Алгоритмы быстрого умножения

Р. Р. Айдагулов[1]

Здесь рассматриваются алгоритмы быстрого умножения как для больших чисел, так и для больших квадратных матриц. При умножении чисел вводится групповая алгебра, и преобразование Фурье выражается как представление элементов групповой алгебры в другом базисе, связанном с характерами. Далее вводится бигрупповая алгебра как расширение операторов групповой алгебры с использованием характеров, действующих как диагональные матрицы в стандартном базисе групповой алгебры. Аналог умножения больших чисел преобразованием Фурье распространяется на бигрупповую алгебру, т.е. на алгебру матриц.

Ключевые слова. Групповая алгебра, символы, бигрупповая алгебра, знаковые автоморфизмы, симметрии, значения.

Ключевые слова: кластер, алгоритм, плотность, метод осреднения.

Большие числа на компьютере представляются в M – ичной системе исчисления как значения многочлена:

$$X = x_0 + x_1 M + ... + x_{k-1} M^{k-1}.$$

M есть степень двойки, обычно $M = 2^d,\ d = 32$. Считаем, что $0 \le x_i < M$. Соответственно $X < M^k = 2^n, n = kd$. Пусть задано другое большое число $Y = y_0 + ... + y_{l-1} M^{l-1}$ и требуется найти произведение, которое не превышает $M^m, m = k + l$. Произведение представляется в виде:

$$Z = XY = \sum_{i=0}^{m-1} z_i M^i, \quad z_i = \sum_{k+j=i} x_k y_j. \tag{1}$$

Правда, здесь после вычисления надо осуществить переносы, когда цифры становятся не меньше M. Для этого складываем перенос из нижнего уровня и делим на M, остаток от деления будет настоящей цифрой этого уровня, а целая часть от деления пойдет в следующий уровень как перенос.

[1] *Айдагулов Рустем Римович* — Старший научный сотрудник. Кафедра теоретической информатики, механико-математический факультет, Московский государственный университет имени М.В. Ломоносова, Ленинские горы 1, Москва, 119991, Россия, a_rust@bk.ru.

Aidagulov Rustem Rimovich — Senior Researcher. Department of Theoretical Informatics, Faculty of Mechanics and Mathematics, Moscow Lomonosov State University, Leninskiye Gory 1, Moscow, 119991, Russia, a_rust@bk.ru.

Пусть задана конечная абелева группа G и групповая алгебра над кольцом $K(G)$, элементы которой являются формальными суммами:

$$a = \sum_{g \in G} a(g)g,\ b = \sum_{g \in G} b(g)g.$$

Их произведение определяется по такой же формуле, как и в (1)

$$ab = c = \sum_{g} c(g)g,\ c(g) = \sum_{g_1 g_2 = g} a(g_1)b(g_2). \tag{2}$$

Заметим, что если сопоставим элементам циклической группы $g_i \leftrightarrow M^i$, форма вычисления коэффициентов полностью совпадают. Для этого порядок группы должен быть не меньше $k+l-1$. Для вычислений удобнее, когда порядок группы разлагается на малые множители. Для умножения очень больших чисел можно использовать и не циклические группы $G = (Z_m)^k$. При этом появляются сложности не соответствия размеров и произведения в группе сложению степеней многочлена, которые преодолеваются с некоторой потерей эффективности.

Для эффективности вычисления коэффициентов в (2) надо сопоставить элементам группы числа из кольца коэффициентов $\mu_k : g^i \to \theta^{ik}, \theta \in K$ так, чтобы $\theta^n = 1$. Расспространяя вычисление характера на всю групповую алгебру получим n значений для n характеров. Произведение значений сомножителей будут значениями произведения.

В дальнейшем считаем, что $n = |G| = |G^*|$ обратим в кольце коэффициентов. Для каждого из n характеров определим средние (с весами) элементы

$$t_\mu = \frac{1}{|G|} \sum_{g \in G} \mu(g)g. \tag{3}$$

Характеры можно применять и к этим n различным элементам:

$$\mu_1(t_\mu) = \frac{1}{|G|} \sum_{g \in G} \mu(g)\mu_1(g)g = t_{\mu\mu_1}. \tag{4}$$

Лемма 1. *Пусть G конечная коммутативная группа порядка n, изоморфная своей группе характеров. Тогда между характерами и элементами группы имеется соотношение:*

$$\sum_{\mu \in G^*} \mu(g) = \begin{cases} |G|,\ g = e, \\ 0,\ g \neq e. \end{cases} \qquad \sum_{g \in G} \mu(g) = \begin{cases} |G|,\ \mu = e, \\ 0,\ \mu \neq e. \end{cases} \tag{5}$$

Из него получаем ортогональность базиса t_μ:

$$t_\mu t_{\mu_1} = \frac{1}{|G|^2} \sum_{g, g_1} \mu(g)\mu_1(g_1)gg_1 = \frac{1}{|G|} \sum_{g} \mu(g)\mu_1(g^{-1})t_{\mu_1} = \begin{cases} t_\mu, \mu = \mu_1, \\ 0, \mu \neq \mu_1. \end{cases} \tag{6}$$

Пусть многочлен представляется (задан) как элемемент групповой алгебры $f = \sum_g a(g)g$. Тогда его представление в базисе t_μ имеет вид:

$$f = \sum_g a(g)g = \sum_\mu t_\mu \sum_g a(g)\mu(g^{-1}) = \sum_\mu \overline{a}(\mu)t_\mu, \quad \overline{a}_\mu = \sum_g \mu(g^{-1})a(g). \tag{7}$$

Аналогично, обратный переход

$$f = \sum_\mu \overline{a}(\mu)t_\mu = \frac{1}{n}\sum_{\mu,g} \overline{a}(\mu)\mu(g)g = \sum_g a(g)g, \quad a(g) = \frac{1}{n}\sum_\mu \overline{a}(\mu)\mu(g). \tag{8}$$

Таким образом, обратное преобразование Фурье получается вычислением значений многочлена $\sum_\mu \overline{a}(\mu)t_\mu$ заменяя переменные t_μ на $\mu(g)$ и поделив результат на n.

1. Бигрупповая алгебра

Пусть G конечная абелева группа порядка n, K коммутативное кольцо с единицей, где n обратимо и имеются корни из 1 соответствующей степени, $K(G)$ групповая алгебра. Элементы групповой алгебры можно рассматривать как линейные операторы, действующее в $V = K(G)$ через умножение. Отметим, что все эти операторы в базисе t_μ приводятся к диагональному виду $gt_\mu = \mu^{-1}(g)t_\mu$. Введем еще операторы-характеры, действующие диагонально в базисе g: $\mu : g \to \mu(g)g$. Полученная алгебра операторов на $V = K(G)$, называемая в далнейшем бигрупповой алгеброй группы G [1], состоит из формальных линейных сумм:

$$\sum_{\mu,g} a(\mu, g)\mu g.$$

Образующие этой алгебры μ, g удовлетворяют коммутационным соотношениям:

$$\mu g = \mu(g)g\mu. \tag{9}$$

В дальнейшем ограничимся рассмотрением бигрупповой алгебры группы $(Z_2)^k$, которая изоморфна алгебре матриц $n \times n$, $n = 2^k$ (для характеристики, отличной от 2). В дальнейшем базис Сильвестра бигрупповой алгебры, состоящий из n^2 элементов обозначим через $G = \{g\}$, для сходства с первой частью (групповой алгеброй). Особым элементом базиса является единица, коммутирующая со всеми остальными. Все другие элементы базиса с половиной из остальных антикоммутируют, с другой половиной (включая себя и единицу) коммутируют. Если $t \neq 1$ антикоммутирует с элементом s, то множества цветов $P_0(t), P_1(t)$

коммутирующих и антикоммутирующих с элементом t связаны соотношением $P_0(t) = P_1(t) \oplus s, P_1(t) = P_0(t) \oplus s$. Для каждого элемента базиса Сильвестра t определим характер на элементах базиса Сильвестра $t(g) = tgt^{-1}g^{-1}$ и значение многочлена (на элементах бигрупповой алгебры) $t(\sum_g a(g)g) = \sum_g a(g)t(g)$. Очевидно, что лемма 1 остается справедливой с учетом того, что сейчас $|G| = |G^*| = n^2$.

Определим инволюцию на элементах базиса Сильвестра и антиизоморфизм на всей бигрупповой алгебре через значения на образующих алгебры исходя из формулы:

$$I(x_i) = -x_i, I(y_i) = -y_i, I(x_iy_i) = -x_iy_i.$$

Имеется еще другой антиизоморфизм-транспонирование $x_i^T = x_i, y_i^T = y_i, (x_iy_i)^T = y_ix_i = -x_iy_i$. Все $n^2 = 4^k$ цветов разделяются на 4 типа:

0 - (0,0) $\{g|I(g) = g, g^T = g\}$ их количество $4^{k-1} + y_k,\ y_k = \frac{2^k+(-2)^k}{4}$.

1 - (0,1) $\{g|I(g) = g, G^T = -g\}$ их количество $4^{k-1} - 2y_k$.

2 - (1,0) $\{g|I(g) = -g, G^T = g\}$ их количество $4^{k-1} + 2y_k$.

3 - (1,1) $\{g|I(g) = -g, G^T = -g\}$ их количество $4^{k-1} - y_k$.

Зная разложения множителей

$$A = \sum_{g_1} a(g_1)g_1,\ B = \sum_{g_2} b(g_2)g_2$$

можем определить левые и правые значения и по ним вычислить произведение $C = \sum_g c(g)g$.

Несмотря на то, что $t : G \to Z_2, t(g) = tgt^{-1}g^{-1} = \pm 1$ гомоморфизм из группы цветов, мы не можем определить даже значение $t(g) = t(g^{-1})$, для $g = xy = -yx = -g^{-1}, t(g_1g_2)) = t(g_1)t(g_2)$. Поэтому произведение значений вычислим двумя способами для не единичного характера. Пусть произведения элементов $a(g_1)b(g_2^{-1}) = c_1g_1g_2^{-1}, a(g_3^{-1})b(g_4) = c_2g^{-1}$. Нам надо правильно определить суммы разных составляющих одного цвета и привести их к единому виду. Для этого достаточно правильно определить знаки каждого произведения на каждом уровне $g_i = (g_{i1}, g_{i2}, ..., g_{ik})$, т.е. достаточно правильно определить знаки перед $g = g_1g_2^{-1}$ для каждого случая $g_1 = 1, x, y, xy;\ g_2 = 1, x, y, xy$; и правильно определить знак перехода из коэффициентов перед g к коэффициенту перед g^{-1}. Последнее верно, если менять знак только для случая $g = xy$. Тогда знак перед $g = 1$ будет вычислен правильно, если знаки перед g и g^{-1} будут одинаковы . В случае, когда $g_1 = 1$ или $g_2 = 1$ так же знак произведения будет определен правильно. Остается рассмотреть случай, когда g_1 и g_2 антикоммутируют. В этом случае, из $g_1g_2 = g_3$ следует $(-g_2)(-g_1) = (-g_3)$. Таким образом, отображение $I(g) = (I(g_1), I(g_2), ..., I(g_k)) = (-1)^l g, I(g_i) = 1,\ if\ g_i = 1,\ I(g_i) =$

$-g_i \ if \ g_i \neq 1$ является нужным антиизоморфизмом, определяющим сопряженные значение $\bar{t}(g) = t(I(g))$ к значению $t(g)$.

Обозначим через $\bar{t}(\sum_g a(g)g) = \sum_g a(g^{-1})t(g)$. Аналогично (3) можно ввести средние

$$t_\mu = \frac{1}{|G|}\sum_{g\in G}\mu(g)g, \quad \bar{t}_\mu = \frac{1}{|G|}\sum_{g\in G}\mu(g)g^{-1}, \ |G| = n^2.$$

При этом остается справедливой (4). Соотношение (6) несколько изменится:

$$t_\mu \bar{t}_{\mu_1} = \begin{cases} 1_\mu, \mu = \mu_1 \\ 0, \ \mu \neq \mu_1 \end{cases}$$

Отметим, что аналоги формул (7) и (8) так же имеются. Однако, у нас в вычислениях используются характеры парами на подобии спинорных:

$$\sum_g c(g)g = \sum_{g_1,g_2} a(g)b(g_2^{-1})g_1 g_2^{-1},$$

$$t(C) = \sum_g c(g)t(g) = (\sum_{g_1} a(g_1)t(g_1))(\sum_{g_2} b(g_2^{-1})t(g_2^{-1}) = t(A)\bar{t}(B).$$

$$\bar{t}(C) = \sum_g c(g)t(g) = (\sum_{g_1} a(g_1^{-1})t(g_1^{-1}))(\sum_{g_2} b(g_2)t(g_2) = \bar{t}(A)t(B) = t(C^T).$$

$$c(g) = \frac{1}{|G|}[1(C) + \sum_{t\neq 1} t(g)\frac{t(C) + g^2\bar{t}(C)}{2}], \ |G| = n^2.$$

Отметим, что $g^2 = \pm 1$ и поэтому формула вычисления коэффициента $c(g)$ перед элементом базиса Сильвестра корректна.

Элемент $t = \prod_i t_i$ базиса Сильвестра определяется адресом, где хранится значение коэффициента перед t. Компоненты t_i, определяются двумя битами адреса. Пусть значения битов соответствуют

$$00 - t_i = 1, \quad 01 - t_i = x_i, \quad 10 - t_i = y_i, \quad 11 - t_i = x_i y_i.$$

Так удается вычислять коэффициенты разложения в базисе Сильвестра на месте самих матриц. На самом деле можно вычислять и значения прямо на этом месте (в массиве коэффициентов матриц) за $O(n^2 \log n)$ операций и обратно, коэффициенты матриц по значениям произведения матриц за $O(n^2 \log n)$ операций. При этом $O(n^2 \log n)$ операций сложения вычитания элементов массива и примерно столько же еще более быстрых логических операций. На порядок медленных операций умножения всего $2n^2 - 1$.

Список литературы

1. Айдагулов Р.Р. Бигрупповые алгебры и их автоморфизмы. В эл. журнале Дневник науки №1 2019г. (20 стр.)

Fast multiplication algorithms
Aidagulov R.R.

Fast multiplication algorithms for both large numbers and large square matrices are considered here. When multiplying numbers, a group algebra is introduced, and the Fourier transform is expressed as a representation of the elements of the group algebra in another basis associated with characters. Next, bigroup algebra is introduced as an extension of group algebra operators using characters acting as diagonal matrices in the standard basis of group algebra. The analogue of multiplication of large numbers by the Fourier transform extends to group algebra, i.e. to the algebra of matrices.

Keywords: Group algebra, symbols, b and group algebra, sign automorphisms, symmetries, values.

References

[1] Aidagulov R.R., “Bigroup algebras and their automorphisms.”, *Electronic journal "Diary of Science"*, 2019 N1. (In Russian), 20 pp.