Квантовые компьютеры и труднорешаемые (NP-полные) задачи

Владимир Черны
(Vladimir Černý)[1]

В статье обсуждаются физические аспекты труднорешаемых (NP-полных) вычислительных задач. В рамках специфической модели показано, что квантовый компьютер может, в принципе, решить любую NP-полную задачу за полиномиальное время, однако вычисление потребует экспоненциально больших затрат энергии. Высказывается предположение, что предложенная модель отражает справедливость принципа дополнительности применительно к энергии и времени, необходимых для выполнения NP-полного вычисления.

1. Введение

В этой статье будут обсуждены физические аспекты труднорешаемых (NP-полных) задач вычислений. Формальная математическая теория NP-полноты [1] основана на строгих определениях таких понятий, как задача, алгоритм и сложность и, конечно, на строгих математических рассуждениях. Однако компьютеры, в конечном счете, физические устройства, так что физические аспекты задачи (дополнительно к чисто математическим аспектам) также следует обсудить с достаточной полнотой. Не можем ли мы научиться новым методам вычислений, представляя компьютер как физическую машину? Известная открытая проблема теории сложности — P = NP-задача. В этой статье будут обсуждены ее физические аспекты. Мы попробуем решить NP-полную

[1]Institute of Physics, Comenius University, Mlynská dolina, 842 15 Bratislava, Czechoslovakia.

Перевод О. А. Хрусталева.

задачу за полиномиальное время. При этом вместо строгого математического языка будет использован язык физический. Наши построения не будут иметь прямых математических аналогий.

Мы обсудим известную задачу о коммивояжере (TSP — traveling-salesman-problem): дано множество N городов и расстояния d_{ij} между каждой парой городов. Нужно найти кратчайший маршрут, проходящий через все города. (Фактически, будет решаться ограниченная задача, когда предполагается, что все d_{ij} ограничены сверху числом L. Это — все еще NP-полная задача.) Есть простой алгоритм решения этой задачи: перенумеруем все возможные маршруты и найдем длину каждого из них. Время решения в этом случае экспоненциально растет с N, поскольку число маршрутов — величина порядка $N!$. Неизвестно, существует ли эффективный алгоритм, требующий полиномиального по N времени вычисления (точная формулировка $\mathrm{P} = \mathrm{NP}$-задачи дана в [1]). Параллельный перебор всех $N!$ маршрутов одновременно потребует конечного времени вычисления. Но если для этого случая потребуется $N!$ процессоров, придется считаться с экспоненциально большим размером компьютера и экспоненциально большим временем чтения. Прямолинейный параллелизм принесет мало пользы. Наивный подход к задаче может привести к выводу, что в конечной системе нельзя одновременно реализовать «экспоненциально большое» число возможностей. Однако справедливо обратное. Квантовая система может управлять экспоненциально большим числом возможностей одновременно. Это свойство можно, в принципе, использовать при вычислениях. Квантовые компьютеры обсуждались, например, Дойчем [3] и Фейнманом [4]. Наш метод аналогичен методу Фейнмана [4], хотя его цель в некоторой степени противоположна нашей. Фейнман показал, что квантовый компьютер можно, в принципе, применить для выполнения тех же вычислений, которые выполняет стандартный компьютер, используя логические гейты. Здесь обсуждается в некотором смысле дополнительная проблема: можно ли, хотя бы в принципе, придумать альтернативный способ вычисления, в основе своей отличный от вычислений на стандартной машине (подчеркнем слова «в принципе»). В этом отношении наши рассуждения близки к рассуждениям Фейнмана. Мы не хотим изобретать технически осуществимую машину. Мы придумаем что-то вроде мысленного эксперимента: будем работать с системой, которая, может быть, не существует в реальном мире, но ее существование не противоречит ни одному из законов принятой теории. Такие системы могут быть реализованы принципиально. Нашим теоретическим полем деятельности будет квантовая механика. Будет показано, что можно решить NP-полную задачу за «полиномиальное» время в «полиномиальном» пространстве. Для этого будет построена специфическая квантовая модель TSP-решателя.

2. Квантовый TSP-решатель

Наш гипотетический квантовый компьютер выглядит как многощелевая интерференционная машина с приборами Штерна–Герлаха между щелями. В этом разделе мы ограничимся ее кратким описанием. Детали можно найти в дополнении.

Для TSP с N городами нужна машина, состоящая из $N-1$ слоев из $N-1$ щелей в каждом слое. Таким образом, каждую щель можно единственным образом задать парой целых чисел (i, j). В дополнение к щелям машина содержит источник частиц («лазер»), расположенный в точке S, и детектор частиц в точке D (см. рис. 1).

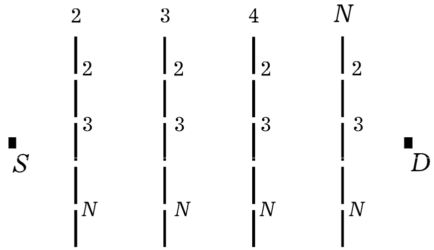

Рис. 1. Многощелевая интерференционная машина — TSP-решатель.

Существует $(N-1)^{(n-1)}$ возможных траекторий, по которым частица может попасть из точки S в точку D. Траекторию можно единственным образом задать перечислением щелей на ней, например, траектория на рис. 2 задается так:

$$S,\ (2,2),\ (3,4),\ (4,3),\ (5,5),\ D.$$

Ясно, что указатели слоев можно опустить и описать эту траекторию последовательностью

$$S,\ 2,\ 4,\ 3,\ 5,\ D. \tag{1}$$

Последовательность (1) можно принять в качестве кода маршрута коммивояжера по пяти городам, если только отождествить точки S и D с началом и концом маршрута (город 1). Тогда траектория (1) будет представлять маршрут 1, 2, 4, 3, 5, 1. Однако существуют траектории, которые не могут быть маршрутами коммивояжера, например, S, 3, 2, 2, 5, D. Здесь город 2 посещается дважды, а город 4 пропущен.

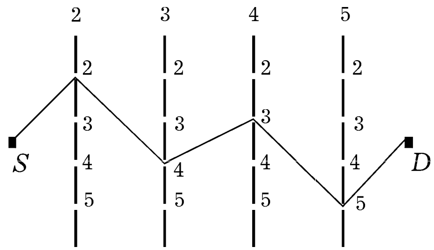

Рис. 2. Траектория, соответствующая TSP-маршруту.

Следует избавиться от всех «запрещенных» траекторий и определить динамику движения частицы так, чтобы частица, проходящая сквозь машину, знала длину соответствующего TSP-маршрута.

Чтобы удовлетворить этим условиям, нужно иметь частицы с некоторым числом степеней свободы, которые могли бы взаимодействовать с машиной. Можно использовать внутренние степени свободы, подобные изотопическому спину. Еще раз подчеркнем, что перед нами гипотетический мир, так что можно изобретать любые внутренние степени свободы, даже если они не соответствуют частицам реального мира.

Предположим, что внутренние состояния наших гипотетических частиц можно описать следующим кэт-вектором:

$$|k; c_2, c_3, \dots, c_N; p\rangle,$$

где

$$k \in (0, 1, \dots, NL), \quad c_i \in (0, 1), \quad p \in (0, 1).$$

Квантовое число k будет измерять «число километров» маршрута, числа c_i скажут, посещался i-й город или нет. Квантовое число p не имеет отношения к TSP. Оно связано с дополнительной степенью свободы, необходимой для реализации принятой динамики.

Для описания работы машины все готово. Теперь рассмотрим часть траектории между двумя щелями из соседних слоев, $(i, m) \to (i+1, n)$.

Это — часть маршрута путешествующего торговца (TS) между городами m и n. Предположим, что если частица проходит сквозь щель $(i,\, n)$, то квантовое число c_n изменяется следующим образом:

$$c_n = 0 \to c_n = 1. \tag{2}$$

Предположим также, что наша частица движется между щелями не в свободном пространстве, но в некотором поле, которое задано так, что квантовое число k возрастает на отрезке траектории между щелями $(i,\, n)$ и $(i+1,\, m)$ как

$$k \to k + d_{nm}, \tag{3}$$

где d_{nm} — расстояние между городами n и m. Соотвествующая динамика обсуждается в дополнении.

Предположим, что все частицы рождаются в точке S в состоянии

$$|0;\, 0,\, 0,\, \ldots\, ,\, 0;\, 0\rangle.$$

После того как частицы пройдут сквозь машину, они окажутся в состоянии

$$\sum_{\text{траектории}} |k; c_2, c_3,\, \ldots\, , c_N; p\rangle_{\text{траектория}}. \tag{4}$$

Некоторые из траекторий в этой сумме соответствуют разрешенным TS-маршрутам. Легко понять, что это — те траектории, для которых все квантовые числа c_i равны 1, что гарантируется правилом (2). Для таких траекторий значение квантового числа k равно длине соответствующего маршрута.

Представим теперь, что в точку D помещен фильтр, который подавляет все состояния, кроме тех, для которых все c_i равны 1. Тогда состояния на выходе машины равны

$$\sum_{\text{траектории}} |\text{Длина маршрута} k; 1, 1,\, \ldots\, , 1; p\rangle_{\text{траектория}}. \tag{5}$$

Соответствующий фильтр должен состоять из серии устройств типа приборов Штерна–Герлаха, чувствительных к квантовым числам c и поглощающих состояния с $c = 0$. Заметим, что пока наши рассуждения следуют духу фейнмановских лекций [2].

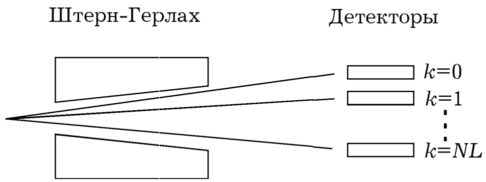

Рис. 3. Устройство Штерна–Герлаха, измеряющее минимальное значение k.

Задача почти решена. Нужно только поместить в точку D дополнительное устройство Штерна–Герлаха, на этот раз чувствительное к квантовому числу k. Оно должно разделить поток выходящих частиц на NL потоков, каждый из которых соответствует некоторому значению k (см. рис. 3). Если снабдить выходные потоки детекторами частиц, то детектор у потока с $k = ML$ откликнется в том случае, если существует маршрут длины M. Из тех детекторов, которые откликнутся, можно выбрать детектор, соответствующий минимальному значению k. Он и укажет коммивояжеру кратчайший путь.

3. Проблема измерения

Следует, однако, тщательнее обсудить вопрос о детектировании минимального k. Ортодоксальная квантовая механика учит, что каждая частица, прошедшая сквозь нашу машину, находится в суперпозиции состояний, определяемой суммой (5). Каждая частица ощущает все траектории и именно поэтому каждая частица «знает» минимальное значение k. TSP-решение скрыто в конечном состоянии каждой частицы, прошедшей сквозь машину. Чтобы пройти сквозь машину, частице нужно лишь «полиномиальное время», поэтому именно за такое время решается задача о коммивояжере. Что надо сделать, чтобы мы (а не только частица) также знали решение? Задача состоит в том, чтобы измерить (в смысле квантового измерения) минимальное значение k, содержащееся в суперпозиции (5). В сумме (5) содержится (по порядку величины) $N!$ состояний, и может случиться, что только одно из них соответствует минимальному значению k. В этом случае придется искать состояние, которое входит в суперпозицию (5) с экстремально малой амплитудой $\frac{1}{\sqrt{N!}}$. Таким образом, чтобы заставить детекторы откликаться с разумной вероятностью, надо пропускать сквозь машину очень большое число частиц одновременно. Это, в принципе, возможно, если мы имеем дело с бозонами, из которых можно построить классическое поле, примерно таким же образом, как лазерное излучение формируется из большого числа когерентных фотонов. Однако, наш «лазер» должен быть очень энергичным: ведь требуется, чтобы интенсивность классического поля соответствовала собранию $N!$ бозонов. К несчастью, для этого необходима «экспоненциально большая» энергия. Таким образом, «вычисление» действительно можно выполнить за полиномиальное время, но чтение результата потребует экспоненциально больших затрат энергии.

4. Выводы

Хотя в работе обсуждалась некоторая частная модель, нельзя отделаться от чувства, что она указывает на некоторый более общий результат. Кажется, что мы имеем дело с некоторым принципом дополнительности, касающегося энергии и времени, необходимых для выполнения NP-полного вычисления. Случай, противоположный нашему, уже был подробно обсужден: показано, что можно вычислять с нулевой затратой энергии, если только смириться с медлительностью вычислительной машины [4–6]. Здесь был рассмотрен другой предельный случай: быстрое вычисление, но экстремально большая затрата энергии. Действительно ли мы столкнулись с новым принципом, или это — следствие некоторых известных законов природы, например, второго закона термодинамики? Могут ли приведенные выше рассуждения научить тому, как следует «математически» подойти к P=NP-задаче? Мы не знаем. Нашу простую модель лучше рассматривать как возможное начало дискуссии, чем как решение задачи.

5. Дополнение

Обсудим технические подробности динамической схемы, которая проводит к определяющим поведение системы уравнениям (1) и (3). Начнем с первого из них. Поскольку речь там идет только о квантовых числах c_n, забудем о других квантовых числах, а также об индексе n в обозначениях. Предположим, что в гнезде имеется поле, которое «взаимодействует» с квантовым числом c и что гамильтониан взаимодействия равен

$$\hat{H}_1 = \omega_1(\hat{a}^+ + \hat{a}),$$

где $\hat{a}^+$ и $\hat{a}$ — такие операторы:

$$\hat{a}^+|0\rangle = |1\rangle, \quad \hat{a}^+|1\rangle = 0,$$
$$\hat{a}|0\rangle = 0, \qquad \hat{a}|1\rangle = |0\rangle.$$

В этом случае

$$\exp(-i\hat{H}_1 t_1)|0\rangle = \cos(\omega_1 t_1)|0\rangle - i\sin(\omega_1 t_1)|1\rangle.$$

Если распорядиться частотой ω_1 и временем пролета частицы сквозь гнездо t_1 так, чтобы было $\omega_1 t_1 = \frac{\pi}{2}$, то уравнение (2) будет удовлетворено.

Перейдем к уравнению (3). Нужно построить аппарат, который будет менять состояние частицы по закону

$$|k\rangle \to |k+1\rangle. \tag{6}$$

Для этого необходимо дополнительное квантовое число p, с помощью которого изменение состояния (6) можно представить как последовательность изменений

$$|k;p=0\rangle \to |k+1;p=1\rangle \to |k+1;p=0\rangle. \tag{7}$$

Представим, что частица взаимодействует с некоторым внешним полем и гамильтониан взаимодействия равен

$$\hat{H}_2 = \omega_2(\hat{b}^+\hat{d}^+ + \hat{b}\hat{d}),$$

где

$$\hat{b}^+|k;p\rangle = |k+1;p\rangle \quad \text{для} \quad k<L, \quad \hat{b}^+|k;p\rangle = 0 \quad \text{для} \quad k=L,$$
$$\hat{b}|k;p\rangle = |k-1;p\rangle \quad \text{для} \quad k>0, \qquad \hat{b}|k;p\rangle = 0 \quad \text{для} \quad k=0,$$
$$\hat{d}^+|k;p=0\rangle = |k;p=1\rangle, \qquad \hat{d}^+|k;p=1\rangle = 0,$$
$$\hat{d}|k;p=0\rangle = 0, \qquad \hat{d}|k;p=1\rangle = |k;p=0\rangle.$$

В этом случае

$$\exp(-i\hat{H}_2 t_2)|k;0\rangle = \cos(\omega_2 t_2)|k;0\rangle - i\sin(\omega_2 t_2)|k+1;1\rangle.$$

Выбирая ω_1 и t_2 (время пролета сквозь поле) так, что $\omega_1 t_1 = \frac{\pi}{2}$, получим требуемое изменение состояния:

$$|k, 0\rangle \to |k+1, 1\rangle.$$

Чтобы привести квантовое число p к значению $p = 0$, можно использовать взаимодействие с гамильтонианом

$$\hat{H}_2' = \omega_2'(\hat{d}^+ + \hat{d})$$

и взять время пролета t_2' таким, чтобы выполнялось $\omega_2' t_2' = \frac{\pi}{2}$.

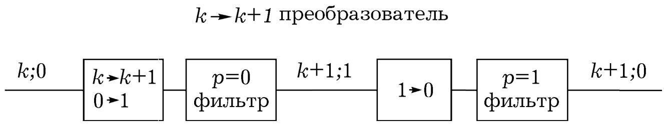

Рис. 4. Последовательность шагов $k \to k+1$, подразумевающая изменение состояния.

Однако, здесь следует соблюдать осторожность. Если времена t_2 и t_2' подобраны недостаточно аккуратно, получатся состояния с малой добавкой неверных квантовых чисел k и p. Это опасно: ведь окончание работы связано с поиском экспоненциально малой амплитуды. Даже экспоненциально малая добавка с «неверными» квантовыми числами может привести к ложному результату. К счастью, дополнительную переменную p можно заставить проверять, правильно ли изменяется состояние. Нужно только поставить после устройства, осуществляющего замену $|k; 0\rangle \to |k+1; 1\rangle$, фильтр, который поглотит возможную добавку состояния $|k; 0\rangle$. Это можно сделать, проверяя только значение переменной p. Гамильтониан $\hat{H}_1$ сохраняет корреляцию между значениями p и k. Именно это обстоятельство было главной причиной определения дополнительной переменной p. Далее, мы не можем проверить правильность значения $k+1$, поскольку нам неизвестно значение k. Можно снова добавить фильтр, который после изменения $|k+1; 1\rangle \to |k+1, 0\rangle$ поглотит добавку состояния $|k+1; 1\rangle$. В этом случае перед входом в следующий $(k \to k = 1)$-аппарат состояние будет иметь правильное значение $p = 0$. Полный $(k \to k+1)$-аппарат изображен на рис. 4. Теперь ясно, как обеспечить необходимое изменение состояния $(k \to k + d_{mn})$ между гнездами m и n: вложим d_{mn}-части $(k \to k+1)$-устройств в траекторию между гнездами m и n. Такие устройства необходимо поместить между каждой из пар гнезд m и n. Фильтры уменьшают яркость квантового компьютера (некоторые частицы теперь не пройдут сквозь машину), однако это неважно, потому что яркость должна быть экспоненциально большой. Подчеркнем еще раз, что полное число $(k \to k+1)$-преобразований, необходимое для решения задачи, растет с ростом N только полиномиально, так что построенный компьютер лишь «полиномиально велик» в пространстве и во времени.

Литература

[1] В качестве обзора можно рекомендовать, например, M. R. Garey and D. S. Johnson. *Computers and Intractability, A Guide of the Theory of NP completeness* (Freeman, San Francisco,1979).

Есть русский перевод: М. Гэри, Д. Джонсон. *Вычислительные машины и труднорешаемые задачи* (Москва «Мир»,1982).

[2] R. P. Feynman, R. B. Leighton and M. Sands. *The Feynman Lectures on Physics*, Vol. 3 (Addison-Wesley, Reading, MA,1963).

[3] D. Deutch. Proc. R. Soc. London, Ser. **A400**, 97, (1985).

[4] R. P. Feynman. Found. Pyes. **16**, 507 (1986).

[5] C. H. Bennet. IBM J. Res. Dev. **6**, 525 (1979).

[6] T. J. Toffoli. J. Comput. Syst. Sci. **15**, 213 (1979).