



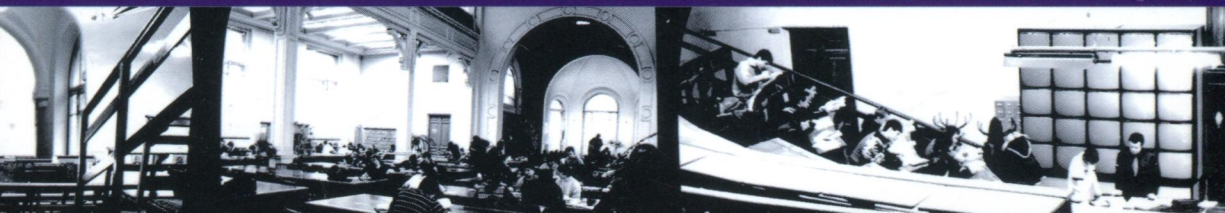
С. А. Запрягаев

Квантовые информационные системы

Теория и практика применения

- Квантовая теория
- Классическая модель информационных систем
- Квантовая модель информационных систем
- Квантовые алгоритмы
- Квантовые каналы связи
- Элементная база квантовых компьютеров
- Языки программирования квантовых компьютеров
- Практическая работа на IBM квантовых компьютерах

bhv[®]



С. А. Запрягаев

Квантовые информационные системы

Теория и практика применения

Санкт-Петербург
«БХВ-Петербург»
2023

УДК 519.6+004.42
ББК 32.973я73
3-33

Запрягаев С. А.

3-33 Квантовые информационные системы. Теория и практика применения. — СПб.: БХВ-Петербург, 2023. — 320 с.: ил. — (Учебная литература для вузов)
ISBN 978-5-9775-1710-2

Учебное пособие представляет собой введение в квантовые информационные системы. Рассмотрены основные вопросы квантовой теории, классическая и квантовая модели информационных систем, квантовые алгоритмы и квантовые каналы связи, элементная база квантовых компьютеров. Дан обзор физических методов реализации кубитов, квантовых языков программирования (Open QASM, Qiskit) и программных оболочек (IBM Q Experience, Quantum Composer, Jupiter Notebooks). Рассмотрены практические вопросы реализации квантовых алгоритмов, применения квантовых информационных систем к решению задач квантовой криптографии, использования защищенных квантовых каналов связи и др.

*Для студентов направлений «Математика и компьютерные науки»
и «Информационные системы и технологии»*

УДК 004.4
ББК 32.973.26-018.2

Группа подготовки издания:

Руководитель проекта	<i>Евгений Рыбаков</i>
Зав. редакцией	<i>Людмила Гауль</i>
Корректор	<i>Анна Брезман</i>
Дизайн серии	<i>Инны Тачиной</i>
Оформление обложки	<i>Зои Канторович</i>

Рецензенты:

А. Ф. Клиских — д-р физ.-мат. наук, проф., проф. кафедры общей физики Воронежского государственного университета;
А. С. Сидоркин — д-р физ.-мат. наук, проф., проф. кафедры экспериментальной физики Воронежского государственного университета.

Подписано в печать 29.07.22.
Формат 70×100^{1/16}. Печать офсетная. Усл. печ. л. 25,8.
Тираж 500 экз. Заказ № 5074.
"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

Отпечатано с готового оригинал-макета
ООО "Принт-М", 142300, М.О., г. Чехов, ул. Полиграфистов, д. 1

ISBN 978-5-9775-1710-2

© Запрягаев С. А., 2023
© Оформление. ООО "БХВ-Петербург", ООО "БХВ", 2023

Оглавление

Предисловие	7
Часть I Квантовая теория	12
1 Основы квантовой теории	13
1.1 Постулат состояния	13
1.2 Алгебра операторов	19
1.3 Принцип суперпозиции состояний	23
1.4 Постулат об операторах физических величин	25
1.5 Постулат об измерении физической величины	28
1.6 Постулат об эволюции квантовых состояний	31
1.7 Представление квантовых состояний и операторов	33
1.8 Координатное представление квантовой теории	38
1.9 Преобразование квантовых состояний	43
1.10 Оператор момента импульса	48
1.11 Оператор углового момента	50
1.12 Квантовая теория и уравнение Шрёдингера	53
1.13 Квантовые интегралы движения	57
1.14 Примеры решения уравнения Шрёдингера	59
2 Спин	73
2.1 Спин электрона	73
2.2 Свойства матриц Паули	75
2.3 Собственные векторы оператора спина $1/2$	78
2.4 Вращение собственных векторов матриц Паули	81
2.5 Уравнение Паули	84
2.6 Прецессия спина в однородном магнитном поле	86
2.7 Спиновый резонанс для свободного электрона	88
2.8 Многоэлектронные атомы. Молекулы	92
2.9 Кубит	99

3	Матрица плотности	102
3.1	Чистые и смешанные состояния	102
3.2	Эволюция оператора матрицы плотности	109
3.3	Спиновая матрица плотности	111
3.4	Теорема Шмидта	115
Часть II Классическая модель информационных систем		117
4	Компьютерные технологии	118
4.1	Основные понятия алгебры логики	119
4.2	Классические логические гейты	121
4.3	Обратимые логические гейты	129
4.4	Коррекция ошибок в классических каналах связи	136
4.5	Классическое шифрование. RSA алгоритм	138
Часть III Квантовая модель информационных систем		141
5	Квантовые компьютерные технологии	142
5.1	Введение	142
5.2	Сфера Блоха	144
5.3	Однокубитовые гейты	145
5.4	Квантовый интерферометр	150
5.5	Квантовый регистр	153
5.6	Многокубитовые квантовые гейты	156
5.7	Преобразование многокубитовых регистров	162
5.8	Невозможность клонирования кубита	165
5.9	Запутанные состояния	166
5.10	Декогеренция	170
5.11	Вычисление функций и квантовый параллелизм	174
5.12	Общие свойства оператора Уолша – Адамара	179
6	Квантовые алгоритмы	182
6.1	Алгоритм Дойча (Deutsch)	182
6.2	Алгоритм Дойча–Йोजи (Deutsch–Jozsa)	187
6.3	Алгоритм Саймона	191
6.4	Квантовое преобразование Фурье	195
6.5	Квантовая цепь алгоритма преобразования Фурье	198
6.6	Оценка фазы	206
6.7	Квантовая цепь оценки фазы	209
6.8	Возврат фазы в регистр данных	213

6.9	Собственные значения унитарного оператора	215
6.10	Алгоритм Шора	218
6.11	Алгоритм Гровера	224
Часть IV Квантовые каналы связи		229
7	Применение квантовых каналов связи	230
7.1	Квантовый канал связи	230
7.2	Квантовая телепортация	231
7.3	Сверхплотное кодирование	236
7.4	Коррекция ошибок в квантовых каналах связи	239
7.5	Протокол квантового распределения ключа BB84	242
7.6	Обнаружение злоумышленника в протоколе BB84	247
7.7	Протокол квантового распределения ключа B92	249
7.8	Протоколы на основе запутанных состояний	253
7.9	Атаки на протоколы распределения ключа	256
Часть V Физические реализации квантовых вычислений		259
8	Элементная база	260
8.1	Ионная ловушка	260
8.2	Ядерный магнитный резонанс	267
8.3	Сверхпроводники	271
8.4	Другие технологии	276
8.5	Квантовый компьютер IBM	278
8.5.1	Платформа IBM Quantum Experience	279
8.5.2	Quantum Composer	280
8.5.3	Язык Open QASM	285
8.5.4	Отладочный комплект Qiskit	287
Приложения		290
A	Алгоритм факторизации чисел	290
A.1	Порядок числа по модулю	291
A.2	Алгоритм разложения числа	291
B	Алгоритм Шора для произвольного периода	294
B.1	Пример	295

С	Алгоритм RSA	298
С.1	RSA-шифрование	299
С.2	Цифровая подпись	300
С.3	Взлом RSA-шифрования	300
D	Практическая работа на IBM Q	302
D.1	Работа с IBM Q	303
D.2	Пример	312
	Литература	315