УДК 512+519.6

БИГРУППОВЫЕ АЛГЕБРЫ И ИХ АВТОМОРФИЗМЫ

Айдагулов Р.Р.,
кандидат физико-математических наук, старший научный сотрудник
Московский государственный университет им. М.В.Ломоносова
Институт машиноведения РАН им. А.А. Благонравова
Россия, г. Москва

Аннотация: Бигрупповые алгебры играют роль групповых алгебр в не коммутативном случае. Они позволяют создать аналоги быстрого преобразования Фурье и алгоритмы быстрого умножения в не коммутативных алгебрах. Эти алгебры представляют так же самостоятельный интерес для изучения, как имеющие различные приложения.
Ключевые слова: градуированные алгебры, группа цветов, базисы Сильвестра и Вейля-Швингера.

B AND GROUP ALGEBRAS AND THEIR AUTOMORPHISMS

Aidagulov R. R.,
candidate of physical and mathematical Sciences, senior researcher
Moscow state University. M. V. Lomonosov
Institute of mechanical engineering RAS. A. A. Blagonravova
Russia, Moscow

Abstract: B and group algebras play the role of group algebras in the noncommutative case. They allow us to create analogues of fast Fourier transform and fast multiplication algorithms in commutative algebras. These algebras are also of independent interest for study as having different applications.
Keywords: graded algebra, group of colors, the bases of Sylvester and the Weyl-Schwinger.

Групповые алгебры и умножение многочленов

Пусть G группа, K коммутативное кольцо с единицей. Групповая алгебра $K(G)$ определяется как множество функций $f: G \to K$ со значениями в кольце K. Если f, φ две такие функции (элементы $K(G)$), то определен элемент $f + \varphi \in K(G)$. Для любого $k \in K$ и $f \in K(G)$ определен $kf \in K(G)$. Пусть S конечное подмножество группы G, замкнутое относительно произведений, f, φ функции равные 0 вне S. Тогда определена функция $f\varphi: G \to K$, равная нулю вне S - $(f\varphi)(s) = \sum_{s_1 s_2 = s} f(s_1)\varphi(s_2)$. Таким образом, произведение элементов групповой алгебры представляет из себя свертку функций на группе. Для бесконечных групп, чтобы определилось произведение элементов, кольцо K должно иметь топологию, и алгебра $K(G)$ должна состоять только из функций, для которых определена бесконечная сумма в свертке в виде суммы ряда или интеграла по мере Хаара в группе. Мы здесь рассматриваем только конечные группы, соответственно произведение элементов всегда определено и групповая алгебра действительно является алгеброй над кольцом K. Для конечных групп элементы групповой алгебры $f: G \to K$ имеют вид линейной комбинации $f = \sum_{g \in G} f(g)g$, где элементам $g \in G$ соответствуют функции, равные 1 на элементе g и равные нулю на остальных элементах группы. Так можно вложить группу G в групповую алгебру $K(G)$. При этом элементы групповой алгебры можно представить как линейные функционалы на групповой алгебре, распространяя функции на группе по линейности до функций на групповой алгебре. Так значение элемента $a \in K(G)$ на элементе b определяет скалярное произведение (a,b) на $K(G)$. Однако, обычно пользуются эрмитовым скалярным произведением $a \cdot b = (a, \bar{b})$, где сопряжение определяется из соотношения $\bar{b}(g) = b(g^{-1})$.

В дальнейшем ограничимся случаем, когда G является конечной коммутативной группой. Конечная абелева группа является прямой суммой циклических групп

$$G = G_1 \oplus G_2 \oplus \dots \oplus G_k\,, g_i \in G_i, (g_i)^{n_i} = 1,\ \ n_1|n_2|\dots|n_k.$$

Тогда групповая алгебра $K(G)$ представляет из себя алгебру коммутативных многочленов от переменных g_i с соотношениями $(g_i)^{n_i} = 1$ и произведение в групповой алгебре совпадает с привычным умножением многочленов.

Характер группы определяется как мультипликативная функция

$$\mu: G \to K^* \subset K, \qquad \mu(g_1 g_2) = \mu(g_1)\mu(g_2),$$

соответственно может рассматриваться как элемент групповой алгебры.

Лемма 1. *Характер, распространенная как линейная функция на всю групповую алгебру, остается мультипликативной и на алгебре.*

Действительно, пусть $a, b \in K(g)$ и

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

Тогда

$$\mu(c) = \sum_{g_1, g_2} a(g_1)b(g_2)\mu(g_1)\mu(g_2) = \mu(a)\mu(b).$$

Лемма 2. *Разные характеры ортогональны.*

Доказательство. Пусть μ_1, μ_2 два разных характера. Тогда их эрмитово скалярное произведение равно

$$\mu_1 \cdot \mu_2 = \sum_g \mu_1(g)\mu_2(g^{-1}) = \sum_{g \in G} (\mu_1 \mu_2^{-1})(g) = \prod_{i=1}^{k} \sum_{j=1}^{n_i} \big(\mu(g_i)\big)^j = 0.$$

Здесь $\mu = \mu_1 \mu_2^{-1}$ и хотя бы для одного $i:\ \mu(g_i) \neq 1$, соответственно, при $\mu_1 \neq \mu_2$ хотя бы один из сомножителей равен нулю.

Лемма 3. *Если в кольце имеется примитивный корень степени n_k и порядок группы $|G|1 \in K^*$- обратим, то группа G является группой характеров*

для своей группы характеров G^*. *Группа характеров образует полный ортогональный базис.*

Доказательство. Пусть θ_i примитивный корень степени $n_i|n_k$. Определим характеры μ_i из условия $\mu_i(g_j) = 1, i \neq j,\ \mu_i(g_i) = \theta_i$. Различные произведения характеров μ_i образуют всю группу характеров и эта группа изоморфна (не канонический) группе G. Элементы g_i играют роль элементов μ_i при интерпретации их как характеров группы характеровG^*. Таким образом, $G = G^{**}$. Соотношение, полученное при доказательстве леммы 2, запишем как для группы характеров, так и для самой группы, являющейся группой характеров для группы G^*:

$$\sum_{g\in G}(\mu_1\mu_2^{-1})(g) = \begin{cases} 0, & \mu_1 \neq \mu_2 \\ |G|, & \mu_1 = \mu_2 \end{cases}, \quad (1)$$

$$\sum_{\mu\in G^*}(\mu)(g) = \begin{cases} 0, & g \neq 1 \\ |G|, & g = 1 \end{cases}. \quad (2)$$

Это доказывает лемму.

На этой ортогональности строится быстрое умножение многочленов преобразованием Фурье. Пусть $a(y_1, \dots, y_k), b(y_1, \dots, y_k)$ два многочлена и пусть $n_i = deg_{y_i}(a) + deg_{y_i}(b) + 1$. Тогда произведение многочленов совпадет с произведением элементов групповой алгебры с образующими y_i и с соотношениями $y_i^{n_i} = 1$. заданных своими коэффициентами перед одночленами-степенями от $y_1, \dots, y_k$. Вычисляем все $n = n_1 \cdot \dots \cdot n_k$ значения многочленов (при различных характерах) для обеих многочленов. Значениями произведения многочленов будут попарные произведения значений. Коэффициенты многочлена произведения находятся по этим значениям как значения для характеров с обратной степенью и с множителем $\frac{1}{n}$. Вычисления значений представляют из себя преобразование Фурье и осуществляется за $O(n\log(n))$ операций. Кратное преобразование можно привести к простому

(однократному), однако, такое приведение скорее только усложняет и бесполезно. Умножение больших чисел осуществляется представлением их в некоторой системе счисления как многочленов. После умножения их как многочленов, коэффициенты многочлена, вообще говоря, превзойдут основание исчисления и потребуется переносы в другие разряды.

Бигрупповая алгебра

Элементы групповой алгебры можно представить и как операторы на $K(G)$. как на линейном пространстве. При этом элементам группы g соответствует сдвиг аргумента как у функций на группе. Сопоставим характерам диагональные операторы $\mu: g \to \mu(g)g$. Эти операторы не коммутируют с операторами сдвига:

$$(\mu g)(l) = \mu(gl) = \mu(g)\mu(l)gl = \mu(g)(g\mu)(l).$$

Линейные операторы, являющиеся линейной комбинации базиса $\mu g, \mu \in G^*, g \in G$ образуют алгебру операторов на K(G). Эту алгебру мы называем бигрупповой алгеброй. Если заданы две градуированные алгебры A,B с градуировками G_1, G_2 и бимультипликативная функция $\alpha: G_1 \times G_2 \to K$, то определяется скрещенное произведение алгебр C с градуировкой $G_1 \times G_2$ как формальных сумм

$$\sum_{g_1 \in G_1, g_2 \in G_2,} c(g_1, g_2) g_1 g_2$$

с коммутационными соотношениями $g_1 g_2 = \alpha(g_1, g_2) g_2 g_1$. В этом смысле, введенная нами бигрупповая алгебра является скрещенным произведением групповых алгебр групп G^*, G с бимультипликативной функцией $\alpha(\mu, g) \equiv \mu(g)$. Она является так же цветной градуированной алгеброй с группой цветов [1] - $G^* \times G$.

Таким образом, бигрупповая алгебра состоит из формальных сумм:

(3) $$a = \sum_{\mu \in G^*, g \in G,} a(\mu, g)\mu g$$

с коммутационными соотношениями

(4) $$\mu g = \mu(g) g \mu.$$

Лемма 4. *Бигрупповая алгебра прямой суммы двух коммутативных групп является тензорным произведением бигрупповых алгебр этих групп.*

Доказательство. Как группа, так и группа характеров состоят из попарных произведений $g = g_1 g_2, \mu = \mu_1 \mu_2$, причем группа характеров можно считать разложенным в прямую сумму так, что

$$\mu_i(g_1 g_2) = \mu_i(g_i), i = 1,2.$$

Тогда, согласно (3), элементы бигрупповой алгебы представляются в виде попарных произведений элементов бигрупповых алгебр $, \mu g = \mu_1 g_1 \mu_1 g_2$, которые коммутируют между собой. Это и означает выполнение утверждения леммы.

Используем эту лемму для доказательства следующей теоремы:

Теорема 1. *Пусть коммутативная группа* $G = Z_{n_1} \oplus \ldots \oplus Z_{n_k}$ $(n_1 | n_2 | \ldots | n_k$ *имеет* $n = n_1 \cdot \ldots \cdot n_k$ *элементов и в коммутативном кольце* K *имеется примитивный корень степени* n_k*и число* n *обратима. Тогда бигрупповая алгебра изоморфна алгебре матриц* $M_n(K)$.

Доказательство. В соответствии с леммой 4 достаточно рассмотреть случай циклической группы $(k = 1, n_1 = n)$. Пусть μ образующая группы характеров, g образующая группы и $\theta = \theta_1 = \mu(g)$ примитивный корень степени $n_1 = n$. Рассмотрим следующие матрицы:

$$x = x_1 = \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & \theta & & 0 & 0 \\ \vdots & & \ddots & \vdots & \\ 0 & 0 & & \theta^{n-2} & 0 \\ 0 & 0 & \ldots & 0 & \theta^{n-1} \end{pmatrix}, y = y_1 = \begin{pmatrix} 0 & 0 & \ldots & 0 & 1 \\ 1 & 0 & & 0 & 0 \\ \vdots & & \ddots & \vdots & \\ 0 & 0 & & 0 & 0 \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}$$

Ясно, что $x^n = E = y^n$ и выполняется соотношение $xy = \theta yx$. Сопоставляя образующим бигрупповой алгебры $\mu \to x, g \to y$ получим

гомоморфизм из бигрупповой алгебры в алгебру матриц. В бигрупповой алгебре n^2 корней из 1 степени n - $\mu^i g^j, i = 0,1, \dots, n-1, j = 0,1, \dots, n-1$ g образуют базис алгебры. Вообще то $(\mu^i g^j)^n = \theta^{ijn(n-1)/2}$ равно -1, когда $ij(n-1)$ нечетно, но это не важно. Ядро гомоморфизма состоит из таких элементов, что

$$\sum_i a(\mu^i, g^j)\theta^{ik} = 0 \ \ \forall j, k.$$

Так как определитель Вондермонда $\det(\theta^{ik}) \neq 0$, ядро тривиальное. Чтобы показать, что любая матрица является образом гомоморфизма, достаточно для любых $k, l, 0 \leq k, l \leq n-1$ найти прообраз матрицы $M_{kl} = (m_{ij})$, у которой все элементы $m_{ij} = 0$ за исключением $m_{kl} = 1$. Матрица $M_{kl} = D_k y^{k-l}$. Все индексы, типа $k - l$ вычисляются по модулю n. Здесь D_k диагональная матрица, все элементы которой равны нулю за исключением $d_{kk} = 1$. Любой диагональной матрице D соответствует многочлен от x:

$$D = \sum_i a_i x^i, \qquad a_i = \frac{1}{n}\sum_k d_{kk}\theta^{-ik},$$

являющийся обратным преобразованием Фурье от диагональных элементов. Так как в кольце K число n обратимо и имеется примитивный корень ε, наше утверждение доказано.

Приведем явный вид образующих в общем случае. Пусть

$$N_0 = 1, \qquad N_i = n_i N_{i-1}.$$

Представим индексы в соответствующей системе исчисления:

$$J = j_1 N_0 + j_2 N_1 + \cdots + j_k N_{k-1}, \qquad 0 \leq j_l < n_l.$$

Через x_i обозначим диагональную матрицу $D_i = (d_{JJ}), d_{JJ} = \theta_i^{j_i}$, где θ_i примитивный корень степени n_i. Через y_i обозначим матрицу, у которой в каждой строчке J все элементы равны нулю кроме $Y_{J,J-N_{i-1}} = 1$.

Таким образом, алгебру матриц (или бигрупповую алгебру) можно представить как алгебру не коммутативных многочленов от переменных x_i, y_i со следующими соотношениями:

(5) $$x_i y_i = \theta_i y_i x_i, \quad x_i y_j = y_j x_i, i \neq j, \qquad x_i^{n_i} = 1 = y_i^{n_i}.$$

Образующие алгебры x_i, y_i называем образующими Дарбу, базис из n^2 однородных элементов, являющихся произведением степеней элементов x_i на степени элементов y_i назовем базисом Сильвестра.

Автоморфизмы.

Пусть A автоморфизм конечномерной алгебры. Очевидно, что единица e переходит в единицу $A(e) = e$, ноль в ноль. Вообще элемент $\lambda e, \lambda \in K$ переходит в λe. Аналогично, если$x^m = \lambda e$, то $x_0^m = \lambda e$, где $x_0 = A(x)$. В частности, корни из единицы (или нильпотентные элементы) под действием автоморфизма переходят в корни из единиц (или нильпотентные элементы) соответствующего порядка. В частности, если $xyx^{-1}y^{-1} = \lambda e$, то $x'y'x'^{-1}y'^{-1} = \lambda e$, где $x' = A(x), y' = A(y)$. Взяв образующие алгебры, состоящей из корней от единицы или нильпотентов, автоморфизм можно определить заданием их образов, являющихся такими же корнями от единицы или нильпотентами, при условии сохранения коммутационных соотношений. Таким образом, система образующая базис и состоящая из корней из единицы и нильпотентных элементов, переходит в аналогичную систему с соответствующими коммутационными соотношениями.

Мы изучаем алгебру матриц, являющейся бигрупповой (цветной) алгеброй. Из указанного не следует, что автоморфизм обязательно является однородным (цветным), переводящим однородные (градуированные) элементы в однородные. В алгебре матриц все автоморфизмы являются внутренними $A(x) = CxC^{-1}$, соответственно сохраняют инварианты матриц, в частности детерминант и след матрицы. Тем не менее, мы в дальнейшем ограничимся рассмотрением только однородных (или цветных) автоморфизмов относительно естественного разбиения на однородные элементы. Заметим, что в таком более

узком классе изоморфизмов, две бигрупповые алгебры для групп $G_1 = Z_{m^2}$ и $G_2 = Z_m \oplus Z_m$, изоморфные алгебре матриц порядка m^2, не изоморфны как цветные алгебры. При этом, как будет видно ниже, у второй бигрупповой алгебры, цветных автоморфизмов больше. Разлагая коммутативную группу G на прямую сумму силовских подгрупп, получаем разложение на тензорное произведение бигрупповых алгебр, а автоморфизмов на независимые произведения автоморфизмов сомножителей. Максимальное количество автоморфизмов при заданном порядке будет у силовской группы $G = Z_p \oplus \ldots \oplus Z_p = (Z_p)^k$. В дальнейшем ограничимся рассмотрением только таких бигрупповых алгебр. Цветной автоморфизм такой бигрупповой алгебры задается $2k(2k+1)$ числами из Z_p:

(6) $$A(x_i) = \theta^{b_i} x_j^{a_{ji}}, \qquad i = 1,2,\ldots,2k, x_{i+k} = y_i, b_i, a_{ji} \in Z_p.$$

Образы остальных однородных корней из единиц вычисляются однозначно, если выполняются коммутационные соотношения:

$$A(x_i)A(x_l)A(x_i)^{-1}A(x_l)^{-1} = \theta^{[a_{ji},a_{jl}]} = \theta^{\delta_l^{i+k} - \delta_i^{l+k}}.$$

Здесь $[\cdot,\cdot]$ симплектическое скалярное произведение на группе цветов $(Z_p)^k \oplus (Z_p)^k$, являющееся $2k$- мерным симплектическим пространством [2,3] над полем Z_p, т.е

(7) $$[a_{ji}, a_{jl}] = \sum_{j=1}^{k} (a_{j,i}a_{j+k,l} - a_{j+k,i}a_{j,l}).$$

Так как столбцы $a_{ji,}, a_{jl}$ определяют цвет, это означает, что сохраняется симплектическая структура на группе цветов. Пусть $J = (J_{il})$, $J_{il} = \delta_l^{i+k} - \delta_i^{l+k}$ – матрица, определяющая симплектическую структуру. Тогда условие (7) на столбцы $A = (a_{ji})$ можно записать в виде:

(8) $$A^T J A = J.$$

Кроме этого, должны сохраняться нормировки цветов. При нечетном p для всех цветов можем считать выполненным $x_i^p = 1$ и это условие будет выполняться автоматический и для образов. При $p = 2$ это не так. Например, если $x^2 = y^2 = 1$, то$(xy)^2 = -1$. В этом случае, удобнее нормировать $x^2 = y^2 = -1$, при этом $(xy)^2 = -x^2y^2 = -1$.

При $k = 1$ условие симплектичности (8) эквивалентно $\det(A) = 1$. Соответственно, легко вычисляется количество симплектичных матриц. Для циклической группы $G = Z_{p^k}$ матрица $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, a, b, c, d \in Z_{p^k}$ симплектична в $p^{3k-2}(p^2 - 1)$ случаях. В случае группы $G = \left(Z_p\right)^k$, первую строку (или столбец) можем выбрать любой, за исключением нулевого. Это дает $p^{2k} - 1$ возможностей. Выбор сопряженного к нему вектора, кососимметричное скалярное произведение с которым равно 1, возможно из p^{2k-1} вариантов. Итого выбор двух строк (или столбцов) осуществляется из $(p^{2k} - 1)p^{2k-1}$ вариантов. Оставшиеся вектора осуществляются из $2k - 2$ мерного пространства, ортогонального этой плоскости. Соответственно, количество симплектичных матриц равно $p^{k^2}\prod_{i=1}^{k}\left(p^{2i} - 1\right) > p^{2k^2}$. Например, при k=2 количество симплектических матриц для группы $G = \left(Z_p\right)^k$ больше в $(p^4 - 1)$ раз, чем для циклической группы такого же порядка. Автоморфизмы, когда матрица $A = E$, назовем знаковыми. Знаковые автоморфизмы не меняют цвета у однородных элементов и меняют только знаки (множители) θ^{b_i}. Количество возможных вариантов изменения знака $n^2 = p^{2k}$ независимо от структуры группы.

Большое количество автоморфизмов может быть использовано в гомоморфной криптографии. Вычисления с данными отправляются в облако, предварительно зашифровав их с помощью некоторого цветного автоморфизма. Получив результаты вычисления раскодируем обратным цветным изоморфизмом.

В базисе Сильвестра вычисление знаков после применения некоторой степени автоморфизма представляет некоторую сложность. Задача упрощается в базисе Вейля-Швингера, отличающегося от базиса Сильвестра только знаками. Базис Сильвестра для группы $G = \left(Z_p\right)^k$ определялся $2k$ – мерным вектором $c = (c_1, c_2, \dots, c_{2k})$ в симплектическом пространстве цветов над полем Z_p с кососимметричным скалярным произведением:

$$[a, b] = \sum_{i=1}^{k} (a_i b_{i+k} - a_{i+k} b_i).$$

Базис Вейля-Швингера отличается от базиса Сильвестра только знаками:

$$W(c) = \theta^{-\frac{1}{2}\sum_i c_i c_{i+k}} x^c,\ x^c = \prod_{i=1}^{2k} x_i^{c_i}. \quad (9)$$

Произведение двух элементов базиса Вейля-Швингера $W(a), W(b)$ вычисляется просто:

$$W(a)W(b) = \theta^{\frac{[a,b]}{2}} W(a + b). \quad (10)$$

Из определения (9) следует, что образующие Дарбу входят в базис Вейля-Швингера с положительным знаком, как и в базис Сильвестра. Под положительным знаком понимается множитель θ^{α}, когда он равен 1. Докажем следующую теорему о знаках:

Теорема 2. *Пусть автоморфизм переводит образующие в элементы базиса Вейля-Швингера. Тогда он является положительным автоморфизмом, т.е. переводит элементы базиса Вейля-Швингера в элементы базиса Швингера без знакового множителя.*

Доказательство. Базис Вейля-Швингера состоит из k произведений взаимно коммутирующихся элементов базиса, у которых все координаты равны 0, кроме двух:

$$W(c) = \prod_{i=1}^{k} W(c_i), c_i = (0, \dots, c_i, 0, \dots, 0, c_{i+k}, 0, \dots, 0).$$

Разложив таким образом приходим к упрощенной задаче, к достаточности доказательства для случая k=1. Пусть

$$A(x) = \theta^{-\frac{ab}{2}} x^a y^b, (y_i = x_{i+k}), \qquad A(y) = \theta^{-\frac{cd}{2}} x^c y^d.$$

Тогда

$$A\big(W(i,j)\big) = A\left(\theta^{-\frac{ij}{2}} x^i y^j\right) = \theta^{\alpha} x^{ia+jc} y^{ib+jd},$$

где

$$2\alpha = -ij - abi - i(i-1)ab - cdj - j(j-1)cd - 2bcij$$
$$= -(ia+jc)(ib+jd) + ij(ad - bc - 1).$$

Из сохранения коммутационных соотношений следует $ad - bc = 1$. Это доказывает теорему.

Симметричные функции и порядки автоморфизмов.

Пусть A положительный автоморфизм. Он переставляет $n^2 - 1$ не единичных элементов базиса Вейля-Швингера (единичный элемент сохраняется при автоморфизмах). Соответственно, некоторая степень автоморфизма станет единичным (тождественным) отображением $A^m = E$. Взяв некоторый элемент x бигрупповой алгебры и корень ε степени m из 1 можно построить собственные функции автоморфизма:

$$(11) \qquad \varphi = x + \varepsilon A(x) + \cdots + \varepsilon^{m-1} A^{m-1}(x), \qquad A(\varphi) = \varepsilon^{-1}\varphi.$$

Произведение собственных функций является так же собственной функцией, с собственным значением, равным произведению собственных значений сомножителей. Эти не нулевые собственные функции назовем симметричными функциями. Они упрощает задачу умножения некоммутативных многочленов, разлагая множители предварительно по собственным векторам (функциям) автоморфизма. Однако, здесь есть одна досада – произведение собственных функций может оказаться нулем. В том, что произведения могут равняться нулю, нет ничего плохого при вычислении

произведения. Беря разные однородные элементы в качестве x получим разные орбиты автоморфизма и разные собственные функции. Если x в выражении (11) является однородным, то все $A^i(x)$ будут разные (линейно независимые) однородные величины, соответственно (11) дает разные не нулевые собственные функции с разными собственными значениями. Однако, это относится к собственным значениям и собственным векторам линейного отображения пространства размерности $n^2 = p^{2k}$ над кольцом K. Порядок автоморфизма определяется его собственными значениями как линейного отображения в группе цветов, являющегося линейным (симплектическим) пространством размерности $2k$ над конечным полем F_p. Положительный автоморфизм полностью определяется симплектической матрицей (8). Поэтому, мы далее будем интересоваться собственными значениями именно симплектической матрицы над полем F_p. Рассмотрим вначале случай $k = 1$. В этом случае характеристическое уравнение выглядит просто:

$$\lambda^2 - a\lambda + 1 = 0, \;\; a = tr(A), \det(A) = 1.$$

Автоморфизм является гиперболическим [3], если уравнение над F_p имеет два (не обязательно разных) собственных значения и два (линейно независимых) собственных вектора. Он параболический, если собственные значения одинаковые и имеется только один собственный вектор. Он эллиптический, если собственные значения не принадлежат F_p. Если автоморфизм гиперболический, то его порядок является делителем числа $p - 1$. Если автоморфизм эллиптический, то его порядок делит $p + 1$. Покажем, что существуют автоморфизмы, когда порядки совпадают с указанными ограничениями. Пусть c – образующая мультипликативной группы поля. Тогда гиперболический автоморфизм

$$A(x) = x^c, A(y) = y^{c^{-1}}, \qquad a = \; tr(A) = c + \frac{1}{c}$$

имеет точный порядок $p - 1$. В эллиптическом случае автоморфизм можно привести в некотором базисе к виду

$$A(x) = y, A(y) = \theta^{a/2} x^{-1} y^a = W(-1.a), \qquad a = tr(A), \det(A) = 1.$$

Матрица $A = \begin{pmatrix} 0 & c^{-1} \\ -c & a \end{pmatrix}, (c = 1)$ возводится в степень с использованием чисел Люка-Фибоначчи:

$$A^i = \begin{pmatrix} 0 & c^{-1} \\ -c & a \end{pmatrix}^i = \begin{pmatrix} -F_{i-1} & c^{-1}F_i \\ -cF_i & F_{i+1} \end{pmatrix},$$

где $F_{i+1} = aF_i - F_{i-1}, F_0 = 0, F_1 = 1, F_i = \frac{\lambda^i - \lambda^{-i}}{\lambda - \lambda^{-1}}$, λ – корень характеристического уравнения $\lambda^2 - a\lambda + 1 = 0$. Пусть ω мультипликативная образующая поля F_{p^2}. Взяв в качестве числа $a = \omega^{(p-1)/2} - \omega^{-(p-1)/2}$ получим, что $a^p = \omega^{p(p-1)/2} - \omega^{-\frac{p(p-1)}{2}} = \omega^{\frac{p^2-1}{2}-\frac{p-1}{2}} - \omega^{-\frac{p^2-1}{2}+\frac{p-1}{2}} = a$. Это значит число a действительно принадлежит полю F_p. При этом порядок автоморфизма равен минимальному значению m, что $F_m = 0, F_{m+1} = 1$, что выполняется для нашего выбора λ. Можно еще говорить о параболическом автоморфизме:

$$A(x) = x, A(y) = x^c y, A(x) = x^{-1}, A(y) = x^c y^{-1}, \qquad c \neq 0\,.$$

Его порядок равен p.

Заметим, что характеристическое уравнение симплектического отображения симметрично относительно замены $\lambda \to \lambda^{-1}$. Докажем теперь это в общем случае. Вначале группу цветов представим в виде прямой суммы двух сопряженных Лагранжевых подпространств, натянутых $C = X \oplus Y$, где X имеет нулевые координаты в позициях от k+1 до 2k, а Y нулевые координаты в первых k позициях. Автоморфизм можно записать в виде:

$A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}$ и из условий симплектичности получаем:

$A_1^T A_4 - A_3^T A_2 = E$, $A_1^T A_3, A_2^T A_4$ – симметричные матрицы.

Автоморфизм переводит один базис Дарбу в другой базис Дарбу. По заданному автоморфизму построим базис Дарбу, при котором автоморфизм имеет наиболее простой вид. Для линейного отображения можно ввести базис

таким образом: берем некоторый вектор x_1 и определяем последовательность векторов $x_i = A^{i-1}x_1$. Как только x_{m+1}становится линейной комбинацией предыдущих, выделяем инвариантное подпространство, натянутое на векторы $x_1, x_2, \dots, x_m$, где отображение имеет простой вид – единицы на диагонали ниже главной и некоторые числа на последнем столбце. Симплектическая матрица сохраняет кососимметричное скалярное произведение. Если окажется, что $[x_1, x_i] = 0, i = 1, \dots, m$ и x_{m+1} линейная комбинация остальных, то взяв в качестве y_1 сопряженный к x_1 цвет, получим два инвариантных сопряженных друг другу подпространства размерности m каждый. Если ограничение автоморфизма в первом пространстве обозначим через A_1, то во втором инвариантном пространстве в силу $A_2 = 0 = A_3$ получим $A_4 = (A_1^T)^{-1}$. Соответственно каждому собственному значению λ матрицы A_1, будет соответствовать собственное значение λ^{-1} матрицы A_4. Сумма двух инвариантных подпространств даст инвариантное подпространство размерности 2m, ограничение автоморфизма на котором гиперболична и с порядоком, являющемся делителем числа $p^m - 1$.

Подпространство ортогональное (относительно симплектического скалярного произведения) к инвариантному пространству - инвариантно. Его размерность будет меньше $2k$ на размерность выделенного инвариантного подпространства, что позволяет применять индукцию далее.

Если $[x_1, x_i] = 0, i = 1, \dots, l, [x_1, x_{l+1}] = c \neq 0,$ то $[x_i, x_{l+i}] = c, i \leq l.$ Соответственно, все вектора $x_i, i = 1,2, \dots,2l$ линейно независимы. Допустим, что x_{2l+1} является линейной комбинацией остальных. Так как $[x_{l+1}, x_{2l+1}] = [x_1, x_{l+1}] = c,$ вводя переменные $y_i = \frac{1}{c}x_{l+i}$ в базисе (x_i, y_i) матрица автоморфизма приводится к ниже треугольному виду из матриц 2×2, на диагонали которой клетки 2×2 имеют вид $\begin{pmatrix} 0 & -c^{-1} \\ c & b \end{pmatrix}$. Это приводит к тому, что характеристическое уравнение будет симметричной относительно замены $\lambda \to \lambda^{-1}$. В более общем случае, линейно независимых векторов из орбиты будет 2m,

причем m делится на l. В базисе, сформированном по клеткам 2×2, матрица автоморфизма будет иметь аналогичный вид. Это приводит к следующей теореме:

Теорема 3. *Характеристическое уравнение симплектического отображения симметрично относительно замены* $\lambda \to \lambda^{-1}$.

Имеет место так же следующая теорема:

Теорема 4. *Если характеристическое уравнение автоморфизма сепарабельное и не приводимо, то порядок автоморфизма делит q+1, где* $n = q = p^k$.

Доказательство. Так как для собственного корня λ величина $\eta = \lambda + \lambda^{-1} \in F_q$ (из- за симметричности уравнения), выполняются соотношения:

$$\lambda + \lambda^{-1} = \eta = \eta^q = \lambda^q + \lambda^{-q}.$$

Это значит, что $\lambda^q = \lambda$ (порядок собственного значения делит $q - 1$) или $\lambda^q = \lambda^{-1}$ (порядок собственного значения делит $q + 1$). Все собственные значения имеющие порядок q − 1 образуют делитель многочлена $\lambda^{q-1} - 1$, а все собственные значения имеющие порядок q + 1 образуют делитель многочлена $\lambda^{q+1} - 1$. Их общий делитель $\lambda^2 - 1$ (p-нечетное) (или λ − 1). Наличие и тех и других собственных значений приводит к приводимости характеристического уравнения. Если все собственные значения имеют порядок q − 1, то они принадлежат расширению F_q, а не F_{q^2} . Следовательно, характеристическое уравнение, имеющее степень 2k приводимо. Это доказывает

теорему.

Группа цветов имеет структуру симплектического пространства над полем F_p. Введем структуру векторного пространства над $F_q, q = p^k$. Пусть ω мультипликативная образующая поля F_q. Любой элемент поля может быть представлено в виде линейной комбинации

$$f = \omega^I = \sum_{i=0}^{k-1} f_i \omega^{p^i}, \quad f_i \in Z_p. \tag{12}$$

Если f ненулевой элемент, то существует такой $I < p^k$, что $f = \omega^I$. Сопоставим такому элементу поля цвет с координатами $(f_0, \dots, f_{k-1}, 0, \dots, 0)$. Обозначим через $\pi: I \to (f_0, \dots, f_{k-1})$ взаимно однозначное отображение вычетов по модулю $q-1$ в не нулевые векторы k- мерного подпространства цветов. Тогда можно определить произведение двух цветов перенесением произведения вычетов:

$$(f_0, \dots, f_{k-1}) * (\varphi_0, \dots, \varphi_{k-1}) = \pi\left(\pi^{-1}\big((f_0, \dots, f_{k-1})\big) + \pi^{-1}\big((\varphi_0, \dots, \varphi_{k-1})\big)\right).$$

Естественно, что эта перенесенная операция коммутативна и ассоциативна и дистрибутивна относительно сложения. Умножение, когда один из цветов представляет нулевой вектор, естественно определяется как нулевой вектор. Так мы определяем масштабирование, введенное ранее при k=1 $x \to x^c, c < p$, когда повторное применение масштабирования приводит к умножению показателей масштабирования по модулю $p^k - 1$. В базисе Вейля-Швингера для положительного автоморфизма масштабирование коммутирует автоморфизмом, т.е. $A\big(W(c * f)\big) = W\big(c * A(f)\big)$. Как и в случае k=1, можно построить эллиптический автоморфизм с сепарабельным неприводимым характеристическим уравнением, имеющим, согласно теореме 4, порядок q+1. При этом не нулевые цвета расщепляются на q-1 орбит автоморфизма длиной q+1, что можно выразить теоремой:

Теорема 5. *Существует эллмптический автоморфизм расщепляющий пространство не нулевых цветов на q-1 орбит по q+1 элементов.*

Нулевой цвет соответствует единице алгебры и ее орбита состоит только из него самого (длина 1). В этом базисе удобнее расписать умножение матриц.

Ранг умножения.

Ранг умножения в конечномерной алгебре А над коммутативным кольцом определяется как минимальное значение r, такое, что любое произведение $a * b$ представляется в виде линейной комбинации:

$$(13) \qquad a * b = \sum_{i=1}^{r} C_i f_i(a) \cdot \varphi_i(b).$$

Здесь f_i, φ_i – линейные функционалы, C_i фиксированные элементы, не зависящие от сомножителей a, b. Это понятие не требует ассоциативности умножения. Многие математики [3, 107-166; 7,8] для быстрого умножения матриц пошли по пути оценки сверху ранга умножения. Однако, такой алгоритм не является эффективным при не очень больших значениях размерности алгебры. Действительно, при умножении квадратных матриц порядка $n \times n$, умножение по формулам (13) кроме r_n операций функционального умножения, требует порядка $n^2 r_n$ операций умножения на коэффициенты и примерно столько операций сложения. Это получится существенно больше, чем при стандартном вычислении произведения – n^3 умножений и $n^2(n-1)$ сложений. Когда размерность большая – $N = n^k$, используя формулу (13) по элементом порядка n, количество операций можно сократить до $O(n^2 N^\alpha) = O\left(N^{\alpha+\frac{2}{k}}\right), \alpha = \frac{\log(r_n)}{\log(n)}$.

Число α называется экспонентой умножения. Так как ранг умножения $r_n \geq 2n^2 - 1$, полученные алгоритмы заметно лучше стандартного алгоритма умножения только при размерностях больше миллиарда. Умножение полноценных матриц такого порядка не осуществима даже на современных суперкомпьютерах.

При разработке алгоритмов быстрого умножения автор ввел бигрупповые алгебры, представляющие собой алгебру квазикоммутативных многочленов с простыми коммутационными соотношениями, соответствующими симплектической структуре на пространстве цветов. Заметим, что любая конечномерная ассоциативная алгебра над коммутативным кольцом является подалгеброй матриц, соответственно, умножение в алгебре сводится к умножению квазикоммутативных многочленов. Как и при умножении больших

чисел, размерность пространства преобразования Фурье удобнее разбить на мелкие множители. Здесь эту роль играет разбиение размерности матрицы на одинаковые множители $n = p^k$. В дальнейшем будет показано, что ранг умножения матриц равен $2n^2 - 1$, по крайней мере в случае $n = 2^k$. При умножении многочленов вычисление упрощается через использование попарных произведений значений сомножителей. Формула (13) в этом случае принимает вид:

$$\psi_j(a * b) = \sum_{i=1}^{r_j} c_{ji} f_{ji}(a) \varphi_{ji}(b). \quad (14)$$

Получается, что если мы минимизируем количество используемых попарных произведений значений до $r = 2n^2 - 1$, то вычисление каждого значения в среднем потребует не меньше, чем $O(n)$ операций и умножение становится менее эффективной, чем при стандартном алгоритме. Поэтому, для быстрого умножения надо минимизировать не ранг, а количество $R = \sum_j r_j$ и добиться уменьшения общего количества операции $O(R + n^2 \log n)$. Здесь $O(n^2 \log n)$ количество операций, необходимое для вычисления n^2 значений многочленов и восстановление матрицы по этим значениям.

Заключение

Здесь введено понятие бигрупповой алгебры, полученной при разработке алгоритмов быстрого умножения матриц. Эти алгебры имеют многочисленные приложения и в других сферах. В дальнейшем будут продолжены их исследование автором, как имеющие самостоятельный интерес. При их использовании для умножения матриц, задача сводится к квантовой комбинаторике, которая рассматривается в отдельной статье.

Библиографический список:

1. Айдагулов Р.Р., Шамолин М.В. Группа цветов. Современная математика. // Фундаментальные направления. – 2009 – Т.62 - С. 14-26.

2. Вейль А. Основы теории чисел. – Москва /Мир - 1972.

3. Жданович Д.В. Экспонента сложности матричного умножения. // Фундаментальная и прикладная математика. - 2011/2012 - Т 17 - №2 – С. 107-166.

4. Постников М.М. Группы и алгебры Ли. – Москва. / Наука Физматлит - 1982.

5. Фоменко А.Т. Симплектическая геометрия. Методы и приложения. – Москва – МГУ – 1988.

6. Шимура Г. Введение в арифметическую теорию автоморфных функций / Мир. – 1973.

7. Coppersmith D., Winograd S. Matrix multiplication via arithmetic progressions. J. Symbol. Comput. -1990. – Vol. 9. P. 251-280.

8. Francois Le Gall. Powers of Tensors and Fast Matrix Multiplication. 2014 (архив).

Оригинальность 98%