Сложность вычисления: решённые задачи и открытые проблемы ММРО-2019, Москва

Екатерина А. Карацуба

Федеральный исследовательский центр «Информатика и управление» Российской Академии Наук

29 ноября 2019 г.

Понятие сложности вычисления появилось в результате развития вычислительных методов и теории информации. Современные основы теории сложности вычислений в информатике были заложены работами Г. Найквиста [1] и Р. Хартли [2], с введением понятия меры информации. Первые постановки задач о битовой сложности вычислений (1956 г.) принадлежат А.Н. Колмогорову [3]. при этом он сам отмечал: «цикл моих работ по теории информации был создан под большим влиянием публикаций Норберта Винера и Клода Шеннона».

Под алгоритмом мы будем понимать правило или способ вычисления, не формализуя это понятие. Далее будем считать, что числа записаны в двоичной системе счисления, знаки которой 0 и 1 называются битами.

Опр. 1. Запись знаков 0, 1 , плюс, минус, скобка; сложение, вычитание и умножение двух битов назовём одной элементарной или битовой операцией.

Рассмотрим наиболее простой пример вычисления вещественной функции $y = f(x)$ вещественного переменного x, $a \leq x \leq b$. Пусть вещественная функция $f(x)$ вещественного переменного x, $a \leq x \leq b$, удовлетворяет на (a, b) условию Липшица порядка α, $0 < \alpha < 1$, так что при $x_1, x_2 \in (a, b)$: $|f(x_1) - f(x_2)| \leq |x_1 - x_2|^\alpha$. Пусть n — натуральное число.

Опр. 2. Вычислить функцию $y = f(x)$ в точке $x = x_0 \in (a, b)$ с точностью до n знаков, значит найти такое число A, что $|f(x_0) - A| \leq 2^{-n}$.

Опр. 3. Количество битовых операций, достаточное для вычисления функции $f(x)$ в точке $x = x_0$ с точностью до n знаков посредством данного алгоритма, называется сложностью (битовой) вычисления $f(x)$ в точке $x = x_0$.

Таким образом, сложность вычисления $f(x)$ в точке $x = x_0$ есть функция n, а также $f(x)$ и $x = x_0$. Эту функцию обозначают символом $S_{f(n)} = S_{f,x_0(n)}$. Ясно, что S_f зависит также от алгоритма вычисления и при разных алгоритмах будет разной. Сложность вычисления непосредственно связана со временем, затрачиваемым компьютером на это вычисление и потому иногда в литературе (например, в книге "Искусство программирования на ЭВМ"Д. Кнута) обозначается «временной» функцией $T(n)$.

Битовая сложность точнее всего определяет меру эффективности реальных вычислений. В то же время в разных задачах можно определять меру эффективности вычислений разными способами. Так, наряду с битовой, существуют алгебраическая, колмогоровская, рациональная и т.д. сложности. Одни из них определяются количеством затрачиваемых на вычисление битовых, алгебраических и т.п. операций; другие – количеством шагов вычислительного процесса, например, количеством шагов работы машины Тьюринга.
По-видимому, первым алгоритмом, проанализированным с точки зрения его сложности (см. [4]), был алгоритм Евклида вычисления наибольшего общего делителя двух целых чисел. Мерой его сложности служило количество шагов-делений в этом алгоритме.
Задача была решена полностью (ещё в XIX веке), была получена оптимальная оценка сложности алгоритма.
Оценки сложности алгоритма Евклида получили [4] А.-А.-Л. Рейно (грубая оценка числа шагов алгоритма, 1811 г.), П.-Ж.-Э. Финк (оценка шагов алгоритма, близкая к оптимальной, 1841 г.) и Г. Ламе (оптимальная оценка, 1844 г.). Последний результат известен в литературе, как теорема Ламе.

В теории (битовой) сложности вычислений, на которой сосредоточено наибольшее внимание современных исследователей, остаётся много открытых проблем. Более того, до сих пор построение этой теории (включая основные определения и понятия) не завершено. Разные определения и постановки задач имеют следствием неверные оценки сложности, и как следствие неверный вывод о том, является ли алгоритм быстрым.

Кроме того, история показала, что некоторые естественные логические умозаключения в этой области не работают: в 50-х гг. А.Н. Колмогоров высказал гипотезу, что нижняя оценка сложности умножения $M(n)$ при любом методе умножения есть величина порядка n^2 («гипотеза n^2 Колмогорова»), на том основании, что все известные к тому времени методы умножения имеют сложность n^2, используются не менее 4-х тысячелетий, и если бы был более быстрый метод умножения, то он, вероятно, уже был бы найден. Тем не менее, в 1960 г. [5] был найден новый метод умножения двух n-значных чисел с оценкой сложности

$$M(n) = O(n^{\log_2 3}), \log_2 3 = 1,5849\ldots,$$

опровергая гипотезу n^2. С момента построения этого метода умножения началась теория быстрых вычислений, и было построено множество быстрых алгоритмов обычного и матричного умножений, Фурье-преобразований и вычислений элементарных и высших трансцендентных функций и классических констант.

В 1991 автор построил [6]-[7] метод БВЕ (Быстрого Вычисления Е-функций) – метод быстрого суммирования специального вида рядов, который позволяет вычислить любую элементарную трансцендентную функцию для любого аргумента, классические константы e, π, постоянную Эйлера γ, постоянные Апери и Каталана, такие высшие трансцендентные функции, как гамма-функцию Эйлера, гипергеометрические функции, сферические функции, цилиндрические функции и т. д. для алгебраических значений аргумента и параметров, дзета-функцию Римана для целых значений аргумента, дзета-функцию Гурвица для целого аргумента и алгебраических значений параметра, а также такие специальные интегралы, как интеграл вероятности, интегралы Френеля, интегральную экспоненциальную функцию, интегральные синус и косинус и т. д. при алгебраических значениях аргумента с оценкой сложности вычисления, близкой к оптимальной, а именно

$$S_f(n) = O(M(n)\log^2 n).$$

Дополнительным преимуществом метода является возможность распараллеливания основанных на БВЕ алгоритмов.

Построение алгоритмов вычисления широкого класса функций с оценкой битовой сложности, близкой к оптимальной, а также получение нетривиальных нижних оценок битовой сложности – основные задачи в той области вычислительной математики, которая называется быстрые алгоритмы или быстрые вычисления. В настоящее время (ноябрь 2019) здесь остаётся много нерешённых проблем, таких как

1. получение нетривиальной оценки снизу сложности умножения или сложности вычисления трансцендентных функций;
2. построение быстрых алгоритмов вычисления высших трансцендентных функций в трансцендентных точках;
3. построение быстрых алгоритмов вычисления таких констант, как константа Бруна, значения дзета-функции Римана в нецелых точках и т.д.
4. оценка сложности вычисления решений систем дифференциальных, интегро-дифференциальных, матричных и т.п. уравнений, когда решение не выписывается конечной комбинацией известных трансцендентных функций.

В то же время существуют и более общие проблемы теории сложности вычисления, скажем, как оценивать эффективно сложность вычисления решений задач посредством слабо-структурированных методов, при которых заранее нельзя гарантировать определённую точность вычисления (множество методов классификации и распознавания), или, как адаптировать теорию битовой сложности (предполагающей бесконечную память компьютера) на реальные технические ограничения.

- *Nyquist H.*Certain factors affecting telegraph speed//Bell System Technical Journal, 3, 324-346 (1924).
- *Hartley R.*Transmission of Information//Bell System Technical Journal, 7, 535-563 (1928).
- *Колмогоров А. Н.* О некоторых асимптотических характеристиках вполне ограниченных метрических пространств//Доклады Акад. Наук СССР, 108:3, 385-388 (1956).
- *Shallit J.*Origins of the Analysis of the Euclidean Algorithm//Historia Mathematica, 21, 401-419 (1994).
- *Карацуба А., Офман Ю.*Умножение многозначных чисел на автоматах//Доклады Акад. Наук СССР, 145: 2, 293-294 (1962).
- *Карацуба Е. А.*Быстрое вычисление трансцендентных функций//Проблемы передачи информации, 27:4, 87-110 (1991).
- *Карацуба Е. А.* Быстрые аппроксимации некоторых теоретико-числовых констант//Доклады Акад. Наук, 462:2, 137-140 (2015).