Классические и квантовые вычисления

А. Китаев; написал М. Вялый

8 лекция (02/04/98)

1. Измерение (продолжение)

Напомним, что диагональная матрица плотности соответствует классическому состоянию; если

$$\rho = \begin{pmatrix} w_1 & & & \\ & \ddots & & 0 \\ & & w_n & \\ & 0 & & \ddots \end{pmatrix},$$

то w_k — вероятность состояния k. Преобразование матриц плотности, "забывающее" внедиагональные элементы — $\rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix} \mapsto \begin{pmatrix} \rho_{00} & 0 \\ 0 & \rho_{11} \end{pmatrix}$ — физически реализуемо (с помощью копирования бита: $|0\rangle \mapsto |00\rangle$, $|1\rangle \mapsto |11\rangle$). Это можно так интерпретировать: *если постоянно наблюдать за системой (делать копии), то система будет вести себя как классическая.*

В прошлый раз рассматривались квантово-классические системы

$$\rho = \sum_k w_k \rho^{(k)} \otimes |k\rangle\langle k| = \sum_k w_k \left(\rho^{(k)}, k\right),$$

последняя запись — введеное спеицально для этого случая обозначение; $\operatorname{Tr}\rho^{(k)} = 1$, w_k — вероятность классического состояния k, $\rho^{(k)}$ — условная матрица плотности.

Было также введено понятие измерения. Пусть имеется ряд взаимоисключающих возможностей, что выражается рзложением пространства состояний в прямую сумму $\mathcal{N} = \bigoplus_{j\in\Omega} \mathcal{L}_j$ попарно ортогональных подпространств, где $\Omega = \{1, \ldots, r\}$ — множество возможностей.

Измерение (преобразование матриц плотности) состоит в том, что для состояний из подпространства $\mathcal{L}_j$ "измеряющий прибор" помещает в классический регистр номер состояния j. Т. е.

$$\text{если } |\xi\rangle \in \mathcal{L}_j, \text{ то } |\xi\rangle\langle\xi| \mapsto (|\xi\rangle\langle\xi|, j). \qquad (*)$$

Хотя измерение отображает пространство $\mathbf{L}(\mathcal{N})$ в $\mathbf{L}(\mathcal{N}\otimes\mathcal{K})$, результат всегда диагонален по второй компоненте, поэтому можно считать, что измерение отображает $\mathbf{L}(\mathcal{N})$ в $\bigoplus_{j=1}^{\dim\mathcal{K}} \mathbf{L}(\mathcal{N})$.

Из соображений линейности можно доопределить измерение на всех остальных матрицах плотности

$$\rho \;\mapsto\; \sum_j \left(\Pi_{\mathcal{L}_j}\rho\Pi_{\mathcal{L}_j}, j\right).$$

Приведем простейший пример измерения. Сделаем две копии бита. Пусть $\Pi_{\mathcal{L}_0} = |0\rangle\langle 0|$, а $\Pi_{\mathcal{L}_1} = |1\rangle\langle 1|$. Тогда

$$\rho = \begin{pmatrix} \rho_{00} & \rho_{01} \\ \rho_{10} & \rho_{11} \end{pmatrix} \mapsto (\rho_{00}|0\rangle\langle 0|, 0) + (\rho_{11}|1\rangle\langle 1|, 1).$$

2. Измеряющие операторы

Введем особый класс операторов — *измеряющие операторы*. Пусть есть пространство состояний $\mathcal{N}\otimes\mathcal{K}$, причем первый сомножитель разложен в прямую сумму попарно ортогональных подпространств: $\mathcal{N} = \bigoplus\limits_j \mathcal{L}_j$. Тогда всякий оператор вида $W = \sum\limits_j \Pi_{\mathcal{L}_j}\otimes U_j$ будем называть измеряющим.

Чтобы оправдать название, рассмотрим следующий процесс. Пусть имеется некоторое состояние, описываемое матрицей плотности $\rho\in\mathbf{L}(\mathcal{N})$. Подсоединим к нему *прибор*, т. е. перейдем к состоянию $\rho\otimes\overbrace{|0^m\rangle\langle 0^m|}^{\text{прибор}}$ (считаем, что во втором сомножителе есть выделенный базис, например, что это $\mathbb{B}^{\otimes n}$).

Теперь применяем измеряющий оператор W. Получаем состояние

$$W\Big(\rho\otimes|0^m\rangle\langle 0^m|\Big)W^\dagger = \sum_j \Pi_{\mathcal{L}_j}\rho\Pi_{\mathcal{L}_j}\otimes U_j|0\rangle\langle 0|U_j^\dagger$$

(мы воспользовались характеристическим свойством проектора $\Pi^\dagger=\Pi$, $\Pi^2=\Pi$).

И последнее действие: прибор становится классическим. Это означает, что матрица диагонализуется по второму сомножителю. Посмотрим, во что переходят при этом вторые сомножители в написанной сумме:

$$\gamma_j = |\xi_j\rangle\langle\xi_j| \longmapsto \sum_k |\langle k|\xi_j\rangle|^2\,|k\rangle\langle k| \qquad \Big(\text{т. к. } (\gamma_j)\,\big|_{kk} = \langle k|\gamma_j|k\rangle\Big)$$

Теперь запишем получившийся результат

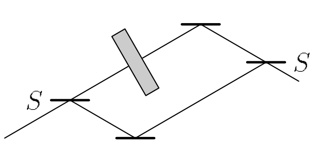
$$\sum_j\sum_k \Big(\Pi_{\mathcal{L}_j}\rho\Pi_{\mathcal{L}_j}\,|\langle k|U_j|0\rangle|^2,\,k\Big) \;=\; \sum_j\sum_k \mathbf{P}(k|j)\,\big(\Pi_{\mathcal{L}_j}\rho\Pi_{\mathcal{L}_j},k\big)\,,$$

где введены *условные вероятности* $\mathbf{P}(k\big|j) = |\langle k|U_j|0\rangle|^2$. Заметим, что для измерения $\mathbf{P}(k\big|j) = \delta_{jk}$. Введенные таким образом условные вероятности ведут себя как обычные, если рассматриваются композиции измеряющих операторов, построенных на одном и том же ортогональном разложении пространства состояний (квантовый аналог множества элементарных событий).

Приведем примеры измеряющих операторов.

1. Оператор $\Lambda(U) = \Pi_0\otimes\mathrm{id}+\Pi_1\otimes U$, дествующий на пространстве $\mathbb{B}\otimes\mathcal{N}$ — измеряющий.

1′. Нетривиально, что он измеряющий и по второй компоненте. Поскольку U — унитарный оператор, его можнно разложить в сумму проекторов по собственным подпространствам: $U = \sum_j \lambda_j\Pi_{\mathcal{L}_j},\ |\lambda_j| = 1$. Тогда $\Lambda(U) = \sum_j(\Pi_0+\lambda_j\Pi_1)\otimes\Pi_{\mathcal{L}_j} = \sum_j \begin{pmatrix}1 & 0\\ 0 & \lambda_j\end{pmatrix}\otimes\Pi_{\mathcal{L}_j}$. В этом случае условные вероятности равны $\mathbf{P}(0\big|j) = 1$ и $\mathbf{P}(1\big|j) = 0$, поэтому такой оператор, хотя и является измеряющим по определению, фактически ничего не измеряет



Замечание для физиков. Пусть U — оператор фазового сдвига света при прохождении сквозь стеклянную пластинку. Мы можем разделить луч света на дваа, пропутив его через полупрозрачное зеркало, затем один из полученных лучей пропустить через стеклянную пластинку, а затем заставить полученные в результате лучи интерферировать. По картине интерференции можно узнать фазовый сдвиг.

Математический вариант предыдущего примера. Аналогом полупрозрачного зеркала будет служить оператор $S = \dfrac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$. Как видно из приведенной выше картинки, его нужно применить в начале и в конце. Строго говоря, рассмотрим такой оператор

$\Xi(U) = (S\otimes \mathrm{id})\Lambda(U)(S\otimes\mathrm{id})$. Если начальный вектор имеет вид $|\psi\rangle = |\eta\rangle\otimes|\xi\rangle \quad (|\xi\rangle\in\mathcal{L}_j)$, то $\Xi(U)|\psi\rangle = |\eta'\rangle\otimes|\xi\rangle$, где

$$|\eta'\rangle \;=\; \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & \lambda_j\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}|\eta\rangle \;=\; \frac{1}{2}\begin{pmatrix}1+\lambda_j & 1-\lambda_j\\ 1-\lambda_j & 1+\lambda_j\end{pmatrix}|\eta\rangle.$$

Поэтому $\Xi(U) \;=\; \sum\limits_j \overbrace{\frac{1}{2}\begin{pmatrix}1+\lambda_j & 1-\lambda_j\\ 1-\lambda_j & 1+\lambda_j\end{pmatrix}}^{R_j}\otimes\Pi_{\mathcal{L}_j}$. Теперь посчитаем условные вероятности. Собственные числа унитарного оператора равны по модулю 1, поэтому можно полагать $\lambda_j = e^{2\pi\mathrm{i}\varphi_j}$. В результате имеем

$$\mathbf{P}(0|j) = |\langle 0|R_j|0\rangle|^2 = \left|\frac{1+\lambda_j}{2}\right|^2 = \frac{1+\cos(2\pi\varphi)}{2}.$$

В дальнейшем именно с помощью такого оператора мы будем оценивать собственные числа. Для этого придется брать разные биты в качестве первых сомножителей (разные “приборы”). Конечно, следует убедиться, что это корректно (т. е., что вероятности будут перемножаться).

Свойства измеряющих операторов

Мы будем рассматривать измеряющие операторы, соответствующие **одному и тому же** ортогональному разложению $\mathcal{N} = \sum_j \mathcal{L}_j$.

1. Произведение измеряющих операторов — измеряющий оператор.

Действительно, пусть есть два измеряющих оператора $W^{(1)} = \sum_j R_j^{(1)}\otimes\Pi_{\mathcal{L}_j}$ и $W^{(2)} = \sum_j R_j^{(2)}\otimes\Pi_{\mathcal{L}_j}$. Поскольку $\Pi_{\mathcal{L}_j}\Pi_{\mathcal{L}_k}\neq 0 \;\Leftrightarrow j=k$, имеем $W^{(2)}W^{(1)} = \sum_j R_j^{(2)}R_j^{(1)}\otimes\Pi_{\mathcal{L}_j}$.

2. Условные вероятности для произведения измеряющих “разными приборами” операторов перемножаются.

Более точно, пусть $R^{(1)} = \tilde{R}^1\otimes\mathrm{id}$, а $R^{(2)} = \mathrm{id}\otimes\tilde{R}^2$. Тогда $\mathbf{P}(k_1,k_2|j) = \mathbf{P}_1(k_1|j)\mathbf{P}_2(k_2|j)$. Это равенство следует непосредственно из определения условных вероятностей и из очевидного тождества $\Big(\langle\xi_1|\otimes\langle\xi_2|\Big)\Big(U_1\otimes U_2\Big)\Big(|\eta_1\rangle\otimes|\eta_2\rangle\Big) \;=\; \langle\xi_1|U_1|\eta_1\rangle\,\langle\xi_2|U_2|\eta_2\rangle$.

3. Формула полной вероятности.

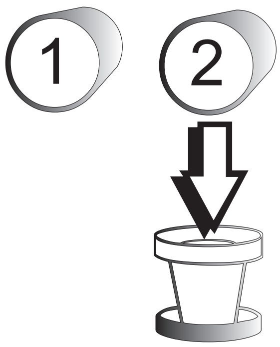
Пусть есть оператор $W = \sum R_j\otimes\Pi_{\mathcal{L}_j}$, применим его к состоянию $|0\rangle\langle 0|\otimes\rho$, $\rho\in\mathbf{L}(\mathcal{N})$. После этого вероятность наблюдения состояния k, т. е. $\mathbf{P}\Big(W(|0\rangle\langle 0|\otimes\rho)W^\dagger,\,(k)\otimes\mathcal{N}\Big)$ равна $\sum\limits_j \mathbf{P}(k|j)\mathbf{P}(\rho,\mathcal{L}_j)$.

Доказательство. $W\Big(|0\rangle\langle 0|\otimes\rho\Big)W^\dagger \;=\; \gamma \;=\; \sum\limits_j\Big(R_j|0\rangle\langle 0|R_j^\dagger\Big)\otimes\Pi_{\mathcal{L}_j}\rho\Pi_{\mathcal{L}_j}$. Ранее было доказано, что $\mathbf{P}(\gamma,(k)\otimes\mathcal{N}) \;=\; \mathbf{P}(\mathrm{Tr}_{\mathcal{N}}\gamma,(k))$, а $\mathrm{Tr}_{\mathcal{N}}\gamma \;=\; \sum\limits_j\Big(R_j|0\rangle\langle 0|R_j^\dagger\Big)\times\mathrm{Tr}\left(\Pi_{\mathcal{L}_j}\rho\Pi_{\mathcal{L}_j}\right)$. Поскольку $\mathrm{Tr}\left(\Pi_{\mathcal{L}_j}\rho\Pi_{\mathcal{L}_j}\right) = \mathrm{Tr}\Big(\Pi^2_{\mathcal{L}_j}\rho\Big) = \mathrm{Tr}\left(\Pi_{\mathcal{L}_j}\rho\right) \stackrel{\mathrm{def}}{=} \mathbf{P}\left(\rho,\mathcal{L}_j\right)$, получаем искомое выражение $\mathbf{P}(\gamma,(k)\otimes\mathcal{N}) = \sum\limits_j\mathbf{P}(k|j)\mathbf{P}(\rho,\mathcal{L}_j)$. □

Упражнение. *Доказать формулу полной вероятности напрямую, не используя взятия частичного следа.*

3. Определение квантового вычисления

*... Мы не можем применить здравый смысл,
мы можем только стремиться понять
внутреннюю логику этого безумия, которая
наверняка есть ...* — А. Шень

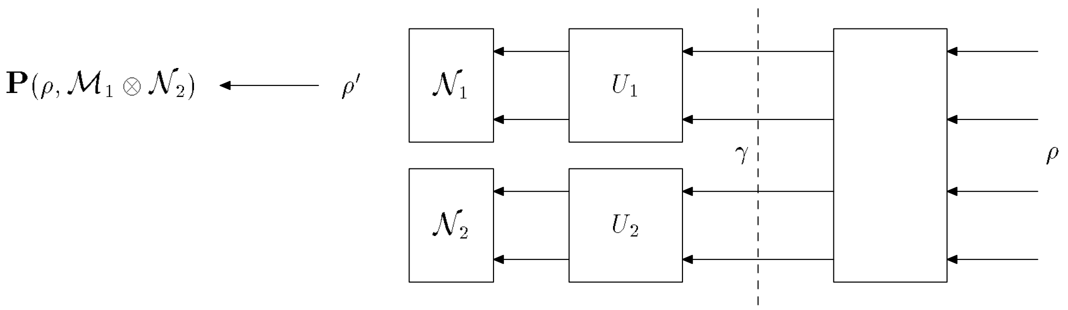


Определение квантового вычисления будет использовать подсчет вероятностей. Следует сделать еще одно напоминание о способах такого подсчета. Пусть мы в какой-то момент использовали дополнительную подсистему (2 на врезке). После того, как она стала нам не нужна, мы можем выбросить ее в мусорное ведро. Это соответствует взятию частичного следа по пространству состояний системы 2. А можно тянуть весь этот мусор до самого конца и считать вероятность для событий вида $\mathcal{M}_1 \otimes \mathcal{N}_2$ (раз уж мы перестали использовать вторую систему, то никакие детали ее состояния нам не важны — нам безразлично, что именно произойдет с системой 2 в "мусорном ведре"). Как уже говорилось, эти вероятности равны: $\mathbf{P}(\rho, \mathcal{M}_1 \otimes \mathcal{N}_2) = \mathbf{P}(\mathrm{Tr}_{\mathcal{N}_2} \rho, \mathcal{M}_1)$.

Пусть теперь у нас имеется квантовая схема, причем в выходном состоянии нас интересует событие, зависящее только от части выходных q-битов, ему соответствует подпространство $\mathcal{M}_1 \subseteq \mathcal{N}_1$. Начинаем мы из состояния $\rho \in \mathbf{L}(\mathcal{N}_1 \otimes \mathcal{N}_2)$, спустя некоторое время из него получается состояние $\gamma \in \mathbf{L}(\mathcal{N}_1 \otimes \mathcal{N}_2)$. К этому состоянию уже применяются операторы U_1 и U_2, действующие по отдельности на $\mathcal{N}_1$ и $\mathcal{N}_2$. Считать вероятность наблюдения события $\mathcal{M}_1 \otimes \mathcal{N}_2$ можно двумя способами:

$$\mathbf{P}\left((U_1 \otimes U_2)\gamma(U_1^\dagger \otimes U_2^\dagger),\, \mathcal{M}_1 \otimes \mathcal{N}_2\right) \quad \text{или} \quad \mathbf{P}(U_1 \,\mathrm{Tr}_{\mathcal{N}_2}\, \gamma U_1^\dagger,\, \mathcal{M}_1).$$

Из второго выражения ясно, что эта вероятность не зависит от U_2.



Определение квантового вычисления соответсвуте нарисованному процессу. На вход квантовой схемы подаются базисные состояния (кодирующие аргументы вычисляемой функции, на выходе получается ответ.

Пусть есть функция $F : \{0,1\}^n \to \{0,1\}^m$. Рассмотрим квантовую схему, работающую с N битами: $U = U_L \dots U_2 U_1 : \mathbb{B}^{\otimes N} \to \mathbb{B}^{\otimes N}$. Эта схема вычисляет F, если после применения U к начальному состоянию $|x, 0^{N-n}\rangle$ (или, как мы обозначали это раньше, $\overset{n}{\boxed{x}}\overset{N-n}{\boxed{0}}$) в первых m битах с большой вероятностью получиться $F(x)$.

Определение. *Схема $U = U_L \dots U_2 U_1$ вычисляет F, если для любого x выполнено*

$$\mathbf{P}\Big(U|x, 0^{N-n}\rangle, \mathcal{M}\Big) = \sum_z \Big|\langle F(x), z|\, U\, |x, 0^{N-n}\rangle\Big|^2 > 1 - \varepsilon,$$

где ε — некоторое фиксированное число, большее $1/2$, а $\mathcal{M} = |F(x)\rangle \otimes \mathbb{B}^{N-m}$. (Обратите также внимание, что $F(x)$ и x состоят из разного количества битов, хотя суммарная длина $(F(x), z)$ и $(x, 0^{N-n})$ одинакова и равна N).

Как и для вероятностных вычислений, выбор ε несущественен, поскольку можно запустить несколько экземпляров схеы независимо и взять значение по большинству.