УДК 519.7 DOI: 10.34708/GSTOU.CONF.2020.18.59.030

ОБ ОДНОМ МЕТОДЕ ПОИСКА СИММЕТРИЧНЫХ БИЛИНЕЙНЫХ АЛГОРИТМОВ УМНОЖЕНИЯ МАТРИЦ

Чокаев Б. В.
ГГНТУ им. акад. М.Д. Миллионщикова,
Чеченский государственный университет,
г. Грозный

Известно, что билинейный алгоритм для умножения матриц 3x3 можно задавать с помощью упорядоченных троек 3x3-матриц A, B, C. Широко изучаемыми являются алгоритмы, обладающие различными симметриями. Актуальной задачей является разработка алгоритмов, обладающих различными симметриями. В данной статье представлены два алгоритма сложности 25, обладающие определенными симметриями. Показано, что найденные алгоритмы являются различными и новыми.

Ключевые слова: умножение матриц, алгоритм Штрассена, билинейная сложность.

Одной из центральных областей алгебраической теории сложности является сложность умножения в алгебрах. Задача сложности умножения в алгебре заключается в том, чтобы построить алгоритм, который для любых двух элементов алгебры вычислял бы их произведение, и имел бы наименьшую сложность. При этом под сложностью алгоритма могут подразумеваться различные понятия. Например, можно учитывать все арифметические операции над полем, которые требуются для вычисления произведения в алгебре. Возникающая сложность называется арифметической (тотальной) сложностью. Другой способ определения сложности – учитывать только так называемые существенные умножения, то есть такие операции умножения, оба операнда в которых зависят от входных переменных. В этом случае возникают понятия билинейного алгоритма и билинейной сложности (или ранга). Если рассматривать последовательность билинейных алгоритмов, сходящаяся к билинейному алгоритму для умножения в данной алгебре, то возникают более общие понятия – приближенного билинейного алгоритма и граничного ранга алгебры.

Во многих практических алгоритмах (в частности, в криптографии и в комбинаторных алгоритмах) активно используются различные алгебраические операции. В частности, операция умножения матриц лежит в основе сложности не только большинства задач линейной алгебры, но и множества комбинаторных задач. Например, для получения быстрых алгоритмов для задач построения замыкания графа и нахождения всех кратчайших путей в графе достаточно иметь быстрый алгоритм умножения матриц.

Кроме того, задача нахождения ранга билинейного отображения, в частности ранга умножения в алгебре, лежит в основе многих прикладных задач из различных областей науки. Примерами могут служить следующие задачи: интерпретация магнитно-резонансной томографии в медицине, интерпретация магнитотеллурических данных для одномерных и двумерных региональных структур в геофизике, определение соединений в растворе с использованием флуоресцентной спектроскопии в химии, определение местоположения источника радиосигнала по данным из нескольких приемников в радиотехнике.

Задача умножения матрицы размера m на n на матрицу размера n на p – это задача вычисления системы из mp билинейных форм. *Билинейным алгоритмом сложности r* для этой задачи называется следующая последовательность шагов: 1) вычисление 2r линейных форм от входных переменных; 2) вычисление r их попарных произведений; 3) вычисление каждой из mp искомых билинейных форм в виде линейной комбинации найденных билинейных форм. Билинейной сложностью этой задачи называется наименьшее r среди всех билинейных алгоритмов для нее, она обозначается rk(m,n,p).

Исследование билинейной сложности умножения матриц даже малых размеров является непростой задачей – на сегодняшний день установлены значения билинейной сложности только для трех наборов значений параметров[2] m,n и p: rk(2,2,2)=7, rk(2,2,3) = 11, rk(2,2,4) = 14. Для умножения матриц 3x3 еще в 1976 г. Дж. Ладерманом был найден алгоритм сложности 23, но с тех пор понизить эту оценку не удалось (текущая нижняя оценка равна 19). Тем не менее, периодически появляются статьи, посвященные билинейным алгоритмам умножения матриц 3x3. Статья [1] посвящена исследованию симметрий известных алгоритмов. В работе [2] приводится не известный ранее алгоритм сложности 23, симметричный относительно действия циклических групп порядков 3 и 4. В статье [3] показывается, как аналитически строить алгоритм сложности 25, симметричный относительно группы перестановок порядка 4 и имеющий некоторую дополнительную симметрию.

Симметричные алгоритмы для задач малой размерности представляют интерес по нескольким причинам. Во-первых, они являются более простыми для понимания, чем билинейные алгоритмы общего вида. Во-вторых, для того чтобы их задать, достаточно обозначить некоторую часть алгоритма и определить правила порождения остальных частей при помощи действия группы. В-третьих, такие алгоритмы могут помочь понять, как устроены оптимальные билинейные алгоритмы для общей задачи (произвольной размерности), так как в симметричных алгоритмах легче заметить закономерность. К тому же, так как сама операция умножения как билинейное отображение обладает рядом симметрий, то, вероятно, оптимальный алгоритм для него также будет обладать этими симметриями.

[2] С учетом того, что rk(m,n,p) не меняется при любой перестановке параметров m,n и p, а также, не считая тривиальных случаев, когда один или несколько параметров из m,n и p равны 1 (в этих случаях rk(m,n,p)=mnp).

Данная работа посвящена методу поиска симметричных (в некотором смысле) билинейных алгоритмов умножения матриц 3x3 путем численного решения системы уравнений.

Можно легко показать, что существование билинейного алгоритма сложности r для задачи умножения матрицы размера m на n на матрицу размера n на p эквивалентно существованию r(mn+np+pm) чисел, таких, что выполнена система из nmpnmp уравнений.

Алгоритм умножения матриц 3x3 сложности r представляет собой решение системы из 729 уравнений с 27r неизвестными (m=n=p=3). То есть алгоритм сложности r задается с помощью r упорядоченных троек матриц A, B, C размера 3x3. Под *симметричным алгоритмом* в данной работе будем понимать билинейный алгоритм, обладающий двумя свойствами[3]: 1) в алгоритме присутствует тройка единичных матриц; 2) если в алгоритме присутствует тройка A, B, C, то в нем также присутствуют две другие тройки B, C, A и C, A, B.

В данной работе проводился поиск симметричного алгоритма сложности[4] r=19 или r=22. Для симметричного алгоритма система уравнений преобразуется в систему, в которой число неизвестных равно 9(r-1), а число различных уравнений – 249 (часть переменных и уравнений отождествляется между собой в силу свойства 2 алгоритма). Для решения этой системы использовался метод Монте-Карло, примененный к нахождению глобального минимума функционала невязки. Расчеты проводились на суперкомпьютере IBM BlueGene/P, установленном на факультете ВМК МГУ.

В первом случае минимизировался функционал, соответствующий системе с r=22 и числом переменных 9(r-1)=189 . В найденном наборе значений переменных только одно уравнение из 249 давало существенный вклад в невязку, остальные уравнения давали вклад, близкий к нулю. Во втором случае минимизировался функционал, соответствующий системе с r=19 и числом переменных 9(r-1)=162. Найденная последовательность значений переменных была такова, что три уравнения из 249 давали существенный вклад в невязку, остальные – вклад, близкий к нулю. В обоих этих случаях визуальный анализ найденного решения позволил его преобразовать в симметричный билинейный алгоритм сложности 25 с коэффициентами из множества {0, 1, -1, 0.5, -0.5, 2/3, -2/3}.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта 18–31–00044-мол-а.

[3] Отметим, что этими свойствами обладает алгоритм Штрассена для умножения матриц 2x2. А также алгоритм для умножения матриц 3x3 сложности 25 из [3]. Кроме того, алгоритм Ладермана и алгоритм из [2] обладают следующим свойством, которое близко свойству 2: если в алгоритме присутствует тройка A, B, C, то либо в нем также присутствуют две другие тройки B, C, A и C, A, B, либо A = B = C.

[4] Так как в симметричных алгоритмах r-1 делится на 3, а r заведомо расположено между 19 и 23, то для r остается всего два варианта.

Список литературы

1. Burichenko V.P. Symmetries of matrix multiplication algorithms// arXiv:1508.01110[cs.CC]. 2015.

2. Ballard G., Ikenmeyer C., Landsberg J.M., Ryder N. The geometry of rank decompositions of matrix multiplication in 3x3 matrices// arXiv:1610.08364. [cs.SC]. 2017.

3. Grochow J. A., Moore C. Matrix multiplication algorithms from group orbits // arXiv:1612.01527. 2016.