Quantum Machine Learning

1 Введение

В данном документе содержит введение в квантовые вычисления, основные алгоритмы и их применение в машинном обучении.

1.1 Квантовый компьютер

Квантовый компьютер — это вычислительное устройство, которое использует некоторые явления квантовой механики (суперпозиция состояний (superposition), квантовая запутанность (entanglement)). Квантовые компьютеры могут решать некоторые задачи значительно быстрее классических архитектур за счет того, что все операции выполняются сразу над всеми возможными состояниями системы.

1.2 Кубиты

В классической архитектуре информация представляется битами, которые могут принимать только одно из двух значений: 0 или 1. В системе из L битов, соответсвенно, может быть 2^L различных состояний. Как правило, при выполнении операций с системой мы производим операции с одним (может быть несколькими) состоянием системы.

В квантовом же компьютере аналогом бита является квантовый бит — кубит. Это некоторая квантовая система, обладающая двумя базисными состояниями ($|0\rangle$ и $|1\rangle$). Система из L кубитов обладает 2^L базисными состояниями.

Пример 1. При $L = 3$ получаем следующие состояния: $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$, $|111\rangle$.

Для удобства в дальнейшем состояния системы будем обозначать $|j\rangle, j = \overline{1, N}, N = 2^L$. Общее состояние системы описывается *суперпозицией* ее базисных состояний

$$|\psi\rangle = \sum_{j=1}^{N} \lambda_j |j\rangle, \quad \sum_{j=1}^{N} |\lambda_j|^2 = 1,$$

где $\lambda_j \in \mathbb{C}$ — это комплексные амплитуды.

1.3 Базовые операции

Пространством состояний квантовой системы является 2^L-мерное гильбертово пространство (или N-мерное в наших обозначениях). Базовые состояния $\{|j\rangle\}_{j=1}^{N}$ образуют ортонормированный базис. Обозначение $|v\rangle$ соответствует вектор-столбцу v, а $\langle v|$ — его эрмитово сопряжению $v^\dagger$

$$v = \begin{pmatrix} a_1 \\ \cdots \\ a_N \end{pmatrix}, \quad v^\dagger = \begin{pmatrix} \overline{a_1} & \cdots & \overline{a_N} \end{pmatrix}.$$

Тогда скалярное произведение векторов v, u может быть записано как $\langle v|u\rangle$.

Над системой можно проводить два типа операций:

1. Измерение.
2. Унитарное преобразование.

Измерение. Единственный способ получить информацию о состоянии системы это провести операцию *измерение*. Измерение возвращает случайную величину, которая принимает одно из значений $|j\rangle, j = \overline{1,N}$ с вероятностью $|\lambda_j|^2$. Эта операция необратима, то есть повторное измерение вернет то же самое состояние системы. Поэтому в квантовых системах нет условных операций `if ... else ...` (хотя есть некоторые условные операции, например, вентилем controlled-NOT или CNOT, подробнее смотри в следующих разделах). Спонтанные измерения системы вносят неустойчивость и создают трудности в создании систем с большим количеством кубитов.

Математическим языком измерения описываются следующим образом. Пусть $P_S : V \to S$ проектор из множества всех возможных состояний системы V на некоторое его подмножество S. Запишем $|v\rangle = s_1 + s_2$, где $s_a \in S, s_2 \in S^\perp$. Тогда $P_S|v\rangle$ вернет состояние $|v\rangle$ с вероятностью $|P_S|v\rangle|^2$. Заметим, что $|v\rangle$ не обязательно базисный вектор $|j\rangle$, а некоторая суперпозиция базисных векторов. Этим можно пользоваться для проведения менее тривиальных измерений.

Пример 2 (Проверка на совпадение битов)**.** Рассмотрим систему из двух кубитов. В этой системе $|v\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$ Пусть $S_1 = span(|00\rangle, |11\rangle)$. Тогда проектор P_{S_1} с вероятностью $a_{00}^2 + a_{11}^2$ вернет вектор из S_1, в котором оба биты одинаковые. При этом мы не будем знать точные значения битов, а только то, что они совпадают.

Для дальнейшего удобства обычно используют самосопряженные операторы для обозначения измерений (Это можно делать, так как для любого разложения пространства V в прямую сумму подпространств существует самосопряженный оператор, $\sum_{j=1}^{k} \lambda_j P_j$ — самоспряженный оператор). Заметим, что не все самосопряженные операции одинаково легко реализуемы на практике с точки зрения физической реализации.

Унитарные преобразования. Так как квадрат модуля комплексной амплитуды показывает вероятность оказаться в соответствующем состоянии, а вероятности должны суммироваться в 1, то с системой можно производить только унитарные преобразования (неунитарные преобразования запрещены). Кроме того, унитарные преобразования гарантируют обратимость каждого шага алгоритма.

Из унитарности преобразований вытекает правило (no-cloning): нельзя копировать состояния подсистемы, то есть не существует такого оператора U, что для любого $|a\rangle$ выполнялось бы $U|a\rangle 0 = |a\rangle|a\rangle$. Хотя отдельные операции копирования все же существуют (например, $a|0\rangle + b|1\rangle \to a|0\ldots0\rangle + b|1\ldots1\rangle$).

Любые преоразования n-кубитной системы могут представлены в виде композиции 1- и 2-кубитных преобразований. Такие преобразования называются *квантовыми вентилями* (quantum gates), а композиции этих преобразований — *квантовыми цепями* (quantum gate arrays или quantum circuits).

Преобразования Паули:

1. $I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
2. $X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ — замена $|0\rangle$ на $|1\rangle$ и наоборот (аналог операции `NOT`).
3. $Y = XZ = |0\rangle|1\rangle - |1\rangle|0\rangle = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.
4. $Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ — сдвиг фазы.

Преобразование Адамара

5 $H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ или

$$H: \begin{cases} |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle, \\ |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle. \end{cases}$$

Controlled NOT

6 $C_{not} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$.

Оператор изменяет второй бит, если первый бит равен 1. C_{not} является обратным самому себе. Эта операция делает 2 независимых кубита запутанными и наоборот, так как обратна сама себе.

Замечание: при применении к запутанным состояниям контроль может изменяться. Кроме того, вместо операции NOT можно выполнять произвольное унитароное преобразование U (тогда вентиль называется controlled-U).

Данные операции используются для построения обратимых квантовых версий классических логических операций (подробнее можно посмотреть в Quantum computing. A gentle introduction.).

Пример 3 (Алгоритм Дойча)**.** Для функции $f\colon \{0,1\} \to \{0,1\}$ определить, является ли она константной. Любой классический алгоритм решает эту задачу за 2 вызова функции. Квантовый алгоритм делает это за один вызов функции.

Пусть U_f — это унитарное преобразование над двух-кубитной системой, $U_f\colon\ |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$. Тогда

$$U_f(|+\rangle|-\rangle) = \frac{1}{2}\sum_{x=0}^{1}|x\rangle\left(|0\oplus f(x)\rangle - |1\oplus f(x)\rangle\right) = \left|\frac{1}{\sqrt{2}}(|0\oplus f(x)\rangle - |1\oplus f(x)\rangle) = (-1)^{f(x)}|-\rangle\right|$$
$$= \sum_{x=0}^{1}(-1)^{f(x)}|x\rangle|-\rangle.$$

При $f(x) = const$ получаем $\pm|+\rangle|-\rangle$, в противном случае — $\pm|-\rangle|-\rangle$. Применяя преобразование Адамара к первому кубиту, а затем измеряя его, мы гарантированно получим 1 в случае постоянной функции, и 0 в противном случае.

Обобщение на случай, когда на вход подается n бит, а на выходе один бит, тоже решается за один вызов U_f.

1.4 Квантовое преобразование Фурье и оценка фазы

Квантовое преобразование Фурье следующим образом преобразует базовые состояния

$$|j\rangle \to \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1} e^{2\pi ijk/N}|k\rangle.$$

Пусть $j = j_1 j_2 \dots j_n$ — битовое представление числа j. Введем также обозначение $0.j_1 j_2 \dots j_n = j_1/2 + j_2/4 + \dots + j_n/2^n$. Тогда преобразование Фурье можно представить в виде

$$|j\rangle \to \frac{(|0\rangle + e^{2\pi i 0.j_n}|1\rangle)\cdots(|0\rangle + e^{2\pi i 0.j_1\dots j_n}|1\rangle)}{2^n}.$$

Из выражения становится понятно, какие вентили надо использовать для построения цепи (см. Рис.1): сначала вентиль H (преобразование Адамара для перехода к $|0\rangle \pm |1\rangle$), а затем controlled-R_k вентиль, где R_k делает сдвиг фазы во втором кубите:

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k}. \end{pmatrix}$$

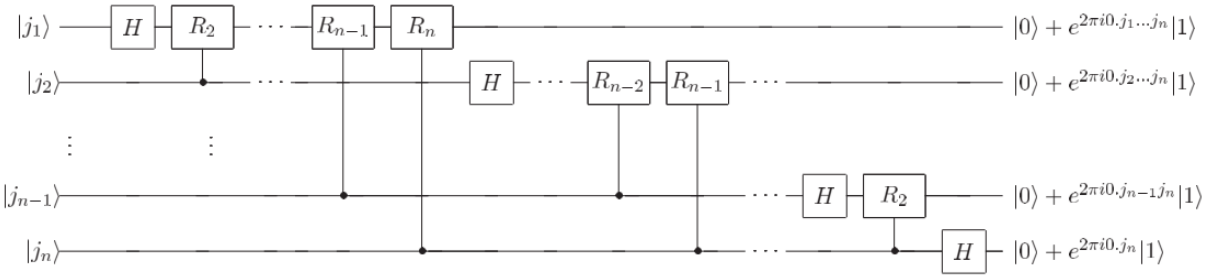

Рис. 1: Схема вычисления преобразования Фурье. Черные точки обозначают управляющее состояние для controlled-операций