Лекция 13. Квантовые алгоритмы

14 Декабря, 2015

Теория алгоритмов 2015

Определение

$\psi(x, y, z, r)$ - *вероятность нахождения данной частицы в данном месте в данное время.*

С помощью квантовых свойств можно построить машину, которая будет хранить кубиты. Кубиты могут находиться в трех состояниях: 1, 0 и неопределенность(пока не измерили).

Определение

$\alpha|0> +\beta|1>$ - *запись состояния кубита.* α,β - *коэффициенты, причем* α^2, β^2 - *вероятность измерения соответсвующего состояния.*

Следствие

$\alpha^2 + \beta^2 = 1$

Далее запись вида $\boldsymbol{2 \mid 0> + \mid 1>}$ подразумевает собой то, что на самом деле сущесвтует нормализирующий коэффициент, который принято опускать. В данном случае полная запись выглядит так:
$\frac{1}{\sqrt[2]{5}}\ (2|0> +|1>)$

Пример для записи состояния из двух кубитов:
$(\alpha_1|0> +\beta_1|1>) * (\alpha_2|0> +\beta_2|1>)$

Однако вся соль квантовых алгоритмов заключается в том, что состояние квантовых систем из двух кубитов записывается таким образом:

$$\alpha_1|00> + \alpha_2|01> + \alpha_3|10> + \alpha_4|11>$$

Замечание

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 = 1$$

Замечание

Если система состоит из n кубитов, то имеем $2^n - 1$ степеней свободы. То есть мы получаем экспоненциальное пространство состояний достаточно маленькими усилиями.

Возникает резонный вопрос - как пользоваться этими регистрами для вычислений?
Нам нужно каким-то образом менять значения регистров. На самом деле существуют некоторые физические процессы, которые меняют коэффициенты регистров.
Все эти процессы математические сводятся к следующему:

$$(\alpha_1, \alpha_2, ..., \alpha_n) * M = (\beta_1, \beta_2, ..., \beta_n)$$

Где M - некая матрица, а $(\beta_1, \beta_2, ..., \beta_n)$ - новое состояние.

Замечание

1. $|M| = 1$
2. M *- Эрмитова матрица*

Пример

$$f(x, y) = x \wedge y$$

На самом деле функция $f(x, y)$ выглядит так:

$$f(x, y, z) = (x, y, x \wedge y)$$

Матрица должна быть размера $8 * 8$:

$$M = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

Определение

Матрица M называется гейт.

Определение

Гейт Адамара:

$$\frac{1}{\sqrt[2]{2}} * \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$|0 > \to |0 > + |1 > \to |0 >$$

$$|1 > \to |0 > - |1 > \to |1 >$$

Попробуем определить, как действует гейт Адамара на такое произведение кубитов:

$$|x >= |X_1 > *|X_2 > *... * |X_n >$$

После применения гейта Адамара на X_1 получим:

$$|X_1 > \rightarrow |0 > +(-1)^{X_1}|1 >$$

Если всюду подставить эту формулу, то получим:

$$\sum_{y \in \{0,1\}^n} -1^{x \star y}|y >$$

Где $x \star y$ - скалярное произведение по модулю 2.
Для более ясного понимания, разберем эту задачу при $n = 3$

$$(|0> + (-1)^{X_1}|1>) * (|0> + (-1)^{X_2}|1>) * (|0> + (-1)^{X_3}|1>)$$

Раскарыв скобки, мы получим элементы вида:

$$\begin{array}{ll} |000> & |100> \\ |001> & |101> \\ |010> & |110> \\ |011> & |111> \end{array}$$

Перед каждым из них стоит множитель. Например $|011>$ умножается на $(-1)^0 * (-1)^{X_2} * (-1)^{X_3}$ и т.д.
Этот множитель как раз и получается скалярным произведением булевых векторов.

Задача

Задача Саймона

$f(x_1, x_2, ..., x_n) = (y_1, y_2, ..., y_n)$ - булева функция

$f : \{0,1\}^n \to \{0,1\}^n$

$\exists a : f(x \bigoplus a) = f(x) \forall x$ - условие существования периода.

Задача Саймона - найти период функции.

Замечание

Эта задача имеет экспоненциальную сложность. Квантовые алгоритмы умеют делать это за линейное время.

Алгоритм Саймона

$\underbrace{|00..0>}_{\text{n}}\underbrace{|00..0>}_{\text{m}}$

1. $|00..0>|00..0>$

2. Применим гейт Адамара к первой части

$\sum_{x\in\{0,1\}^n}|x>|0>$

3. Теперь уже к обоим регистрам применяем функцию f. Другими словами применяем преобразование $x, 0 \to x, f(x)$. Тогда получим

$\sum_{x\in\{0,1\}^n}|x>|f(x)>=\sum_{x\in\{0,1\}^n}(|x>+|x+a>)|f(x)>$

Измерим последние m кубитов. 4. Измерение одного кубита влечет изменения состояния второго кубита. Это явление называется квантовой запутанностью.

После измерения мы будем знать что в первых n кубитах будет лежать:
$\underbrace{(|x> +|x+a>)}_{\text{n}}\underbrace{f(x)}_{\text{m}}$
Применим гейт Адамара еще раз:

$\sum_y (-1)^{x*y}|y> + \sum_y (-1)^{(x+a)*y}|y> =$
$\sum_y [(-1)^{x*y} + (-1)^{x*y} * (-1)^{a*y}]|y>$
Пусть $a * y = 1$. Тогда получим:
$(-1)^{x*y} + (-1) * (-1)^{x*y} = 0 \implies a * y = 1$ - событие нулевой вероятности. Тогда получим, что нам выпадают только такие y, что $a * y = 0$
Далее запускаем весь этот процесс несколько раз, чтобы получить k независимых y. Строим систему линейных уравнений над полем Z_2, решаем её методом Гаусса и получаем период a.

Конец алгоритма