subset Q$, где Q — множество всевозможных наборов $q = (s, y)$ состояний и памяти;
P — программа;
$J \subset Q$ — множество задания программы, т. е. $P : J \to Q$, причем $E \cap J = \emptyset$, и
F — оператор эволюции состояний и памяти.

Алгоритм работы обобщенной МТ описывается следующим образом: в любой момент времени t, если набор q из состояния и памяти машины попадает в терминальное множество E, то машина останавливается, если $q \in J$, то в эволюции обобщенной МТ происходит "скачок": $q \to P(q)$, в остальных случаях состояние и память машины "естественно" (например, непрерывно) эволюционируют, и этот процесс определяется оператором F. Другими словами, изменения состояния и памяти обобщенной МТ происходят как в гибридных системах, т. е. обычно они эволюционируют согласно некоторому закону, а в определенные моменты времени, задаваемые достижением некоторых подмножеств пространства Q, происходят скачкообразные изменения состояния и памяти.

Нетрудно убедиться, что классическая МТ представляет собой частный случай обобщенной МТ (см. [2]).

Для более точного описания способа функционирования новой модели вычислений в [2] было предложено использовать средства нестандартного математического анализа, которые, наверное, более естественным для информатики способом помогают описать новые понятия.

В новой концепции исключено понятие рабочей ячейки, т. е. изменение состояния может зависеть от содержимого всей памяти в данный момент, а содержимое памяти может меняться одновременно на всем пространстве X. Разделение описания процесса изменения состояния и памяти на две составляющие: программу P и эволюцию F, на первый взгляд, может показаться искусственным. На самом деле, вводя такое разделение, хочется сразу же размежевать "принудительные" изменения, обычно вносимые в систему извне, задаваемые кем-то "осознанно", и те "естественные" процессы, которые происходят в определенной физической (или биологической) системе в силу законов природы.

В концепции обобщенной МТ переосмысливается понятие "такт". Если в классической МТ — это фиксированный интервал времени, то в обобщенной машине Тьюринга длина такта определяется достижением некоторого условия, после чего происходит "скачкообразное" изменение состояния и памяти. В частном случае J может совпадать с $Q \setminus E$, и тогда внешнее воздействие является постоянным, или же J может быть пустым, и поведение машины определяется только эволюцией.

Набор моделей. Важным обобщением классической МТ является вычислительная схема, которую можно назвать "набор моделей". Пусть в новой схеме вычислений

$$Y = \{\langle S, X, \bar{Y}, s, s_0, \bar{y}, \bar{y}_0, E, J, P, F\rangle\}$$

— это множество обобщенных МТ (набор моделей), т. е. мы считаем, что каждая ячейка памяти представляет собой отдельное устройство (квантовый или аналоговый компьютер, нейронная сеть, некоторая динамическая система), решающее

свою собственную задачу. Таких устройств может быть конечное или бесконечное число. Заметим, что обычную ячейку памяти с целыми значениями тоже можно считать моделью с одной ячейкой памяти и тождественной эволюцией. В соответствии с общей программой при достижении набором состояний и одной из моделей определенных условий происходит изменение состояния и содержимого некоторых ячеек памяти, понимаемое как изменение состояния и памяти соответствующего устройства.

В [2] для иллюстрации рассмотрены модельные примеры алгоритмов дифференцирования и интегрирования функции, поиска глобального минимума.

Представляется перспективным направление разработки некоторого "гипотетического" искусственного интеллекта из набора блоков, в каждом из которых для реализации эффективного решения определенной задачи используется соответствующий специальный набор атомов. Возможно, при решении разнообразных конкретных практических задач можно будет применять эквивалентность описаний многих явлений в микро и макромире. Все блоки будут работать параллельно, составляя в совокупности некоторый набор моделей.

Другим обобщением машины Тьюринга может быть вероятностное задание отображений P и F, что позволит реализовывать с помощью новой модели динамические системы, не описываемые детерминированными законами, а также стохастические гибридные системы [54], вероятностные автоматы, системы со стохастическим управлением и т. п. Кроме того, в [38] показан пример эффективности использования рандомизированных программных воздействий на систему в условиях динамически изменяющейся структуры пространства состояний. Рандомизация позволяет частично устранить влияние на работу системы систематических погрешностей [5, 37], которые практически неизбежны при изменяющейся со временем модели динамической системы.

Глава 3

Квантовые вычисления

3.1. Примеры квантовых алгоритмов

Классический компьютер обрабатывает биты $\{0, 1\}$, квантовый — квантовые биты (кубиты).

3.1.1. Задача Дойча

Пусть некоторая функция $f : \{0, 1\} \longrightarrow \{0, 1\}$ задана как "черный ящик" и процесс ее вычисления занимает, например, 24 часа.

Требуется ответить на вопрос: является ли функция $f(x)$ константой или сбалансированной?

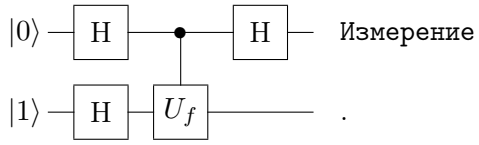
В классическом случае для ответа на вопрос, очевидно, необходимо не менее 48 часов. Пусть на самом деле задан квантовый "черный ящик", который вычисляет $f(x)$. Более точно, пусть определено двух кубитовое унитарное преобразование:

$$U_f : |x\rangle|y\rangle \longrightarrow |x\rangle|y \oplus f(x)\rangle,$$

которое зеркально отражает второй кубит если значение f от первого кубита равно 1. Наша задача состоит в том, чтобы

определить будет ли $f(0) = f(1)$? Если мы ограничены "классическим" вводом $|0\rangle$ и $|1\rangle$, то для того, чтобы получить ответ, мы должны обратиться к ящику дважды ($x = 0$ и $x = 1$). Но если нам разрешено ввести когерентное наложение этих классических состояний, тогда для ответа на вопрос достаточно — одного раза!

Рассмотрим квантовую цепь, которая решает эту задачу



Здесь H обозначает преобразование Адамара:

$$H : |x\rangle \longrightarrow \frac{1}{\sqrt{2}} \sum_y (-1)^{xy} |xy\rangle,$$

или $H : \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} \longrightarrow \begin{pmatrix} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{pmatrix}$, т. е. H — это 2×2 матрица: $\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$.

Если на вход цепи подать пару квантовых битов $|0\rangle|1\rangle$, то последовательно получаем

$$|0\rangle|1\rangle \longrightarrow \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \longrightarrow$$

$$\longrightarrow \frac{1}{2}[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle](|0\rangle - |1\rangle) \longrightarrow$$

$$\longrightarrow \frac{1}{2}\left[\left((-1)^{f(0)} + (-1)^{f(1)}\right)|0\rangle + \left((-1)^{f(0)} - (-1)^{f(1)}\right)|1\rangle\right] \otimes$$

$$\otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Итак, когда мы измеряем первый кубит, мы находим результат $|0\rangle$ с вероятностью единица, если $f(0) = f(1)$ (т. е. f — постоянная функция) и результат $|1\rangle$ с вероятностью единица, если $f(0) \neq f(1)$ (сбалансированная функция).

Это преимущество квантового вычисления перед классическим объясняется квантовым параллелизмом. Поскольку мы подаем на вход наложение $|0\rangle$ и $|1\rangle$, то вывод чувствителен к обоим значениям $f(0)$ и $f(1)$, даже при том, что мы запустили "черный ящик" только один раз.

В последующих примерах для прояснения вопроса о "сложности" того или иного алгоритма мы будем предполагать, что имеем семейство "черных ящиков" ("квантовых оракулов") с входом переменного размера. Нас будет интересовать вопрос о том, как при выяснении того, что находится внутри черного ящика, количество запросов к ящику ("время") соотносится с размером ввода.

Рассмотрим обобщение алгоритма решения задачи Дойча. Пусть функция f преобразует n битов к одному:

$$f : \{0,1\}^n \longrightarrow \{0,1\},$$

и мы уверены, что f является или константой ($f(x) = c\ \forall x$) или сбалансированной ($f(x) = 0$ точно для половины возможных входных значений). Мы должны решить задачу: f — это константа или сбалансированная функция?

Эту задачу также можно решить, обратившись к ящику только один раз, используя ту же самую цепь, что и в задаче Дойча (но с аргументом x, расширенным от одного бита до n битов). Заметим, что, если применить n схем Адамара параллельно к n кубитам

$$H^{(n)} = H \otimes H \otimes ... \otimes H,$$

то n-кубитовое состояние преобразуется оператором $H^{(n)}$ так

$$|x\rangle \longrightarrow \prod_{i=1}^{n} \left(\frac{1}{\sqrt{2}} \sum_{y_i=\{0,1\}} (-1)^{x_i y_i} |y_i\rangle \right) \equiv \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} (-1)^{x \cdot y} |y\rangle,$$

где x, y представляют n-битовые строки, и $x \cdot y$ обозначает побитовый AND (или скалярное произведение по модулю 2)

$$x \cdot y = (x_1 \wedge y_1) \oplus (x_2 \wedge y_2) \oplus ... \oplus (x_n \wedge y_n).$$

Подавая на вход цепи $(|0\rangle)^n|1\rangle$, получаем

$$(|0\rangle)^n|1\rangle \longrightarrow \left(\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle\right) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \longrightarrow$$

$$\longrightarrow \left(\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|x\rangle\right) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \longrightarrow$$

$$\longrightarrow \left(\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{f(x)}(-1)^{x\cdot y}|y\rangle\right) \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{3.1}$$

Теперь вычислим сумму

$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)}(-1)^{x\cdot y}.$$

Если f — постоянная функция, то сумма будет равна

$$(-1)^{f(x)} \left(\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{x\cdot y}\right) = (-1)^{f(x)}\delta_{y,0},$$

т. е. она не исчезает, если $y = 0$. Следовательно, когда мы измеряем n-битовый регистр, то получаем с вероятностью единица результат $|y = 0\rangle \equiv (|0\rangle)^n$. Но если функция сбалансирована, то для $y = 0$ сумма становится равной нулю

$$\frac{1}{2^n} \sum_{x=0}^{2^{n-1}} (-1)^{f(x)} = 0,$$

т. к. половина членов равна $(+1)$, а другая — (-1). Поэтому, вероятность получения результата измерения $|y = 0\rangle$ является нулевой.

Можно сделать вывод: одного запроса квантовому оракулу достаточно для того, чтобы отличить постоянную функцию от сбалансированной с 100% достоверностью. Результат измерения $y = 0$ означает функцию-константу, любой другой результат — сбалансированную.

3.1.2. Задача Бернштейна-Вазирани

Давайте предположим, что наш квантовый "черный ящик" вычисляет одну из функций

$$f_a(x) = a \cdot x,$$

где a — n-битовая строка. *Требуется* определить a.

Описанный выше квантовый алгоритм может с уверенностью решить и эту задачу, сделав только один (n-кубитовый) квантовый запрос. Для этой специфической функции, квантовое состояние первых n регистров в формуле (3.1) становится равным

$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{y=0}^{2^n-1} (-1)^{a \cdot x} (-1)^{x \cdot y} |y\rangle.$$

Но фактически

$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{a \cdot x} (-1)^{x \cdot y} = \delta_{a,y},$$

т. е. это состояние и есть $|a\rangle$. Итак, мы выполняем цепь один раз и измеряем n-кубитовый регистр, находя n-битовую строку a с вероятностью единица.

Если разрешены только классические запросы, то мы можем приобрести только один бит информации из каждого

запроса, т. е. требуется n запросов, чтобы определить значение a. Таким образом мы имеем четкое разделение между квантовой и классической трудностью задачи.

3.1.3. Задача Саймона

Рассмотрим пример, предложенный Дэниэлом Саймоном. Пусть функция

$$f : \{0,1\}^n \longrightarrow \{0,1\}^n,$$

имеет "период", задаваемый n-битовой строкой a, т. е.

$$f(x) = f(y) \text{ если } y = x \oplus a,$$

где $\oplus$ означает побитовую операцию XOR (если считать x принимающим значения в $(Z_2)^n$, а не в Z_{2^n}, то a является периодом).

Требуется определить значение a.

Для классических вычислений это трудная задача. Мы должны запросить оракула экспоненциально большое количество раз, чтобы иметь какую-то разумную вероятность нахождения a. Мы не узнаем ничего, пока нам не повезет выбрать такие два запроса x и y, которые удовлетворят условию $x \oplus y = a$. Предположим, например, что мы выбираем $2^{n/4}$ запросов. Число пар запросов меньше чем $(2^{n/4})^2$, и для каждой пары $\{x, y\}$ вероятность того, что $x \oplus y = a$, равна 2^{-n}. Поэтому вероятность успешного нахождения меньше, чем

$$2^{-n}(2^{n/4})^2 = 2^{-n/2}.$$

Даже с экспоненциально большим количеством запросов, вероятность успеха экспоненциально мала.

Но с квантовыми запросами задача становится проще! Используем почти ту же самую цепь как и ранее, но теперь оба регистра расширим до n кубитов.

Вначале приготовим равномерно взвешенную суперпозицию всех n-битовых строк (действуя $H^{(n)}$ на $(|0\rangle)^n$), а затем запрашиваем оракула:

$$U_f : \left(\sum_{x=0}^{2^n-1} |x\rangle \right) |0\rangle \longrightarrow \sum_{x=0}^{2^n-1} |x\rangle |f(x)\rangle.$$

После этого измеряем второй регистр. Результат измерения отобран наугад из 2^{n-1} возможных значений $f(x)$, каждое из которых может появиться равновероятно. Предположим, что результат это $f(x_0)$. Так как только x_0 и $x_0 \oplus a$ отображаются в $f(x_0)$, то в первом регистре имеем состояние

$$\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 \oplus a\rangle).$$

Мы хотим извлечь некоторую информацию относительно a. Ясно, что не имеет смысла измерять первый регистр в этой точке. Мы получили бы или результат x_0 или $x_0 \oplus a$ с равной вероятностью появления каждого, но никакой результат ничего не скажет о значении a.

Но если перед измерением регистра применить к нему преобразование Адамара $H^{(n)}$, то получаем

$$\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 + a\rangle) \longrightarrow \frac{1}{2^{\frac{n+1}{2}}} \sum_{y=0}^{2^n-1} \left[(-1)^{x_0 \cdot y} + (-1)^{(x_0 \oplus a) \cdot y} \right] |y\rangle =$$

$$= \frac{1}{2^{(n-1)/2}} \sum_{a \cdot y = 0} (-1)^{x_0 \cdot y} |y\rangle.$$

Если $a \cdot y = 1$, то в коэффициенте при $|y\rangle$ оба слагаемых имеют разные знаки и в итоге дают нуль. Следовательно, только состояния $|y\rangle$ с $a \cdot y = 0$ остаются в сумме по y. Таким образом при измерении результат выбирается случайно из всех возможных значений y, для которых $a \cdot y = 0$, с вероятностью $2^{-(n-1)}$.

Выполним этот алгоритм несколько раз, получая другие значения y, удовлетворяющие условию $a \cdot y = 0$. Как только мы нашли n таких значений $\{y_1, y_2, y_3, \ldots, y_n\}$ линейно независимых в $(Z_2)^n$, то для определения уникального значения a остается решить систему уравнений

$$\begin{aligned} y_1 \cdot a &= 0, \\ y_2 \cdot a &= 0, \\ &\vdots \\ y_n \cdot a &= 0. \end{aligned}$$

Таким образом с количеством повторений порядка n можно достичь вероятности успеха, которая экспоненциально близка к единице.

3.1.4. Поиск в квантовой базе данных

Следующий алгоритм также демонстрирует ускорение, которое может быть достигнуто с помощью квантового алгоритма. Но в этом случае квантовое время подобно квадратному корню классического времени, в отличие от экспоненциального ускорения при решении задачи Саймона. Однако полученный Гровером результат чрезвычайно интересен из-за большой актуальности проблемы.

Задача заключается в следующем: нам дана очень большая неотсортированная база данных, содержащая $N \gg 1$ элементов, и мы должны найти один конкретный элемент, как иголку в стоге сена. Пусть база данных представлена таблицей или функцией $f(x)$ с $x \in \{0, 1, 2...N-1\}$. Будем считать, что запись встречается в таблице ровно один раз, т. е. $f(x) = a$ только для одного значения x. *Требуются* по данному a найти значение x.

Если база данных (например, телефонная книга) должным образом отсортирована (по номерам), то поиск x (фамилии) прост. Это можно сделать, просмотрев только $\log_2 N$ записей. Если номера перечислены в произвольном порядке, то

для поиска фамилии по номеру с вероятностью $P = \frac{1}{2}$ надо просмотреть $\frac{1}{2}N$ записей. Гровер обнаружил, что в квантовой телефонной книге можно с высокой вероятностью узнать фамилию, консультируясь с телефонной книгой около $\sqrt{N}$ раз.

Рассмотрим оракул ("черный ящик"), которому можно задавать фамилию (значение x) и оракул выдает либо 0, если $f(x) \neq a$, либо 1, если $f(x) = a$. Задача состоит в том, чтобы как можно быстрее найти значение x:

$$f(x) = a.$$

Оракул. Пусть $N = 2^n$. Оракул "знает", что из 2^n возможных строк длины n одна "помеченная" строка w — особая ("решение"). Мы подаем оракулу запрос x, и он сообщает нам равен ли $x = w$ или нет. Другими словами, он возвращает, значение функции $f_w(x)$:

$$\begin{aligned} f_w(x) &= 0, \quad x \neq w, \\ f_w(x) &= 1, \quad x = w. \end{aligned}$$

Но пусть это квантовый оракул, т. е. он может отвечать на запросы, которые является наложениями строк. Оракул — квантовый "черный ящик", который осуществляет унитарное преобразование

$$U_{f_w} : |x\rangle|y\rangle \longrightarrow |x\rangle|y \oplus f_w(x)\rangle,$$

где $|x\rangle$ является n-кубитовым состоянием, а $|y\rangle$ — однокубитовым состоянием.

Как и ранее, можно выбрать состояние однокубитового регистра равным $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, тогда получаем ответ оракула:

$$U_{f_w} : |x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \longrightarrow (-1)^{f_w(x)}|x\rangle\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Мы можем теперь проигнорировать второй регистр и получить

$$U_w : |x\rangle \longrightarrow (-1)^{f_w(x)}|x\rangle \quad \text{или} \quad U_w = 1 - 2|w\rangle\langle w|.$$

Оракул зеркально отражает знак состояния $|w\rangle$, но действует тривиально на любое состояние, ортогональное к $|w\rangle$. Это преобразование имеет простую геометрическую интерпретацию. Действуя на любой вектор в 2^n-мерном Гильбертовом пространстве, U_w отражает вектор относительно гиперплоскости, ортогональной к $|w\rangle$ (сохраняет ту часть, что лежит в гиперплоскости, и зеркально отображает другую вдоль $|w\rangle$).

Мы знаем, что оракул выполняет это отображение для некоторого специфического вычислительного базиса состояния $|w\rangle$, но *априорно* мы ничего не знаем относительно значения строки w. Наша задача состоит в том, чтобы определить с высокой вероятностью w, обращаясь к оракулу минимальное число раз.

Итерация Гровера. В качестве первого шага подготовим состояние

$$|s\rangle = \frac{1}{\sqrt{N}} \left(\sum_{x=0}^{N-1} |x\rangle \right),$$

являющееся равномерно распределенным наложением всех состояний вычислительного базиса. Это сделать легко, применяя преобразование Адамара к каждому кубиту начального состояния $|x = 0\rangle$. Хотя значение w неизвестно, но мы знаем, что $|w\rangle$ — состояние вычислительного базиса, т. е.

$$|\langle w|s\rangle| = \frac{1}{\sqrt{N}},$$

независимо от значения w. Мы должны измерить состояние $|s\rangle$, спроектировав его на вычислительный базис. Вероятность того, что мы "найдем" помеченное состояние $|w\rangle$ равна только $\frac{1}{N}$. Но можно выполнить определенное количество итераций преобразования Гровера, которое увеличивает амплитуду вероятности искомого неизвестного состояния $|w\rangle$ при подавлении амплитуды всех нежелательных состояний $|x \neq w\rangle$.

Итерация Гровера состоит в комбинации неизвестного отображения U_w, которое выполняется оракулом, с известным отображением

$$U_s = 2|s\rangle\langle s| - 1,$$

которое мы можем выполнить самостоятельно. Отображение U_s сохраняет $|s\rangle$, но меняет знак любого вектора, ортогонального к $|s\rangle$. Геометрически, действуя на произвольный вектор, оно сохраняет его составляющую по $|s\rangle$ и зеркально отображает ту часть, что лежит в гиперплоскости ортогональной к $|s\rangle$. Т. к. $|s\rangle = H^{(n)}|0\rangle$, где $H^{(n)}$ — побитовое преобразование Адамара, то можно записать

$$U_s = H^{(n)}(2|0\rangle\langle 0| - 1)H^{(n)}.$$

Одна итерация Гровера — это унитарное преобразование

$$R_{\texttt{гровера}} = U_s U_w,$$

при котором один запрос оракула U_w сопровождается задаваемым нами отображением U_s.

Рассмотрим как $R_{\texttt{гровера}}$ действует в плоскости, заполненной $|w\rangle$ и $|s\rangle$. Это действие проще понять, если представить его геометрически. Напомним, что

$$|\langle s|w\rangle| = \frac{1}{\sqrt{N}} \equiv \sin\theta,$$

так что $|s\rangle$ поворачивается в плоскости на угол θ относительно оси $|w^\perp\rangle$ нормальной к $|w\rangle$. Оператор U_w отображает вектор в плоскости относительно оси $|w^\perp\rangle$, а U_s отображает вектор относительно оси $|s\rangle$. Таким образом итерация Гровера является ничем иным как поворотом на угол 3θ в плоскости, определенной $|w\rangle$ и $|s\rangle$.

Нахождение 1 из 4. Пусть в базе данных $N = 4$ элементов и один из них “отмеченный”. С классическими запросами, отмеченный элемент мог бы быть найден в 1, 2, 3 или

4-м запросе; в среднем необходимо $2\frac{1}{2}$ запросов для достижения успеха, и четыре — в самом плохом случае. Но так как $\sin\theta = 1/\sqrt{N} = \frac{1}{2}$, то $\theta = 30°$ и $2\theta = 60°$. Следовательно, после одной итерации Гровера мы поворачиваем $|s\rangle$ на угол $90°$ с $|w^{\perp}\rangle$; то есть он выстраивается в линию с $|w\rangle$. Когда мы измеряем, проецируя на вычислительный базис, мы с вероятностью 1 получаем результат $|w\rangle$. Таким образом достаточно только одного квантового запроса для того, чтобы найти отмеченное состояние.

Можно итерацию Гровера визуализировать и по-другому. Этот иногда полезный способ называется “инверсия среднего числа”. Если представить некоторое состояние $|\psi\rangle$ в вычислительном базисе

$$|\psi\rangle = \sum_x a_x |x\rangle,$$

то его внутреннее произведение с $|s\rangle = \frac{1}{\sqrt{N}} \sum_x |x\rangle$ это

$$\langle s|\psi\rangle = \frac{1}{\sqrt{N}} \sum_x a_x = \sqrt{N}\langle a\rangle,$$

где

$$\langle a\rangle = \frac{1}{N} \sum_x a_x$$

является средним значением амплитуды. Если применить оператор $U_s = 2|s\rangle\langle s| - 1$ к $|\psi\rangle$, то получиться

$$U_s|\psi\rangle = \sum_x (2\langle a\rangle - a_x)|x\rangle,$$

и амплитуды преобразуются как

$$U_s : a_x - \langle a\rangle \longrightarrow \langle a\rangle a_x,$$

т. е. коэффициент при $|x\rangle$ инвертируется относительно среднего значения амплитуды.

Для случая $N = 4$ в состоянии $|s\rangle$ каждая амплитуда будет равна $\frac{1}{2}$. Один запрос оракула меняет знак амплитуды отмеченного состояния и поэтому уменьшает среднюю амплитуду до $\frac{1}{4}$. Тогда инвертирование относительно среднего приводит амплитуды всех непомеченных состояний от $\frac{1}{2}$ к нулю и увеличивает амплитуду отмеченного состояния от $-\frac{1}{2}$ до 1. Следовательно, мы снова можем сделать вывод о том, что одного запроса достаточно для уверенного нахождения отмеченного состояния.

Также можно легко убедиться в том, что если имеются N записей в базе данных и точно $\frac{1}{4}$ из них отмечены, то одного запроса достаточно для того, чтобы найти отмеченное состояние.

Нахождение 1 из N. Вернемся к случаю, в котором база данных содержит N элементов и только один элемент отмечен. Каждая Гроверовская итерация поворачивает квантовое состояние в плоскости, определенной $|s\rangle$ и $|w\rangle$. После T итераций состояние поворачивается на угол $\theta + 2T\theta$ от оси $|w^{\perp}\rangle$. Чтобы оптимизировать вероятность нахождения отмеченного состояния при окончательном выполнении измерения, итерации надо выполнять до тех пор, пока этот угол не приблизится к 90°

$$(2T + 1)\theta \simeq \frac{\pi}{2} \Longrightarrow 2T + 1 \simeq \frac{\pi}{2\theta}.$$

Вспомним, что $\sin\theta = \frac{1}{\sqrt{N}}$, или

$$\theta \simeq \frac{1}{\sqrt{N}},$$

для больших значений N. Если выбрать

$$T = \frac{\pi}{4}\sqrt{N}(1 + O(N^{-1/2})),$$

то вероятность получения результата измерения $|w\rangle$ будет

$$Prob(w) = \sin^2((2T + 1)\theta) = 1 - O(\frac{1}{N}).$$

Таким образом для определения w с высокой вероятностью необходимо только около $\frac{\pi}{4}\sqrt{N}$ запросов, т. е. имеем квадратичное ускорение относительно классического результата. Кроме того, можно показать, что алгоритм Гровера обеспечивает самый быстрый из возможных квантовый поиск в несортированной базе данных, если "время" измеряется согласно числу запросов оракула.

3.1.5. Периодичность, квантовое преобразование Фурье

Саймон изучал периодические функции, принимающие значения в $(Z_2)^n$. Для этой цели n-битовое преобразование Адамара $H^{(n)}$ было мощным инструментом. Для изучения периодических функций, принимающих значения в Z_{2^n}, инструментом сопоставимой мощности является дискретное преобразование Фурье.

Мораль решения задачи Саймона состоит в том, что процесс обнаружении игл в стоге сена может быть труден, в то время как нахождение игл в стоге сена, разбросанных периодически, может оказаться гораздо проще. Например, если мы рассеиваем фотон на периодическом массиве игл, то он будет рассеиваться в одном из множества преимущественных направлений, где удовлетворяется условие рассеивания Брэгга. Эти преимущественные направления зависят от расстояния между иглами, так что, даже рассеивая только один фотон, мы уже можем собрать некоторую полезную информацию об этом расстоянии. Далее будет исследовано значения этого явления для построения эффективных квантовых алгоритмов.

Итак, вообразим квантового оракула, который вычисляет функцию

$$f : \{0,1\}^n \longrightarrow \{0,1\}^m,$$

имеющую неизвестный период r, где r — положительное целое число, удовлетворяющее условию: $1 \ll r \ll 2^n$. Т. е. для

любого целого числа m, если x и $x + mr \in \{0, 1, 2, ..., 2^n - 1\}$, то значения функции совпадают: $f(x) = f(x + mr)$,

Требуется найти период r.

Классически это трудная задача. Если r, скажем, порядка $2^{n/2}$, то мы должны будем запросить оракула порядка $2^{n/4}$ раз прежде, чем с большой вероятностью найдем два значения x, которые отображаются на одно и то же значение $f(x)$, и, следовательно, сможем что-то узнать о величине r. Питер Шор показал, что имеется квантовый алгоритм, который находит r за время полиномиальное относительно n [59]. Эффективное нахождение периода позволит нам эффективно решать множество (очевидно) тяжелых задач типа разложения на целые множители или вычисления дискретного логарифма.

Ключевая идея, лежащая в основе квантового алгоритма нахождения периода, состоит в том, что преобразование Фурье может вычисляться с помощью эффективной квантовой цепи, использующей мощь квантового параллелизма для достижения экспоненциального ускорения хорошо известного (классического) быстрого преобразования Фурье (FFT).

Так как FFT имеет широкий спектр применения, возможно, квантовое преобразование Фурье (QFT) также будет когда-нибудь широко использоваться.

Нахождение периода. Пусть QFT — унитарное преобразование, которое действует на вычислительный базис следующим образом

$$QFT : |x\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y / N} |y\rangle,$$

где $N = 2^n$. Давайте предположим, что мы можем эффективно выполнять QFT, и посмотрим, как это позволит нам найти период функции $f(x)$.

Как и в алгоритме Саймона, сначала запросим оракула, предложив в качестве ввода $\frac{1}{\sqrt{N}} \sum_x |x\rangle$. Таким образом готовим состояние:

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |f(x)\rangle.$$

После этого, измерив регистр вывода, получаем результат $|f(x_0)\rangle$ для некоторых $0 \leq x_0 < r$. Это измерение готовит во входном регистре когерентное наложение A значений x, которые отображаются в $f(x_0)$:

$$\frac{1}{\sqrt{A}} \sum_{j=0}^{A-1} |x_0 + jr\rangle, \tag{3.2}$$

где

$$N - r \leq x_0 + (A-1)r < N$$

или

$$A - 1 < \frac{N}{r} < A + 1.$$

Фактически измерение регистра вывода не нужно. Если этот шаг опустить, то состояние входного регистра — несвязное наложение состояний (3.2) (сумма по $x_0 \in \{0, 1, \ldots, r-1\}$). Остальная часть алгоритма работает точно также, действуя на это начальное состояние.

Теперь наша задача состоит в том, чтобы извлечь значение r из состояния (3.2), которое мы уже подготовили. Измеряя входной регистр в этой точке, т. е. проецируя на вычислительный базис, мы ничего не узнаем про r. Вместо этого, как и в алгоритме Саймона, мы сначала должны применить преобразование Фурье, а затем произвести измерение.

Применяя QFT к состоянию (3.2), мы получаем

$$\frac{1}{\sqrt{NA}} \sum_{y=0}^{N-1} e^{2\pi i x_0 y} \sum_{j=0}^{A-1} e^{2\pi i j r y / N} |y\rangle.$$

Если теперь произвести измерение в вычислительном базисе, то вероятность получения результата y будет равна

$$Prob(y) = \frac{A}{N} \left| \frac{1}{A} \sum_{j=0}^{A-1} e^{2\pi i j r y / N} \right|^2 .$$

Этому распределению строго удовлетворяют те значения y, для которых отношение yr/N близко к целому числу. Например, если бы N/r получилось целым числом (и поэтому равнялось A), мы имели бы

$$Prob(y) = \frac{1}{r} \left| \frac{1}{A} \sum_{j=0}^{A-1} e^{2\pi i j y / A} \right| = \begin{cases} \frac{1}{r}, \ y = A \cdot (\texttt{целое}), \\ 0, \ \texttt{в противном случае}. \end{cases}$$

В более общем случае, мы можем просуммировать геометрический ряд

$$\sum_{j=0}^{A-1} e^{i\theta j} = \frac{e^{iA\theta} - 1}{e^{i\theta} - 1}, \tag{3.3}$$

где

$$\theta_y = \frac{2\pi y r (mod N)}{N}.$$

Имеется точно r значений y в $\{0, 1, \ldots, N-1\}$, которые удовлетворяют условию

$$-\frac{r}{2} \leq yr(modN) \leq \frac{r}{2}. \tag{3.4}$$

(Чтобы в этом убедиться, вообразите разметку множителей r и N на числовой прямой в интервале от 0 до $rN - 1$. Для каждого множителя N имеется множитель r на расстоянии не больше, чем $r/2$). Для каждого из этих значений соответствующие величины θ_y удовлетворяют условию

$$-\pi \frac{r}{N} \leq \theta_y \leq \pi \frac{r}{N}.$$

Так как $A - 1 < \frac{N}{r}$, то для этих значений θ_y все члены в сумме по j в (3.3) лежат в одной и той же полуплоскости, т. е. они конструктивно интерферируют друг с другом и сумма существенна.

Мы знаем, что

$$|1 - e^{i\theta}| \leq | \theta|,$$

потому что расстояние от начала координат по прямой меньше чем длина дуги по кругу, и для $A|\theta| \leq \pi$ имеем

$$\left|1 - e^{iA\theta}\right| \geq \frac{2A|\theta|}{\pi},$$

так как графически (или вычисляя производную) можно убедиться в том, что это расстояние — выпуклая функция. Мы фактически имеем $A < \frac{N}{r} + 1$, и, следовательно, $A\theta_y < \pi(1 + \frac{r}{N})$, но, применяя вышеуказанное ограничение к

$$\left|\frac{e^{i(A-1)\theta} - 1}{e^{i\theta}} + e^{i(A-1)\theta}\right| \geq \left|\frac{e^{i(A-1)\theta} - 1}{e^{i\theta}}\right| - 1,$$

мы еще можем заключить, что

$$\left|\frac{e^{iA\theta} - 1}{e^{i\theta} - 1}\right| \geq \frac{2(A-1)|\theta|}{\pi|\theta|} - 1 = \frac{2}{\pi}A - (1 + \frac{2}{\pi}).$$

Пренебрегая возможной поправкой порядка $2/A$, находим

$$Prob(y) \geq \left(\frac{4}{\pi^2}\right)\frac{1}{r}$$

для каждого из r значений y, которые удовлетворяют условию (3.4). Поэтому с вероятностью не меньшей $4/\pi^2$ измеренное значение y будет удовлетворять условию

$$k\frac{N}{r} - \frac{1}{2} \leq y \leq k\frac{N}{r} + \frac{1}{2} \tag{3.5}$$

или

$$\frac{k}{r} - \frac{1}{2N} \leq \frac{y}{N} \leq \frac{k}{r} + \frac{1}{2N},$$

где k — целое число, выбранное из $\{0, 1, \ldots, r-1\}$. Есть все основания считать, что результат вычисления будет на расстоянии $1/2$ от целого, являющегося множителем N/r.

Предположим, что мы знаем M: $r < M \ll N$. Тогда N/r — рациональное число со знаменателем меньше чем M. Два различных рациональных числа со знаменателями меньше, чем M, могут находиться на расстоянии друг от друга не ближе, чем $1/M^2$, т. к. $\frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd}$. Если результат измерения y удовлетворяет (3.5), тогда при условии $N \geq M^2$ имеется единственное значение k/r (с $r < M$), определяемое y/N. Это значение k/r может быть успешно извлечено из измеренного y/N, методом цепной дроби.

Таким образом с вероятностью превышающей $4/\pi^2$, мы нашли значение k/r, где k выбрано (приблизительно равновероятно) из $\{0, 1, \ldots, r-1\}$. Вполне вероятно, что k и r являются взаимно простыми (не имеют общего множителя), поэтому наши поиски r увенчались успехом. С помощью оракула, мы можем проверить, действительно ли $f(x) = f(x+r)$. Но если $\texttt{НОД}(k; r) \neq 1$, то мы нашли только множитель r_1 числа r .

Если бы нас постигла неудача, то можно было бы проверить некоторые близлежащие значения y (измеренное значение могло быть близко к диапазону $-r/2 \leq yr(modN) \leq r/2$ но, фактически, не внутри его), или можно было бы пробовать несколько множителей r (если значение $\texttt{НОД}(k; r) \neq 1$, то, наверное, является небольшим). В случае неудачи, мы прибегаем к повторению квантовой цепи, получая новое значение k'.

Оценим вероятность того, что случайно выбранные k и k' являются взаимно простыми. Так как простое число p делит только $1/p$ часть всех чисел, то вероятность того, что p делит

одновременно и k, и k' равна $1/p^2$. Оба числа k и k' взаимно просты тогда и только тогда, когда не существует никакого простого p, на которое они оба делятся. Поэтому,

$$Prob(\texttt{НОД}(k;k')=1)=\prod_{\substack{\texttt{простые}\\ p}}\left(1-\frac{1}{p^2}\right)=\frac{1}{\varsigma(2)}=\frac{6}{\pi^2}\simeq .607,$$

где $\varsigma(z)$ обозначает Риманову дзета-функцию. Поэтому, у нас, наверное, получится найти период r после некоторого постоянного (независимого от N) количества повторений алгоритма.

От FFT до QFT. Преобразование Фурье:

$$\sum_x f(x)|x\rangle \longrightarrow \sum_y \left(\frac{1}{\sqrt{N}}\sum_x e^{2\pi ixy/N} f(x)\right)|y\rangle,$$

является умножением на унитарную матрицу $N\times N$, у которой элемент $(x;y)$ — это $(e^{2\pi i/N})^{xy}$. Очевидно, оно требует порядка N^2 элементарных операций. Но существует хорошо известная и очень полезная (классическая) процедура, которая приводит порядок числа операций к $N\log N$. Принимая $N=2^n$, представим x и y как бинарные разложения

$$x = x_{n-1}\cdot 2^{n-1}+x_{n-2}\cdot 2^{n-2}+...+x_1\cdot 2+x_0,$$

$$y = y_{n-1}\cdot 2^{n-1}+y_{n-2}\cdot 2^{n-2}+...+y_1\cdot 2+y_0.$$

В произведении x и y можно отказаться от любых членов, содержащих n-ую или большие степени 2, поскольку они не имеют никакого значения для $e^{2\pi ixy/2^n}$. Следовательно,

$$\begin{aligned}\tfrac{xy}{2^n} \equiv\ & y_{n-1}(.x_0)+y_{n-2}(.x_1x_0)+y_{n-3}(.x_2x_1x_0)+\ldots+\\ & +y_1(.x_{n-2}x_{n-3}...x_0)+y_0(.x_{n-1}x_{n-2}...x_0),\end{aligned}\tag{3.6}$$

где множители в круглых скобках — бинарные разложения; например,

$$.x_2x_1x_0=\frac{x_2}{2}+\frac{x_1}{2^2}+\frac{x_0}{2^3}.$$

Теперь для каждого из N значений x можно вычислить

$$\tilde{f}(x) = \frac{1}{\sqrt{N}} \sum_y e^{2\pi i x y/N} f(y),$$

причем суммирование по y может быть выполнено последовательно за время порядка n.

Используя квантовый параллелизм, процедура может быть осуществлена гораздо эффективнее. Из (3.6) получаем

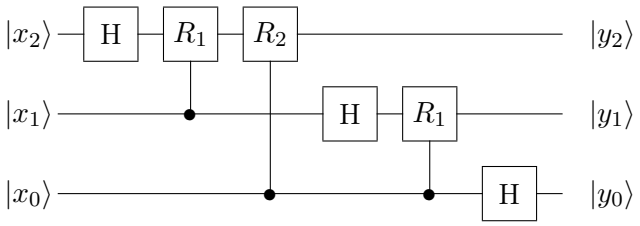
$$QFT : |x\rangle \longrightarrow \frac{1}{\sqrt{N}} \sum_y e^{2\pi i x y/N} |y\rangle =$$

$$= \frac{1}{\sqrt{2^n}} (|0\rangle + e^{2\pi i (.x_0)} |1\rangle) \otimes (|0\rangle + e^{2\pi i (.x_1 x_0)} |1\rangle) \otimes \ldots$$

$$\ldots \otimes (|0\rangle + e^{2\pi i (.x_{n-1} x_{n-2} \ldots x_0)} |1\rangle).$$

QFT приводит состояние каждого вычислительного базиса к несвязанному состоянию n-кубитов. По крайней мере, мы ожидаем, что это может быть эффективно осуществлено.

Действительно, давайте рассмотрим случай $n = 3$. Мы видим, что цепь



выполняет свое предназначение (но заметим, что порядок битов в выводе реверсирован).

Каждая модифицированная схема Адамара действует следующим образом

$$H : |x_k\rangle \longrightarrow \frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i (.x_k)} |1\rangle \right).$$

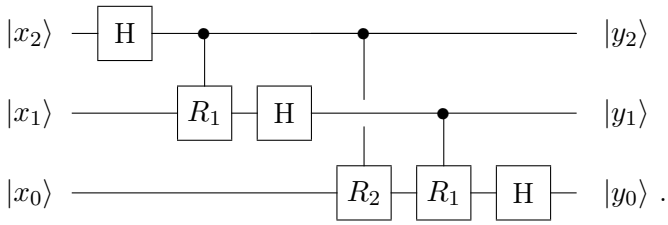
Другие вклады в относительную фазу $|0\rangle$ и $|1\rangle$ в k-ом кубите вносятся двухкубитовыми условными поворотами, где

$$R_d = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2^d} \end{pmatrix} \tag{3.7}$$

и $d = (k - j)$ — "расстояние" между кубитами.

В случае $n = 3$ QFT создается из трех H-схем и трех управляемых R_d-схем. Для общего случая n очевидное обобщение этой цепи требует n H-схем и $\binom{n}{2} = \frac{1}{2}n(n-1)$ управляемых R_d-схем. Двухкубитовые управляемые R_d-схемы применяются ко всем парам кубитов с управляемой относительной фазой $\pi/2^d$, в которой d — "расстояние" между кубитами. Таким образом семейство цепи, которое осуществляет QFT, имеет размер порядка $(\log N)^2$.

Фактически, если мы собираемся измерять в вычислительном базисе сразу же после осуществления QFT (или его инверсии), то возможно дальнейшее упрощение — двухкубитовые схемы не нужны вообще! Сначала заметим, что управляемая R_d-схема действует симметрично на эти два кубита — она действует тривиально на $|00\rangle, |01\rangle$ и $|10\rangle$, и изменяет фазу $|11\rangle$ на $e^{i\theta_d}$. Таким образом мы можем обмениваться "управляющими" и "получающими" битами без изменения схемы. С этим изменением, наша цепь для QFT с тремя кубитами может быть повторно представлена:



Как только мы измерили $|y_0\rangle$, мы узнали значение управ-

ляющего бита в управляемой R_1-схеме, которая действовала на первые два кубита. Поэтому, мы получим то же самое вероятностное распределение результатов измерения, если вместо применения управляемой R_1-схемы и затем измерения, мы сначала измерим y_0, а затем применим $(R_1)^{y_0}$ к следующему кубиту, обусловленному результатом измерения первого кубита. Точно так же после того, как значения y_1 и y_0 были измерены, мы можем заменить управляемую R_1 и управляемую R_2-схемы, действующие на третий кубит, поворотом одного кубита

$$(R_2)^{y_0}(R_1)^{y_1},$$

(поворот с относительной фазой $\pi(.y_1y_0)$).

В целом, если мы собираемся измерять после выполнения QFT, тогда только n схем Адамара и $n-1$ поворот одного кубита необходимы для осуществления QFT.

3.2. Решение диофантовых уравнений

На втором Международном конгрессе математиков в Париже Давид Гильберт сделал свой знаменитый доклад "Математические проблемы", содержащий 23 проблемы или, точнее, 23 группы родственных проблем. Проблема номер десять была посвящена диофантовым уравнениям:

Пусть задано диофантовое уравнение $D(x_1, \ldots, x_n) = 0$, где D — некоторый многочлен от n переменных с целыми числовыми коэффициентами. Указать способ, при помощи которого после конечного числа операций возможно установить: разрешимо ли это уравнение в целых числах.

Неразрешимость десятой проблемы Гильберта при помощи классической машины Тьюринга была показана Ю. В. Матиясевичем в 1970 году [12].

3.2.1. Квантовый гармонический осциллятор

Исследование гармонического осциллятора имеет большое значение в квантовой теории, так как гамильтонианы такого типа встречаются во всех задачах, где имеют место квантованные колебания: мы находим его в квантовой электродинамике и квантовой теории поля, в теории молекулярных и кристаллических колебаний. С другой стороны, проблемы, относящиеся к гармоническому осциллятору, служат прекрасной иллюстрацией основных принципов и формализма квантовой теории. Поэтому вполне оправдано подробное изучение этой задачи.

Квантовая задача формулируется как задача об одномерной частице с массой m и гамильтонианом

$$\mathbf{H} = (p^2 + m^2\omega^2 q^2)/2m,$$

причем переменные положения q и импульса p связаны соотношением коммутации

$$[q, p] = i\hbar.$$

Чтобы не загромождать вычисления постоянными, положим

$$\mathbf{H} = H\hbar\omega, \quad q = (\frac{\hbar}{m\omega})^{1/2}Q, \quad p = (m\hbar\omega)^{1/2}P.$$

Тогда гамильтониан осциллятора принимает вид:

$$H = (P^2 + Q^2)/2,$$

где эрмитовы операторы P и Q удовлетворяют коммутационному соотношению $[Q, P] = i$.

Введем операторы a и $a^\dagger$ по правилу:

$$a = \frac{1}{\sqrt{2}}(Q + iP), \qquad a^\dagger = \frac{1}{\sqrt{2}}(Q - iP).$$

Соответствующее обратное преобразование есть:

$$Q = \frac{1}{\sqrt{2}}(a + a^\dagger), \qquad P = \frac{1}{i\sqrt{2}}(a - a^\dagger).$$

Следовательно, операторы a и $a^\dagger$ удовлетворяют коммутационному соотношению

$$[a, a^\dagger] = 1, \quad [a, a] = [a^\dagger, a^\dagger] = 0,$$

и для гамильтониана получаем $H = \frac{1}{2}(aa^\dagger + a^\dagger a)$. Если положить $N = a^\dagger a$, тогда $H = N + 1/2$.

Спектр собственных значений оператора N образован последовательностью целых неотрицательных чисел. Последовательность собственных векторов, принадлежащих каждый одному из значений спектра, получается повторным действием операторов a и $a^\dagger$ на один из этих векторов. Оператор N образует сам по себе полный набор коммутирующих наблюдаемых и ни одно из его собственных значений не может быть вырождено. В результате находим последовательность ортонормированных векторов

$$|0\rangle, |1\rangle, \ldots, |n\rangle, \ldots,$$

принадлежащих, соответственно, следующим собственным значениям $N : 0, 1, \ldots, n, \ldots$. Эти вектора связаны друг с другом рекуррентными соотношениями:

$$a^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle,$$

$$a|0\rangle = 0, \quad a|n\rangle = \sqrt{n}|n-1\rangle.$$

Все они получаются из вектора $|0\rangle$ по формуле

$$|n\rangle = \frac{a^{\dagger n}}{\sqrt{n!}}|0\rangle$$

и удовлетворяют уравнению на собственные значения

$$N|n\rangle = n|n\rangle.$$

Операторы N, a и $a^\dagger$ имеют определенный физический смысл. Ввиду того, что уровни энергии эквидистантны с промежутком $\hbar\omega$, то можно рассматривать $\mathbf{H}$ как гамильтониан системы тождественных частиц, находящихся в одном энергетическом состоянии $\hbar\omega$, число которых N может изменяться так, что каждое собственное состояние $\mathbf{H}$ соответствует определенному значению N и, следовательно, определенному значению полной энергии. Тогда вектор $|n\rangle$ представляет состояние, в котором присутствует n частиц, вектор $|0\rangle$ представляет состояние без частиц (вакуум). При переходе от состояния $|n\rangle$ к состоянию $|n+1\rangle$ число частиц увеличивается на единицу, а полная энергия системы возрастает на величину $\hbar\omega$. Согласно этой интерпретации оператор N представляет число частиц, и его собственные значения суть целые числа от 0 до $+\infty$. Оператор $a^\dagger$ преобразует состояние с n частицами в состояние с $(n+1)$ частицей: $a^\dagger$ есть оператор рождения. Оператор a наоборот уменьшает на единицу число присутствующих частиц: a есть оператор уничтожения.

Рассмотрим задачу на собственные значения и состояния оператора a :

$$a|\alpha\rangle = \alpha|\alpha\rangle.$$

Здесь $\alpha-$ любое, в общем случае, комплексное число. Состояние $|\alpha\rangle$ имеет очень важное свойство: $|\alpha\rangle$ — это основное состояние осциллятора, в котором минимизируется соотношение неопределенностей. Такое состояние называется когерентным. Разложение состояния $|\alpha\rangle$ по известным состояниям гармонического осциллятора имеет следующий вид:

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_n \frac{\alpha^n}{\sqrt{n!}}|n\rangle.$$

Система когерентных состояний $|\alpha\rangle$ неортогональна, но полна.

3.2.2. Квантовые адиабатические вычисления

Если система замкнута, то ее гамильтониан от времени явно не зависит. Если система испытывает внешнее воздействие, то гамильтониан зависит от времени. Часто возникают задачи определения изменения состояния системы, учитывая внешние воздействия. Как правило, получаемые результаты существенно зависят от времени T, в течение которого происходило изменение гамильтониана. Рассмотрим предельные случаи, когда T очень мало (мгновенное изменение) и очень велико (адиабатическое изменение).

В случае бесконечно быстрого (или мгновенного) перехода динамическое состояние системы остается неизменным.

В случае бесконечно медленного (или адиабатического) перехода система, первоначально находившаяся в собственном состоянии начального гамильтониана, в конечный момент времени перейдет в собственное состояние конечного гамильтониана, которое получается из исходного состояния по непрерывности, если выполняются некоторые сформулированные ниже условия. Этот важный результат известен как адиабатическая теорема [14]. Эта теорема применяется для исследования модели квантовых вычислений, использующих основное состояние. На практике время T конечно и удовлетворяет условию

$$T \gg \frac{\max_{0\leq t\leq T} |\langle e(t)|H(T) - H(0)|g(t)\rangle|}{\min_{0\leq t\leq T}(E_e(t) - E_g(t))^2},$$

в котором $|g(t)\rangle$ и $|e(t)\rangle$ соответственно мгновенное основное состояние и первое возбужденное состояние с мгновенными собственными значениями $E_g(t), E_e(t)$.

Рассмотрим предложенную в [35] квантовую адиабатическую эволюцию. Динамика квантовой системы описывается уравнением Шредингера

$$i\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle.$$

Адиабатическая теорема утверждает, как может происходить эволюция системы в случае медленно изменяющегося гамильтониана $H(t)$. Для гамильтониана $\tilde{H}(s),\ 0 \leq s \leq 1$:

$$H(t) = \tilde{H}(t/T),$$

определим мгновенное собственное состояние и собственное значение гамильтониана следующим образом

$$\tilde{H}(s)|l;s\rangle = E_l(s)|l;s\rangle,$$

где

$$E_0(s) \leq E_1(s) \leq \cdots \leq E_{N-1}(s)$$

и N — размерность гильбертового пространства. Предположим, что $|\psi(0)\rangle$ основное состояние гамильтониана $\tilde{H}(0)$, т. е.

$$|\psi(0)\rangle = |l=0;s=0\rangle.$$

Согласно адиабатической теореме, если промежуток между двумя наименьшими уровнями энергии: $E_1(s)-E_0(s)$, строго больше нуля для всех $0 \leq s \leq 1$, то

$$\lim_{T\to\infty} |\langle l=0;s=1|\psi(T)\rangle| = 1.$$

Это означает, что существование ненулевого промежутка между энергетическими уровнями гарантирует близость $|\psi(T)\rangle$, отвечающего уравнению Шредингера, мгновенному основному состоянию гамильтониана $H(t) = \tilde{H}(t/T)$ для всех t от 0 до T, если T достаточно велико. Определим минимальный промежуток:

$$g_{min} = \min_{0\leq s\leq 1}(E_1(s) - E_0(s)).$$

Если взять время

$$T \gg \frac{\max_{0\leq s\leq 1} |\langle l=1;s|\frac{d\tilde{H}}{ds}|l=0;s\rangle|}{g_{min}^2},$$

то по адиабатической теореме можно получить очень близкое к единице значение величины $|\langle l = 0; s = 1|\psi(T)\rangle|$. Таким образом величина T управляется величиной g_{min}^{-2}.

Воспользуемся квантовой адиабатической эволюцией для того, чтобы прийти из основного состояния известного гамильтониана H_I к неизвестному основному состоянию гамильтониана H_P. Пусть

$$H(t) = (1 - t/T)H_I + (t/T)H_P,$$

и тогда

$$\tilde{H}(s) = (1 - s)H_I + sH_P.$$

Приготовим систему так, чтобы в начальный момент времени $t = 0$ она находилась в основном состоянии гамильтониана $H(0) = H_I$. Согласно адиабатической теореме, если g_{min} не нуль, то для достаточно большого T состояние $|\psi(T)\rangle$ будет очень близко к основному состоянию гамильтониана H_P.

Решение диофантовых уравнений. В статье Т. Д. Кью [44] был описан квантовый адиабатический алгоритм для решения диофантовых уравнений.

Заметим, что достаточно рассматривать задачу о наличии только неотрицательных целых решений диофантовых уравнений, так как общая проблема к ней сводится.

Рассмотрим пример:

$$(x + 1)^3 + (y + 1)^3 - (z + 1)^3 + cxyz = 0,\ c \in Z,$$

с неизвестными x, y, z. Для нахождения неотрицательных целых решений этого уравнения с помощью квантового алгоритма, требуется реализация пространства Фока, построенного в "вакууме" из состояния $|0\rangle$ повторяющимся применением операторов рождения $a_x^\dagger, a_y^\dagger, a_z^\dagger$ подобно простому гармоническому осциллятору. Соотношения коммутации выглядят следующим образом:

$$[a_j, a_j^\dagger] = 1, \text{ для } j = x, y, z, \quad [a_k, a_j] = [a_k, a_j^\dagger] = 0, \text{ для } j \neq k.$$

Построим гамильтониан, соответствующий заданному диофантовому уравнению: $H_P =$

$$= ((a_x^\dagger a_x + 1)^3 + (a_y^\dagger a_y + 1)^3 - (a_z^\dagger a_z + 1)^3 + c(a_x^\dagger a_x)(a_y^\dagger a_y)(a_z^\dagger a_z))^2.$$

Операторы $N_j = a_j^\dagger a_j$ имеют только неотрицательные целые собственные значения n_j и коммутируют по правилу

$$[N_j, H_P] = 0 = [N_i, N_j].$$

Следовательно, эти наблюдаемые совместимы и одновременно измеримы. Основное состояние $|g\rangle$ построенного таким методом гамильтониана имеет следующие свойства:

$$N_j|g\rangle = n_j|g\rangle,$$

$$H_P|g\rangle = ((n_x+1)^3 + (n_y+1)^3 - (n_z+1)^3 + cn_x n_y n_z)^2|g\rangle \equiv E_g|g\rangle,$$

для некоторых n_x, n_y, n_z.

Итак, проективное измерение энергии E_g основного состояния $|g\rangle$ будет давать ответ на поставленную задачу: диофантовое уравнение имеет хотя бы одно целое решение тогда и только тогда, когда $E_g = 0$, и не имеет решений в противном случае.

Если есть единственное решение, то проективное измерение наблюдаемых, соответствующих операторам N_j, будет определять значения различных переменных. Если есть множество решений, конечное или бесконечное (например, как в случае теоремы Пифагора $x^2 + y^2 - z^2 = 0$), то основное состояние $|g\rangle$ будет линейной суперпозицией состояний $|n_x\rangle \otimes |n_y\rangle \otimes |n_z\rangle$, где n_x, n_y, n_x — решения. В таком случае измерение может не дать все решения. Однако нахождение всех решений не является нашей целью.

Измерение N_j для основного состояния будет всегда давать результат в виде некоторых значений n_x, n_y, n_z и непосредственная их подстановка будет показывать, имеет уравнение решение или нет.

Квантовый алгоритм с оракулом основного состояния можно записать так:

1. Возьмем диофантовое уравнение с k неизвестными x_j :

$$D(x_1, ..., x_k) = 0.$$

Для этого уравнения построим соответствующий квантовый гамильтониан в некотором подходящем пространстве Фока:

$$H_P = (D(a_1^\dagger a_1, ..., a_k^\dagger a_k))^2.$$

2. Если основное состояние будет получено с высокой вероятностью и будет однозначно определено, что именно это состояние является основным, то измерение соответствующих наблюдаемых даст решение задачи.

Вместо поиска нулей многочлена $D(x_1, ..., x_k)$, которых может и не существовать, будем искать глобальный минимум его квадрата

$$0 \leqslant min(D(x_1, ..., x_k))^2 \leqslant (D(0, ..., 0))^2,$$

который существует и конечен [44].

В классическом случае даже если глобальный минимум был бы обнаружен, то в общем случае нельзя сказать, что именно он и есть глобальный минимум (исключая нуль диофантового уравнения). Используя понятия только математической логики, мы должны будем продолжать сравнивать это значение с другими значениями из оставшейся непросмотренной бесконечной области определения, но оказывается, что мы не можем закончить это сравнение за конечное время — это и есть понятие математической невычислимости. В квантовом случае, глобальный минимум закодирован в основном состоянии некоторого гамильтониана. Измеряя энергию, глобальный минимум может быть найден за конечное время и будет ясно, что это и есть глобальный минимум, если только это будет основное состояние, которое получено в конце вычислений.

Способ построения гамильтониана. Рассмотрим эрмитовы операторы

$$X_j = \frac{1}{\sqrt{2}}(a_j + a_j^\dagger),\ P_j = \frac{i}{\sqrt{2}}(a_j - a_j^\dagger),\ [P_j, X_k] = i\delta_{jk},$$

в которых $j = 1, \ldots, k$ — индексы неизвестных в диофантовом уравнении.

Вместе с наличием фундаментальных гамильтонианов

$$X_j, P_j, (X_j^2 + P_j^2), \pm(X_k P_j + P_j X_k), (X_j^2 + P_j^2)^2$$

можно построить унитарные временные процессы, соответствующие гамильтонианам произвольных эрмитовых полиномов в представлении $\{X_j, P_j\}$ (следовательно, и в представлении $\{a_j^\dagger a_j\}$) с произвольной степенью точности. С построением полиномиального гамильтониана нам следует получить его основное состояние. Для этого будет достаточно воспользоваться любым приближением. Один из способов — применение метода квантовых адиабатических вычислений [35]. Другой способ — возможность использовать алгоритм квантового отжига (или охлаждения) [42].

В адиабатическом подходе к решению задачи вычисление начинается с гамильтониана H_I, чье основное состояние $|g_I\rangle$ легко получаемо. Затем формируем медленно изменяющийся гамильтониан $H(s), s = t/T$, который интерполируется между H_I и H_P в интервале $t \in [0, T]:\ H(s) = (1 - s)H_I + sH_P$.

Отметим, что линейную интерполяцию можно заменить на некоторую нелинейную, обеспечивающую условия выполнения адиабатической теоремы. Согласно этой теореме, начальное основное состояние перейдет в наше ожидаемое основное состояние $|g\rangle$ до фазы:

$$\lim_{T\to\infty} \mathbf{T} exp\{-iT \int_0^1 H(\tau) d\tau\} |g_I\rangle = e^{i\phi}|g\rangle, \tag{3.8}$$

где $\mathbf{T}$ — хронологический оператор.

Пусть $|g(t)\rangle$ и $|e(t)\rangle$ соответственно мгновенное основное состояние и первое возбужденное состояние интерполяционного гамильтониана с мгновенными собственными значениями $E_g(t), E_e(t)$. Если обозначить

$$\|H_I - H_P\| \equiv \max_{0\leq t\leq T} |\langle e(t)|(H_I - H_P)|g(t)\rangle|$$

и

$$g \equiv \min_{0\leq t\leq T} (E_e(t) - E_g(t)),$$

то для интерполяционного гамильтониана оценка времени T, после которого система останется с высокой вероятностью в основном состоянии это

$$T \gg \frac{\|H_I - H_P\|}{g^2}.$$

Для $N\Delta\tau = 1$ и $\Delta\tau\|H_I - H_P\| \ll 1$ зависящий от времени оператор в левой части (3.8) может быть приближен как

$$exp\{-iTH(\tau_N)\Delta\tau\} \cdots exp\{-iTH(\tau_1)\Delta\tau\}.$$

Заметим, что определенная здесь "норма" $\|\cdot\|$ может использоваться для различных гамильтонианов. Она удобна в вычислениях еще и тем, что использует только низшие энергетические состояния интерполированного гамильтониана.

В каждом интервале $\Delta\tau$ унитарные операторы

$$exp\{-iH(\tau_k)T\Delta\tau\}, \;\; k = 1, ..., N,$$

могут быть выражены через подразбиение $T\Delta\tau$ на m интервалов достаточного малого размера $\delta_s : \; m\delta_s = T\Delta\tau$, следующим образом:

$$exp\{-iH(\tau_k)T\Delta\tau\} = (exp\{-iH(\tau_k)\delta_s\})^m.$$

Для каждого m правые части последней формулы могут быть промоделированы приближениями из [45], где было показано,

что число шагов m растет полиномиально в зависимости от степени исследуемого многочлена.

Итак, построение гамильтониана на временном интервале $T\Delta\tau$ может быть выполнено вполне удовлетворительно.

Адиабатический алгоритм. Для решения 10 проблемы Гильберта у нас, с одной стороны, должен быть соответствующий зависящий от времени физический (адиабатический) процесс. С другой, квантовая механика может использоваться для определения основного состояния через обычные статистические прогнозы из уравнения Шредингера для зависящего от времени гамильтониана $H(t/T)$ с конечным усеченным числом энергетических состояний. Таким образом возникает еще одна проблема: какие состояния следует включать в усеченный базис для численного исследования уравнения Шредингера.

В общем случае намного легче реализовать сам гамильтониан H_P, чем получить его основное состояние $|g\rangle$. Мы должны начать вычисления с другого и вероятно достижимого начального основного состояния $|g_I\rangle$ некоторого начального гамильтониана H_I. Потом для преобразования этого гамильтониана H_I адиабатически во времени T в гамильтониан, чье основное состояние подходит нам, выполняем интерполяционный зависящий от времени процесс $H(s) = (1-s)H_I + sH_P$ для s, изменяющегося от 0 до 1. Квантовая адиабатическая теорема утверждает, что в результате мы получим очень близкое состояние к основному состоянию $|g\rangle$ гамильтониана H_P.

При некоторых $\alpha_1, \ldots, \alpha_k$ можно начинать вычисления с известного гамильтониана

$$H_I = \sum_{i=1}^{k} (a_i^\dagger - \alpha_i^*)(a_i - \alpha_i),$$

допускающего как основное вероятно достижимое когерентное состояние $|g_I\rangle = |\alpha_1 \cdots \alpha_k\rangle$. Затем, формируем зависящий от времени гамильтониан $H(t/T)$, который интерполируется во временном интервале $t \in [0, T]$ между H_I и H_P.

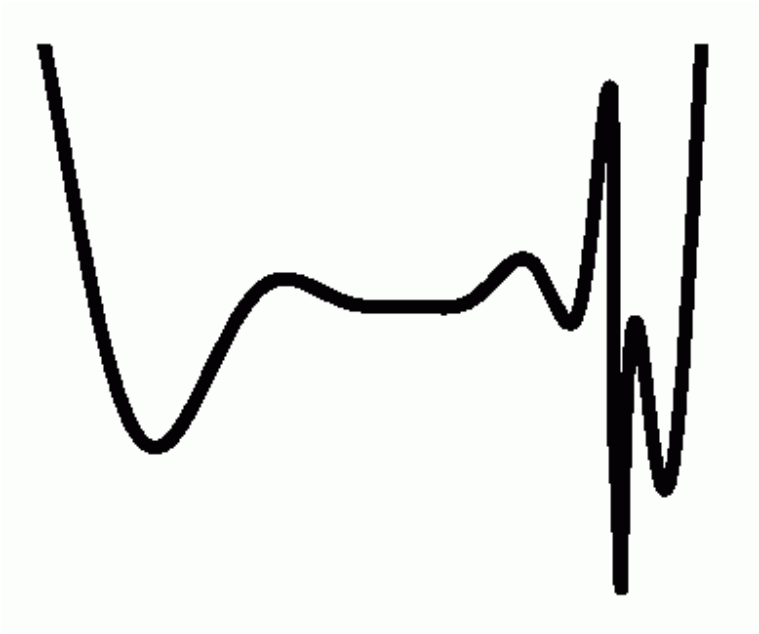


Рис. 3.1: Гамильтониан H_P.

На Рис. 3.1 приведен возможный пример гамильтониана H_P. Найти квантомеханическое основное состояние такой функции довольно-таки сложно.

Используя квантовую адиабатическую теорему, мы начнем нахождение основного состояния, приближая исследуемую функцию некоторой простой начальной функцией в момент времени $s = 0$, далее адиабатически изменяя ее до момента времени $s = 1$. На Рис. 3.2 иллюстрируется эвристический подход квантовой адиабатической теоремы для нахождения основного состояния гамильтониана H_P.

Шаг 0: Выберем длительность процесса T, вероятность P (достаточно близкую к единице) и точность $0 < \epsilon < 1$ (доста-

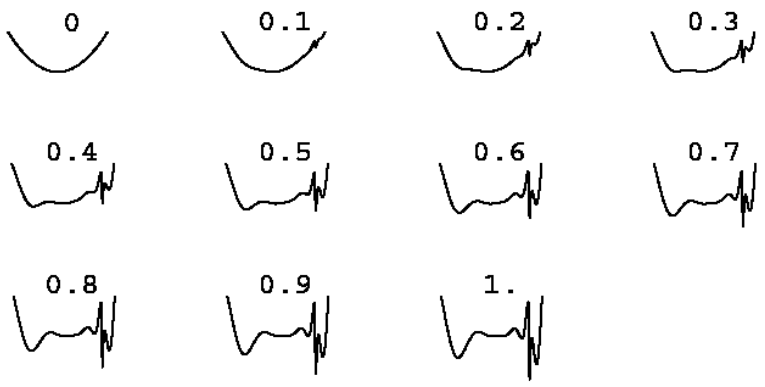


Рис. 3.2: Последовательное приближение гамильтониана H_P.

точно малую).

Шаг 1 (на физическом приборе): Выполним квантовый эволюционный процесс, который управляется зависящим от времени гамильтонианом $H(t/T)$ и останавливается после прохождения времени T. Затем, через проекционное измерение или наблюдение H_p (или множество операторов $\{N_1, \ldots, N_k\}$) мы получим некоторое состояние в форме $|\cdots n_i \cdots\rangle$, $i = 1, \ldots, k$.

Шаг 2 (на физическом приборе): Повторим физический процесс первого шага $L(\epsilon, P)$ раз для создания гистограммы частоты обнаружения всех состояний, полученных в результате измерений. Число повторений $L(\epsilon, P)$ должно гарантировать получение вероятностного распределения $\mathrm{P}(T;\epsilon)$ в момент времени T с точностью ϵ для всех измеренных состояний. Сходимость этого повторяемого процесса обеспечивается законом больших чисел теории вероятностей, из которого дополнительно следует, что реальные частоты будут отличаться от $\mathrm{P}(T;\epsilon)$ на величину большую ϵ с вероятностью $1 - P$, если количество повторений $L \geq 1/(\epsilon^2(1 - P))$. Заметим, что

достигнутое таким образом низшее энергетическое состояние $|n_c\rangle$ является кандидатом в основное состояние.

Шаг 3 (на классическом компьютере): Выберем усеченный базис из m векторов, состоящих из $|\alpha_1 \cdots \alpha_k\rangle$ и их возбужденных состояний, для последующего применения смещенных операторов рождения $b_i^\dagger \equiv (a_i^\dagger - \alpha_i^*)$ к начальному состоянию.

Шаг 4 (на классическом компьютере): Решив уравнение Шредингера в этом базисе для $\psi(T)$, с начальным состоянием $\psi(0) = |\alpha_1 \cdots \alpha_k\rangle$, получим с такой же как и на шаге 2 точностью вероятностное распределение $\mathrm{P}_{\mathrm{est}}(T; m)$ (через вычисление $|\langle\psi(T)| \cdots n_i \cdots\rangle|^2$), которое зависит от общего числа векторов M в базисе.

Шаг 5 (на классическом компьютере): Если полученные нами выше вероятностные распределения не удовлетворяют желаемой точности, т. е. $|\mathrm{P}_{\mathrm{est}}(T; m) - \mathrm{P}(T; \epsilon)| > \epsilon$, то мы расширяем наш базис, увеличив m, и возвращаемся к шагу 4.

Шаг 6 (на классическом компьютере): Если два вероятностных распределения удовлетворяют желаемой точности, т. е. $|\mathrm{P}_{\mathrm{est}}(T; m) - \mathrm{P}(T; \epsilon)| < \epsilon$, то мы используем наш усеченный базис для диагонализации H_P с целью получения приближенного основного состояния $|g'\rangle$ и его энергии $E_{g'}$ (принимая точность, которая может быть определена по ϵ).

Шаг 7 (на классическом компьютере): Оцениваем в усеченном базисе промежуток между основным состоянием и первым возбужденным состоянием. Исходя из величины этого промежутка, мы можем воспользоваться квантовой адиабатической теоремой и выбрать время T так, чтобы вероятность системы главным образом находиться в основном состоянии была бы очень близкой к единице

$$\big||\langle g'|\psi(T)\rangle|^2 - 1\big| < \epsilon.$$

Затем возвращаемся к шагу 1 с этим новым значением T, которое усилит и таким образом утвердит кандидатуру основного состояния для реального основного состояния.

Энергия $E_{g'}$, численно полученного основного состояния, приблизительно такая же, как и H_P — энергия E_c, соответствующая кандидату в основное состояние $|n_c\rangle$, полученного при измерениях,

$$E_{g'} = E_c + \delta.$$

Заметим, что E_c может быть ненулевая. С другой стороны, если она нулевая, то мы нашли решение для диофантового уравнения и можем остановить наше вычисление. Полученная в следствии усечения флуктуация δ в формуле для $E_{g'}$ может так же быть численно оценена как функция от ϵ. Нетрудно показать, что флуктуация $\delta(\epsilon)$ стремится к нулю, если ϵ стремится к нулю. Для того, чтобы $E_{g'}$ не было равно нулю, нужно выполнить условие

$$|\delta(\epsilon)| < E_c,$$

выбрав ϵ независимым способом. Отсюда (с вероятностью P) можно заключить, что $E_{g'} > 0$ и, следовательно, диафантовое уравнение не имеет решения.

Покажем, что используемый статистический подход удовлетворяет цели идентификации основного состояния. Предположим, что низшее энергетическое состояние $|n_c\rangle$ получено физически при $t = T$, но пусть оно не является на самом деле основным состоянием. После выбора усеченного базиса вычисления на классическом компьютере для того же времени эволюции T будут проходить по одному из двух различных сценариев:

1) численное вычисление покажет, что $|n_c\rangle$ не является основным состоянием в выбранном нами усеченном базисе, и мы численно обнаружим другое состояние $|g'\rangle$ с энергией меньшей, чем у $|n_c\rangle$;

2) численное вычисление покажет, что $|n_c\rangle$ на самом деле является основным состоянием в выбранном нами усеченном базисе.

В первом случае мы можем проигнорировать $|n_c\rangle$, так как оно не является основным состоянием в усеченном простран-

стве, и тем более в неусеченном. Во втором случае мы повторим физический процесс и численные вычисления, выбрав соответствующее время эволюции.

Численное решение. Рассмотрим начальный гамильтониан:

$$H_I = \sum_{i=1}^{K} (a_i^\dagger - \alpha_i^*)(a_i - \alpha_i),$$

который принимает в качестве основного состояния когерентное состояние

$$|g_I\rangle = |\alpha_1\rangle \otimes \cdots \otimes |\alpha_k\rangle, \text{ где } \quad |\alpha_i\rangle = e^{-\frac{1}{2}|\alpha_i|^2} \sum_{n=0}^{\infty} \frac{\alpha_i^n}{\sqrt{n!}} |n\rangle.$$

Надо решить зависящее от времени уравнение Шредингера для $t \in [0, T]$

$$i\partial_t \psi(t) = H(t/T)\psi(t), t \in [0, T],$$

с начальным состоянием, являющимся когерентным.

Аналитически можно в общем показать два наиболее важных результата:

1. Основное состояние для $H(t/T)$ является невырожденным для $t \in [0, T]$. Так как промежуток минимума энергии между основным состоянием и первым возбужденным состоянием отличен от нуля, то для адиабатического процесса требуется конечное время T, обеспечивающееся квантовой адиабатической теоремой, для получения состояния, которое с очень высокой вероятностью будет основным состоянием для H_P.

2. В момент времени T вероятность оказаться в некотором состоянии $|\langle\psi(T)|n_0\rangle|^2$ больше чем $1/2$ тогда и только тогда, когда $|n_0\rangle$ основное состояние для H_P. Т. о. нам нужно решить только уравнение для увеличивающегося T, пока большинство условий не станут удовлетворять условиям для определения нужного основного состояния.

Вычисления. 1). Решим численно уравнение Шредингера в некотором конечном пространстве Фока размерностью достаточной для аппроксимации начального когерентного состояния с произвольно заданной точностью. Т. е. m выберем так, чтобы для

$$|\alpha_i; m\rangle = e^{-\frac{1}{2}|\alpha_i|^2} \sum_{n=0}^{m} \frac{\alpha_i^n}{\sqrt{n!}} |n\rangle$$

и некоторого выбранного ϵ выполнялось условие на норму

$$|1 - \sqrt{\langle \alpha_i; m | \alpha_i; m \rangle}| \leq \epsilon.$$

2). На каждом интервале δt с точностью $O(\delta t^2)$ имеем

$$\psi(t + \delta t) = e^{-iH(\frac{t}{T})\delta t}\psi(t) = \left(1 - iH(\frac{t}{T})\delta t - \frac{1}{2}H^2(\frac{t}{T})\delta t^2\right)\psi(t),$$

т. о. максимально возможно только два порождающих оператора $a_i^\dagger a_j^\dagger$, и мы можем использовать этот факт для исследования бесконечного пространства Фока, увеличивая усеченное значение размерности пространства Фока вдвое на каждом временном шаге.

3). Применим унитарное вычисление:

$$\psi(t + \delta t) = \frac{1 - \frac{i}{2}H(t/T)\delta t}{1 + \frac{i}{2}H(t/T)\delta t}\psi(t),$$

которое аппроксимирует $e^{-iH(\frac{t}{T})\delta t}$ до второго порядка от δt методом сопряженных градиентов. Это вычисление, будучи унитарным, сохраняет норму вектора состояния даже если размер пространства Фока будет по необходимости увеличен.

4). Временной шаг δt в момент времени t — это функция времени, при этом шаг выбирается таким способом, что деление $\delta t(t)$ пополам дает верные результаты с точностью $O(\delta t^2)$.

Полученные результаты обосновывают идею реализации и выполнения нашего квантового алгоритма для физического процесса:

Шаг 1. Запускаем физический процесс (соответствующий диофантовому уравнению) на некоторое время T.

Шаг 2. Повторяем процесс во времени T, для получения статистических данных с помощью измерений.

Шаг 3. Если ни один из измеренных результатов не будет получен с вероятностью более $1/2$, то увеличим T и вернемся к предыдущему шагу.

Шаг 4. В итоге, с некоторым достаточно большим T, измеренное состояние с очень высокой вероятностью может быть определено как основное состояние, завершая физический процесс и вычисления.

Шаг 5. Подстановка квантовых чисел в определенное нами основное состояние позволяет убедиться $E_g = 0$ или нет и, следовательно, сделать вывод имеет ли диофантовое уравнение решение или нет.

Итак, основным состоянием гамильтониана H_P является некоторое состояние $|n_0\rangle$, вероятность измерения которого в момент времени T, в результате эволюционного процесса с гамильтонианом $H(t/T)$ из начального состояния $|\alpha_I\rangle$, больше $1/2$. При этом $|\langle\psi(T)|n_0\rangle|^2$ больше чем $1/2$ тогда и только тогда, когда $|n_0\rangle$ основное состояние для H_P. Утверждение "тогда" следует из квантовой адиабатической теоремы, а в [44] доказана вторая часть — "и только тогда, когда". Также в [44] показано, что требуемое время T для достижения искомого основного состояния конечно. Последнее утверждение остается наиболее спорным, многие исследователи считают его не достаточно доказанным. Если все-таки можно было бы принять это утверждение, то из него следовало бы, что алгоритм остановится за конечное время.

3.3. Минимизация функционала среднего риска

Рассмотрим задачу минимизации функции

$$f(x) = \mathrm{E}_w\{F(w, x)\}$$

(типа функционала среднего риска), зависящей от векторного q-мерного аргумента x. Предположим, что w — случайный вектор и $\mathrm{E}_w\{\cdot\}$ — операция усреднения по его распределению.

Пусть $f(\cdot)$ — непрерывно дифференцируемая функция.

Необходимым условием того, что θ — точка минимума функции $f(\cdot)$, является равенство нулю в этой точке ее вектор-градиента $\nabla f(\theta) = 0$.

Предположим, что известны значения вектор-градиента функции $f(\cdot)$ и матицы ее вторых производных (гессиана). Для нахождения точки минимума можно воспользоваться классической схемой вычислений по методу Ньютона:

$$\hat{\theta}_k = \hat{\theta}_{k-1} - [\nabla^2 f(\hat{\theta}_{k-1})]^{-1} \nabla f(\hat{\theta}_{k-1}),$$

где $n = 1, 2, \ldots$. Если матрица-гессиан $\nabla^2 f(\hat{\theta}_{k-1})$ в некоторой окрестности точки θ задает положительный ограниченный оператор и начальное значение $\hat{\theta}_0$ выбрано достаточно близко к точке локального минимума θ, то последовательность оценок $\{\hat{\theta}_k\}$ сходится к θ. Недостатком этого алгоритма является необходимость обращать матрицу-гессиан на каждом шаге, что может представлять собой определенную трудность при большой размерности. В некоторых случаях удается выбрать рекуррентный способ для пересчета матриц, обратных к гессиану. Для упрощения алгоритма их иногда обоснованно заменяют на положительные числа α_k, получая в результате алгоритм типа стохастической аппроксимации.

Если значения градиента функции $f(\cdot)$ неизвестны, то стандартным подходом к решению задачи является использование конечных разностей для аппроксимации градиента.

Пусть $\{\beta_k\}$ — некоторая последовательность положительных чисел. Обозначим через e_i стандартный единичный вектор в направлении i-й координаты. В качестве аппроксимации i-й компоненты вектор-градиента можно использовать

$$\nabla f(\hat{\theta}_{k-1})^{(i)} \approx \frac{f(\hat{\theta}_{k-1} + \beta_k e_i) - f(\hat{\theta}_{k-1} - \beta_k e_i)}{2\beta_k}.$$

Отметим, что этот стандартный подход к аппроксимации вектор-градиента требует на каждом шаге алгоритма оценивания произвести $2q$ измерений значений минимизируемой функции при размерности искомого минимизирующего вектора, равной q.

3.3.1. Процедура Кифера–Вольфовица

Как поступить, если нельзя использовать в алгоритме не только градиент функции $f(\cdot)$, но и ее точные значения? Такая проблема возникает, если вид функций $f(\cdot)$ и $F(\cdot,\cdot)$ известен не полностью либо если на вычисление соответствующих значений затрачивается чрезмерное количество усилий при дороговизне экспериментов или большой размерности вектора неизвестных параметров. Более того, в задачах оптимизации достаточно часто можно воспользоваться только зашумленной информацией о значениях функции $F(w,x)$ в выбираемых точках x с неконтролируемыми при этом значениями случайной величины w.

Дж. Кифер с Дж. Вольфовицем [43] при $q = 1$ и Дж. Блюм в многомерном случае для построения последовательности оценок предложили использовать процедуру следующего вида:

$$\hat{\theta}_k = \hat{\theta}_{k-1} - \alpha_k \frac{Y_k^+ - Y_k^-}{2\beta_k},$$

с некоторыми выбираемыми пользователем последовательностями положительных чисел $\{\alpha_k\}$ и $\{\beta_k\}$, стремящимися к нулю при $k \to \infty$. Они обосновали состоятельность оценок при

определенных предположениях о распределениях соответствующих случайных величин, свойствах функции $F(\cdot,\cdot)$ и числовых последовательностей $\{\alpha_k\}$ и $\{\beta_k\}$. Выше было использовано обозначение:

$$Y_k^{\pm} = \begin{pmatrix} F\Big(w_{2q(k-1)+\frac{3\pm1}{2}}, \hat{\theta}_{k-1} \pm \beta_k e_1\Big) \\ F\Big(w_{2q(k-1)+\frac{7\pm1}{2}}, \hat{\theta}_{k-1} \pm \beta_k e_2\Big) \\ \vdots \\ F\Big(w_{2qk-\frac{1\pm1}{2}}, \quad \hat{\theta}_{k-1} \pm \beta_k e_q\Big) \end{pmatrix}.$$

Из накладываемых условий обычно следует, что в среднем по всевозможным реализациям w значение $(Y_k^+ - Y_k^-)/(2\beta_k)$ совпадает со значением градиента функции $f(\cdot)$ в точке $\hat{\theta}_{k-1}$, и асимптотическое поведение оценок, получаемых с помощью процедуры Кифера–Вольфовица, характеризуется свойствами решений системы обыкновенных дифференциальных уравнений (ОДУ):

$$\dot{\theta} = -\nabla f(\theta).$$

В более широком смысле алгоритмы такого типа принято называть *псевдоградиентными*. При внешней простоте, оригинальная процедура Кифера–Вольфовица имеет ряд существенных недостатков. Для доказательства состоятельности оценок приходится накладывать достаточно ограничительные условия на неконтролируемые возмущения; при измерениях значений функции с почти произвольными помехами (см. [5]) состоятельность оценок не получается; и даже в тех случаях, когда ограничениями на неконтролируемые возмущения и помехи в наблюдении можно пренебречь, на каждом шаге алгоритма приходится делать $2q$ наблюдений, что в многомерном случае при большом q может оказаться трудно осуществимым.

3.3.2. Рандомизированные алгоритмы стохастической аппроксимации

Классическую процедуру Кифера–Вольфовица (КВ) в последнее время часто называют *алгоритмом стохастической аппроксимации с фиксированными направлениями*. Существенно улучшить характеристики ее оценок позволяет включение одновременно в канал наблюдения, через выбираемый параметр, и в направление вектора изменения очередной оценки так называемого *пробного одновременного возмущения*. В отличие от классической процедуры Кифера–Вольфовица при выборе очередной точки измерения функции случайному возмущению подвергаются одновременно все координаты.

Пусть $\{\Delta_k\}$ — последовательность наблюдаемых, одинаково симметрично распределенных случайных векторов с матрицами ковариаций

$$\operatorname{cov}\{\Delta_k \Delta_j^{\mathrm{T}}\} = \delta_{kj}\, \sigma_\Delta^2 \mathrm{I},$$

где $\sigma_\Delta > 0$, и ограниченным вторым статистическим моментом. Например, для задания пробного одновременного возмущения удобно использовать независимые бернуллиевские случайные векторы (координаты вектора Δ_k не зависят друг от друга и принимают с равной вероятностью значения плюс/минус единица). Оказывается, что при зашумленных наблюдениях без существенных потерь в скорости сходимости для построения состоятельной последовательности оценок можно воспользоваться алгоритмом, похожим внешне на классическую процедуру Кифера–Вольфовица, но использующим всего два зашумленных измерения функции $F(\cdot,\cdot)$ на каждой итерации:

$$\hat\theta_k = \hat\theta_{k-1} - \alpha_k \Delta_k \frac{y_k^+ - y_k^-}{2\beta_k}, \qquad y_k^\pm = F(w_k^\pm, \hat\theta_{k-1} \pm \beta_k \Delta_k) + v_k^\pm.$$

Более того, аналогичными свойствами обладает алгоритм с

одним зашумленным наблюдением на каждой итерации:

$$\hat{\theta}_k = \hat{\theta}_{k-1} - \frac{\alpha_k}{\beta_k}\Delta_k y_k, \qquad y_k = F(w_k, \hat{\theta}_{k-1} + \beta_k\Delta_k) + v_k.$$

Эти рекуррентные процедуры называются *рандомизированными алгоритмами стохастической аппроксимации*, так как в их структуру неотъемлемой частью входит случайное пробное одновременное по всем координатам возмущение, которое также одновременно используется и в задании направления очередного изменения оценки и при выборе новой точки измерения. Иногда встречаются названия *стохастическая аппроксимация со случайными направлениями, поисковый алгоритм стохастической аппроксимации* или *стохастическая аппроксимация с возмущением на входе*. В англоязычной литературе широко используется название *одновременно возмущаемая стохастическая аппроксимация* ("simultaneous perturbation stochastic approximation", SPSA).

В [4, 5, 6, 16, 26, 62] приведены точные условия, обеспечивающие состоятельность оценок рандомизированных алгоритмов стохастической аппроксимации, из которых наиболее существенным является условие о слабой коррелированности пробного возмущения $\{\Delta_k\}$ и последовательностей неопределенностей $\{w_k\}$ и $\{v_k\}$. Естественно, что среднеквадратичная скорость сходимости первого рандомизированного алгоритма с двумя измерениями обычно выше, чем у второго. Но стоит заметить, что в целом ряде практических задач оптимизации систем реального времени, обнаружения сигналов и адаптивного управления важно иметь возможность использовать алгоритм только с одним наблюдением на каждом шаге, так как в этих задачах трудно сделать не только $2q$ наблюдений, как в классической процедуре Кифера–Вольфовица, но недоступны даже два наблюдения с независимыми от Δ_k помехами.

В отличие от оценивания по классической процедуре Кифера–Вольфовица применение рандомизированных алгоритмов эффективно и при почти произвольных аддитивных поме-

хах в наблюдении $\{v_k\}$ (см. [5]). В подтверждение этого факта в случае неизвестной, но ограниченной детерминированной последовательности помех $\{v_k\}$ остановимся здесь только на неформальном объяснении, близком к идее доказательства в работе [4].

Пусть дважды непрерывно дифференцируемая вещественная функция $f(x)$ вещественного аргумента x имеет в $\mathbb{R}$ единственный минимум в некоторой точке θ:

$$(x-\theta)\nabla f(x) \geq \mu(x-\theta)^2,\ \forall x \in \mathbb{R}$$

с некоторой постоянной $\mu > 0$, и для градиента функции выполнено условие Липшица:

$$\|\nabla f(x) - \nabla f(\theta)\| \leq A\|x-\theta\|,\ \forall x, \theta \in \mathbb{R}$$

с некоторой постоянной A. Выберем пробное одновременное возмущение Δ_k принимающим с равной вероятностью значения плюс/минус единица независимо от v_k.

Рассмотрим последовательность оценок $\{\hat{\theta}_k\}$, формируемых по рандомизированному алгоритму стохастической аппроксимации с одним измерением. Обозначим $D_k = (\hat{\theta}_k - \theta)^2$ и, учитывая центрированности Δ_k и независимость Δ_k от v_k, оценим условное математическое ожидание:

$$\mathrm{E}\{D_k|\hat{\theta}_i, i<k\} \leq D_{k-1} - \frac{\alpha_k}{\beta_k}(\hat{\theta}_{k-1}-\theta)\mathrm{E}\{\Delta_k y_k|\hat{\theta}_i, i<k\}+$$

$$+\frac{\alpha_k^2}{\beta_k^2}\mathrm{E}\{\Delta_k^2 y_k^2|\hat{\theta}_i, i<k\} = D_{k-1}-$$

$$-\frac{\alpha_k}{\beta_k}(\hat{\theta}_{k-1}-\theta)\mathrm{E}\{\Delta_k f(\theta_{k-1}+\beta_k\Delta_k)|\hat{\theta}_i, i<k\}+\frac{\alpha_k^2}{\beta_k^2}\mathrm{E}\{y_k^2|\hat{\theta}_i, i<k\}.$$

Разложив значение функции $f(\hat{\theta}_{k-1}+\beta_k\Delta_k)$ по формуле Тейлора, получим

$$f(\hat{\theta}_{k-1}+\beta_k\Delta_k) = f(\hat{\theta}_{k-1}) + \beta_k\Delta_k\nabla f(\hat{\theta}_{k-1}) + \beta_k^2\zeta_k,$$

где ζ_k — некоторое число между $\hat{\theta}_{k-1}$ и $\hat{\theta}_{k-1} + \beta_k \Delta_k$ (вообще говоря, ζ_k — случайная величина). С учетом последней формулы, принимая во внимание центрированность Δ_k, выводим:

$$\mathrm{E}\{D_k|\hat{\theta}_i, i<k\} \le \Big(1+\frac{1}{2}\alpha_k\beta_k\Big)D_{k-1} - \alpha_k(\hat{\theta}_{k-1}-\theta)\nabla f(\hat{\theta}_{k-1}) + \xi_k,$$

где $\xi_k = \mathrm{E}\{\alpha_k\beta_k\zeta_k^2/2 + \alpha_k^2\beta_k^{-2}y_k^2|\hat{\theta}_i, i<k\}$. Отсюда, в силу сильной выпуклости функции $f(\cdot)$, видно, что последовательность $\{D_k\}$ — почти супермартингал:

$$\mathrm{E}\{D_k|\hat{\theta}_i, i<k\} \le (1-\gamma_k)D_{k-1} + \xi_k,$$

где $\gamma_k = \mu\alpha_k - \alpha_k\beta_k/2$. Если предположить, что для числовых последовательностей $\{\alpha_k\}$ и $\{\beta_k\}$ выполняются условия

$$\sum_k \alpha_k = \infty, \quad \beta_k \to 0, \quad \sum_k \frac{\alpha_k^2}{\beta_k^2} < \infty, \quad \sum_k \alpha_k\beta_k < \infty,$$

то выполнены все условия леммы Роббинса–Сигмунда о сходимости почти супермартингалов (см. [5]). Следовательно, последовательность оценок $\{\hat{\theta}_n\}$ сходится к θ с вероятностью единица. При этом дисперсия ошибки оценивания прямо пропорциональна α_n^2/β_n^2.

3.3.3. Квантовый компьютер и вычисление оценки вектора-градиента функции

Рассмотрим проблему выбора вычислительного устройства, наилучшим образом подходящего для выполнения рандомизированного алгоритма стохастической оптимизации с одним измерением функции штрафа на итерации.

Пусть разрядность используемого квантового вычислителя равна n, $f : \mathbb{R}^q \to \mathbb{R}$ — некоторая функция, удовлетворяющая условиям из предыдущего пункта, и

$$U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle,$$

— унитарный оператор, реализующий на квантовом компьютере функцию $f(x)$ (его можно задать на всех классических двоичных цепочках x длины $q\,n$, определяющих аргумент функции). Здесь y — произвольная двоичная цепочка длины n, $\oplus$ — побитовоя операция "логического или". Это способ задания оператора на базисных векторах. На все остальные вектора оператор продолжается линейно. Легко видеть, что построенный оператор обратим и действует в комплексном пространстве размерности 2^{qn+n}.

Рассмотрим задачу: получить следующую оценку точки минимума функции по рандомизированному алгоритму стохастической аппроксимации с одним измерением. Для подачи на вход вычислителя подготовим суперпозицию 2^q возмущенных значений текущего вектора оценки:

$$x_k = \frac{1}{2^{\frac{q}{2}}} \sum_{\Delta_i \in \{-1,+1\}^q} |\hat{\theta}_{k-1} + \beta_k \Delta_i\rangle,$$

где ± 1 рассматриваются как n-разрядные числа. После применения унитарного оператора U_f к $|x_k\rangle|0\rangle$ получаем

$$U_f|x_k\rangle|0\rangle = \frac{1}{2^q} \sum_{\Delta_i \in \{-1,+1\}^q} |\hat{\theta}_{k-1} + \beta_k \Delta_i\rangle|f(\hat{\theta}_{k-1} + \beta_k \Delta_i)\rangle.$$

Из общих свойств модели квантовых вычислений следует, что после измерения полученного состояния, с вероятностью $\frac{1}{2^q}$ будет получен один из векторов вида

$$|\hat{\theta}_{k-1} + \beta_k \Delta_i\rangle|f(\hat{\theta}_{k-1} + \beta_k \Delta_i)\rangle, \;\; \Delta_i \in \{-1,+1\}^q.$$

Из первых $q\,n$ разрядов этого вектора легко получить реализацию вектора случайного возмущения Δ_i. По рандомизированному алгоритму оценивания координаты вектора Δ_i надо умножить на соответствующее значение функции потерь в возмущенной точке, которое записано в последних n разрядах полученного после измерения результата.

Глава 4

Заключение

Заключение

Гибридные, квантовые и нейрокомпьютеры обещают существенным образом изменить представления о вычислительной мощности современных вычислительных устройств. Увеличение вычислительной мощности, возможное за счет использования новых моделей вычислений, основывающихся на физических явлениях, позволяет предположить, что в будущем новые компьютеры смогут решать задачи, невыполнимые для обычных компьютеров.

Предложенная новая концепция процесса вычислений позволяет описывать если не все, то подавляющее большинство процессов, происходящих в реальном мире, а также работу всевозможных существующих и будущих вычислительных устройств, включая аналоговые и биокомпьютеры, нейрокомпьютеры, квантовые компьютеры и т. д. Особенностью предлагаемого нового подхода является отказ от редукции сложности в процессе вычисления. Сложность вычислимого объекта должна быть эквивалентна сложности вычисляемого. Таким образом, понятие вычислительной сложности правильнее рассматривать относительно выбранной системы базисных эволюционных примитивов, а не относительно традиционно рассматриваемых битовых преобразований $\{0, 1\}$.

Описанные в книге новые экспериментальные результаты дают надежду на возможность практической реализации гибридных сверхбыстрых компьютеров уже в ближайшее время.

Глава 5

1. **Амбарян Т. Р., Тимофеев А. В.** Модели квантовых и нейронных вычислений в задачах обработки информации // Известия вузов. Приборостроение. 2005. 48. №7. С. 35–40.
2. **Владимирович А. Г., Граничин О. Н., Макаров А. А.** Нестандартная машина Тьюринга // "Стохастическая оптимизация в информатике" под ред. О. Н. Граничина. Изд-во С.-Петерб. ун-та. 2005. С. 28–48.
3. **Владимирович А. Г., Граничин О. Н.** Обобщение концепции машины Тьюринга // "УИТ-2005" материалы трудов конф. СПб. 2005. Т. 2. С. 90–98.
4. **Граничин О. Н.** Стохастическая аппроксимация с возмущением на входе при зависимых помехах наблюдения // Вест. ЛГУ. 1989. Сер. 1. Вып. 4. С. 27–31.
5. **Граничин О. Н., Поляк Б. Т.** Рандомизированные алгоритмы оценивания и оптимизации при почти произвольных помехах. М.: Наука. 2003. 291 С.
6. **Граничин О. Н., Сысоев С. С., Вахитов А.Т.** Точность оценивания рандомизированного алгоритма стохастической оптимизации // Автоматика и Телемеханика. 2006. № 4.
7. **Граничин О. Н., Жувикина И. А.** Новая концепция процесса вычислений, основанная на эволюционных примитивах // "Системное программирование" под ред. А. Н. Терехова и др.. Изд-во С.-Петерб. ун-та. 2006. С. 67–82.
8. **Жувикина И. А.** Анализ сложных материальных систем на основе P-меры Хаусдорфа // Проблемы управления безопасностью сложных систем. Материалы VII международной конференции. М. 1999. С. 31–33.
9. **Нариньяни А. С.** Модель или алгоритм: новая парадигма информационных технологий. Российский НИИ ИИ. 2004.
10. **Макаров А. А.** Пример обобщения концепции машины Тьюринга. Дипломная работа студента кафедры системного программирования СПбГУ. 2005.
11. **Мартыненко Б. К.** Языки и трансляции. Изд-во СПбГУ. 2002.

12. **Матиясевич Ю. В.** Диофантовость перечислимых множеств // Докл. Акад. Наук СССР. 1970. Т. 191. С. 279–282.

13. **Матиясевич Ю. В., Терехов А. Н.** 16-разрядная виртуальная ЭВМ, ориентированная на АЯВУ. Программирование микропроцессорной техники // Микропроцессорная техника. Таллин. 1984.

14. **Мессия А.** Квантовая механика. Т. 2. М.: Наука. 1979.

15. **Пайтген Х.-О., Рихтер П. Х.** Красота фракталов. Образы комплексных динамических систем. М.: Мир. 1993. 176 С.

16. **Поляк Б. Т., Цыбаков А. Б.** Оптимальные порядки точности поисковых алгоритмов стохастической аппроксимации // Пробл. передачи информ. 1990. № 2. С. 45–53.

17. **Садовничий В. А.** Квантовый компьютер и квантовые вычисления. Т. 2. Ижевск. 1999.

18. **Самко С. Г., Килбас А. А., Маричев О. И.** Интегралы и производные дробных порядков и некоторые их приложения. Минск: Наука и техника. 1987. 688 С.

19. **Толстов Г. П.** Мера и интеграл. М.: Наука. 1976. 392 С.

20. **Фаддеев Л. Д., Якубовский О. А.** Лекции по квантовой механике для студентов-математиков. Ижевск. Изд-во РХД. 2001.

21. **Adleman L. M.** Molecular computation of solutions to combinatorial problems // Science **266** (1994) 1021.

22. **Allemand J.-F., Bensimon D., Jullien L., Bensimon A., Croquette V.** pH-dependent specific binding and combing of DNA // Biophysical Journal **73** (1997) 2064.

23. **Bayer M., Hawrylak P., Hinzer K., Fafard S., Korkusinski M., Wasilewski Z. R., Stern O., Forchell A.** Coupling and entangling of quantum states in quantum dot molecules // Science **291** (2001) 451.

24. **Bensimon A., Simon A., Chiffaudel A., Croquette V., Heslot F., Bensimon D.** Alignment and sensitive detection of DNA by a moving interface // Science **265** (1994) 2096.

25. **Bensimon D., Simon A. J., Croquette V., Bensimon A.** Stretching DNA with a reced-ing meniscus: Experiments and models // Phys. Rev. Lett. **74** (1995) 4754.

26. **Chen H. F., Duncan T. E., Pasik–Duncan B.** A Kiefer–Wolfowitz Algorithm with Randomized Differences // IEEE Trans. Automat. Contr. **44** (1999) No 3. P. 442–453.

27. **Cerf N. J., Adami C., Kwiat P. G.** Optical simulation of quantum logic // Phys. Rev. A **57** (1998) R1477.

28. **Church A.** A note on the Entscheidung problem // Journal of Symbolic Logic (1936) № 1. P. 56–68.

29. **Cirac J. I.,Zoller P.** Quantum computations with cold trapped ions // Phys. Rev. Lett. **74** (1995) 4091.

30. **Copeland J. B.** The Church-Turing Thesis // NeuroQuantology (2004) № 2. P. 101–115

31. **Deutsch D.** Quantum theory, the Church-Turing Principle and the Universal Quantum Computer // Proceedings of the Royal Society of London. Ser. A. **400** (1985) P. 97–117.

32. **Diez S., Reuther C., Dinu C., Seidel R., Mertig M., Pompe W., Howard J.** Stretching and transporting DNA molecules using motor proteins // Nano Lett. **3** (2003) 2251.

33. **Engelhardt H.** http://www.biochem.mpg.de/baumeister/membran/home.html.

34. **Engelhardt H., Saxton W. O., Baumeister W.** Three-dimensional structure of the tetragonal surface layer of Sporosarcina ureae // J. Bacteriol. **168** (1986) 309.

35. **Farhi E., Goldstone J., Gustmann S., Sipser M.** Quantum computation by adiabatic evolution //Archive quant-ph/0001106(2000).

36. **Feynman R.** Modeling of physics on computers // Int. Journal of Theoretical Physics **21** (1982) № 6/7.

37. **Granichin O. N.** Linear regression and filtering under nonstandard assumptions (Arbitrary noise) // Trans. on Automat. Contr. **49** (2004) Oct. № 10. P. 1830–1835.

38. **Granichin O. N., Khantuleva T. A.** Hybrid systems and randomized measuring in nonequilibrium processes // Differential Equation and Control Processes (2004) № 3. Electronic J. N P23275 at 07.03.97.

39. **Hausdorff F.** Dimension und ausseres // Math. Ann. **79** (1919).

40. **Hurewics W., Wallman H.** Dimension theory (1941).

41. **Ireta J., Galvan M., Cho K., Joannopoulos J. D.** Local reactivity of charybdotoxin, a K^+ channel blacker // J. Am. Chem. Soc. **120** (1998) 9771.

42. **Kadowaki T., Nishimori H.,** Quantum annealing in the transverse Ising model // Phys. Rev. E. **58** (1998) 5355.

43. **Kiefer J., Wolfowitz J.** Statistical estimation on the maximum of a regression function // Ann. Math. Stat. **23** (1952) P. 462–466.

44. **Kieu Tien D.** Computing the non-computable // Contemporary Physics **44** (2003) 51.

45. **Lloyd S., Braunstain S. L.,** Quantum computation over continuous variables. // Phys. Rev. Lett. **82** (1999) 1784.

46. **Kane B. E.** A silicon-based nuclear spin quantum computer // Nature **393** (1998) 133137.

47. **Mertig M., Kirsch R., Pompe W., Engelhardt E.** Fabrication of highly oriented nanocluster arrays by biomolecular templating // European Physical Journal D **9** (1999) 45.

48. **Mertig M., Colombi Ciacchi L., Seidel R., Pompe W., De Vita A.** DNA as a selective metallization template // Nano Lett. **2** (2002) 841.

49. **Mertig M., Pompe W.** in: Nanobiotechnology - Concepts, Applications and Perspectives. Eds: C. M. Niemeyer, C. A. Mirkin. WILEY. Weinheim (2004) 256.

50. **Mooij J. E., Orlando T. P., Levitov L., Lin Tian, van der Wai C. H., Lloyd S.** Josephson persistent current qubit // Science **285** (1999) 1036.

51. **Moore H.** Electronics **38** (1965) April 19. № 8.

52. **Moore J. T., Beale P. D., Winningham Th. A., Douglas K.** Creation of nanometer-scale patterns with selected metal films // Appl. Phys. Lett. **72** (1998) 1840.

53. **Ortner G., Bayer M., Larionov A., Timofeev V. B., Forchel A., Lyanda-Geller Y. B., Reinecke T. L., Hawrylak P., Fafard S., Wasilewski Z.** Fine structure of excitons in InAs/GaAs coupled quantum dots: A sensitive test of electronic coupling // Phys. Rev. Lett. **90** (2003) 086404.

54. **Pola G., Bujorianu M. L., Lygeros J., Di Benedetto M. D.** Stochastic Hybrid Models: an Overview.

55. **Pum D., Sleytr U.** Large-scale reconstitution of crystalline bacterial surface-layer proteins at the air-water-interface and on lipid films // Thin Solid Films **244** (1994) 882.

56. **Preskill J.** Quantum computing.
http:// www.theory.caltech.edu/p̃reskill/ph229.

57. **Richter J., Seidel R., Kirsch R., Mertig M., Pompe P., Plaschke J., Schackert H. K.** Nanoscale palladium metallization of DNA // Advanced Materials **12** (2000) 507.

58. **Seidel R., Colombi Ciacchi L., Weigel M., Pompe W., Mertig M.** Synthesis of Plati-num cluster chains on DNA templates: Conditions for a template-controlled cluster growth // J. Phys. Chem. B **108** (2004) 10801.

59. **Shor P.** Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM J. Comput. **26** (1997) P. 1484–1509.

60. **Sleytr U. B., Messner P., Pum D., Sara M.** Crystalline bacterial cell surface proteins // Academic Press. San Diego (1996).

61. **Soreni M., Yogev S., Kossoy E., Shoham Y., Keinan E.** Parallel biomolecular computation on surfaces with advanced finite automata // J. Am. Chem. Soc. **127** (2005) 3935.

62. **Spall J.C.** A one–measurement form of simultaneous perturbation stochastic approximation // Automatica **33** (1997) P. 109–112.

63. **Stolze J., Dietr Suter D.** Quantum Computing: A Short Course from Theory to Experiment. Wiley (2004) 244 p.

64. **Terekhov A. N.** The main concepts of a new HLL computer CAMCOH // Computer Science Journal of Moldova **1** (1993) № 1.

65. **Turing A.** On Computable Numbers, With an Application to the Entcheindungsproblem // Proc. London Math. Soc. **42** (1936) 230.

66. **Vandersypen L., Steffen M., Breyta G., Yannoni C. S., Sherwood M. H., Chuang I. L.** Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance // Nature **414** (2001) 20/27 Dec. 883.

67. **Vyalikh D. V., Danzenbacher S., Mertig M., Kirchner A., Pompe W., Dedkov Yu. S., Molodtsov S. L.** Electronic Structure of Regular Bacterial Surface Layers // Phys. Rev. Lett. **93** (2004) 238103.

68. **Vyalikh D. V., Kirchner A., Danzenbacher S., Dedkov Yu. S., Kade A., Mertig M., Molodtsov S. L.** Photoemission and NEXAFS Studies of the Bacterial Surface Protein Layer of Bacillus Sphaericus NCTC 9602 // J. Phys. Chem. B. **109** (2005) 18620.

69. **Zhuvikina I. A.** Evolutions of mesostructures: from microscopics to hydrodynamics // Proc. of the 2^{nd} Int. Arctic seminar. Physics and Mathematics. Murmansk (1997) 127.

70. **Zhuvikina I. A.** Hausdorff dimensionality as bridging the gap between the domains of discreetness and of continuity // Proc. of the 3^{rd} Int. Arctic seminar. Physics and Mathematics. Murmansk (1998) 143.

71. **Zhuvikina I. A.** Additive variables, p-densities and the conservation laws // Ibid. 148.

Н а у ч н о е и з д а н и е

Олег Николаевич Граничин, Сергей Львович Молодцов

Создание гибридных сверхбыстрых компьютеров и системное программирование

Печатается без издательского редактирования

Обложка художника *Е. И. Егоровой*
Оригинал–макет *О. Н. Граничина*

Лицензия ИД №05679 от 24.08.2001

Подписано в печать 03.04.06. Формат $60 \times 84/_{16}$.
Бумага офсетная. Печать офсетная
Усл. печ. л. 6,28. Тираж 100 экз.
Заказ №

Издательство СПбГУ. 199004, С.-Петербург, В.О., 6-я линия, 11/21.
Тел. (812) 328–96–17; факс (812) 328–44–22
E-mail: editor@unipress.ru
www.unipress.ru
Типография Издательства СПбГУ.
199061, С.-Петербург, Средний пр., 41.

Литература

[1] *Амбарян Т. Р., Тимофеев А. В.* Модели квантовых и нейронных вычислений в задачах обработки информации // Известия вузов. Приборостроение. 2005. **48**. №7. С. 35–40.

[2] *Владимирович А. Г., Граничин О. Н., Макаров А. А.* Нестандартная машина Тьюринга // "Стохастическая оптимизация в информатике" под ред. О. Н. Граничина. Изд-во С.-Петерб. ун-та. 2005. С. 28–48.

[3] *Владимирович А. Г., Граничин О. Н.* Обобщение концепции машины Тьюринга // "УИТ-2005" материалы трудов конф. СПб. 2005. Т. 2. С. 90–98.

[4] *Граничин О. Н.* Стохастическая аппроксимация с возмущением на входе при зависимых помехах наблюдения // Вест. ЛГУ. 1989. Сер. 1. Вып. 4. С. 27–31.

[5] *Граничин О. Н., Поляк Б. Т.* Рандомизированные алгоритмы оценивания и оптимизации при почти произвольных помехах. М.: Наука. 2003. 291 С.

[6] *Граничин О. Н., Сысоев С. С., Вахитов А.Т.* Точность оценивания рандомизированного алгоритма стохастической оптимизации // Автоматика и Телемеханика. 2006. № 2 (в печати).

[7] *Граничин О. Н., Жувикина И. А.* Новая концепция процесса вычислений, основанная на эволюционных примитивах // В сб. "Системное программирование" под ред. А. Н. Терехова и др.. Изд-во С.-Петерб. ун-та. 2006 (в печати).

[8] *Жувикина И. А.* Анализ сложных материальных систем на основе Р-меры Хаусдорфа // Проблемы управления безопасностью сложных систем. Материалы VII международной конференции. М. 1999. С. 31–33.

[9] *Нариньяни А. С.* Модель или алгоритм: новая парадигма информационных технологий. Российский НИИ ИИ. 2004.

[10] *Макаров А. А.* Пример обобщения концепции машины Тьюринга. Дипломная работа студента кафедры системного программирования СПбГУ. 2005.

[11] *Мартыненко Б. К.* Языки и трансляции. Изд-во СПбГУ. 2002.

[12] *Матиясевич Ю. В.* Диофантовость перечислимых множеств // Доклады Академии Наук СССР. 1970. Т. 191. С. 279–282.

[13] *Матиясевич Ю. В., Терехов А. Н.* 16-разрядная виртуальная ЭВМ, ориентированная на АЯВУ. Программирование микропроцессорной техники // В сб. "Микропроцессорная техника". Таллин. 1984.

[14] *Мессия А.* Квантовая механика, т.2 // М.: Наука. 1979.

[15] *Пайтген Х.-О., Рихтер П. Х.* Красота фракталов. Образы комплексных динамических систем. М.: Мир. 1993. 176 С.

[16] *Поляк Б. Т., Цыбаков А. Б.* Оптимальные порядки точности поисковых алгоритмов стохастической аппроксимации // Пробл. передачи информ. 1990. № 2. С. 45–53.

[17] *Садовничий В. А.* Квантовый компьютер и квантовые вычисления. Т. 2. Ижевск. 1999.

[18] *Самко С. Г., Килбас А. А., Маричев О. И.* Интегралы и производные дробных порядков и некоторые их приложения. Минск: Наука и техника. 1987. 688 С.

[19] *Толстов Г. П.* Мера и интеграл. М.: Наука. 1976. 392 С.

[20] *Фаддеев Л. Д., Якубовский О. А.* Лекции по квантовой механике для студентов-математиков. Ижевск. Изд-во РХД. 2001.

[21] *Adleman L. M.* Molecular computation of solutions to combinatorial problems // Science 266 (1994) 1021.

[22] *Allemand J.-F., Bensimon D., Jullien L., Bensimon A., Croquette V.* pH-dependent specific binding and combing of DNA // Biophysical Journal **73** (1997) 2064.

[23] *Bayer M., Hawrylak P., Hinzer K., Fafard S., Korkusinski M., Wasilewski Z. R., Stern O., Forchell A.* Coupling and entangling of quantum states in quantum dot molecules // Science **291** (2001) 451.

[24] *Bensimon A., Simon A., Chiffaudel A., Croquette V., Heslot F., Bensimon D.* Alignment and sensitive detection of DNA by a moving interface // Science **265** (1994) 2096.

[25] *Bensimon D., Simon A. J., Croquette V., Bensimon A.* Stretching DNA with a reced-ing meniscus: Experiments and models // Phys. Rev. Lett. **74** (1995) 4754.

[26] *Chen H. F., Duncan T. E., Pasik–Duncan B.* A Kiefer–Wolfowitz Algorithm with Randomized Differences// IEEE Trans. Automat. Contr. **44** (1999) No 3. P. 442–453.

[27] *Cerf N. J., Adami C., Kwiat P. G.* Optical simulation of quantum logic // Phys. Rev. A **57** (1998) R1477.

[28] *Church A.* A note on the Entscheidung problem // Journal of Symbolic Logic (1936) № 1. P. 56–68.

[29] *Cirac J. I.,Zoller P.* Quantum computations with cold trapped ions // Phys. Rev. Lett. **74** (1995) 4091.

[30] *Copeland J. B.* The Church-Turing Thesis // NeuroQuantology (2004) № 2. P. 101–115

[31] *Deutsch D.* Quantum theory, the Church-Turing Principle and the Universal Quantum Computer // Proceedings of the Royal Society of London Ser. A. **400** (1985) P. 97–117.

[32] **Diez S., Reuther C., Dinu C., Seidel R., Mertig M., Pompe W., Howard J.** Stretching and transporting DNA molecules using motor proteins // Nano Lett. **3** (2003) 2251.

[33] *Engelhardt H.* http://www.biochem.mpg.de/baumeister/membran/home.html.

[34] *Engelhardt H., Saxton W. O., Baumeister W.* Three-dimensional structure of the tetragonal surface layer of Sporosarcina ureae // J. Bacteriol. **168** (1986) 309.

[35] *Farhi E., Goldstone J., Gustmann S., Sipser M.* Quantum computation by adiabatic evolution //Archive quant-ph/0001106 (2000).

[36] *Feynman R.* Modeling of physics on computers // International Journal of Theoretical Physics. **21** (1982) № 6/7.

[37] *Granichin O. N.* Linear regression and filtering under nonstandard assumptions (Arbitrary noise) // Trans. on Automat. Contr. **49** (2004) Oct. № 10. P. 1830–1835

[38] *Granichin O. N., Khantuleva T. A.* Hybrid systems and randomized measuring in nonequilibrium processes // Differential Equation and Control Processes (2004) № 3. Electronic J. N P23275 at 07.03.97

[39] *Hausdorff F.* Dimension und ausseres // Math. Ann. **79** (1919).

[40] *Hurewics W., Wallman H.* Dimension theory. (1941).

[41] *Ireta J., Galvan M., Cho K., Joannopoulos J. D.* Local reactivity of charybdotoxin, a K^+ channel blacker // J. Am. Chem. Soc. **120** (1998) 9771.

[42] *Kadowaki T., Nishimori H.,* Quantum annealing in the transverse Ising model // Phys. Rev. E. **58** (1998) 5355.

[43] *Kiefer J., Wolfowitz J.* Statistical estimation on the maximum of a regression function // Ann. Math. Stat. **23** (1952) P. 462–466.

[44] *Kieu Tien D.* Computing the non-computable // Contemporary Physics. **44** (2003) P. 51–71.

[45] *Lloyd S., Braunstain S. L.,* Quantum computation over continuous variables. // Phys. Rev. Lett **82** (1999) 1784.

[46] *Kane B. E.* A silicon-based nuclear spin quantum computer // Nature **393** (1998) 133137.

[47] *Mertig M., Kirsch R., Pompe W., Engelhardt E.* Fabrication of highly oriented nanocluster arrays by biomolecular templating // European Physical Journal D **9** (1999) 45.

[48] **Mertig M., Colombi Ciacchi L., Seidel R., Pompe W., De Vita A.** DNA as a selective metallization template // Nano Lett. **2** (2002) 841.

[49] **Mertig M., Pompe W.** in: Nanobiotechnology - Concepts, Applications and Perspectives. Eds: C. M. Niemeyer, C. A. Mirkin. WILEY. Weinheim (2004) 256.

[50] *Mooij J. E., Orlando T. P., Levitov L., Lin Tian, van der Wai C. H., Lloyd S.* Josephson persistent current qubit // Science **285** (1999) 1036.

[51] *Moore H.* Electronics. **38** (1965) April 19. № 8.

[52] **Moore J. T., Beale P. D., Winningham Th. A., Douglas K.** Creation of nanometer-scale patterns with selected metal films // Appl. Phys. Lett. **72** (1998) 1840.

[53] *Ortner G., Bayer M., Larionov A., Timofeev V. B., Forchel A., Lyanda-Geller Y. B., Reinecke T. L., Hawrylak P., Fafard S., Wasilewski Z.* Fine structure of excitons in InAs/GaAs coupled quantum dots: A sensitive test of electronic coupling // Phys. Rev. Lett. **90** (2003) 086404.

[54] *Pola G., Bujorianu M. L., Lygeros J., Di Benedetto M. D.* Stochastic Hybrid Models: an Overview.

[55] *Pum D., Sleytr U.* Large-scale reconstitution of crystalline bacterial surface-layer proteins at the air-water-interface and on lipid films // Thin Solid Films **244** (1994) 882.

[56] *Preskill J.* Quantum computing.
http://www.theory.caltech.edu/˜ preskill/ph229.

[57] **Richter J., Seidel R., Kirsch R., Mertig M., Pompe P., Plaschke J., Schackert H. K.** Nanoscale palladium metallization of DNA // Advanced Materials **12** (2000) 507.

[58] **Seidel R., Colombi Ciacchi L., Weigel M., Pompe W., Mertig M.** Synthesis of Plati-num cluster chains on DNA templates: Conditions for a template-controlled cluster growth // J. Phys. Chem. B **108** (2004) 10801.

[59] *Shor P.* Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM J. Comput. **26** (1997) P. 1484–1509.

[60] *Sleytr U. B., Messner P., Pum D., Sara M.* Crystalline bacterial cell surface proteins // Academic Press. San Diego (1996).

[61] *Soreni M., Yogev S., Kossoy E., Shoham Y., Keinan E.* Parallel biomolecular computation on surfaces with advanced finite automata // J. Am. Chem. Soc. **127** (2005) 3935.

[62] *Spall J.C.* A one–measurement form of simultaneous perturbation stochastic approximation // Automatica. **33** (1997) P. 109–112.

[63] **Stolze J., Dietr Suter D.** Quantum Computing: A Short Course from Theory to Experiment. Wiley (2004) 244 p.

[64] *Terekhov A. N.* The main concepts of a new HLL computer "CAMCOH" // Computer Science Journal of Moldova. **1** (1993) № 1.

[65] *Turing A.* On Computable Numbers, With an Application to the Entcheindungsproblem // Proc. London Math. Soc. **42** (1936) № 2. P. 230–265.

[66] *Vandersypen L., Steffen M., Breyta G., Yannoni C. S., Sherwood M. H., Chuang I. L.* Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance // Nature. **414** (2001) 20/27 Dec. P. 883–887.

[67] *Vyalikh D. V., Danzenbacher S., Mertig M., Kirchner A., Pompe W., Dedkov Yu. S., Molodtsov S. L.* Electronic Structure of Regular Bacterial Surface Layers // Phys. Rev. Lett. **93** (2004) 238103.

[68] *Vyalikh D. V., Kirchner A., Danzenbacher S., Dedkov Yu. S., Kade A., Mertig M., Molodtsov S. L.* Photoemission and NEXAFS Studies of the Bacterial Surface Protein Layer of Bacillus Sphaericus NCTC 9602 // J. Phys. Chem. B. **109** (2005) P. 18620-18627.

[69] *Zhuvikina I. A.* Evolutions of mesostructures: from microscopics to hydrodynamics // Proc. of the 2^{nd} Int. Arctic seminar. Physics and Mathematics. Murmansk (1997) P. 127–132.

[70] *Zhuvikina I. A.* Hausdorff dimentionality as bridging the gap between the domains of discretness and of continuity // Proc. of the 3^{rd} Int. Arctic seminar. Physics and Mathematics. Murmansk (1998) P. 143–147.

[71] *Zhuvikina I. A.* Additive variables, p-densities and the conservation laws // Ibid. P. 148-152.