Современная математика и ее приложения. Том 100 (2016). С. 19–23

УДК 512+519.6

БЫСТРОЕ УМНОЖЕНИЕ МАТРИЦ С ПОМОЩЬЮ ЦВЕТНЫХ АЛГЕБР

© 2016 г. **Р. Р. АЙДАГУЛОВ, М. В. ШАМОЛИН**

Аннотация. В работе предлагается метод вычисления произведения матриц, который использует цветные алгебры.

Аналог быстрого умножения чисел по алгоритму Карацуба для матриц был создан Штрассеном в 1969 г. (см. [9]). Аналога метода быстрого умножения чисел Кули—Тьюки, основанном на быстром преобразовании Фурье, для матриц до сих пор не было. Методы групповой алгебры для умножения матриц близки к методам быстрого преобразования матриц (см. [7]), но они не дали хороших результатов. Причины этого можно понять из нижеизложенного.

Более сильные результаты получились при оценке ранга трилинейного тензора (см. [4]). Однако и здесь после работы [6] существенного продвижения не было (см. [8]). Здесь предлагается метод вычисления произведения матриц, являющегося аналогом использования быстрого преобразования Фурье при умножении больших чисел.

Приведенный ниже метод умножения матриц использует цветные алгебры (см. [2]). Точнее, мы используем квазикоммутативную алгебру, названную здесь бигрупповой алгеброй, по аналогии с групповой алгеброй и бихарактерами. В зарубежной литературе эта алгебра имеет другое название. Однако по мнению авторов, название «бигрупповая алгебра» более естественно.

Пусть G — конечная абелева группа. Бигрупповая алгебра определяется как расширение групповой алгебры, состоящей из формальных сумм:

$$\sum_{\mu,g} a_{\mu g}\mu g, \quad a_{\mu g} \in K, \quad \mu \in G^*, \quad g \in G.$$

Здесь $a_{\mu g} \in K$ — коэффициенты из некоторого поля K, $\mu \in G^*$ — характеры из группы характеров нашей группы.

Групповая алгебра является коммутативной подалгеброй бигрупповой алгебры и состоит из элементов, где коэффициенты перед неединичными характерами равны нулю. В групповой алгебре, как в линейном пространстве, выберем базис $e_g = g$, $g \in G$. Определим бигрупповую алгебру как алгебру операторов в линейном пространстве (в групповой алгебре). Действие элемента $h \in G$ определяется согласно закону умножения в группе, а характеры действуют как диагональные матрицы:

$$h(e_g) = e_{hg}, \quad \mu(e_g) = \mu(g)e_g.$$

Определим действие операторов μg, $g\mu$ на векторы:

$$\mu g(e_h) = \mu(e_{gh}) = \mu(gh)e_{gh} = \mu(g)\mu(h)g(e_h) = \mu(g)(g\mu)(e_h).$$

Таким образом,

$$\mu g = \mu(g)g\mu,$$

т.е. бигрупповая алгебра является цветной алгеброй с группой цветов, являющейся прямой суммой двух изоморфных групп: группы характеров и самой группы.

Будем дальше использовать следующую известную лемму.

Работа выполнена при поддержке Российского фонда фундаментальных исследований (грант № 12-01-00020-а).

ISSN 1512–1712 © Грузинский технический университет, 2016

Лемма 1. *Пусть G — конечная коммутативная группа порядка n и в K^* имеется примитивный корень степени n. Тогда между характерами и элементами группы имеются следующие соотношения:*

$$\sum_{\mu\in G^*}\mu(g)=\begin{cases}|G|, & g=e,\\ 0, & g\neq e;\end{cases}\qquad \sum_{g\in G}\mu(g)=\begin{cases}|G|, & \mu=e,\\ 0, & \mu\neq e.\end{cases}$$

Используя лемму 1, докажем следующую (известную алгебраистам) теорему.

Теорема 1. *Пусть G — коммутативная группа порядка n. Тогда бигрупповая алгебра изоморфна алгебре матриц порядка $n\times n$.*

Доказательство. Бигрупповая алгебра имеет размерность n^2, как и алгебра матриц. Рассмотрим матрицы вида e_l^g, состоящие сплошь из нулей, за исключением одного элемента (равного 1), стоящего на пересечении строки с номером g и столбца с номером l. Достаточно показать, что такой матрице e_l^g соответствует некоторый элемент бигрупповой алгебры. Для этого покажем, что многочлену

$$a=\frac{1}{|G|}g\sum_{\mu}\mu l^{-1}=\frac{1}{|G|}\sum_{\mu}\mu(g^{-1})\mu g l^{-1}$$

соответствует некоторая матрица e_l^g в базисе e_g.

Вычислим действие элемента a на один из векторов e_h:

$$a(e_h)=\frac{1}{|G|}\sum_{\mu}\mu(l^{-1}h)e_{gl^{-1}h}.$$

В соответствии с леммой 1 данная сумма равна нулю при $h\neq l$, а при $h=l$ получаем, что вектор переходит в e_g. Это означает, что элементу a бигрупповой алгебры соответствует матрица e_l^g.

Поставим в соответствие матрице

$$A=\sum_{g,l}a_{gl}e_l^g$$

многочлен по формуле

$$\sum_{\mu,g}\bar a_{\mu g}\mu g,\quad \bar a_{\mu g}=\frac{1}{|G|}\sum_{l}\mu(g^{-1}l^{-1})a_{g+l,l}.$$

Умножим данное равенство слева и справа на множитель $\mu(s)$ и просуммируем по всем характерам. Это даст формулу обратного перехода:

$$a_{sl}=\sum_{\mu}\mu(s)\bar a_{\mu l}.$$

Теорема доказана. □

Выберем образующие в циклическом разложении на подгруппы,

$$G=\mathbb{Z}_{n_1}\oplus\mathbb{Z}_{n_2}\ldots\oplus\mathbb{Z}_{n_k},$$

и поставим им в соответствие переменные $y_1,\ldots,y_k$. Аналогично разложению в группе характеров поставим в соответствие переменные $x_1,\ldots,x_k$. Все переменные между собой коммутируют, за исключением взаимных (т.е. $x_i\leftrightarrow y_i$) и их степеней:

$$x_iy_i=\theta_iy_ix_i,$$

где θ_i — примитивный корень из 1 степени n_i. Заметим, что переменные $x_i^{n_i}$, $y_i^{n_i}$ коммутируют со всеми многочленами от этих переменных, поэтому можно считать, что они принадлежат полю:

$$x_i^{n_i}=a_i,\quad y_i^{n_i}=b_i.$$

Так получаются квазикоммутативные многочлены, соответствующие бигрупповой алгебре. Мы будем использовать нормированные константы $a_i = b_i = 1$, хотя спиноры нормируют из условия $a_i = -1 = b_i$.

Когда $k > 1$, удобно пользоваться мультииндексами

$$i = (i_1, i_2, \dots, i_k), \quad \theta = (\theta_1, \dots, \theta_k), \quad x = (x_1, x_2, \dots, x_k), \quad y = (y_1, \dots, y_k).$$

При этом операции с мультииндексными величинами вычисляются покомпонентно:

$$i + j = (i_1 + j_1, \dots, i_k + j_k), \quad ij = (i_1 j_1, \dots, i_k j_k), \quad x^i = x_1^{i_1} x_2^{i_2} \dots x_k^{i_k}.$$

Тогда многочлены можно рассматривать как многочлены от двух (мультииндексных) переменных с коммутационным соотношением

$$x^i y^j = \theta^{ij} y^j x^i.$$

Эти обозначения удобны и представляют простые обозначения для тензорных произведений k объектов.

С учетом мультииндексных обозначений элементы бигрупповой алгебры мы можем записать в следующем виде:

$$\sum_{i,j} a_{ij} x^i y^j, \quad \sum_{i,j} b_{ij} x^i y^j.$$

Их произведение имеет вид

$$\sum_{i,j} c_{ij} x^i y^j.$$

Коэффициенты при этом вычисляются по формуле

$$c_{ij} = \sum_{k,l} a_{kl} b_{i-k,j-l} \theta^{l(k-i)}.$$

Определим теперь разбиение многочленов на части, коммутирующие одинаково. Пусть

$$f_j(x) = \sum_i a_{ij} x^i, \quad \varphi_i = \sum_j b_{ij} y^j.$$

Тогда произведение многочленов будет выражаться следующим образом:

$$\sum_{i,j} \theta^{-ij} x^i f_j(x) \varphi_i(y) y^j.$$

При этом такие пары i, j, что θ^{ij} дают одно и то же значение, можно объединить, и это даст мультипликативную свертку наших величин.

Произведение многочленов через его значения вычисляется обратным преобразованием Фурье от значений для группы $G \oplus G$ порядка n^2:

$$g(x, y) = \sum_{i,j} g_{ij} x^i y^j, \quad g_{ij} = \frac{1}{n^2} \sum_{\alpha,\beta} \theta^{-i\alpha - j\beta} \bar{g}_{\alpha\beta}, \quad \bar{g}_{\alpha\beta} = g(\theta^\alpha, \theta^\beta).$$

Таким образом, значения многочленов полностью определяют сам многочлен. Вычислим значения многочлена произведения через значения

$$f_{\alpha j} = f_j(\theta^\alpha), \quad \varphi_{i\beta} = \varphi_i(\theta^\beta).$$

Для получения этих значений понадобится всего $2n$ преобразований Фурье длины n. Таким образом,

$$\bar{g}_{\alpha\beta} = \sum_i \theta^{\alpha i} \varphi_{i\beta} \sum_j \theta^{(\beta - i)j} f_{\alpha j}.$$

Внутреннее суммирование есть преобразование Фурье и вычисляется легко. Запишем это в виде $\bar{f}_{\alpha,\beta-i}$. Остается вычислить

$$\bar{g}_{\alpha\beta} = \sum_i \theta^{\alpha i} \varphi_{i\beta} \bar{f}_{\alpha,\beta-i}.$$

Введем обозначение

$$F_{\alpha k} = \theta^{-k\alpha} \bar{f}_{\alpha k}.$$

Тогда

$$\bar{g}_{\alpha\beta} = \theta^{\alpha\beta} \sum_i \varphi_{\beta-i,\beta} F_{\alpha i}.$$

Необходимые вычисления надо произвести одновременно для всех наборов с постоянным произведением $\alpha\beta = \gamma$. Для этого предварительно вычислим значения, соответствующие $\alpha = 0$ и $\beta = 0$, и члены, соответствующие $i = 0$, т.е. $\varphi_{\beta\beta} F_{\alpha 0}$. На это уйдет всего $O(n^2)$ операций. Остается вычислить значения одновременно для всех наборов $\alpha\beta = \gamma \neq 0$ с ненулевым произведением. Это вынуждает нас сводить вычисления к мультипликативной свертке. Заметим, что абелеву группу можно разложить в прямую сумму силовских подгрупп. При этом умножение в бигрупповой алгебре соответствует умножению в тензорном произведении матриц порядков, являющихся степенями простых чисел.

Так как степени простых чисел занимают нулевую плотность среди таких чисел, для простоты ограничимся случаем, когда число $n = p$ простое. При этом все ненулевые индексы мультипликативно обратимы.

Рассмотрим многочлены

$$F(x,z) = \sum_{0 \leqslant i,a < p-1} F_{g^a,g^i} x^i z^a, \quad \Phi(x,z) = \sum_{0 \leqslant j,b < p-1} \varphi_{g^b - g^{b-j},g^b} x^j z^b.$$

Здесь g — образующая в мультипликативной группе $\mathbb{Z}_p^*$. Тогда произведение многочленов вычисляется по формуле:

$$F(x,z)\Phi(x,z) = \sum_{c=a+b} z^c \sum_b x^b \sum_{i+j=b} F_{g^a,g^{i\varphi} g^b - g^{b-j},g^b}.$$

Отдельно вычисляем значения, соответствующие $\alpha = 0$, $\beta = 0$, $i = 0$:

$$\bar{g}_{0\beta} = \sum_i \varphi_{\beta-i,\beta} F_{0i}, \quad \bar{g}_{\alpha 0} = \sum_i \varphi_{-i,0} F_{\alpha 0}, \quad \bar{g}'_{\alpha\beta} = \varphi_{\beta,\beta} F_{\alpha 0}.$$

На это уйдет не более $O(n^2)$ операций. Тогда для обратимых индексов получаем выражение через мультипликативную свертку:

$$\bar{g}_{\alpha\beta}\theta^{-\alpha\beta} = \bar{g}'_{\alpha\beta} + \sum_{i+j=b} F_{g^a,g^{i\varphi} g^b - g^{b-j},g^b}, \quad \alpha = g^a, \quad \beta = g^b.$$

Эта мультипликативная свертка, соответствующая коэффициенту перед $z^{a+b}x^b$ произведения вышеуказанных многочленов, вычисляется за $O(n^{2+\varepsilon})$ операций.

Сводя при необходимости преобразование Фурье с p элементами к преобразованию с $p-1$ элементами (см. [5]), находим, что общее количество необходимых операций оценивается как $O(n^{2+\varepsilon})$ (см. также [1,3]).

СПИСОК ЛИТЕРАТУРЫ

1. *Айдагулов Р. Р., Шамолин М. В.* Некоторое уточнение алгоритма Конвея// Вестн. Моск. ун-та. Сер. 1. Мат. Мех. — 2005. — № 3. — С. 53–55.
2. *Айдагулов Р. Р., Шамолин М. В.* Группы цветов// Совр. мат. прилож. — 2009. — *62*. — С. 15–27.
3. *Айдагулов Р. Р., Шамолин М. В.* Формулы интегрирования десятого порядка точности и выше// Вестн. Моск. ун-та. Сер. 1. Мат. Мех. — 2010. — № 4. — С. 3–7.
4. *Жданович Д. В.* Экспонента сложности матричного умножения// Фундам. прикл. мат. — 2011/2012. — *17*, № 2. — С. 107–166.
5. *Ноден П., Китте К.* Алгебраическая алгоритмика. — М.: Мир, 1999.
6. *Coppersmith D., Winograd S.* Matrix multiplication via arithmetic progressions// J. Symbol. Comput. — 1990. — *9*, № 3. — С. 251–280.

7. *Demmel J., Dumitriu I., Holtz O., Kleinberg R.* Fast matrix multiplication is stable// http://arxiv.org/abs/math/0603207
8. *Le Gall F.* Powers of tensors and fast matrix multiplication// http://simons.berkeley.edu/talks/francois-le-gall-2014-11-12
9. *Strassen V.* Gaussian elimination is not optimal// Numer. Math. — 1969. — *13*, № 4. — С. 354–356.

Р. Р. Айдагулов
Московский государственный университет им. М. В. Ломоносова
М. В. Шамолин
Институт механики МГУ им. М. В. Ломоносова
E-mail: shamolin@rambler.ru, shamolin@imec.msu.ru