

УДК 531:530.145
ББК 22.314.1
К 15

Интернет-магазин
MATHESIS

<http://shop.rcd.ru>

- физика
- математика
- биология
- нефтегазовые технологии



Издание осуществлено при финансовой поддержке Российского фонда фундаментальных исследований по проекту №08-02-07057.

Кайе Ф., Лафламм Р., Моска М.

Введение в квантовые вычисления. — М.–Ижевск: НИЦ «Регулярная и хаотическая динамика», Институт компьютерных исследований, 2009. — 360 с.

Эта книга, написанная кратко и доступно, обеспечивает всестороннее введение в квантовые вычисления — захватывающую и быстро развивающуюся область, которая находится на пересечении компьютерных, инженерно-технических, математических и физических наук.

Книга предназначена для студентов старших курсов и начинающих аспирантов перечисленных дисциплин, она насыщена техническими деталями и иллюстрирована пояснительными диаграммами и упражнениями.

ISBN 978-5-93972-766-2

ББК 22.314.1

“**An Introduction to Quantum Computing**” was originally published in English 2007. This translation is published by arrangement with *Oxford University Press*.

Книга «Введение в квантовые вычисления» впервые вышла на английском языке в 2007 году. Перевод публикуется по соглашению с издательством *Oxford University Press*.

© Phillip R. Kaye, Raymond Laflamme and Michele Mosca, 2007

© Перевод на русский язык:

НИЦ «Регулярная и хаотическая динамика», 2009

<http://shop.rcd.ru>

<http://ics.org.ru>

Оглавление

Предисловие к русскому изданию	ix
Предисловие	x
Благодарности	xi
ГЛАВА 1. Введение и основные понятия	1
1.1. Общие сведения	1
1.2. Компьютеры и строгий тезис Чёрча–Тьюринга	2
1.3. Схемная модель вычислений	7
1.4. Схемная модель в формулировке линейной алгебры	10
1.5. Обратимые вычисления	15
1.6. Знакомство с квантовой физикой	19
1.7. Квантовая физика и квантовые вычисления	24
ГЛАВА 2. Линейная алгебра и дираковская система обозначений	26
2.1. Дираковская система обозначений и гильбертово пространство	26
2.2. Двойственные векторы	28
2.3. Операторы	33
2.4. Спектральная теорема	37
2.5. Функции операторов	39
2.6. Тензорные произведения	41
2.7. Теорема Шмидта о разложении	43
2.8. Некоторые замечания о дираковской системе обозначений	46
ГЛАВА 3. Кубиты и концепции квантовой механики	48
3.1. Состояние квантовой системы	48
3.2. Временная эволюция изолированной системы	54
3.3. Составные системы	57
3.4. Измерение	60
3.5. Смешанные состояния и обобщенные квантовые операции	66
3.5.1. Смешанные состояния	67
3.5.2. Взятие частичного следа	71
3.5.3. Обобщенные квантовые операции	74

ГЛАВА 4. Квантовая модель вычислений	77
4.1. Модель квантовой схемы	77
4.2. Квантовые элементы	79
4.2.1. Однокубитовые элементы	79
4.2.2. Элементы «управляемое- U »	83
4.3. Универсальные множества квантовых элементов	86
4.4. Эффективность аппроксимации унитарных преобразований	90
4.5. Реализация измерений с помощью квантовых схем	92
ГЛАВА 5. Сверхплотное кодирование и квантовая телепортация	98
5.1. Сверхплотное кодирование	99
5.2. Квантовая телепортация	100
5.3. Применение квантовой телепортации	103
ГЛАВА 6. Введение в квантовые алгоритмы	109
6.1. Сравнение вероятностного и квантового алгоритмов	109
6.2. Возврат фазы	115
6.3. Алгоритм Дойча	119
6.4. Алгоритм Дойча–Джозы	125
6.5. Алгоритм Саймона	130
ГЛАВА 7. Алгоритмы с сверхполиномиальным ускорением	139
7.1. Оценка квантовой фазы и квантовое преобразование Фурье	140
7.1.1. Анализ погрешности при оценке произвольных фаз	148
7.1.2. Периодическое состояние	152
7.1.3. НОД, НОК и расширенный алгоритм Евклида	157
7.2. Оценка собственного значения	158
7.3. Вычисление порядка	165
7.3.1. Задача нахождения порядка	165
7.3.2. Предварительные замечания по математике	166
7.3.3. Вычисление порядка методом оценки собственного значения	169
7.3.4. Нахождение порядка по Шору	177
7.4. Вычисление дискретного логарифма	179
7.5. Скрытая подгруппа	185
7.5.1. Еще о квантовом преобразовании Фурье	187
7.5.2. Алгоритм выделения скрытой подгруппы в конечной абелевой группе	189
7.6. Сопутствующие алгоритмы и методы	191

ГЛАВА 8. Алгоритмы, основанные на усилении амплитуды	193
8.1. Квантовый алгоритм поиска Гровера	193
8.2. Усиление амплитуды	207
8.3. Квантовая оценка амплитуды и квантовое перечисление . . .	215
8.4. Поиск с неизвестной вероятностью успеха	222
8.5. Сопутствующие алгоритмы и методы	225
ГЛАВА 9. Квантовая теория вычислительной сложности и нижние	
оценки	227
9.1. Вычислительная сложность	228
9.1.1. Задачи распознавания языковых объектов и классы	
сложности	229
9.2. Модель черного ящика	236
9.2.1. Различимость состояний	238
9.3. Нижние оценки для задачи поиска на модели черного ящика:	
гибридный метод	239
9.4. Нижние оценки общей модели черного ящика	243
9.5. Метод полиномов	246
9.5.1. Применение нижних границ	247
9.5.2. Примеры нижних оценок по методу полиномов	249
9.6. Блоковая чувствительность	250
9.6.1. Примеры нижних оценок по методу блоковой чув-	
ствительности	251
9.7. Метод от противного	251
9.7.1. Примеры нижних оценок по методу от противного . .	254
9.7.2. Обобщения	258
ГЛАВА 10. Исправление квантовых ошибок	259
10.1. Классический метод исправления ошибок	260
10.1.1. Модели ошибок	260
10.1.2. Кодирование	261
10.1.3. Восстановление после ошибки	262
10.2. Классический трехбитовый код	264
10.3. Отказоустойчивость	268
10.4. Исправление квантовых ошибок	269
10.4.1. Модели ошибок для квантовых вычислений	270
10.4.2. Кодирование	274
10.4.3. Восстановление после ошибки	276
10.5. Трех- и девятикубитовые квантовые коды	283

10.5.1. Трехкубитовый код, исправляющий однобитовые ошибки	283
10.5.2. Трехкубитовый код, исправляющий фазовые ошибки	285
10.5.3. Исправление квантовых ошибок без декодирования	287
10.5.4. Девятикубитовый код Шора	291
10.6. Отказоустойчивые квантовые вычисления	296
10.6.1. Конкатенация кодов и пороговая теорема	301
Приложение А.	305
А.1. Инструменты анализа вероятностных алгоритмов	305
А.2. Решение задачи дискретного логарифмирования, когда поря- док a есть составное число	308
А.3. Какой должна быть случайная выборка?	310
А.4. Определение r при заданном $\frac{k}{r}$ для произвольного k	312
А.5. Лемма по методу от противного	313
А.6. Черные ящики для групповых вычислений	316
А.7. Выполнение разложения Шмидта	319
А.8. Общие измерения	321
А.9. Оптимальное различение двух состояний	325
А.9.1. Простая процедура	326
А.9.2. Оптимальность простой процедуры	326
Литература	328
Предметный указатель	340