Квантовые алгоритмы: возможности и ограничения. Лекция 1: стандартная модель

М. Вялый

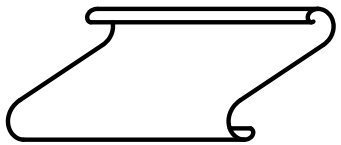
Вычислительный центр
им. А.А.Дородницына
Российской Академии наук

Санкт-Петербург, 2011

План

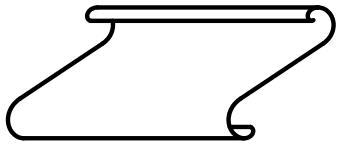
С кем и чем имеют дело в информатике?

Носитель информации:

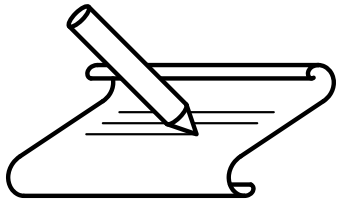


С кем и чем имеют дело в информатике?

Носитель информации:

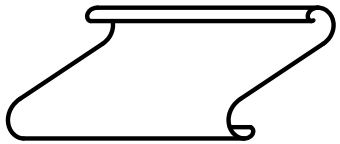


Преобразование информации

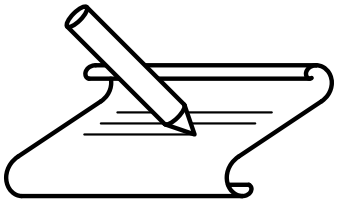


С кем и чем имеют дело в информатике?

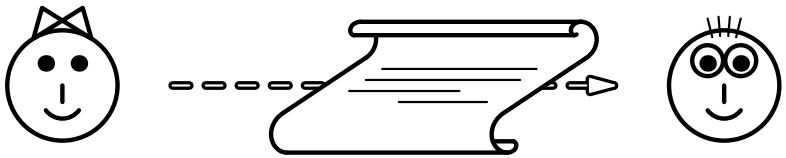
Носитель информации:



Преобразование информации

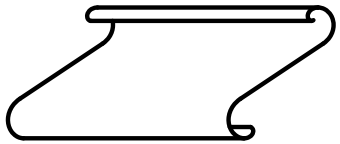


Передача информации

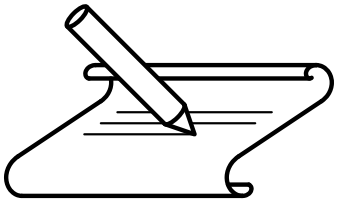


С кем и чем имеют дело в информатике?

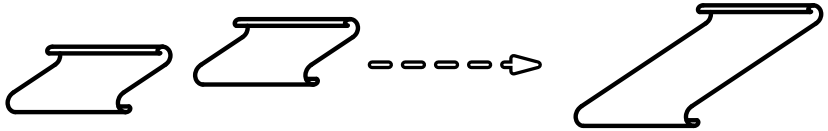
Носитель информации:



Преобразование информации

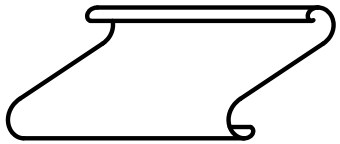


Объединение систем

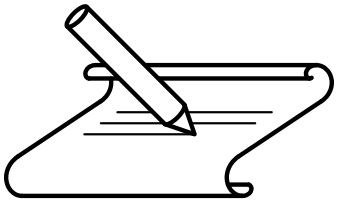


С кем и чем имеют дело в информатике?

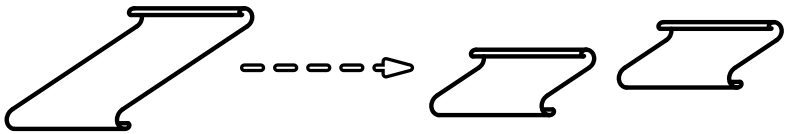
Носитель информации:



Преобразование информации

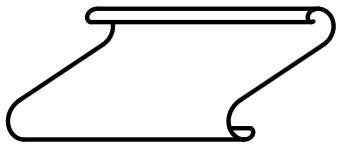


Разделение систем

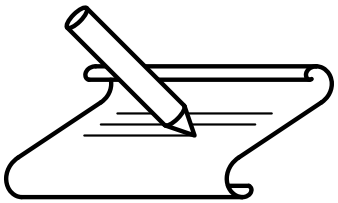


С кем и чем имеют дело в информатике?

Носитель информации:



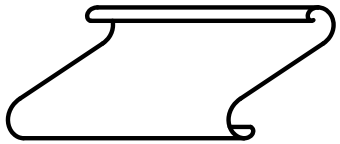
Преобразование информации



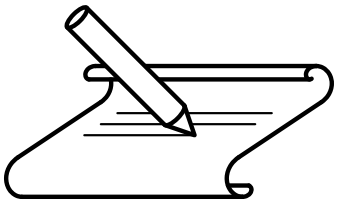
Забывание информации

С кем и чем имеют дело в информатике?

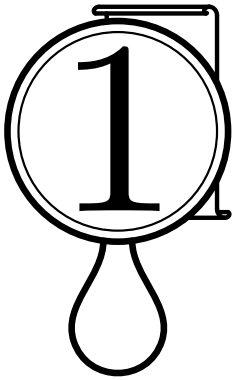
Носитель информации:



Преобразование информации



Измерение



План

Система с конечным числом состояний

- Классическая детерминированная система: конечное множество.

Пример: бит

Множество из двух элементов. Обычное обозначение 0 и 1.

- Вероятностная система.

Пример: поляризация фотона

Равновероятны оба исхода. Поэтому состояние описывается линейной комбинацией

$$\frac{1}{\sqrt{2}}|\text{горизонт}\rangle + \frac{1}{\sqrt{2}}|\text{вертик}\rangle$$

Система с конечным числом состояний

- Классическая детерминированная система: конечное множество.

Пример: бит

Множество из двух элементов. Обычное обозначение 0 и 1.

- Вероятностная система.

Пример: подбрасывание монеты

Равновероятны оба исхода. Поэтому состояние описывается линейной комбинацией

$$\frac{1}{2}\,\text{«орел»} + \frac{1}{2}\,\text{«решка»}.$$

Система с конечным числом состояний

- Классическая детерминированная система: конечное множество.

Пример: бит

Множество из двух элементов. Обычное обозначение 0 и 1.

- Вероятностная система.

Пример: подбрасывание монеты

Равновероятны оба исхода. Поэтому состояние описывается линейной комбинацией

$$\frac{1}{2}\text{«орел»} + \frac{1}{2}\text{«решка»}.$$

Система с конечным числом состояний

- Классическая детерминированная система: конечное множество.

Пример: бит

Множество из двух элементов. Обычное обозначение 0 и 1.

- Вероятностная система.

Пример: подбрасывание монеты

Равновероятны оба исхода. Поэтому состояние описывается линейной комбинацией

$$\frac{1}{2}\text{«орел»} + \frac{1}{2}\text{«решка»}.$$

Состояния вероятностной системы

Исход — это результат наблюдения над системой.

Два возможных исхода 0, 1

Отрезок

$$\{(p_0, p_1) : p_0 \geqslant 0,\ p_1 \geqslant 0,\ p_0 + p_1 = 1\}.$$

Конечное множество возможных исходов $0, 1, \ldots, n-1$

Симплекс

$$\{(p_0, \ldots, p_{n-1}) : p_i \geqslant 0,\ \sum_{i=0}^{n-1} p_i = 1\}.$$

Состояния вероятностной системы

Исход — это результат наблюдения над системой.

Два возможных исхода 0, 1

Отрезок

$$\{(p_0, p_1) : p_0 \geqslant 0,\ p_1 \geqslant 0,\ p_0 + p_1 = 1\}.$$

Конечное множество возможных исходов $0, 1, \ldots, n-1$

Симплекс

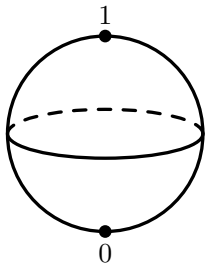
$$\{(p_0, \ldots, p_{n-1}) : p_i \geqslant 0,\ \sum_{i=0}^{n-1} p_i = 1\}.$$

План

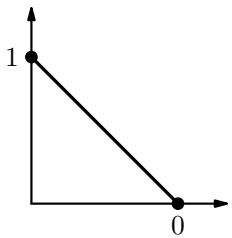
Квантовая система с двумя состояниями: кубит

Пространство состояний кубита — это 2-мерная сфера. Сфера описывает только «чистые» состояния.
В самом общем случае, когда возможны рандомизированные смеси «чистых» квантовых состояний, получается шар.

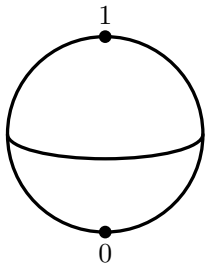
бит



кубит: сфера Блоха



случайный бит



смешанное состояние кубита: шар Блоха

Пространство чистых состояний

Пусть квантовая система имеет конечное количество n исходов (результатов наблюдения).

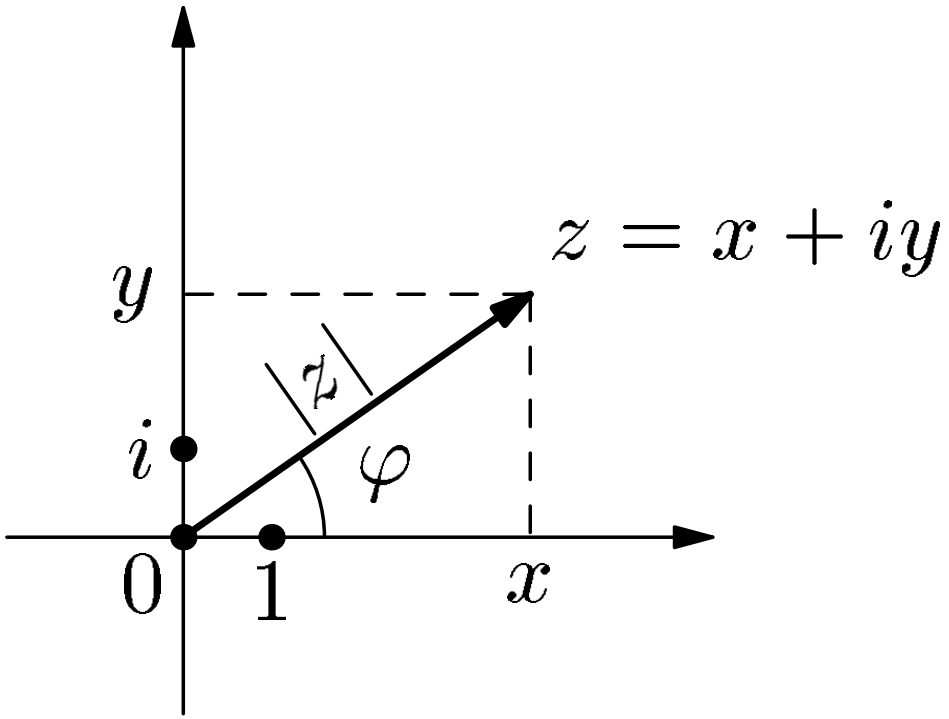
Определение

Пространство чистых состояний — $(n-1)$-мерное комплексное проективное пространство.

Напоминание

Комплексное число представляется в виде $z = x + iy$, где $i^2 = -1$, а x, y — вещественные числа.

Другая форма представления: $r(\cos\varphi + i\sin\varphi) = re^{i\varphi}$. Здесь $|z| = \sqrt{x^2 + y^2}$ — модуль числа z, φ — аргумент (фаза, как говорят физики).



d-мерное комплексное проективное пространство

Определение

Точки d-мерного комплексного проективного пространства задаются ненулевыми наборами из $d+1$ комплексного числа.
Два набора комплексных чисел задают одну и ту же точку, если они различаются на комплексный множитель:

$$(\alpha_0, \alpha_1, \ldots, \alpha_d) \sim (\beta_0, \beta_1, \ldots, \beta_d) \quad \Leftrightarrow \quad \alpha_i = \gamma\beta_i.$$

d-мерное комплексное проективное пространство

Определение

Точки d-мерного комплексного проективного пространства задаются ненулевыми наборами из $d+1$ комплексного числа.
Два набора комплексных чисел задают одну и ту же точку, если они различаются на комплексный множитель:

$$(\alpha_0, \alpha_1, \ldots, \alpha_d) \sim (\beta_0, \beta_1, \ldots, \beta_d) \quad \Leftrightarrow \quad \alpha_i = \gamma\beta_i.$$

Обычно квантовое состояние системы с n исходами задается набором n комплексных чисел — амплитуд, которые нормированы на 1:

$$\{(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) : \quad \alpha_k \in \mathbb{C}, \quad \sum_{k=0}^{n-1} |\alpha_k|^2 = 1\}.$$

d-мерное комплексное проективное пространство

Определение

Точки d-мерного комплексного проективного пространства задаются ненулевыми наборами из $d+1$ комплексного числа.
Два набора комплексных чисел задают одну и ту же точку, если они различаются на комплексный множитель:

$$(\alpha_0, \alpha_1, \ldots, \alpha_d) \sim (\beta_0, \beta_1, \ldots, \beta_d) \quad \Leftrightarrow \quad \alpha_i = \gamma\beta_i.$$

Обычно квантовое состояние системы с n исходами задается набором n комплексных чисел — амплитуд, которые нормированы на 1:

$$\{(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) : \quad \alpha_k \in \mathbb{C}, \quad \sum_{k=0}^{n-1} |\alpha_k|^2 = 1\}.$$

При этом остается еще одна степень свободы: умножение всех амплитуд на множитель $e^{i\varphi}$, по модулю равный 1 (сдвиг фазы). Состояние от такого умножения не меняется.

Вернемся к кубиту

Вопрос

Почему пространство состояний кубита (1-мерное комплексное проективное пространство) — 2-мерная вещественная сфера?

Вернемся к кубиту

Вопрос

Почему пространство состояний кубита (1-мерное комплексное проективное пространство) — 2-мерная вещественная сфера?

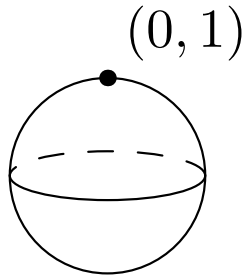
Точки вида $(\alpha_0, \alpha_1) \sim (1, \alpha_1/\alpha_0)$, $\alpha_0 \neq 0$, образуют вещественную плоскость. Есть еще одна точка $(0, \alpha)$ (бесконечно удаленная точка). Получается сфера.

Вернемся к кубиту

Вопрос

Почему пространство состояний кубита (1-мерное комплексное проективное пространство) — 2-мерная вещественная сфера?

Точки вида $(\alpha_0, \alpha_1) \sim (1, \alpha_1/\alpha_0)$, $\alpha_0 \neq 0$, образуют вещественную плоскость. Есть еще одна точка $(0, \alpha)$ (бесконечно удаленная точка). Получается сфера.



Состояния из многих кубитов

В классическом случае состояния n битов — это двоичные слова длины n и их 2^n штук.

Состояния из многих кубитов

В классическом случае состояния n битов — это двоичные слова длины n и их 2^n штук.
В вероятностном случае мы получаем «многомерное» распределение

$$(p_{i_0 i_1 \ldots i_{n-1}}), \quad p_{i_0 i_1 \ldots i_{n-1}} \geqslant 0, \quad \sum_{(i_0, i_1, \ldots, i_{n-1}) \in \{0,1\}^n} p_{i_0 i_1 \ldots i_{n-1}} = 1. \qquad (P_n)$$

Состояния из многих кубитов

В классическом случае состояния n битов — это двоичные слова длины n и их 2^n штук.
В вероятностном случае мы получаем «многомерное» распределение

$$(p_{i_0 i_1 \ldots i_{n-1}}), \quad p_{i_0 i_1 \ldots i_{n-1}} \geqslant 0, \quad \sum_{(i_0, i_1, \ldots, i_{n-1}) \in \{0,1\}^n} p_{i_0 i_1 \ldots i_{n-1}} = 1. \qquad (P_n)$$

В квантовом случае мы получаем вектор в комплексном пространстве:

$$\sum_{(i_0, i_1, \ldots, i_{n-1}) \in \{0,1\}^n} \alpha_{i_0 i_1 \ldots i_{n-1}} |i_0, i_1, \ldots, i_{n-1}\rangle, \quad \sum |\alpha_{i_0 i_1 \ldots i_{n-1}}|^2 = 1. \quad (Q_n)$$

Состояния из многих кубитов

В классическом случае состояния n битов — это двоичные слова длины n и их 2^n штук.
В вероятностном случае мы получаем «многомерное» распределение

$$(p_{i_0 i_1 \ldots i_{n-1}}), \quad p_{i_0 i_1 \ldots i_{n-1}} \geqslant 0, \quad \sum_{(i_0, i_1, \ldots, i_{n-1}) \in \{0,1\}^n} p_{i_0 i_1 \ldots i_{n-1}} = 1. \qquad (P_n)$$

В квантовом случае мы получаем вектор в комплексном пространстве:

$$\sum_{(i_0, i_1, \ldots, i_{n-1}) \in \{0,1\}^n} \alpha_{i_0 i_1 \ldots i_{n-1}} |i_0, i_1, \ldots, i_{n-1}\rangle, \quad \sum |\alpha_{i_0 i_1 \ldots i_{n-1}}|^2 = 1. \quad (Q_n)$$

Обозначения Дирака: $|\psi\rangle$ обозначает вектор, а если этот вектор принадлежит вычислительному базису, то мы между $|$ и $\rangle$ пишем его индекс.

Обратите внимание

$$(p_{i_0 i_1 \ldots i_{n-1}}), \quad p_{i_0 i_1 \ldots i_{n-1}} \geqslant 0, \quad \sum_{(i_0, i_1, \ldots, i_{n-1}) \in \{0,1\}^n} p_{i_0 i_1 \ldots i_{n-1}} = 1. \qquad (P_n)$$

$$\sum_{(i_0, i_1, \ldots, i_{n-1}) \in \{0,1\}^n} \alpha_{i_0 i_1 \ldots i_{n-1}} |i_0, i_1, \ldots, i_{n-1}\rangle, \quad \sum |\alpha_{i_0 i_1 \ldots i_{n-1}}|^2 = 1. \qquad (Q_n)$$

Замечание

Довольно часто особенную силу квантовых вычислений видят в том, что пространство состояний системы из n кубитов имеет очень большую размерность 2^n. Сравнение формул (P_n) и (Q_n) показывает неточность такого наблюдения: 300 кубитов описываются таким же количеством амплитуд, что и 300 случайных битов (вещественных параметров в два раза больше, конечно).

Объединение систем

Правило

Пространство состояний составной системы является тензорным произведением пространств состояний ее частей.

Тензорное произведение: простое определение

Если есть пространства с выделенными базисами $U = (u_1, \ldots, u_n)$; $V = (v_1, \ldots, v_k)$, то их тензорное произведение $U \otimes V$ имеет выделенный базис

$$u_j \otimes v_\ell, \quad 1 \leqslant j \leqslant n;\ 1 \leqslant \ell \leqslant k,$$
$$|j, \ell\rangle \quad \text{(в обозначениях Дирака)}.$$

Разложимые векторы

Тензорное произведение векторов билинейно

$$(\lambda u' + \mu u'') \otimes v = \lambda(u' \otimes v) + \mu(u'' \otimes v);$$
$$u \otimes (\lambda v' + \mu v'') = \lambda(u \otimes v') + \mu(u \otimes v'').$$

Используя билинейность, можно выразить тензорное произведение любой пары векторов через базисные векторы.

Разложимые вектора имеют $u \otimes v$.

В вероятностном случае разложимое распределение обладает таким свойством, что величины, относящиеся к двум подсистемам независимы.

Разложимые векторы

Тензорное произведение векторов билинейно

$$(\lambda u' + \mu u'') \otimes v = \lambda(u' \otimes v) + \mu(u'' \otimes v);$$
$$u \otimes (\lambda v' + \mu v'') = \lambda(u \otimes v') + \mu(u \otimes v'').$$

Используя билинейность, можно выразить тензорное произведение любой пары векторов через базисные векторы.

Разложимые вектора имеют $u \otimes v$.

В вероятностном случае разложимое распределение обладает таким свойством, что величины, относящиеся к двум подсистемам независимы.

Разложимые векторы

Тензорное произведение векторов билинейно

$$(\lambda u' + \mu u'') \otimes v = \lambda(u' \otimes v) + \mu(u'' \otimes v);$$
$$u \otimes (\lambda v' + \mu v'') = \lambda(u \otimes v') + \mu(u \otimes v'').$$

Используя билинейность, можно выразить тензорное произведение любой пары векторов через базисные векторы.

Разложимые вектора имеют $u \otimes v$.

В вероятностном случае разложимое распределение обладает таким свойством, что величины, относящиеся к двум подсистемам независимы.

Разложимые векторы

Тензорное произведение векторов билинейно

$$(\lambda u' + \mu u'') \otimes v = \lambda(u' \otimes v) + \mu(u'' \otimes v);$$
$$u \otimes (\lambda v' + \mu v'') = \lambda(u \otimes v') + \mu(u \otimes v'').$$

Используя билинейность, можно выразить тензорное произведение любой пары векторов через базисные векторы.
Разложимые вектора имеют $u \otimes v$.
В вероятностном случае разложимое распределение обладает таким свойством, что величины, относящиеся к двум подсистемам независимы.

Неразложимые состояния

Вероятностное распределение

$$p_{00} = \frac{1}{2}; \quad p_{11} = \frac{1}{2}; \quad p_{01} = p_{10} = 0.$$

Квантовое состояние

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Замечание

Для неразложимых состояний составных квантовых систем используется специальный термин «сцепленность». Сцепленность играет большую роль в квантовой теории информации. Как, впрочем, и понятие независимости в теории вероятностей.

Неразложимые состояния

Вероятностное распределение

$$p_{00} = \frac{1}{2}; \quad p_{11} = \frac{1}{2}; \quad p_{01} = p_{10} = 0.$$

Квантовое состояние

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Замечание

Для неразложимых состояний составных квантовых систем используется специальный термин «сцепленность». Сцепленность играет большую роль в квантовой теории информации. Как, впрочем, и понятие независимости в теории вероятностей.

Неразложимые состояния

Вероятностное распределение

$$p_{00} = \frac{1}{2}; \quad p_{11} = \frac{1}{2}; \quad p_{01} = p_{10} = 0.$$

Квантовое состояние

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

Замечание

Для неразложимых состояний составных квантовых систем используется специальный термин «сцепленность». Сцепленность играет большую роль в квантовой теории информации. Как, впрочем, и понятие независимости в теории вероятностей.

План

Наблюдение (измерение)

Основное правило

Пусть система находится в состоянии

$$\{(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) : \quad \alpha_k \in \mathbb{C}, \quad \sum_{k=0}^{n-1} |\alpha_k|^2 = 1\}.$$

Тогда при наблюдении этой системы вероятность исхода k равна $|\alpha_k|^2$.

- Умножение всех амплитуд на одно и то же число, равное по модулю 1, не меняет вероятностей исходов.
- Поэтому-то мы и считаем пространством состояний комплексное проективное пространство.
- Однако и умножение амплитуд на разные множители, равные по модулю 1, не изменяет вероятности исходов. Почему же мы не считаем все такие состояния одинаковыми? (В таком случае квантовое пространство состояний выродится в вероятностное.)

Наблюдение (измерение)

Основное правило

Пусть система находится в состоянии

$$\{(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) : \quad \alpha_k \in \mathbb{C}, \quad \sum_{k=0}^{n-1} |\alpha_k|^2 = 1\}.$$

Тогда при наблюдении этой системы вероятность исхода k равна $|\alpha_k|^2$.

- Умножение всех амплитуд на одно и то же число, равное по модулю 1, не меняет вероятностей исходов.
- Поэтому-то мы и считаем пространством состояний комплексное проективное пространство.
- Однако и умножение амплитуд на разные множители, равные по модулю 1, не изменяет вероятности исходов. Почему же мы не считаем все такие состояния одинаковыми? (В таком случае квантовое пространство состояний выродится в вероятностное.)

Наблюдение (измерение)

Основное правило

Пусть система находится в состоянии

$$\{(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) : \quad \alpha_k \in \mathbb{C}, \quad \sum_{k=0}^{n-1} |\alpha_k|^2 = 1\}.$$

Тогда при наблюдении этой системы вероятность исхода k равна $|\alpha_k|^2$.

- Умножение всех амплитуд на одно и то же число, равное по модулю 1, не меняет вероятностей исходов.
- Поэтому-то мы и считаем пространством состояний комплексное проективное пространство.
- Однако и умножение амплитуд на разные множители, равные по модулю 1, не изменяет вероятности исходов. Почему же мы не считаем все такие состояния одинаковыми? (В таком случае квантовое пространство состояний выродится в вероятностное.)

Наблюдение (измерение)

Основное правило

Пусть система находится в состоянии

$$\{(\alpha_0, \alpha_1, \ldots, \alpha_{n-1}) : \quad \alpha_k \in \mathbb{C}, \quad \sum_{k=0}^{n-1} |\alpha_k|^2 = 1\}.$$

Тогда при наблюдении этой системы вероятность исхода k равна $|\alpha_k|^2$.

- Умножение всех амплитуд на одно и то же число, равное по модулю 1, не меняет вероятностей исходов.
- Поэтому-то мы и считаем пространством состояний комплексное проективное пространство.
- Однако и умножение амплитуд на **разные** множители, равные по модулю 1, не изменяет вероятности исходов. Почему же мы не считаем все такие состояния одинаковыми? (В таком случае квантовое пространство состояний выродится в вероятностное.)

Ответ

Мы считаем состояния разными, если можно опытным путем обнаружить отличия между ними.
Разницу между состояниями, амплитуды которых различаются лишь фазовыми множителями (модуль равен 1), можно обнаружить двумя способами:

- Выполнить некоторое преобразование (одно и то же в обоих случаях) и потом произвести то же самое измерение.
- Выполнить измерение другим прибором.

Ответ

Мы считаем состояния разными, если можно опытным путем обнаружить отличия между ними.
Разницу между состояниями, амплитуды которых различаются лишь фазовыми множителями (модуль равен 1), можно обнаружить двумя способами:

- Выполнить некоторое преобразование (одно и то же в обоих случаях) и потом произвести то же самое измерение.
- Выполнить измерение другим прибором.

Свойства измерения

Важно!

Состояние системы после наблюдения k описывается набором чисел

$$(\underbrace{0,\ldots,0}_{k},1,\underbrace{0,\ldots,0}_{n-k-1}).$$

Повторные наблюдения будут давать k с вероятностью 1 (если с системой ничего не делать).
Это полностью аналогично вероятностному случаю: когда подброшенная монета упала на «орла», она так и будет лежать этой стороной вверх, если ее не трогать.

Еще важнее!!

В квантовой физике могут быть разные приборы для наблюдения.
Последовательные измерения разными приборами могут менять состояние системы.

Свойства измерения

Важно!

Состояние системы после наблюдения k описывается набором чисел

$$(\underbrace{0,\ldots,0}_{k},1,\underbrace{0,\ldots,0}_{n-k-1}).$$

Повторные наблюдения будут давать k с вероятностью 1 (если с системой ничего не делать).
Это полностью аналогично вероятностному случаю: когда подброшенная монета упала на «орла», она так и будет лежать этой стороной вверх, если ее не трогать.

Еще важнее!!

В квантовой физике могут быть разные приборы для наблюдения.
Последовательные измерения разными приборами могут менять состояние системы.

Свойства измерения

Важно!

Состояние системы после наблюдения k описывается набором чисел

$$(\underbrace{0,\ldots,0}_{k},1,\underbrace{0,\ldots,0}_{n-k-1}).$$

Повторные наблюдения будут давать k с вероятностью 1 (если с системой ничего не делать).
Это полностью аналогично вероятностному случаю: когда подброшенная монета упала на «орла», она так и будет лежать этой стороной вверх, если ее не трогать.

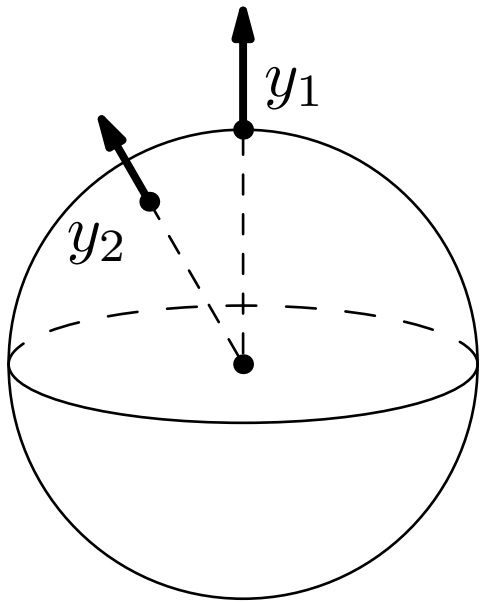
Еще важнее!!

В квантовой физике могут быть разные приборы для наблюдения.
Последовательные измерения разными приборами могут менять состояние системы.

Пример с кубитом и сферой Блоха

Прибор описывается направлением x из центра сферы Блоха (это один и тот же прибор, но по-разному повернутый в пространстве). Вероятность наблюдения 1 в состоянии, описываемом вектором y равна

$$\frac{1 + x \cdot y}{2} .$$



Пусть измерение прибором y_1 дало исход 1. Состояние кубита после измерения стало y_1. Оно обязательно изменится после измерения прибором y_2.

Что такое прибор в нашем формализме?

Ответ

Прибор — это ортонормированный базис $\{u_k\}$ в n-мерном унитарном пространстве:

$$u_k \cdot u_\ell = \delta_{k\ell} = \begin{cases} 1, & \text{если } k = \ell, \\ 0, & \text{иначе.} \end{cases}$$

Слово «унитарный» означает, что пространство снабжено эрмитовым скалярным произведением

$$(\alpha_0, \ldots, \alpha_{n-1}) \cdot (\beta_0, \ldots, \beta_{n-1}) = \alpha_0^* \beta_0 + \cdots + \alpha_{n-1}^* \beta_{n-1}.$$

Здесь $z^* = x - iy$ обозначает число, комплексно сопряженное числу $z = x + iy$.

Амплитуда состояния x относительно k-го вектора u_k в базисе равна скалярному произведению $x \cdot u_k$.

Это не то скалярное произведение, которое использовалось в примере со сферой Блоха!

Что такое прибор в нашем формализме?

Ответ

Прибор — это ортонормированный базис $\{u_k\}$ в n-мерном унитарном пространстве:

$$u_k \cdot u_\ell = \delta_{k\ell} = \begin{cases} 1, & \text{если } k = \ell, \\ 0, & \text{иначе.} \end{cases}$$

Слово «унитарный» означает, что пространство снабжено эрмитовым скалярным произведением

$$(\alpha_0, \ldots, \alpha_{n-1}) \cdot (\beta_0, \ldots, \beta_{n-1}) = \alpha_0^* \beta_0 + \cdots + \alpha_{n-1}^* \beta_{n-1}.$$

Здесь $z^* = x - iy$ обозначает число, комплексно сопряженное числу $z = x + iy$.

Амплитуда состояния x относительно k-го вектора u_k в базисе равна скалярному произведению $x \cdot u_k$.

Это не то скалярное произведение, которое использовалось в примере со сферой Блоха!

Стандартное предположение

Мы почти всегда будем обсуждать ситуации, в которых «прибор» фиксирован. Поэтому у нас, как и в вероятностном случае, есть выделенный базис, который обычно называют вычислительным базисом.

Стандартное предположение

Мы почти всегда будем обсуждать ситуации, в которых «прибор» фиксирован. Поэтому у нас, как и в вероятностном случае, есть выделенный базис, который обычно называют вычислительным базисом.

В этом случае разницу между состояниями, амплитуды которых различаются лишь фазовыми множителями, можно обнаружить, применяя одно и то же преобразование к обоим системам.

Преобразования чистых состояний

Постулат стандартной квантовой механики

Преобразования должны быть линейными.

Правило

Возможны преобразования, задаваемые произвольными унитарными операторами:

$$\psi \mapsto U\psi, \quad \text{где } U^\dagger U = I.$$

Преобразования чистых состояний

Постулат стандартной квантовой механики

Преобразования должны быть линейными.

Правило

Возможны преобразования, задаваемые произвольными унитарными операторами:

$$\psi \mapsto U\psi, \quad \text{где } U^\dagger U = I.$$

Преобразования чистых состояний

Постулат стандартной квантовой механики

Преобразования должны быть линейными.

Правило

Возможны преобразования, задаваемые произвольными унитарными операторами:

$$\psi \mapsto U\psi, \quad \text{где } U^\dagger U = I.$$

Унитарный оператор сохраняет длину вектора

$$\langle\psi|U^\dagger U|\psi\rangle = \langle\psi|\psi\rangle$$

и, более общим образом, скалярное произведение между векторами

$$\langle\xi|U^\dagger U|\psi\rangle = \langle\xi|\psi\rangle$$

Обозначения Дирака: более тесное знакомство

- Кет-векторы: $|\psi\rangle \in V$ (вектор-столбцы).
- Бра-векторы: $\langle\psi| \in V^*$ — линейные функционалы на V (вектор-строки).
- Скалярное произведение: $\langle\psi|\xi\rangle$. Индуцирует изоморфизм $V \to V^*$:

$$|\psi\rangle \mapsto \langle\psi|; \quad \langle\psi|(|\xi\rangle) = \langle\psi|\xi\rangle.$$

Пример

$$|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} i \\ 1 \end{pmatrix}, \qquad \langle\psi| = \frac{1}{\sqrt{2}} \begin{pmatrix} -i & 1 \end{pmatrix}.$$

Обозначения Дирака: более тесное знакомство

- Кет-векторы: $|\psi\rangle \in V$ (вектор-столбцы).
- Бра-векторы: $\langle\psi| \in V^*$ — линейные функционалы на V (вектор-строки).
- Скалярное произведение: $\langle\psi|\xi\rangle$. Индуцирует изоморфизм $V \to V^*$:

$$|\psi\rangle \mapsto \langle\psi|; \quad \langle\psi|(|\xi\rangle) = \langle\psi|\xi\rangle.$$

Пример

$$|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} i \\ 1 \end{pmatrix}, \qquad \langle\psi| = \frac{1}{\sqrt{2}} \begin{pmatrix} -i & 1 \end{pmatrix}.$$

Обозначения Дирака: более тесное знакомство

- Кет-векторы: $|\psi\rangle \in V$ (вектор-столбцы).
- Бра-векторы: $\langle\psi| \in V^*$ — линейные функционалы на V (вектор-строки).
- Скалярное произведение: $\langle\psi|\xi\rangle$. Индуцирует изоморфизм $V \to V^*$:

$$|\psi\rangle \mapsto \langle\psi|; \quad \langle\psi|(|\xi\rangle) = \langle\psi|\xi\rangle.$$

Пример

$$|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} i \\ 1 \end{pmatrix}, \qquad \langle\psi| = \frac{1}{\sqrt{2}} \begin{pmatrix} -i & 1 \end{pmatrix}.$$

Обозначения Дирака: более тесное знакомство

- Кет-векторы: $|\psi\rangle \in V$ (вектор-столбцы).
- Бра-векторы: $\langle\psi| \in V^*$ — линейные функционалы на V (вектор-строки).
- Скалярное произведение: $\langle\psi|\xi\rangle$. Индуцирует изоморфизм $V \to V^*$:

$$|\psi\rangle \mapsto \langle\psi|; \quad \langle\psi|(|\xi\rangle) = \langle\psi|\xi\rangle.$$

Пример

$$|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} i \\ 1 \end{pmatrix}, \qquad \langle\psi| = \frac{1}{\sqrt{2}} \begin{pmatrix} -i & 1 \end{pmatrix}.$$

Операторы и матрицы в обозначениях Дирака

- $\langle\xi|A|\eta\rangle = \langle\xi|A|\eta\rangle = \langle\xi|A|\eta\rangle$
- Второе равенство задает линейный функционал $\langle\psi| = \langle\xi|A$.
- Соответствующий кет-вектор $|\psi\rangle$ получается из $|\xi\rangle$ применением линейного оператора $A^\dagger$, который называется эрмитово сопряженным к A.
- Из определения сразу следует, что

$$\langle A^\dagger\xi|\eta\rangle = \langle\xi|A|\eta\rangle.$$

- Операторы можно задавать матрицами в ортонормированном базисе:

$$A = \sum_{j,k} a_{jk}|j\rangle\langle k|, \quad \text{где } a_{jk} = \langle j|A|k\rangle \text{ — матричный элемент.}$$

Упражнение

Проверьте, что матрица оператора $A^\dagger$ получается транспонированием и комплексным сопряжением: $(A^\dagger)_{jk} = (A_{kj})^*$.

Операторы и матрицы в обозначениях Дирака

- $\langle\xi|A|\eta\rangle = \langle\xi|A|\eta\rangle = \langle\xi|A|\eta\rangle$
- Второе равенство задает линейный функционал $\langle\psi| = \langle\xi|A$.
- Соответствующий кет-вектор $|\psi\rangle$ получается из $|\xi\rangle$ применением линейного оператора $A^\dagger$, который называется эрмитово сопряженным к A.
- Из определения сразу следует, что

$$\langle A^\dagger\xi|\eta\rangle = \langle\xi|A|\eta\rangle.$$

- Операторы можно задавать матрицами в ортонормированном базисе:

$$A = \sum_{j,k} a_{jk}|j\rangle\langle k|, \quad \text{где } a_{jk} = \langle j|A|k\rangle \text{ — матричный элемент.}$$

Упражнение

Проверьте, что матрица оператора $A^\dagger$ получается транспонированием и комплексным сопряжением: $(A^\dagger)_{jk} = (A_{kj})^*$.

Операторы и матрицы в обозначениях Дирака

- $\langle\xi|A|\eta\rangle = \langle\xi|A|\eta\rangle = \langle\xi|A|\eta\rangle$
- Второе равенство задает линейный функционал $\langle\psi| = \langle\xi|A$.
- Соответствующий кет-вектор $|\psi\rangle$ получается из $|\xi\rangle$ применением линейного оператора $A^\dagger$, который называется эрмитово сопряженным к A.
- Из определения сразу следует, что

$$\langle A^\dagger\xi|\eta\rangle = \langle\xi|A|\eta\rangle.$$

- Операторы можно задавать матрицами в ортонормированном базисе:

$$A = \sum_{j,k} a_{jk}|j\rangle\langle k|, \quad \text{где } a_{jk} = \langle j|A|k\rangle \text{ — матричный элемент.}$$

Упражнение

Проверьте, что матрица оператора $A^\dagger$ получается транспонированием и комплексным сопряжением: $(A^\dagger)_{jk} = (A_{kj})^*$.

Операторы и матрицы в обозначениях Дирака

- $\langle\xi|A|\eta\rangle = \langle\xi|A|\eta\rangle = \langle\xi|A|\eta\rangle$
- Второе равенство задает линейный функционал $\langle\psi| = \langle\xi|A$.
- Соответствующий кет-вектор $|\psi\rangle$ получается из $|\xi\rangle$ применением линейного оператора $A^\dagger$, который называется эрмитово сопряженным к A.
- Из определения сразу следует, что

$$\langle A^\dagger\xi|\eta\rangle = \langle\xi|A|\eta\rangle.$$

- Операторы можно задавать матрицами в ортонормированном базисе:

$$A = \sum_{j,k} a_{jk}|j\rangle\langle k|, \quad \text{где } a_{jk} = \langle j|A|k\rangle \text{ — матричный элемент.}$$

Упражнение

Проверьте, что матрица оператора $A^\dagger$ получается транспонированием и комплексным сопряжением: $(A^\dagger)_{jk} = (A_{kj})^*$.

Операторы и матрицы в обозначениях Дирака

- $\langle\xi|A|\eta\rangle = \langle\xi|A|\eta\rangle = \langle\xi|A|\eta\rangle$
- Второе равенство задает линейный функционал $\langle\psi| = \langle\xi|A$.
- Соответствующий кет-вектор $|\psi\rangle$ получается из $|\xi\rangle$ применением линейного оператора $A^\dagger$, который называется эрмитово сопряженным к A.
- Из определения сразу следует, что

$$\langle A^\dagger\xi|\eta\rangle = \langle\xi|A|\eta\rangle.$$

- Операторы можно задавать матрицами в ортонормированном базисе:

$$A = \sum_{j,k} a_{jk}|j\rangle\langle k|, \quad \text{где } a_{jk} = \langle j|A|k\rangle \text{ — матричный элемент.}$$

Упражнение

Проверьте, что матрица оператора $A^\dagger$ получается транспонированием и комплексным сопряжением: $(A^\dagger)_{jk} = (A_{kj})^*$.

Операторы и матрицы в обозначениях Дирака

- $\langle\xi|A|\eta\rangle = \langle\xi|A|\eta\rangle = \langle\xi|A|\eta\rangle$
- Второе равенство задает линейный функционал $\langle\psi| = \langle\xi|A$.
- Соответствующий кет-вектор $|\psi\rangle$ получается из $|\xi\rangle$ применением линейного оператора $A^\dagger$, который называется эрмитово сопряженным к A.
- Из определения сразу следует, что

$$\langle A^\dagger\xi|\eta\rangle = \langle\xi|A|\eta\rangle.$$

- Операторы можно задавать матрицами в ортонормированном базисе:

$$A = \sum_{j,k} a_{jk}|j\rangle\langle k|, \quad \text{где } a_{jk} = \langle j|A|k\rangle \text{ — матричный элемент.}$$

Упражнение

Проверьте, что матрица оператора $A^\dagger$ получается транспонированием и комплексным сопряжением: $(A^\dagger)_{jk} = (A_{kj})^*$.

Какие бывают унитарные операторы

Теорема

Для любого унитарного оператора есть ортонормированный базис, в котором его матрица диагональна:

$$U_{jk} = \lambda_j \delta_{jk}.$$

Из условия унитарности следует, что $\lambda_j^* \lambda_j = 1$, т. е. все собственные числа унитарного оператора равны по модулю 1.

В вычислительном базисе унитарный оператор записывается матрицей, столбцы (и строки) которой образуют ортонормированный базис.

Эрмитовы операторы

Определение

Оператор A эрмитов, если $A^\dagger = A$.

Теорема

Для любого эрмитова оператора есть ортонормированный базис, в котором его матрица диагональна.

Следствие

Собственные числа эрмитова оператора вещественны: $a_{kk} = a^*_{kk}$

Эрмитовы операторы

Определение

Оператор A эрмитов, если $A^\dagger = A$.

Теорема

Для любого эрмитова оператора есть ортонормированный базис, в котором его матрица диагональна.

Следствие

Собственные числа эрмитова оператора вещественны: $a_{kk} = a^*_{kk}$

Эрмитовы операторы

Определение

Оператор A эрмитов, если $A^\dagger = A$.

Теорема

Для любого эрмитова оператора есть ортонормированный базис, в котором его матрица диагональна.

Следствие

Собственные числа эрмитова оператора вещественны: $a_{kk} = a^*_{kk}$

Наблюдаемые

Наблюдаемая A — это эрмитов оператор. Возможные значения наблюдаемой — собственные числа A.

Правило из физики

Если оператор A имеет собственные числа λ_k и собственные векторы $|\psi_k\rangle$, то при измерении состояния

$$|\psi\rangle = \sum_k c_k |\psi_k\rangle$$

наблюдается значение λ_k с вероятностью $|c_k|^2$.

Среднее значение наблюдаемой

$$E(|\psi\rangle, A) = \sum_k |c_k|^2 \lambda_k = \sum_k \langle \psi_k | c_k^* c_k \lambda_k | \psi_k \rangle = \langle \psi | A | \psi \rangle.$$

Наблюдаемые

Наблюдаемая A — это эрмитов оператор. Возможные значения наблюдаемой — собственные числа A.

Правило из физики

Если оператор A имеет собственные числа λ_k и собственные векторы $|\psi_k\rangle$, то при измерении состояния

$$|\psi\rangle = \sum_k c_k |\psi_k\rangle$$

наблюдается значение λ_k с вероятностью $|c_k|^2$.

Среднее значение наблюдаемой

$$E(|\psi\rangle, A) = \sum_k |c_k|^2 \lambda_k = \sum_k \langle\psi_k| c_k^* c_k \lambda_k |\psi_k\rangle = \langle\psi|A|\psi\rangle.$$

Наблюдаемые

Наблюдаемая A — это эрмитов оператор. Возможные значения наблюдаемой — собственные числа A.

Правило из физики

Если оператор A имеет собственные числа λ_k и собственные векторы $|\psi_k\rangle$, то при измерении состояния

$$|\psi\rangle = \sum_k c_k |\psi_k\rangle$$

наблюдается значение λ_k с вероятностью $|c_k|^2$.

Среднее значение наблюдаемой

$$E(|\psi\rangle, A) = \sum_k |c_k|^2 \lambda_k = \sum_k \langle \psi_k | c_k^* c_k \lambda_k | \psi_k \rangle = \langle \psi | A | \psi \rangle.$$

События

- Событие L — подпространство унитарного пространства.
- Наблюдаемая, связанная с событием: проектор на подпространство Π_L.
- Собственные числа проектора равны 1 (событие происходит) и 0 (событие не происходит).
- Вероятность события в состоянии $|\psi\rangle$

$$\mathbf{Pr}(|\psi\rangle, L) = \langle\psi|\Pi_L|\psi\rangle = \langle\psi|\Pi_L^\dagger\Pi_L|\psi\rangle,$$

так как $\Pi_L^2 = \Pi_L$.

- Вероятность события равна квадрату длину проекции вектора состояния на подпространство, отвечающее этому событию.

События

- Событие L — подпространство унитарного пространства.
- Наблюдаемая, связанная с событием: проектор на подпространство Π_L.
- Собственные числа проектора равны 1 (событие происходит) и 0 (событие не происходит).
- Вероятность события в состоянии $|\psi\rangle$

$$\mathbf{Pr}(|\psi\rangle, L) = \langle\psi|\Pi_L|\psi\rangle = \langle\psi|\Pi_L^\dagger\Pi_L|\psi\rangle,$$

так как $\Pi_L^2 = \Pi_L$.

- Вероятность события равна квадрату длину проекции вектора состояния на подпространство, отвечающее этому событию.

События

- Событие L — подпространство унитарного пространства.
- Наблюдаемая, связанная с событием: проектор на подпространство Π_L.
- Собственные числа проектора равны 1 (событие происходит) и 0 (событие не происходит).
- Вероятность события в состоянии $|\psi\rangle$

$$\mathbf{Pr}(|\psi\rangle, L) = \langle\psi|\Pi_L|\psi\rangle = \langle\psi|\Pi_L^\dagger\Pi_L|\psi\rangle,$$

так как $\Pi_L^2 = \Pi_L$.

- Вероятность события равна квадрату длину проекции вектора состояния на подпространство, отвечающее этому событию.

События

- Событие L — подпространство унитарного пространства.
- Наблюдаемая, связанная с событием: проектор на подпространство Π_L.
- Собственные числа проектора равны 1 (событие происходит) и 0 (событие не происходит).
- Вероятность события в состоянии $|\psi\rangle$

$$\mathbf{Pr}(|\psi\rangle, L) = \langle\psi|\Pi_L|\psi\rangle = \langle\psi|\Pi_L^\dagger\Pi_L|\psi\rangle,$$

  так как $\Pi_L^2 = \Pi_L$.
- Вероятность события равна квадрату длину проекции вектора состояния на подпространство, отвечающее этому событию.

События

- Событие L — подпространство унитарного пространства.
- Наблюдаемая, связанная с событием: проектор на подпространство Π_L.
- Собственные числа проектора равны 1 (событие происходит) и 0 (событие не происходит).
- Вероятность события в состоянии $|\psi\rangle$

$$\mathbf{Pr}(|\psi\rangle, L) = \langle\psi|\Pi_L|\psi\rangle = \langle\psi|\Pi_L^\dagger\Pi_L|\psi\rangle,$$

  так как $\Pi_L^2 = \Pi_L$.
- Вероятность события равна квадрату длину проекции вектора состояния на подпространство, отвечающее этому событию.

Преобразования составной системы

Если мы применяем оператор U к первой части (первому регистру) составной системы AB, то на составную систему действует оператор $U \otimes I$.

Определение

Тензорное произведение операторов на разложимых векторах действует покомпонентно:

$$Z = X \otimes Y \;\Leftrightarrow\; Z(u \otimes v) = (Xu) \otimes (Yv),$$

а на остальные продолжается по линейности.

Вопрос

Почему это определение корректно? (Не зависит от выбора представления суммой разложимых векторов.)

Преобразования составной системы

Если мы применяем оператор U к первой части (первому регистру) составной системы AB, то на составную систему действует оператор $U \otimes I$.

Определение

Тензорное произведение операторов на разложимых векторах действует покомпонентно:

$$Z = X \otimes Y \;\Leftrightarrow\; Z(u \otimes v) = (Xu) \otimes (Yv),$$

а на остальные продолжается по линейности.

Вопрос

Почему это определение корректно? (Не зависит от выбора представления суммой разложимых векторов.)

Преобразования составной системы

Если мы применяем оператор U к первой части (первому регистру) составной системы AB, то на составную систему действует оператор $U \otimes I$.

Определение

Тензорное произведение операторов на разложимых векторах действует покомпонентно:

$$Z = X \otimes Y \;\Leftrightarrow\; Z(u \otimes v) = (Xu) \otimes (Yv),$$

а на остальные продолжается по линейности.

Вопрос

Почему это определение корректно? (Не зависит от выбора представления суммой разложимых векторов.)

Корректность определения тензорного произведения операторов

Задача

Пусть $\alpha\colon U \times V \to W$ — билинейное отображение. Тогда существует единственное линейное отображение $\beta\colon U \otimes V \to W$, для которого равенство $\beta(u \otimes v) = \alpha(u, v)$ выполняется для любых векторов $u \in U$, $v \in V$.

Если $\alpha(u, v) = (Xu) \otimes (Yv)$, то β является искомым тензорным произведением.

Корректность определения тензорного произведения операторов

Задача

Пусть $\alpha\colon U \times V \to W$ — билинейное отображение. Тогда существует единственное линейное отображение $\beta\colon U \otimes V \to W$, для которого равенство $\beta(u \otimes v) = \alpha(u, v)$ выполняется для любых векторов $u \in U$, $v \in V$.

Если $\alpha(u, v) = (Xu) \otimes (Yv)$, то β является искомым тензорным произведением.

Свойства тензорного произведения операторов

Задача

Докажите, что тензорное произведение унитарных операторов унитарно.

Указание: используйте следующий факт.

Упражнение

Проверьте мультипликативность скалярного произведения на разложимых векторах в тензорном произведении унитарных пространств

$$\langle \psi', \xi' | \psi'', \xi'' \rangle = \langle \psi' | \psi'' \rangle \cdot \langle \xi' | \xi'' \rangle.$$

Свойства тензорного произведения операторов

Задача

Докажите, что тензорное произведение унитарных операторов унитарно.

Указание: используйте следующий факт.

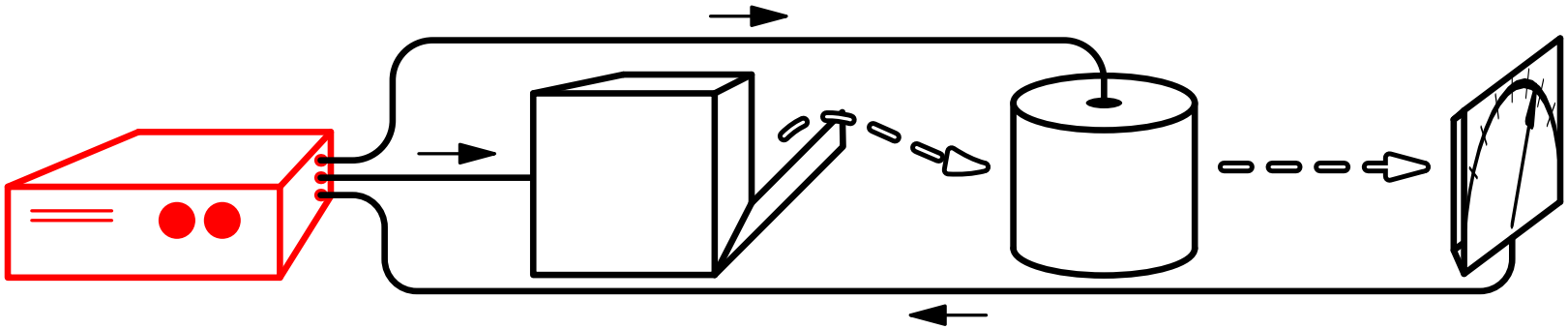
Упражнение

Проверьте мультипликативность скалярного произведения на разложимых векторах в тензорном произведении унитарных пространств

$$\langle \psi', \xi' | \psi'', \xi'' \rangle = \langle \psi' | \psi'' \rangle \cdot \langle \xi' | \xi'' \rangle.$$

План

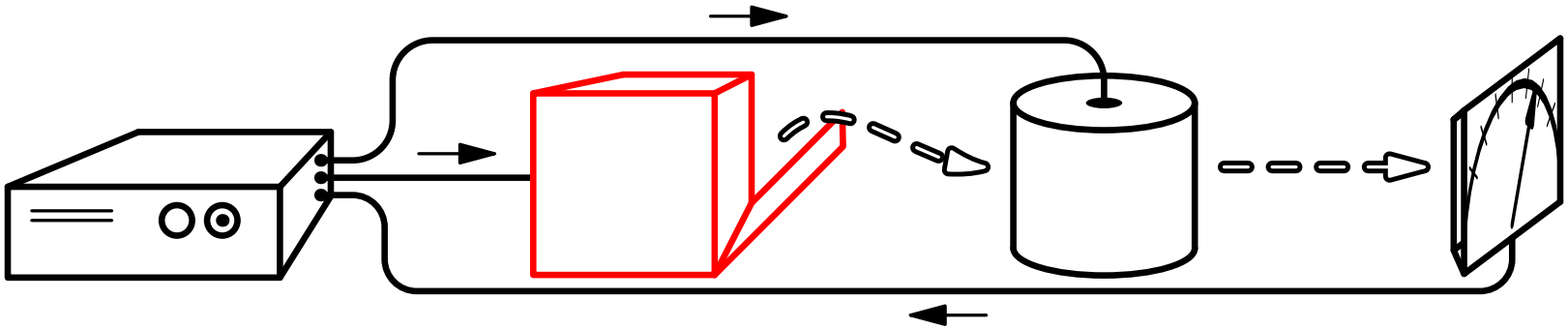
Использование квантового ресурса в алгоритмах



Использование квантового ресурса в алгоритмах

- Предварительные манипуляции с классическими системами;
- приготовление некоторого чистого состояния (обычно это одно из состояний вычислительного базиса);
- унитарные преобразования;
- измерение в вычислительном базисе;
- обработка результатов измерения классическими средствами;
- циклическое повторение предыдущих шагов при необходимости.

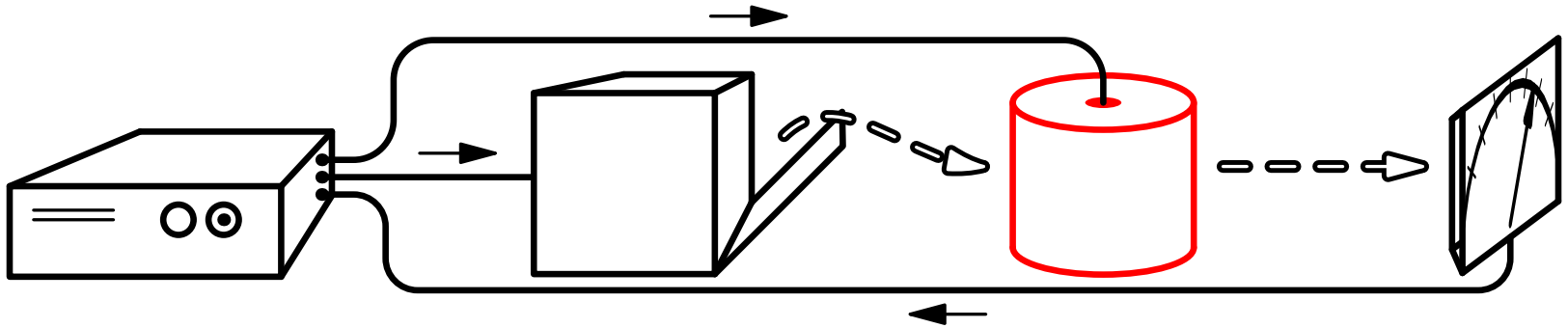
Использование квантового ресурса в алгоритмах



Использование квантового ресурса в алгоритмах

- Предварительные манипуляции с классическими системами;
- приготовление некоторого чистого состояния (обычно это одно из состояний вычислительного базиса);
- унитарные преобразования;
- измерение в вычислительном базисе;
- обработка результатов измерения классическими средствами;
- циклическое повторение предыдущих шагов при необходимости.

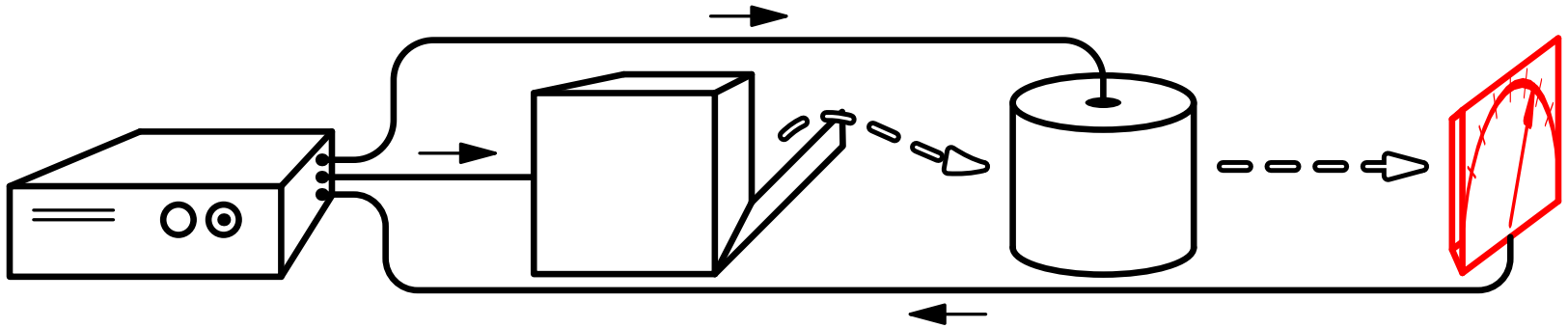
Использование квантового ресурса в алгоритмах



Использование квантового ресурса в алгоритмах

- Предварительные манипуляции с классическими системами;
- приготовление некоторого чистого состояния (обычно это одно из состояний вычислительного базиса);
- унитарные преобразования;
- измерение в вычислительном базисе;
- обработка результатов измерения классическими средствами;
- циклическое повторение предыдущих шагов при необходимости.

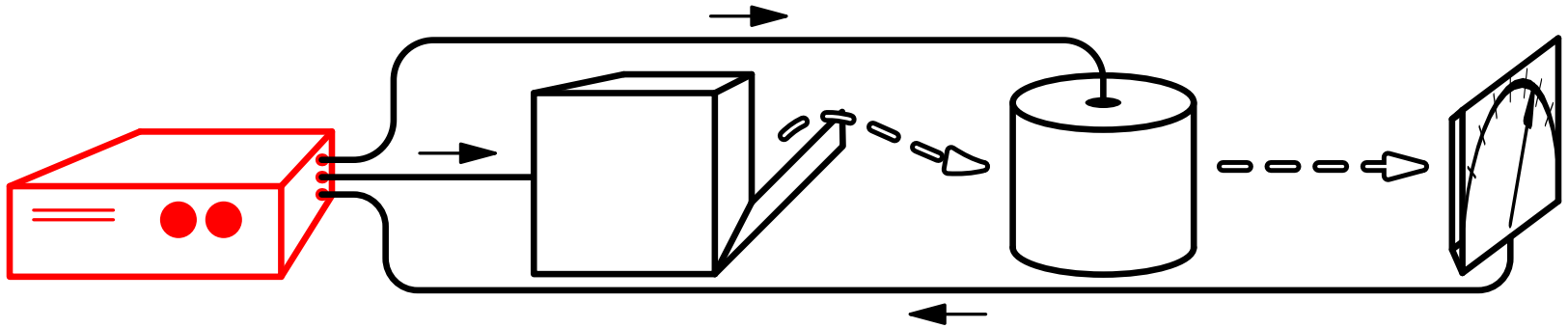
Использование квантового ресурса в алгоритмах



Использование квантового ресурса в алгоритмах

- Предварительные манипуляции с классическими системами;
- приготовление некоторого чистого состояния (обычно это одно из состояний вычислительного базиса);
- унитарные преобразования;
- измерение в вычислительном базисе;
- обработка результатов измерения классическими средствами;
- циклическое повторение предыдущих шагов при необходимости.

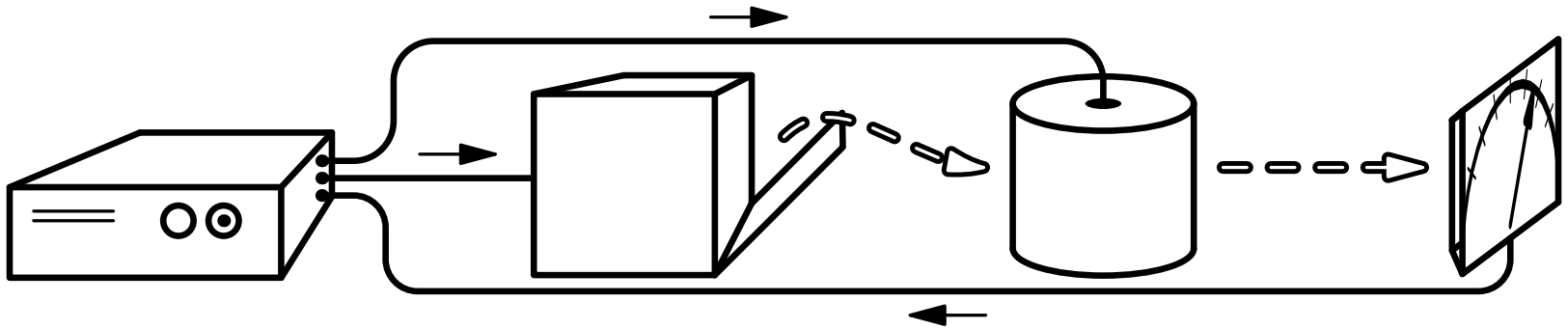
Использование квантового ресурса в алгоритмах



Использование квантового ресурса в алгоритмах

- Предварительные манипуляции с классическими системами;
- приготовление некоторого чистого состояния (обычно это одно из состояний вычислительного базиса);
- унитарные преобразования;
- измерение в вычислительном базисе;
- обработка результатов измерения классическими средствами;
- циклическое повторение предыдущих шагов при необходимости.

Использование квантового ресурса в алгоритмах



Использование квантового ресурса в алгоритмах

- Предварительные манипуляции с классическими системами;
- приготовление некоторого чистого состояния (обычно это одно из состояний вычислительного базиса);
- унитарные преобразования;
- измерение в вычислительном базисе;
- обработка результатов измерения классическими средствами;
- циклическое повторение предыдущих шагов при необходимости.