

ОГЛАВЛЕНИЕ

Предисловие к русскому изданию.....	5
Предисловие.....	7
Благодарности.....	13
Терминология и обозначения.....	14
I Фундаментальные принципы.....	18
1 Введение и общий обзор.....	18
1.1 Глобальные перспективы.....	19
1.1.1 История квантовых вычислений и квантовой информации.....	19
1.1.2 Направления будущих исследований.....	32
1.2 Квантовые биты.....	33
1.2.1 Несколько кубитов.....	37
1.3 Квантовые вычисления.....	38
1.3.1 Однокубитовые элементы.....	39
1.3.2 Многокубитовые элементы.....	42
1.3.3 Измерения в базисах, отличных от вычислительного.....	44
1.3.4 Квантовые схемы.....	45
1.3.5 Схема копирования кубита?.....	47
1.3.6 Пример: состояния Белла.....	48
1.3.7 Пример: квантовая телепортация.....	49
1.4 Квантовые алгоритмы.....	52
1.4.1 Классические вычисления на квантовом компьютере.....	52
1.4.2 Квантовый параллелизм.....	54
1.4.3 Алгоритм Дойча.....	56
1.4.4 Алгоритм Дойча-Йожа.....	58
1.4.5 Классификация квантовых алгоритмов.....	61
1.5 Экспериментальная обработка квантовой информации.....	68
1.5.1 Эксперимент Штерна-Герлаха.....	68
1.5.2 Перспективы практической обработки квантовой информации.....	72
1.6 Квантовая информация.....	78
1.6.1 Квантовая теория информации: примеры задач.....	80
1.6.2 Квантовая информация в более широком контексте.....	87

2	Введение в квантовую механику	90
2.1	Линейная алгебра	91
2.1.1	Базисы и линейная независимость	93
2.1.2	Линейные операторы и матрицы	94
2.1.3	Матрицы Паули	96
2.1.4	Скалярное произведение	96
2.1.5	Собственные векторы и собственные значения	100
2.1.6	Сопряженные и эрмитовы операторы	102
2.1.7	Тензорное произведение	104
2.1.8	Операторные функции	108
2.1.9	Коммутатор и антикоммутиатор	110
2.1.10	Полярное разложение и разложение по сингулярным числам	112
2.2	Постулаты квантовой механики	114
2.2.1	Пространство состояний	114
2.2.2	Эволюция	116
2.2.3	Квантовые измерения	120
2.2.4	Различение квантовых состояний	122
2.2.5	Проективные измерения	122
2.2.6	POVM-измерения	126
2.2.7	Фаза	130
2.2.8	Составные системы	131
2.2.9	Квантовая механика: общий взгляд	134
2.3	Сверхплотное кодирование	135
2.4	Оператор плотности	137
2.4.1	Ансамбли квантовых состояний	137
2.4.2	Общие свойства операторов плотности	140
2.4.3	Редуцированный оператор плотности	145
2.5	Разложение Шмидта и расширения до чистого состояния	149
2.6	Парадокс Эйнштейна - Подольского - Розена и неравенство Белла	152
3	Введение в информатику	163
3.1	Вычислительные модели	165
3.1.1	Машины Тьюринга	166
3.1.2	Схемы	175
3.2	Анализ вычислительных задач	180
3.2.1	Как количественно оценивать компьютерные ресурсы	182
3.2.2	Сложность вычислений	184
3.2.3	Задачи разрешения и классы сложности P и NP	188
3.2.4	Другие классы сложности	199
3.2.5	Вычисления и энергия	202
3.3	Перспективы информатики	212

II	Квантовые вычисления	221
4	Квантовые схемы	221
4.1	Квантовые алгоритмы	222
4.2	Операции на одном кубите	224
4.3	Условные операции	229
4.4	Измерение	238
4.5	Универсальные квантовые элементы	241
4.5.1	Универсальность двухуровневых унитарных операторов	242
4.5.2	Универсальность набора из однокубитовых элементов и CNOT	244
4.5.3	Конечный набор универсальных операций	247
4.5.4	Трудность аппроксимации общего унитарного оператора в общем случае	253
4.5.5	Сложность квантовых вычислений	255
4.6	Модель квантовых схем вычислений	257
4.7	Моделирование квантовых систем	259
4.7.1	Моделирование в действии	260
4.7.2	Алгоритм квантового моделирования	262
4.7.3	Пример	265
4.7.4	Перспективы квантового моделирования	268
5	Квантовое преобразование Фурье и его приложения	274
5.1	Квантовое преобразование Фурье	275
5.2	Определение собственного числа	280
5.2.1	Оценка скорости работы и вероятности ошибки	282
5.3	Приложения: нахождение порядка и факторизация	285
5.3.1	Нахождение порядка	286
5.3.2	Факторизация	293
5.4	Общие приложения квантового преобразования Фурье	297
5.4.1	Нахождение периода	297
5.4.2	Дискретный логарифм	300
5.4.3	Задача о скрытой подгруппе	302
5.4.4	Возможны ли другие квантовые алгоритмы?	305
6	Квантовые алгоритмы поиска	311
6.1	Квантовый алгоритм поиска	311
6.1.1	Оракул	311
6.1.2	Процедура	314
6.1.3	Геометрическая интерпретация	315
6.1.4	Эффективность	317
6.2	Квантовый поиск как квантовое моделирование	321
6.3	Квантовое перечисление	327
6.4	Ускорение решения NP-полных задач	329
6.5	Квантовый поиск в неструктурированной базе данных	331

6.6	Оптимальность алгоритма поиска	335
6.7	Ограничение алгоритмов в модели черного ящика	339
7	Квантовые компьютеры: физическая реализация	346
7.1	Основные принципы	347
7.2	Условия для квантового вычисления	348
7.2.1	Представление квантовой информации	349
7.2.2	Реализация унитарных операторов	351
7.2.3	Приготовление начального состояния	352
7.2.4	Измерение конечного результата	353
7.3	Гармонический осциллятор как модель квантового компьютера	354
7.3.1	Физическая аппаратура	354
7.3.2	Гамильтониан	355
7.3.3	Квантовые вычисления	357
7.3.4	Недостатки	358
7.4	Квантовый компьютер на оптических фотонах	359
7.4.1	Физическая аппаратура	359
7.4.2	Квантовые вычисления	362
7.4.3	Недостатки	370
7.5	Квантовая электродинамика в оптических резонаторах	371
7.5.1	Физическая аппаратура	372
7.5.2	Гамильтониан	377
7.5.3	Поглощение и преломление для одиночного фотона и одиночного атома	378
7.5.4	Квантовые вычисления	382
7.6	Ионы в ловушке	386
7.6.1	Физическая аппаратура	386
7.6.2	Гамильтониан	396
7.6.3	Квантовые вычисления	398
7.6.4	Эксперимент	400
7.7	Ядерный магнитный резонанс	404
7.7.1	Физическая аппаратура	406
7.7.2	Гамильтониан	407
7.7.3	Квантовые вычисления	413
7.7.4	Эксперимент	419
7.8	Другие варианты реализации	427
III	Квантовая информация	440
8	Квантовый шум и квантовые преобразования	440
8.1	Классический шум и марковские процессы	441
8.2	Квантовые преобразования	444
8.2.1	Обзор	444
8.2.2	Окружающая среда и квантовые преобразования	445

8.2.3	Представление операторной суммой	448
8.2.4	Аксиоматический подход к квантовым преобразованиям	455
8.3	Примеры квантового шума и квантовых преобразований	464
8.3.1	След и частичный след	465
8.3.2	Геометрическая картина квантового преобразования одного кубита	466
8.3.3	Каналы с классической ошибкой и переворотом фазы	467
8.3.4	Деполаризующий канал	470
8.3.5	Затухание амплитуды	471
8.3.6	Затухание фазы	476
8.4	Применения квантовых преобразований	480
8.4.1	Мастер-уравнения	481
8.4.2	Томография квантовых процессов	483
8.5	Ограничения формализма квантовых преобразований	490
9	Меры различия квантовой информации	495
9.1	Меры различия классической информации	495
9.2	Насколько близки два квантовых состояния?	499
9.2.1	Следовая метрика	499
9.2.2	Степень совпадения	506
9.2.3	Связь между мерами различия	513
9.3	Насколько квантовый канал сохраняет информацию?	514
10	Исправление квантовых ошибок	525
10.1	Введение	526
10.1.1	Трехкубитовый код, исправляющий классические ошибки	527
10.1.2	Трехкубитовый код, исправляющий фазовые ошибки	531
10.2	Код Шора	533
10.3	Теория исправления квантовых ошибок	536
10.3.1	Дискретизация ошибок	540
10.3.2	Модели независимых ошибок	543
10.3.3	Вырожденные коды	546
10.3.4	Квантовая граница Хэмминга	546
10.4	Построение квантовых кодов	547
10.4.1	Классические линейные коды	547
10.4.2	Коды Кальдербанка–Шора–Стина	552
10.5	Симплектические коды	557
10.5.1	Формализм стабилизаторов	557
10.5.2	Унитарные операторы и формализм стабилизаторов	563
10.5.3	Измерения в формализме стабилизаторов	567
10.5.4	Теорема Готтесмана–Нилла	569
10.5.5	Построение симплектических кодов	570
10.5.6	Примеры	572
10.5.7	Стандартная форма симплектического кода	576

10.5.8	Квантовые схемы для кодирования, декодирования и исправления ошибок	578
10.6	Квантовые вычисления, устойчивые к ошибкам	581
10.6.1	Устойчивость к ошибкам, общая картина	582
10.6.2	Устойчивые к ошибкам квантовые логические элементы	589
10.6.3	Устойчивое к ошибкам измерение	596
10.6.4	Элементы надежного квантового вычисления	602
11	Энтропия и информация	609
11.1	Шенноновская энтропия	609
11.2	Основные свойства энтропии	612
11.2.1	Двоичная энтропия	612
11.2.2	Относительная энтропия	614
11.2.3	Условная энтропия и взаимная информация	616
11.2.4	Неравенство обработки данных	620
11.3	Энтропия фон Неймана	621
11.3.1	Квантовая относительная энтропия	622
11.3.2	Основные свойства энтропии	624
11.3.3	Измерения и энтропия	626
11.3.4	Субаддитивность	627
11.3.5	Вогнутость энтропии	628
11.3.6	Энтропия смеси квантовых состояний	630
11.4	Сильная субаддитивность	631
11.4.1	Доказательство сильной субаддитивности	632
11.4.2	Сильная субаддитивность: основные применения	634
12	Квантовая теория информации	642
12.1	Различение квантовых состояний и доступная информация	643
12.1.1	Граница Холево	646
12.1.2	Примеры применения границы Холево	649
12.2	Сжатие данных	652
12.2.1	Теорема Шеннона о кодировании для канала без шума	653
12.2.2	Теорема Шумахера о кодировании для квантового канала без шума	659
12.3	Передача классической информации по квантовым каналам с шумом	665
12.3.1	Связь по классическому каналу с шумом	665
12.3.2	Связь по квантовым каналам с шумом	673
12.4	Квантовая информация в квантовых каналах с шумом	681
12.4.1	Обменная энтропия и квантовое неравенство Фано	682
12.4.2	Квантовое неравенство обработки данных	684
12.4.3	Квантовая граница Синглтона	690
12.4.4	Исправление квантовых ошибок, охлаждение и демон Максвелла	691
12.5	Запутанность как физический ресурс	693

12.5.1	Преобразование запутанности чистого состояния системы из двух компонент	695
12.5.2	Очищение и разбавление запутанности	701
12.5.3	Очищение запутанности и исправление квантовых ошибок	704
12.6	Квантовая криптография	706
12.6.1	Криптография с закрытым ключом	707
12.6.2	Усиление конфиденциальности и согласование информации	708
12.6.3	Квантовое распределение ключей	711
12.6.4	Секретность и когерентная информация	718
12.6.5	Безопасность квантового распределения ключей	720
Приложение 1. Некоторые сведения из теории вероятностей		739
Приложение 2. Теория групп		741
П2.1	Основные определения	741
П2.1.1	Образующие	742
П2.1.2	Циклические группы	743
П2.1.3	Смежные классы	743
П2.2	Представления	744
П2.2.1	Эквивалентность и приводимость	744
П2.2.2	Ортогональность	745
П2.2.3	Регулярное представление	746
П2.2.4	Преобразования Фурье	747
Приложение 3. Теорема Соловья–Китаева		749
Приложение 4. Теория чисел		758
П4.1	Начальные сведения	758
П4.2	Арифметика остатков и алгоритм Евклида	759
П4.3	Сведение разложения на простые множители к нахождению порядка элемента	767
П4.4	Цепные дроби	769
Приложение 5. Криптография с открытым ключом и система RSA		774
Приложение 6. Доказательство теоремы Липа		780
Список литературы		785
Книги на русском языке из основного списка		808
Список дополнительной литературы на русском языке		809
Предметный указатель		810