

Оглавление

Благодарности	10
Введение	11
От издательства	17
Глава 1. Спин	18
«Квантовые» часы	24
Измерения в одном направлении.....	24
Измерения в разных направлениях.....	25
Измерения	27
Случайность	28
Фотоны и поляризация	30
Заключение	34
Глава 2. Линейная алгебра	36
Комплексные и действительные числа	37
Векторы.....	38
Диаграммы векторов	39
Длина вектора.....	40
Скалярное произведение.....	40
Сложение векторов	41
Ортогональные векторы	43
Умножение бра на кет	43
Произведение бра-кет и длина	44
Произведение бра-кет и ортогональность.....	45
Ортонормированный базис.....	46
Векторы как линейные комбинации базисных векторов	48
Упорядоченные базисы.....	50
Длины векторов	51
Матрицы.....	51
Вычисления с матрицами.....	54
Ортогональные и унитарные матрицы	56
Инструменты линейной алгебры.....	57

Глава 3. Спин и кубиты	59
Вероятность	59
Математика квантового спина	60
Эквивалентные векторы состояний.....	64
Базис, соответствующий заданному направлению спина	66
Поворот установки на 60°	68
Математическая модель поляризации фотона	69
Базис, соответствующий заданному направлению поляризации	71
Эксперименты с поляризованными фильтрами	71
Кубиты	74
Алиса, Боб и Ева.....	75
Амплитуды вероятности и интерференция	78
Алиса, Боб, Ева и протокол BB84.....	79
Глава 4. Запутанность	83
Кубиты Алисы и Боба не запутаны.....	84
Незапутанные кубиты.....	86
Запутанные кубиты	87
Общение со сверхсветовой скоростью	90
Стандартный базис для тензорных произведений.....	92
Как запутать кубиты?	93
Запутывание кубитов с помощью вентиля CNOT	95
Запутанные квантовые часы.....	96
Глава 5. Неравенство Белла	99
Запутанные кубиты в разных базисах	101
Эйнштейн и локальный реализм	104
Эйнштейн и скрытые переменные	106
Классическое объяснение запутанности	107
Неравенство Белла.....	109
Ответ модели квантовой механики	109
Ответ классической модели.....	111
Измерение.....	115
Протокол Экерта для квантового распределения ключей	117
Глава 6. Классическая логика, вентили и цепи	120
Логика.....	121
Отрицание	121
И.....	122
ИЛИ	122

Булева алгебра.....	123
Логическая эквивалентность	125
Функциональная полнота	126
И-НЕ.....	128
Вентили.....	131
Вентиль НЕ.....	131
Вентиль И	131
Вентиль ИЛИ.....	132
Вентиль И-НЕ	132
Цепи.....	132
И-НЕ — универсальный вентиль	134
Вентили и вычисления.....	135
Память	137
Обратимые вычисления.....	138
Управляемое НЕ.....	139
Вентиль Тоффоли	141
Вентиль Фредкина.....	144
Бильярдный компьютер.....	146
Глава 7. Квантовые вентили и цепи	152
Кубиты	153
Управляемое НЕ	154
Квантовые вентили	156
Квантовые вентили, воздействующие на один кубит	156
Вентили I и Z	157
Вентили X и Y.....	158
Вентиль Адамара.....	158
Существуют ли универсальные квантовые вентили?.....	159
Теорема о запрете клонирования	160
Квантовые и классические вычисления	163
Цепь Белла.....	164
Сверхплотное кодирование	166
Квантовая телепортация	170
Коррекция ошибок.....	174
Повторение.....	176
Коррекция с квантовым кубитом.....	177
Глава 8. Квантовые алгоритмы.....	181
Классы сложности P и NP	182
Квантовые алгоритмы быстрее классических?	185

Запрос сложности.....	185
Алгоритм Дойча.....	186
Кронекеровское произведение матриц Адамара	191
Алгоритм Дойча—Джозы	194
Шаг 1. Передача кубитов через вентили Адамара	197
Шаг 2. Передача кубитов через вентиль F.....	198
Шаг 3. Передача верхних кубитов через вентили Адамара.....	199
Шаг 4. Измерение верхних кубитов	200
Алгоритм Саймона	200
Поразрядное сложение последовательностей по модулю 2	201
Формулировка задачи Саймона	201
Скалярное произведение и матрица Адамара	203
Матрицы Адамара и задача Саймона	204
Квантовая цепь для задачи Саймона	206
Классическая часть алгоритма Саймона	209
Классы сложности	212
Квантовые алгоритмы.....	215
Глава 9. Влияние квантовых вычислений	217
Алгоритм Шора и криптоанализ.....	218
Алгоритм шифрования RSA	218
Алгоритм Шора	220
Алгоритм Гровера и поиск данных.....	223
Алгоритм Гровера	224
Применения алгоритма Гровера	228
Химия и моделирование	229
Оборудование	231
Квантовый отжиг.....	233
Квантовое превосходство и параллельные Вселенные.....	235
Вычисления	237

3

Спин и кубиты

В главе 1 описывались особенности измерения спина электрона. Мы видели, что при измерении спина в вертикальном направлении получается не непрерывный диапазон значений, а только два из них: северный полюс электрона направлен либо вертикально вверх, либо вертикально вниз. Если измерить спин в вертикальном направлении, а потом еще раз в том же направлении, в обоих случаях мы получим один и тот же результат. Если первое измерение покажет, что северный полюс электрона направлен вверх, то и второе измерение покажет то же самое. Мы также видели, что если сначала провести измерение в вертикальном направлении, а затем в горизонтальном, половина электронов будет иметь спин N , а половина — спин S в направлении 90° . Совершенно неважно, в каком направлении выполнялось первое измерение; второе измерение даст случайный выбор между N и S . В главе 2 был представлен математический аппарат линейной алгебры. Цель этой главы — соединить знания, полученные в двух первых главах, и представить математическую модель, описывающую измерение спина. Затем я покажу, как эта модель связана с кубитами. Но перед этим познакомимся с математикой вероятности.

Вероятность

Представьте, что мы много раз подряд бросаем монету и подсчитываем количество бросков и выпадений решки. Если монета правильная, без изъянов, то она с равной вероятностью будет падать орлом или решкой

вверх — отношение числа выпадений решки к общему числу бросков будет близко к $1/2$. Мы говорим, что вероятность исхода «решка» равна $0,5$.

В общем случае эксперимент — мы будем называть эксперименты измерениями — имеет ограниченное число возможных исходов. Обозначим их как E_1, E_2, \dots, E_n . Также примем, что результатом эксперимента, или измерения, может быть только один из этих исходов. Выпадение результата E_i имеет *вероятность* p_i . Вероятности — это числа от 0 до 1 и сумма вероятностей всех исходов равна 1 . В случае с броском монеты возможны два исхода, орел или решка. Если монета правильная, без изъянов, вероятность каждого события равна $1/2$.

А теперь вернемся к экспериментам со спином частиц из главы 1 и используем чуть более формальные обозначения для их описания. Допустим, мы собираемся измерить спин в направлении 0° . В данном случае возможны два исхода, которые мы обозначим как N и S . Оба связаны с определенной вероятностью. Обозначим через p_N вероятность исхода N , а через p_S — вероятность исхода S . Если мы уже знаем, что электрон имеет спин N в направлении 0° , то при повторном измерении в том же направлении мы получим тот же результат, то есть в этом случае $p_N = 1$, а $p_S = 0$. С другой стороны, если известно, что электрон имеет спин N в направлении 90° и повторное измерение выполняется в направлении 0° , мы с равной вероятностью получим исход N или S , то есть в этом случае $p_N = p_S = 0,5$.

Математика квантового спина

Теперь познакомимся с математической моделью, описывающей квантовый спин. В ней используются и вероятности, и векторы.

Основная модель задается векторным пространством. Измерение имеет множество возможных исходов. Число исходов определяется размерностью этого базового векторного пространства. Любое измерение спина имеет лишь два возможных исхода, то есть базовое векторное пространство является двумерным. Возьмем пространство \mathbb{R}^2 — это стандартная двумерная плоскость, которую все мы хорошо знаем. В нашем случае это вполне оправданно, потому что мы вращаем измерительную установку только в одной плоскости. Если бы мы захотели рассмотреть все воз-

возможные углы поворота установки в трехмерном пространстве, базовое векторное пространство все равно осталось бы двумерным — любое измерение всегда дает один из двух возможных результатов, — но вместо векторов с действительными числами нам пришлось бы использовать векторы с комплексными элементами. В этом случае базовым векторным пространством было бы комплексное двумерное пространство, обозначаемое как \mathbb{C}^2 . По причинам, перечисленным в предыдущей главе, нас вполне устроит \mathbb{R}^2 .

Мы будем рассматривать не все векторы в \mathbb{R}^2 , а только единичные. Для кетов это означает, что мы ограничимся формулой $|v\rangle = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$, где $c_1^2 + c_2^2 = 1$.

Выбор направления для измерения спина соответствует выбору упорядоченного ортонормированного базиса ($|b_1\rangle, |b_2\rangle$). Два вектора в базисе соответствуют двум возможным результатам измерений. Мы всегда будем ассоциировать N с первым базисным вектором и S — со вторым. До измерения частица имеет *состояние спина*, которое определяется линейной комбинацией $|b_1\rangle$ и $|b_2\rangle$, то есть имеет форму $c_1|b_1\rangle + c_2|b_2\rangle$. Иногда мы будем называть его *вектором состояния* или просто *состоянием*. После измерения вектор состояния перейдет в $|b_1\rangle$ или $|b_2\rangle$. Это одна из основных идей квантовой механики: измерение вызывает изменение вектора состояния. Новое состояние является одним из базисных векторов, связанных с измерением. Вероятность получения конкретного базисного вектора определяется начальным состоянием. Вероятность получить $|b_1\rangle$ равна c_1^2 ; вероятность получить $|b_2\rangle$ равна c_2^2 . Числа c_1 и c_2 называются *амплитудами вероятности*. Важно помнить, что амплитуды вероятности не являются вероятностями. Они могут быть положительными или отрицательными. Вероятностями являются квадраты этих чисел. Чтобы добавить конкретики, вернемся к экспериментам, в которых мы измеряли спин в вертикальном и горизонтальном направлениях.

Как отмечалось в предыдущей главе, упорядоченный ортонормированный базис соответствует измерению спина в вертикальном направлении и задается парой векторов ($|\uparrow\rangle, |\downarrow\rangle$), где $|\uparrow\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ и $|\downarrow\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Первый вектор в базисе соответствует электрону со спином N в направлении 0° , а второй вектор — электрону со спином S в направлении 0° .

Спин в горизонтальном направлении задается упорядоченным ортонормированным базисом $(|\rightarrow\rangle, |\leftarrow\rangle)$, где

$$|\rightarrow\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{bmatrix} \quad \text{и} \quad |\leftarrow\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}.$$

Первый вектор соответствует электрону со спином N в направлении 90° , а второй вектор — электрону со спином S в направлении 90° .

Сначала мы измеряем спин в вертикальном направлении. Первоначально мы можем не знать состояние спина входящего электрона, но это должен быть единичный вектор, и поэтому его можно записать как $c_1|\uparrow\rangle + c_2|\downarrow\rangle$, где $c_1^2 + c_2^2 = 1$. Теперь выполним измерение. Электрон отклонится либо вверх, и в этом случае перейдет в состояние $|\uparrow\rangle$, либо вниз, и в этом случае перейдет в состояние $|\downarrow\rangle$. Вероятность отклонения вверх равна c_1^2 , а вероятность отклонения вниз равна c_2^2 .

Теперь повторим тот же эксперимент, измерив спин еще раз в вертикальном направлении. Допустим, что первая пара магнитов отклонила электрон вверх. Мы знаем, что он имеет состояние спина $|\uparrow\rangle = 1|\uparrow\rangle + 0|\downarrow\rangle$. После повторного измерения состояние перейдет в $|\uparrow\rangle$ с вероятностью $1^2 = 1$ или в $|\downarrow\rangle$ с вероятностью $0^2 = 0$. Это означает, что он просто останется в состоянии $|\uparrow\rangle$ и снова отклонится вверх.

Аналогично, если при первом измерении электрон отклонился вниз, он окажется в состоянии $|\downarrow\rangle = 0|\uparrow\rangle + 1|\downarrow\rangle$. Сколько бы измерений в вертикальном направлении мы ни провели, он все равно останется в этом состоянии, то есть сколько бы раз мы ни повторили эксперимент, электрон всегда будет отклоняться вниз. Как отмечалось в предыдущей главе, повторив тот же эксперимент, мы получим тот же результат.

Теперь, вместо многократного измерения спина в вертикальном направлении, измерим его сначала в вертикальном направлении, а затем в горизонтальном. Допустим, что мы только что выполнили первое измерение — измерение в вертикальном направлении — и выяснили, что электрон имеет спин N в направлении 0° . Теперь он имеет вектор состояния $|\uparrow\rangle$. Поскольку следующее измерение выполняется в горизонтальном направлении, мы

должны записать этот вектор в терминах ортонормированного базиса, соответствующего этому направлению, то есть мы должны найти значения x_1 и x_2 , являющиеся решением уравнения $|\uparrow\rangle = x_1|\rightarrow\rangle + x_2|\leftarrow\rangle$. Мы уже знаем, как это сделать: это второй инструмент из перечисленных в конце предыдущей главы.

Сначала сконструируем матрицу A , расположив кеты из ортонормированного базиса друг за другом.

$$A = [|\rightarrow\rangle|\leftarrow\rangle] = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}.$$

Затем вычислим $A^T|\uparrow\rangle$, чтобы получить амплитуды вероятности относительно нового базиса.

$$A^T|\uparrow\rangle = \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}.$$

В результате получаем $|\uparrow\rangle = \frac{1}{\sqrt{2}}|\rightarrow\rangle + \frac{1}{\sqrt{2}}|\leftarrow\rangle$.

В результате измерения в горизонтальном направлении состояние переходит в $|\rightarrow\rangle$ с вероятностью $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$ или в $|\leftarrow\rangle$ с вероятностью $\left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$. То есть вероятность, что электрон будет иметь спин N в направлении 90° , равна вероятности, что он будет иметь спин S в направлении 90° ; обе вероятности равны точно половине.

Обратите внимание, что в действительности в этих расчетах не требовалось вычислять матрицу A . На самом деле нам нужна была только матрица A^T . Эту матрицу можно получить, если взять бра, соответствующие ортонормированному базису, и расположить их друг под другом. Конечно, векторы должны следовать в том же порядке. Порядок слева направо следования кетов соответствует порядку сверху вниз следования бра, то есть первый элемент базиса будет самым верхним бра.

В одном из экспериментов в главе 1 мы измеряли спин три раза. Первое и третье измерения производились в вертикальном направлении, а второе — в горизонтальном. Опишем третье измерение в математических терминах. После второго измерения вектор состояния нашего электрона будет иметь одно из двух значений: $|\rightarrow\rangle$ или $|\leftarrow\rangle$. Теперь мы собираемся выполнить измерение в вертикальном направлении, поэтому выразим его как линейную комбинацию вертикального ортонормированного базиса. В результате получаем

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{2}|\downarrow\rangle \quad \text{и} \quad |\leftarrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{2}|\downarrow\rangle.$$

В любом случае, в результате измерения спина в вертикальном направлении вектор состояния будет переходить либо в значение $|\uparrow\rangle$, либо в значение $|\downarrow\rangle$, то есть с вероятностью, равной половине.

Эквивалентные векторы состояний

Допустим, дано некоторое число электронов и сказано, что их спины задаются как $|\uparrow\rangle$ или $-|\uparrow\rangle$. Можно ли различить эти два случая? Есть ли такой способ измерения, с помощью которого мы могли бы отличить их друг от друга? Ответ на этот вопрос: «нет».

Чтобы убедиться в этом, предположим, что мы выбираем направление для измерения спина. Это равносильно выбору упорядоченного ортонормированного базиса. Обозначим этот базис как $(|b_1\rangle, |b_2\rangle)$.

Допустим, что электрон имеет состояние $|\uparrow\rangle$. Мы должны найти значения a и b , являющиеся решением уравнения $|\uparrow\rangle = a|b_1\rangle + b|b_2\rangle$. Вероятность, что в результате измерения спин будет иметь значение N , равна a^2 , а вероятность, что спин будет иметь значение S , равна b^2 .

Теперь допустим, что электрон имеет состояние $-|\uparrow\rangle$. Для тех же самых значений a и b мы имеем $-|\uparrow\rangle = -a|b_1\rangle - b|b_2\rangle$. То есть вероятность, что в результате измерения спин будет иметь значение N , равна $(-a)^2 = a^2$, а вероятность, что спин будет иметь значение S , равна $(-b)^2 = b^2$.

В обоих случаях мы получили одинаковые вероятности, а это значит, что нет такого способа измерения, с помощью которого можно было бы различить электроны с векторами состояний $|\uparrow\rangle$ и $-\lvert\uparrow\rangle$.

Аналогично, электроны с состоянием $|v\rangle$ невозможно отличить от электронов с состоянием $-\lvert v\rangle$. Так как эти состояния неразличимы, они считаются эквивалентными. Утверждение, что электрон имеет спин, заданный вектором $|v\rangle$, равноценно утверждению, что электрон имеет спин, заданный вектором $-\lvert v\rangle$.

Для дополнительной иллюстрации этого обстоятельства рассмотрим четыре кета:

$$\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle \quad -\frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\rangle \quad \frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\rangle \quad -\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle.$$

Согласно предыдущему замечанию, мы знаем, что

$$\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle \quad \text{и} \quad -\frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\rangle$$

эквивалентны и что

$$\frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\rangle \quad \text{и} \quad -\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle$$

тоже эквивалентны. Эти четыре кета описывают, самое большее, два различных состояния. Но что можно сказать о состояниях

$$\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle \quad \text{и} \quad \frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\rangle?$$

Являются ли они отличными друг от друга состояниями или нет?

Ответ на этот вопрос требует внимательности. Если говорить об измерении спина в вертикальном направлении, эти два кета неразличимы. В обоих случаях мы получим, что вероятности $|\uparrow\rangle$ и $|\downarrow\rangle$ равны половине. Но мы знаем, что

$$\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle = |\leftarrow\rangle \quad \text{и} \quad \frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\rangle = |\rightarrow\rangle.$$