

ОГЛАВЛЕНИЕ

Предисловие к изданию на русском языке	9
Благодарности	10
Глава 1. Введение	11
1.1. Почему квантовые вычисления?	11
1.2. Зачем нужен еще один учебник по квантовым вычислениям?	12
1.2.1. Квантовые вычисления и квантовая информация	12
Глава 2. Информатика	13
2.1. Введение	13
2.2. История	13
2.3. Машины Тьюринга	16
2.3.1. Двоичные числа и формальные языки	17
2.3.1.1. Двоичное представление	18
2.3.1.2. Формальные языки	19
2.3.2. Машины Тьюринга в действии	19
2.3.3. Универсальная машина Тьюринга	20
2.3.4. Проблема останова	21
2.3.4.1. Проблема останова — доказательство от противного	21
2.4. Цепи	23
2.4.1. Наиболее распространенные логические элементы	23
2.4.2. Сочетание логических элементов	25
2.4.3. Существенные свойства	26
2.4.4. Универсальность	26
2.5. Вычислительные ресурсы и эффективность их использования	27
2.5.1. Количественная мера вычислительных затрат	28
2.5.2. Стандартные классы сложности	30
2.5.3. Физический тезис Черча–Тьюринга	31
2.5.4. Квантовые машины Тьюринга	33
2.6. Энергия и вычисления	33
2.6.1. Обратимость	33
2.6.2. Необратимость	34

2.6.3. Принцип Ландауэра	34
2.6.4. Демон Максвелла	34
2.6.5. Обратимые вычисления	35
2.6.6. Обратимые логические элементы	36
2.6.6.1. Управляемый NOT	36
2.6.6.2. Логический элемент Тоффли	36
2.6.6.3. Логический элемент Фредкина	37
2.6.7. Обратимые цепи	38
Глава 3. Математика квантовых вычислений	39
3.1. Введение	39
3.2. Полиномы	40
3.3. Логическая символика	40
3.4. Краткие сведения из тригонометрии	41
3.4.1. Прямоугольные треугольники	41
3.4.2. Перевод из градусов в радианы и обратно	42
3.4.3. Обратные тригонометрические функции	42
3.4.4. Углы в других квадрантах	42
3.4.5. Наглядные представления и тождества	43
3.5. Краткие сведения о логарифмах	44
3.6. Комплексные числа	45
3.6.1. Полярные координаты и комплексное сопряжение	46
3.6.1.1. Полярные координаты	47
3.6.2. Домножение на сопряженное и деление	48
3.6.3. Экспоненциальная форма	49
3.7. Матрицы	50
3.7.1. Операции над матрицами	50
3.7.1.1. Сложение	50
3.7.1.2. Умножение на скаляр	51
3.7.1.3. Произведение матриц	51
3.7.1.4. Свойства операций над матрицами	51
3.7.1.5. Нулевая матрица	52
3.7.1.6. Единичная матрица	52
3.7.1.7. Обратная матрица	53
3.7.1.8. Транспонирование матриц	53
3.7.1.9. Детерминанты и ранги	53
3.8. Векторы и векторные пространства	54
3.8.1. Введение	54
3.8.1.1. Векторы в $\mathbb{R} \times \mathbb{R}$	55
3.8.1.2. Интересные свойства векторов в \mathbb{R}^3	56
3.8.1.3. Кое-что о векторах в \mathbb{C}	57
3.8.2. Столбцы	57
3.8.3. Нуль-вектор	57
3.8.4. Свойства векторов в \mathbb{C}^n	58
3.8.4.1. Умножение на скаляр и сложение	58
3.8.4.2. Сложение векторов	58

3.8.5.	Дуальный вектор	58
3.8.6.	Линейная комбинация векторов	59
3.8.7.	Линейная независимость векторов	59
3.8.8.	Линейная оболочка	59
3.8.9.	Базис	60
3.8.10.	Теория вероятностей	60
3.8.11.	Амплитуды вероятности	61
3.8.12.	Скалярное произведение	62
3.8.13.	Ортогональность	64
3.8.14.	Единичный вектор	64
3.8.15.	Базисы в \mathbb{C}^n	65
3.8.16.	Метод Грама–Шмидта	66
3.8.17.	Линейные операторы	67
3.8.18.	Векторное произведение и проекторы	68
3.8.19.	Эрмитово сопряжение	70
3.8.20.	Собственные значения и векторы	71
3.8.21.	След	72
3.8.22.	Нормальные операторы	73
3.8.23.	Унитарные операторы	74
3.8.24.	Эрмитовы и положительные операторы	76
3.8.25.	Диагонализируемая матрица	76
3.8.26.	Коммутатор и антикоммутатор	77
3.8.27.	Полярное разложение	78
3.8.28.	Спектральное разложение	78
3.8.29.	Тензорные произведения	79
3.9.	Фурье-преобразования	81
3.9.1.	Ряды Фурье	82
3.9.2.	Дискретное фурье-преобразование	84
Глава 4.	Квантовая механика	87
4.1.	История	87
4.1.1.	Классическая физика	87
4.1.2.	Важные понятия	89
4.1.2.1.	Атомы	89
4.1.2.2.	Термодинамика	90
4.1.3.	Статистическая механика	91
4.1.4.	Великие эксперименты	92
4.1.5.	Фотоэлектрический эффект	93
4.1.6.	Спектры испускания и поглощения	94
4.1.7.	Прото-квантовая механика	95
4.1.8.	Новая теория квантовой механики	99
4.2.	Понятия, которые существенны для квантовых вычислений	102
4.2.1.	Линейная алгебра	102
4.2.2.	Суперпозиция	103
4.2.3.	Обозначения Дирака	105
4.2.4.	Представление информации	105
4.2.5.	Неопределенность	106
4.2.6.	Перепутывание	106

Глава 5. Квантовые вычисления	108
5.1. Элементы квантовых вычислений	108
5.1.1. Введение	108
5.1.2. История	108
5.1.3. Биты и кубиты	109
5.1.3.1. Одиночные кубиты	109
5.1.3.2. Кет-векторы $ \rangle$	112
5.1.3.3. Двумерная визуализация кубитов	113
5.1.3.4. Трехмерная визуализация кубита — сферы Блоха	113
5.1.3.5. Наборы кубитов	114
5.1.3.6. Тензорные произведения	116
5.1.3.7. Частичное измерение	116
5.1.3.8. Проективные измерения	118
5.1.4. Перепутанные состояния	119
5.1.5. Квантовые цепи	120
5.1.5.1. Логические элементы, действующие на один кубит	120
5.1.5.2. Вентиль Паули I	121
5.1.5.3. Вентиль Паули X	121
5.1.5.4. Вентиль Паули Y	122
5.1.5.5. Вентиль Паули Z	122
5.1.5.6. Фазовый вентиль	123
5.1.5.7. $\frac{\pi}{8}$ -вентиль (T-вентиль)	123
5.1.5.8. Вентиль Адамара	123
5.1.5.9. Логический элемент как векторное произведение	125
5.1.5.10. Некоторые свойства вентиля Паули	126
5.1.5.11. Операторы вращения	126
5.1.5.12. Логические элементы, действующие на несколько кубитов	127
5.1.5.13. Двухкубитный вентиль NOT	129
5.1.5.14. Вентиль Тоффоли	130
5.1.5.15. Вентиль Фредкина	130
5.2. Важные свойства квантовых цепей	130
5.2.1. Распространенные цепи	131
5.2.1.1. Управляемый U-вентиль	131
5.2.1.2. Цепь обмена битов	131
5.2.1.3. Цепь копирования	132
5.2.1.4. Логический элемент Белла	133
5.2.1.5. Сверхплотное кодирование	133
5.2.1.6. Телепортация кубита	135
5.3. Особенности построения цепей	136
5.3.1. Построение программируемого квантового компьютера	137
5.4. Постулаты квантовой механики	137
5.4.1. Постулат состояния	138
5.4.2. Постулат унитарности	138
5.4.2.1. Простая форма записи	138
5.4.2.2. Форма записи, учитывающая время	138

5.4.3. Постулат измерений	139
5.4.3.1. Простая форма записи	139
5.4.3.2. Проекторы	139
5.4.4. Постулат тензорного произведения	141
Глава 6. Теория информации	143
6.1. Введение	143
6.2. История	144
6.3. Коммуникационная модель Шеннона	144
6.3.1. Пропускная способность канала связи	145
6.4. Классические источники информации	145
6.4.1. Независимые источники информации	146
6.5. Классические избыточность и сжатие	147
6.5.1. Теорема Шеннона об источнике шифрования	148
6.5.2. Квантовые источники информации	149
6.5.3. Чистые и смешанные состояния	149
6.5.4. Теорема Шумахера о квантовом источнике шифрования	150
6.5.4.1. Матрица плотности	151
6.5.4.2. С точки зрения ансамбля	151
6.5.4.3. С точки зрения подсистем	153
6.5.4.4. Фундаментальная точка зрения	154
6.5.4.5. Энтропия фон Неймана	154
6.6. Шумы и исправление ошибок	156
6.6.0.1. Зашумленные каналы	156
6.6.0.2. Классическая коррекция ошибок	156
6.6.0.3. Коды с повторениями	157
6.6.1. Квантовые шумы	157
6.6.2. Квантовая коррекция ошибок	157
6.6.2.1. Квантовые коды с повторениями	158
6.6.2.2. Исправление ошибок	159
6.7. Белловские состояния	162
6.7.1. Измерения в одном направлении	163
6.7.2. Измерения в разных направлениях	164
6.7.3. Неравенство Белла	165
6.7.3.1. КМ-предсказание	165
6.7.3.2. ЭПР-предсказание	166
6.8. Криптология	169
6.8.1. Классическая криптография	169
6.8.2. Квантовая криптография	170
6.8.2.1. Квантовые деньги	171
6.8.2.2. Квантовый перехват пакетов	172
6.8.2.3. Квантовое распространение ключей	172
6.8.2.4. Комментарии к предыдущему примеру	173
6.9. Альтернативные модели вычислений	173

Глава 7. Квантовые алгоритмы	174
7.0.1. Введение	174
7.1. Алгоритм Дойча	175
7.1.1. Постановка задачи	175
7.1.2. Классическое решение	176
7.1.3. Квантовое решение	176
7.1.4. Физические реализации	178
7.2. Алгоритм Дойча–Йожи	179
7.2.1. Постановка задачи	179
7.2.2. Квантовое решение	179
7.3. Алгоритм Шора	181
7.3.1. Квантовое фурье-преобразование	181
7.3.2. Быстрая факторизация	184
7.3.3. Нахождение порядка	185
7.3.3.1. Цепные дроби	185
7.3.3.2. Алгоритм и логическая цепь быстрой факторизации	186
7.4. Алгоритм Гровера	190
7.4.1. Задача коммивояжера	190
7.4.2. Квантовый поиск	190
Глава 8. Последние достижения в области квантово-механических устройств	194
8.1. Введение	194
8.2. Физическая реализация	195
8.2.1. Технологии реализации	196
8.3. Квантовые компьютерные языки	197
8.4. Устройства шифрования	199
8.5. Последние достижения	199
8.5.1. Аппаратная архитектура	199
8.5.2. Криптография	200
8.5.3. Алгоритмы	200
Литература	201