ПРОГРАММИРОВАНИЕ, *2024*, *№ 2*, *с. 84–92*

КОМПЬЮТЕРНАЯ АЛГЕБРА

УДК 512.554.1

ПРИМИТИВНЫЕ ЭЛЕМЕНТЫ СВОБОДНЫХ НЕАССОЦИАТИВНЫХ АЛГЕБР НАД КОНЕЧНЫМИ ПОЛЯМИ

© 2024 г. М. В. Майсурадзе[a], *, А. А. Михалёв[a], **

[a]*Московский государственный университет имени М. В. Ломоносова, механико-математический факультет 119991 Москва, ГСП-1, Ленинские горы, д. 1, Россия*

**E-mail: maisuradzemv@my.msu.ru*
***E-mail: aamikhalev@mail.ru*

Поступила в редакцию 01.07.2023
После доработки 10.08.2023
Принята к публикации 01.10.2023

Определено представление элементов свободных неассоциативных алгебр в виде набора многомерных таблиц коэффициентов. Рассмотрена операция нахождения частных производных элементов свободных неассоциативных алгебр в таком же виде. С помощью этого представления получен критерий примитивности элементов длины два и три в терминах рангов матриц, а также признак примитивности элементов произвольной длины. Полученный признак позволил оценить число примитивных элементов свободных неассоциативных алгебр над конечным полем с двумя образующими. Построенное представление позволяет оптимизировать алгоритмы символьных вычислений с примитивными элементами. С помощью этих алгоритмов найдено число примитивных элементов длины 4 свободной неассоциативной алгебры ранга 2 над конечным полем.

Ключевые слова: шрайерово многообразие линейных алгебр, свободные неассоциативные алгебры, примитивные элементы свободных алгебр, свободное дифференциальное исчисление в свободных алгебрах

DOI: 10.31857/S0132347424020115 **EDN:** RODPXT

1. ВВЕДЕНИЕ

Многообразие всех алгебр над полем является шрайеровым многообразием алгебр. Свободная алгебра в этом многообразии – свободная неассоциативная алгебра. Утверждение, аналогичное теореме Нильсена–Шрайера в 1947 году доказал А. Г. Курош для неассоциативных свободных алгебр: *всякая подалгебра неассоциативной свободной алгебры с любым множеством свободных образующих, отличная от нуля, является свободной*[2].

Для обозначения символов-букв будем использовать множество $X = \{x_1, x_2, \ldots, x_n\}$ в случае их большого числа либо $\{x, y, z\}$ иначе. Словом длины (степени) k будем называть упорядоченную последовательность из k символов $\chi_1 \ldots \chi_k$, $\chi_i \in X$ с заданной расстановкой скобок. Множество всех слов $W = \Gamma(X)$ образует свободный группоид без единичного элемента в алфавите X с операцией *: $x_i * x_j = x_i x_j$, $x_i * a = x_i(a)$, $a * x_i = (a)x_i$ для $x_i \in X$ и слов $a \in W$ длины больше 1, $a * b = (a)(b)$, для слов $a, b \in W$ степени больше 1.

Неассоциативной свободной алгеброй A (или короче *свободной алгеброй*) над полем F с *системой свободных образующих X* называется алгебра над F, линейной базой которой служит множество всех возможных слов относительно символов из X, при этом умножение индуцируется умножением в $\Gamma(X)$. Всякий элемент свободной алгебры, отличный от нуля, однозначно представим в виде суммы конечного числа различных слов (называемых *членами* этого элемента), взятых с отличными от нуля коэффициентами из поля F. Умножение элемента свободной алгебры на некоторый элемент α поля F сводится к умножению на α коэффициентов всех членов элемента.

Свободная алгебра с точностью до изоморфизма определяется числом свободных образующих X (мощностью X). Система элементов свободной алгебры называется *примитивной*, если ее можно дополнить до множества свободных образующих этой алгебры. Другими словами, подмножество M ненулевых элементов свободной алгебры A шраерова многообразия называется *примитивной системой элементов*, если существует множество свободных образующих алгебры A, содержащее подмножество M. Сами элементы такой системы называются *примитивными элементами*.

В начале 2000-х был получен критерий примитивности системы и отдельного элемента [7], [8, 12.5.1], см. также [1], [2]:

Система $a_1, a_2, \ldots, a_r$ элементов свободной неассоциативной алгебры A примитивна тогда и только тогда, когда матрица $(\partial(a_1), \ldots, \partial(a_r))$ обратима слева над алгеброй $U(A)$. В частности, элемент $a \in A$ является примитивным тогда и только тогда, когда существуют такие элементы $m_1, \ldots, m_n \in U(A)$, что

$$\sum\nolimits_{i=1}^{n} m_i \frac{\partial a}{\partial x_i} = 1.$$

Здесь $U(A)$ – *универсальная мультипликативная обертывающая алгебра* для алгебры A, являющаяся свободной ассоциативной алгеброй с множеством свободных образующих $S = \{r_w, l_w \mid w \in W\}$ – операторов левого и правого умножения на слова из W.

Пусть I_A – свободный правый $U(A)$-модуль с базисом $y_1, \ldots, y_n$.

$$I_A = y_1 U(A) \oplus \ldots \oplus y_n U(A).$$

Линейное отображение $\mathcal{D}\colon A \to I_A$, заданное формулами

$$\mathcal{D}(x_i) = y_i, i = 1 \ldots n$$

$$\mathcal{D}(ab) = \mathcal{D}(a)b + a\mathcal{D}(b),$$

где $a, b \in A$, является универсальным дифференцированием алгебры A. Частные производные

$$\frac{\partial}{\partial x_i}$$

элемента $f \in A$ однозначно определяются соотношением

$$\mathcal{D}(f) = \sum_{i=1}^{n} y_i \frac{\partial f}{\partial x_i}.$$

2. ВЕКТОРНЫЕ ПОДПРОСТРАНСТВА

Элементы свободной алгебры над полем F можно представлять как элементы арифметического векторного пространства – кортежи, составленные из коэффициентов членов. Можно рассматривать свободную алгебру как прямую сумму ее подпространств. При этом можно использовать различные разложения на прямые слагаемые в зависимости от задачи.

Для начала рассмотрим разложение по длине слова и расстановке скобок.

Пусть A – свободная алгебра с n образующими. Разобьем базис векторного пространства на группы по длине слова. В неассоциативном случае также потребуется дополнительное разбиение на группы по расстановке скобок. В каждой группе слов длины k будет n^k элементов, которые можно записать в виде k-мерной таблицы. Коэффициенты при этих мономах также удобно записывать в виде k-мерной таблицы.

Примеры:

• Мономы длины 0 (элементы поля в алгебрах с 1). Таблица $n^0 = 1$ коэффициентов записывается одним числом.

• x_i – мономы длины 1. Таблица $n^1 = n$ коэффициентов записывается вектором длины n.

• $x_i x_j$ – мономы длины 2. Таблица n^2 коэффициентов записывается квадратной матрицей $n \times n$.

• Ассоциативные мономы $x_i x_j x_s$ длины 3. Таблица n^3 коэффициентов записывается кубом $n \times n \times n$ коэффициентов.

• Неассоциативные мономы $(x_i x_j)x_s$, $x_i(x_j x_s)$ длины 3. Две таблицы n^3 коэффициентов записываются $C_{k-1} = C_2 = 2$ ($(k-1)$-е число Каталана) кубами $n \times n \times n$ коэффициентов.

Единицу и слова свободного группоида также удобно представлять в виде многомерных таблиц. Обозначим $\overline{x} \times \ldots \times \overline{x}$ k-мерную таблицу, в которой на месте $(i_1, \ldots, i_k)$ находится элемент $x_{i_1} \ldots x_{i_k}$. В неассоциативном случае расстановка скобок в произведении $\overline{x} \times \ldots \times \overline{x}$ совпадает с расстановкой скобок в элементе $x_{i_1} \ldots x_{i_k}$. Считая умножение между таблицами коэффициентов и слов, как и сложение между элементами одного из подпространств, описанных выше, поэлементным, получим более удобное представление элементов свободных алгебр.

Примеры:

• элемент длины 2 свободной алгебры:

$$h = a_{x_1} x_1 + \ldots + a_{x_n} x_n + a_{x_1 x_1} x_1 x_1 + a_{x_1 x_2} x_1 x_2 + \ldots + a_{x_n x_n} x_n x_n$$

$$h = \begin{pmatrix} a_{x_1} x_1 \\ \vdots \\ a_{x_n} x_n \end{pmatrix} + \begin{pmatrix} a_{x_1 x_1} x_1 x_1 & \cdots & a_{x_1 x_n} x_1 x_n \\ \vdots & \ddots & \vdots \\ a_{x_n x_1} x_n x_1 & \cdots & a_{x_n x_n} x_n x_n \end{pmatrix}$$

$$h = \begin{pmatrix} a_{x_1} \\ \vdots \\ a_{x_n} \end{pmatrix} \overline{x} + \begin{pmatrix} a_{x_1 x_1} & \cdots & a_{x_1 x_n} \\ \vdots & \ddots & \vdots \\ a_{x_n x_1} & \cdots & a_{x_n x_n} \end{pmatrix} \overline{x} \times \overline{x} =$$

$$= a_{\overline{x}} \cdot \overline{x} + a_{\overline{x} \times \overline{x}} \cdot \overline{x} \times \overline{x}$$

• элемент длины 3 свободной неассоциативной алгебры:

$$h = a_{\overline{x}} \cdot \overline{x} + a_{\overline{x} \times \overline{x}} \cdot \overline{x} \times \overline{x} + a_{\overline{x} \times (\overline{x} \times \overline{x})} \cdot \overline{x} \times (\overline{x} \times \overline{x}) + a_{(\overline{x} \times \overline{x}) \times \overline{x}} \cdot (\overline{x} \times \overline{x}) \times \overline{x}$$

Здесь $a_{((\ldots)\ldots)}$ – все коэффициенты при мономах длины k с указанной скобочной структурой, запи-

санные в виде k-мерной таблицы. Такие таблицы неудобно записывать для $k > 2$, но достаточно легко представлять.

3. ВЕКТОРНЫЕ “СЛОИ”

Покажем еще одно разложение свободной алгебры в прямую сумму на примере следующей алгебры. Рассмотрим алгебру с базой из всех возможных слов заданной длины k с заданным распределением скобок с алфавитом из n символов:

$$A = \left\{ \sum_{(i_1,\ldots,i_k)} \alpha_{i_1\ldots i_k} ((x_{i_1}\ldots x_{i_j})\ldots x_{i_k}) \right\},$$

$\alpha_{i_1\ldots i_k} \in F$, $x_i \in X$, $0 \leqslant i_s \leqslant n$. Зафиксируем один из символов, стоящий на j-м месте, и будем рассматривать все возможные комбинации остальных символов слова. В зависимости от значения зафиксированного символа будут получаться прямые слагаемые:

$$A \cong \left\{ \sum \alpha_{i_1\ldots 1\ldots i_k} ((x_{i_1}\ldots x_1)\ldots x_{i_k}) \right\} \oplus \ldots$$
$$\ldots \oplus \left\{ \sum \alpha_{i_1\ldots n\ldots i_k} ((x_{i_1}\ldots x_n)\ldots x_{i_k}) \right\}.$$

В случае 2-мерных матриц мы оперируем понятиями “строк” и “столбцов” матрицы. Пронумеруем стороны этих таблиц так, что в 2-мерном случае строки индексируются вдоль первой стороны, а столбцы – вдоль второй. В трехмерном случае вдоль первой стороны индексируются горизонтальные “слои”.

Пусть $a_{((\bar{x}\ldots\times\bar{x})\ldots\bar{x})}$ – k-мерная таблица коэффициентов. Обозначим i-й “слой” этой таблицы, индексированный по одной из ее сторон, $a_{((\bar{x}\ldots\times x_i)\ldots\bar{x})}$. Это $(k-1)$-мерная таблица с коэффициентами.

Для примера покажем, как записывается представление $A_{\bar{x}\times(\bar{x}\times\bar{x})} \cdot \bar{x} \times (\bar{x} \times \bar{x})$ при $\bar{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$. Размер таблицы равен $2 \times 2 \times 2$. Запишем ее “слои”, индексированные вдоль третьей стороны (“глубины”), в виде расширенных квадратных матриц.

$$A_{\bar{x}\times(\bar{x}\times\bar{x})} = \left(A_{\bar{x}\times(\bar{x}\times x_1)} \mid A_{\bar{x}\times(\bar{x}\times x_2)} \right) =$$
$$= \left(\begin{array}{cc|cc} a_{x_1(x_1x_1)} & a_{x_1(x_2x_1)} & a_{x_1(x_1x_2)} & a_{x_1(x_2x_2)} \\ a_{x_2(x_1x_1)} & a_{x_2(x_2x_1)} & a_{x_2(x_1x_2)} & a_{x_2(x_2x_2)} \end{array} \right)$$
$$\bar{x} \times (\bar{x} \times \bar{x}) =$$
$$= \left(\begin{array}{cc|cc} x_1(x_1x_1) & x_1(x_2x_1) & x_1(x_1x_2) & x_1(x_2x_2) \\ x_2(x_1x_1) & x_2(x_2x_1) & x_2(x_1x_2) & x_2(x_2x_2) \end{array} \right)$$

Отметим, что часто удобнее рассматривать “слои”, индексированные вдоль первой стороны (“высоты”):

$$A_{x_1\times(\bar{x}\times\bar{x})} = \begin{pmatrix} a_{x_1(x_1x_1)} & a_{x_1(x_2x_1)} \\ a_{x_1(x_1x_2)} & a_{x_1(x_2x_2)} \end{pmatrix}$$
$$A_{x_2\times(\bar{x}\times\bar{x})} = \begin{pmatrix} a_{x_2(x_1x_1)} & a_{x_2(x_2x_1)} \\ a_{x_2(x_1x_2)} & a_{x_2(x_2x_2)} \end{pmatrix}$$

4. ТЕХНИКА СВОБОДНОГО ДИФФЕРЕНЦИАЛЬНОГО ИСЧИСЛЕНИЯ В СВОБОДНЫХ НЕАССОЦИАТИВНЫХ АЛГЕБРАХ

При дифференцировании мономов длины 1 получим такой же вектор свободных членов частных производных. Дифференцирование всех мономов длины 2 с коэффициентами, записанными в виде матрицы, даст нам такую же матрицу коэффициентов при правых производных и транспонированную при левых, у которой каждый слой соответствует коэффициентам частных производных. В общем случае при дифференцировании монома длины k получается k различных базисных монома универсальной мультпликативной обертывающей алгебры.

Рассмотрим теперь в алгебре $U(A)$ частные производные, представленные в описанном выше виде:

$$\frac{\partial}{\partial x_i} = a_{x_i} + a_{x_i\times\bar{x}} \cdot r_{\bar{x}} + a_{\bar{x}\times x_i} \cdot l_{\bar{x}} +$$
$$+ a_{x_i\times(\bar{x}\times\bar{x})} \cdot r_{\bar{x}\times\bar{x}} + a_{\bar{x}\times(x_i\times\bar{x})} \cdot r_{\bar{x}} \times l_{\bar{x}} +$$
$$+ a_{\bar{x}\times(\bar{x}\times x_i)} \cdot l_{\bar{x}} \times l_{\bar{x}} + a_{(x_i\times\bar{x})\times\bar{x}} \cdot r_{\bar{x}} \times r_{\bar{x}} +$$
$$+ a_{(\bar{x}\times x_i)\times\bar{x}} \cdot l_{\bar{x}} \times r_{\bar{x}} + a_{(\bar{x}\times\bar{x})\times x_i} \cdot l_{\bar{x}\times\bar{x}} + \ldots$$

Из матриц $a_{((\bar{x}\ldots\times x_i)\ldots\bar{x})}$ можно составить векторы длины n, сгруппировав их по структуре слов алгебры $U(A)$.

Например, для мономов вида $l_{\bar{x}} \times r_{\bar{x}}$ получим вектор слоев коэффициентов:

$$\begin{pmatrix} a_{(\bar{x}\times x_1)\times\bar{x}} \\ \ldots \\ a_{(\bar{x}\times x_n)\times\bar{x}} \end{pmatrix}$$

или, что то же самое, исходную матрицу коэффициентов при $(\bar{x} \times \bar{x}) \times \bar{x}$, с другим порядком сторон.

4.1. Пример дифференцирования группы мономов длины 3 с двумя образующими

Определим “вклад” группы $a_{\bar{x}\times(\bar{x}\times\bar{x})} \cdot \bar{x} \times (\bar{x} \times \bar{x})$ при

$$\overline{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

в выражения для частных производных.

$$\mathcal{D}(a_{\overline{x}\times(\overline{x}\times\overline{x})} \cdot \overline{x} \times (\overline{x} \times \overline{x})) =$$

$$= a_{\overline{x}\times(\overline{x}\times\overline{x})} \cdot \begin{pmatrix} \mathcal{D}(x) \times (\overline{x} \times \overline{x}) + \\ + \overline{x} \times (\mathcal{D}(\overline{x}) \times \overline{x}) + \overline{x} \times (\overline{x} \times \mathcal{D}(\overline{x})) \end{pmatrix} =$$

$$= \begin{pmatrix} a_{x_1\times(\overline{x}\times\overline{x})} \\ a_{x_2\times(\overline{x}\times\overline{x})} \end{pmatrix} \cdot \mathcal{D}(x) \times r_{\overline{x}\times\overline{x}} + \begin{pmatrix} a_{\overline{x}\times(x_1\times\overline{x})} \\ a_{\overline{x}\times(x_2\times\overline{x})} \end{pmatrix} \times$$

$$\times \mathcal{D}(x) \times r_{\overline{x}} \times l_{\overline{x}} + \begin{pmatrix} a_{\overline{x}\times(\overline{x}\times x_1)} \\ a_{\overline{x}\times(\overline{x}\times x_2)} \end{pmatrix} \cdot \mathcal{D}(x) \times l_{\overline{x}} \times l_{\overline{x}}$$

$$\begin{pmatrix} \frac{\partial}{\partial x_1} \\ \frac{\partial}{\partial x_2} \end{pmatrix} = \begin{pmatrix} a_{x_1\times(\overline{x}\times\overline{x})} \\ a_{x_2\times(\overline{x}\times\overline{x})} \end{pmatrix} \cdot r_{\overline{x}\times\overline{x}} + \begin{pmatrix} a_{\overline{x}\times(x_1\times\overline{x})} \\ a_{\overline{x}\times(x_2\times\overline{x})} \end{pmatrix} \times$$

$$\times r_{\overline{x}} \times l_{\overline{x}} + \begin{pmatrix} a_{\overline{x}\times(\overline{x}\times x_1)} \\ a_{\overline{x}\times(\overline{x}\times x_2)} \end{pmatrix} \cdot l_{\overline{x}} \times l_{\overline{x}}$$

$$\begin{pmatrix} a_{x_1\times(\overline{x}\times\overline{x})} \\ a_{x_2\times(\overline{x}\times\overline{x})} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} a_{x_1(x_1x_1)} & a_{x_1(x_2x_1)} \\ a_{x_1(x_1x_2)} & a_{x_1(x_2x_2)} \end{pmatrix} \\ \begin{pmatrix} a_{x_2(x_1x_1)} & a_{x_2(x_2x_1)} \\ a_{x_2(x_1x_2)} & a_{x_2(x_2x_2)} \end{pmatrix} \end{pmatrix} \sim$$

$$\sim \left(\begin{array}{cc|cc} a_{x_1(x_1x_1)} & a_{x_1(x_2x_1)} & a_{x_1(x_1x_2)} & a_{x_1(x_2x_2)} \\ a_{x_2(x_1x_1)} & a_{x_2(x_2x_1)} & a_{x_2(x_1x_2)} & a_{x_2(x_2x_2)} \end{array}\right)$$

$$\begin{pmatrix} a_{\overline{x}\times(x_1\times\overline{x})} \\ a_{\overline{x}\times(x_2\times\overline{x})} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} a_{x_1(x_1x_1)} & a_{x_2(x_1x_1)} \\ a_{x_1(x_1x_2)} & a_{x_2(x_1x_2)} \end{pmatrix} \\ \begin{pmatrix} a_{x_1(x_2x_1)} & a_{x_2(x_2x_1)} \\ a_{x_1(x_2x_2)} & a_{x_2(x_2x_2)} \end{pmatrix} \end{pmatrix} \sim$$

$$\sim \left(\begin{array}{cc|cc} a_{x_1(x_1x_1)} & a_{x_2(x_1x_1)} & a_{x_1(x_1x_2)} & a_{x_2(x_1x_2)} \\ a_{x_1(x_2x_1)} & a_{x_2(x_2x_1)} & a_{x_1(x_2x_2)} & a_{x_2(x_2x_2)} \end{array}\right)$$

$$\begin{pmatrix} a_{\overline{x}\times(\overline{x}\times x_1)} \\ a_{\overline{x}\times(\overline{x}\times x_2)} \end{pmatrix} = \begin{pmatrix} \begin{pmatrix} a_{x_1(x_1x_1)} & a_{x_2(x_1x_1)} \\ a_{x_1(x_2x_1)} & a_{x_2(x_2x_1)} \end{pmatrix} \\ \begin{pmatrix} a_{x_1(x_1x_2)} & a_{x_2(x_1x_2)} \\ a_{x_1(x_2x_2)} & a_{x_2(x_2x_2)} \end{pmatrix} \end{pmatrix} \sim$$

$$\sim \left(\begin{array}{cc|cc} a_{x_1(x_1x_1)} & a_{x_2(x_1x_1)} & a_{x_1(x_2x_1)} & a_{x_2(x_2x_1)} \\ a_{x_1(x_1x_2)} & a_{x_2(x_1x_2)} & a_{x_1(x_2x_2)} & a_{x_2(x_2x_2)} \end{array}\right)$$

Так, дифференцирование 8 неассоциативных мономов с заданной скобочной структурой дает нам 24 ассоциативных монома алгебры $U(A)$ в выражениях частных производных

5. КРИТЕРИЙ ПРИМИТИВНОСТИ ЭЛЕМЕНТА ДЛИНЫ 2 И 3 СВОБОДНОЙ НЕАССОЦИАТИВНОЙ АЛГЕБРЫ С ДВУМЯ ОБРАЗУЮЩИМИ

Приведенные выше рассуждения позволяют нам сформулировать следующий критерий примитивности элементов длины 2 в терминах линейной алгебры.

Предложение 1. *Элемент* $h = a \cdot \overline{x} + B \cdot \overline{x} \times \overline{x} + C \cdot (\overline{x} \times \overline{x}) \times \overline{x} + D \cdot \overline{x} \times (\overline{x} \times \overline{x})$, *примитивен тогда и только тогда, когда ранг матрицы* $(a|B|B^T|C|C^T|D|D^T)$ *больше ранга матрицы* $(B \mid B^T \mid C \mid C^T \mid D \mid D^T)$.

Доказательство. Воспользуемся техникой свободного дифференциального исчисления и критерием примитивности.

Элемент примитивен тогда и только тогда, когда найдутся такие $m_1, m_2, \ldots, m_n \in U(A)$, что

$$m_1 \frac{\partial}{\partial x_1} + m_2 \frac{\partial}{\partial x_2} + \ldots + m_n \frac{\partial}{\partial x_n} = 1.$$

Матрица $(a|B|B^T|\ldots)$ содержит n строк, где n – число свободных образующих. Каждая из строк матрицы соответствует представлению частной производной по одной из переменных в виде многомерных таблиц.

Задача определения примитивности сводится к алгоритму редукции, шагом которого является устранение старших мономов из производных за счет других производных. Поскольку все старшие мономы l_{x_i} и r_{x_i} производных элементов длины 2 (в общем виде будем записывать op_{x_i}) могут быть получены, либо как $a \cdot op_{x_i} = b \cdot (c \cdot op_{x_i})$, либо как $a \cdot op_{x_i} = (b \cdot op_{x_i}) \cdot c$, возможна только линейная редукция (то есть с коэффициентом из F). Аналогично, среди мономов производной элемента длины 3 обязательно встретится $op_{x_i x_j}$ для которого возможна только линейная редукция.

Итак, для редукции используется только умножение на элементы F. В этом случае алгоритм редукции сводится к решению системы линейных уравнений над полем F.

Воспользовавшись критерием Кронекера–Капелли, получаем доказательство утверждения.

Полученное в ходе доказательства утверждение можно сформулировать в виде леммы.

Лемма 1. *Если среди членов неассоциативного элемента длины k встречаются мономы вида* $x_i \cdot w$ *или* $w \cdot x_i$*, то среди соответствующих им мономов частных производных встречаются такие, для которых возможна только линейная редукция.*

Элемент с такими членами примитивен тогда и только тогда, когда выполняются условия, аналогичные (с учетом большего числа матриц коэффициентов) условиям доказанного критерия примитивности.

Доказательство. К доказанному выше осталось доказать только необходимость выполнения условий. После линейной редукции возможны два случая:

1) одно из выражений частных производных стало константой (то есть элемент примитивен);

2) одно из выражений стало меньшей длины, но не стало константой, другое всё ещё содержит моном вида op_w, из чего следует, что дальнейшая редукция невозможна.

6. ПРИЗНАК ПРИМИТИВНОСТИ

Полученный для элементов длины 2 и 3 критерий можно обобщить до признака примитивности элементов произвольной длины. Транспонирование матриц при этом заменяется на перестановку сторон таблиц коэффициентов. А вместо ранга матрицы необходимо рассматривать ранг системы векторов, составленных из элементов слоев многомерных таблиц коэффициентов.

Под действие этого признака попадает только случай, когда производится линейная редукция системы частных производных. То есть решается система линейных уравнений:

$$\alpha_1 \frac{\partial}{\partial x_1} + \ldots + \alpha_n \frac{\partial}{\partial x_n} = 1,\ \alpha_1,\ldots,\alpha_n \in F.$$

7. ОЦЕНКА ЧИСЛА ПРИМИТИВНЫХ ЭЛЕМЕНТОВ С ДВУМЯ ОБРАЗУЮЩИМИ ПРОИЗВОЛЬНОЙ ДЛИНЫ

7.1. Частные производные одной группы мономов

Проиллюстрируем алгоритм расчета числа примитивных элементов на примере рассмотренной выше группы мономов $a_{\overline{x}\times(\overline{x}\times\overline{x})} \cdot \overline{x} \times (\overline{x} \times \overline{x})$. Пусть $\frac{\partial}{\partial x_2} = \alpha + t\frac{\partial}{\partial x_1}$, $\alpha, t \in F$. Тогда

$$\left(\begin{array}{cc|cc} a_{x_1(x_1x_1)} & a_{x_1(x_2x_1)} & a_{x_1(x_1x_2)} & a_{x_1(x_2x_2)} \\ a_{x_2(x_1x_1)} & a_{x_2(x_2x_1)} & a_{x_2(x_1x_2)} & a_{x_2(x_2x_2)} \end{array}\right) =$$

$$= \left(\begin{array}{cc|cc} a_{x_1(x_1x_1)} & a_{x_1(x_2x_1)} & a_{x_1(x_1x_2)} & a_{x_1(x_2x_2)} \\ ta_{x_1(x_1x_1)} & ta_{x_1(x_2x_1)} & ta_{x_1(x_1x_2)} & ta_{x_1(x_2x_2)} \end{array}\right)$$

$$\left(\begin{array}{cc|cc} a_{x_1(x_1x_1)} & a_{x_2(x_1x_1)} & a_{x_1(x_1x_2)} & a_{x_2(x_1x_2)} \\ a_{x_1(x_2x_1)} & a_{x_2(x_2x_1)} & a_{x_1(x_2x_2)} & a_{x_2(x_2x_2)} \end{array}\right) =$$

$$= \left(\begin{array}{cc|cc} a_{x_1(x_1x_1)} & a_{x_2(x_1x_1)} & a_{x_1(x_1x_2)} & a_{x_2(x_1x_2)} \\ ta_{x_1(x_1x_1)} & ta_{x_2(x_1x_1)} & ta_{x_1(x_1x_2)} & ta_{x_2(x_1x_2)} \end{array}\right)$$

$$\left(\begin{array}{cc|cc} a_{x_1(x_1x_1)} & a_{x_2(x_1x_1)} & a_{x_1(x_2x_1)} & a_{x_2(x_2x_1)} \\ a_{x_1(x_1x_2)} & a_{x_2(x_1x_2)} & a_{x_1(x_2x_2)} & a_{x_2(x_2x_2)} \end{array}\right) =$$

$$= \left(\begin{array}{cc|cc} a_{x_1(x_1x_1)} & a_{x_2(x_1x_1)} & a_{x_1(x_2x_1)} & a_{x_2(x_2x_1)} \\ ta_{x_1(x_1x_1)} & ta_{x_2(x_1x_1)} & ta_{x_1(x_2x_1)} & ta_{x_2(x_2x_1)} \end{array}\right)$$

$$a_{x_2(x_2x_2)} = ta_{x_2(x_2x_1)} = t^2 a_{x_1(x_2x_1)} =$$

$$= ta_{x_2(x_1x_2)} = t^2 a_{x_2(x_1x_1)} =$$

$$= ta_{x_1(x_2x_2)} = t^2 a_{x_1(x_1x_2)} = t^3 a_{x_1(x_1x_1)},$$

где t – общий коэффициент пропорциональности между неединичными мономами частных производных. Это равносильно тому, что t – коэффициент пропорциональности при мономах неассоциативной алгебры с одинаковой расстановкой скобок. При выражении $a_{x_2(x_2x_2)}$ через другие коэффициенты его степень равна количеству x_1 в мономе, соответствующем коэффициенту, и обратно, если выражать

$$a_{x_1(x_1x_1)} = \ldots = s^3 a_{x_2(x_2x_2)}.$$

7.2. Число примитивных элементов

Полученное правило справедливо для мономов любой длины свободной неассоциативной алгебры над конечным полем. Если матрица коэффициентов при какой-либо группе мономов длины m записывается m-мерной таблицей $(a_{i_1 i_2 \ldots i_m})$, $i_j \in \{1,2\}$, то либо $a_{11\ldots1} = \ldots = t^m a_{22\ldots2}$, либо $a_{22\ldots2} = \ldots = s^m a_{11\ldots1}$. Это позволяет нам для каждой группы мономов задать лишь один из коэффициентов. Остальные получаются умножением на выбранный коэффициент t.

Обозначим через $S_2^k(q)$ число примитивных элементов длины k свободной неассоциативной алгебры с двумя образующими над конечным полем F_q.

Линейная часть примитивного элемента может быть получена $q^2 - 1 = q(q-1)$ способами.

Для каждого варианта линейной части оценим число способов получения элемента длины k, удовлетворяющего полученным соотношениям. Коэффициент пропорциональности t можно выбрать q способами, при этом в случае $t = 0$ у нас еще возникает необходимость для каждой группы мономов

длины m выбрать $a_{x_2(\dots x_2)} = \dots = t^m a_{x_1(\dots x_1)}$ или $a_{x_1(\dots x_1)} = \dots = t^m a_{x_2(\dots x_2)}$. Включив этот выбор в число способов выбора t, получим $q+1$ вариант.

Далее оценим число способов выбрать коэффициенты при мономах $x_2(\dots x_2)$ либо $x_1(\dots x_1)$ (в зависимости от выбора t) всех групп длины m. Число вариантов расстановки скобок в мономе длины m равно $(m-1)$-му числу Каталана C_{m-1}, число вариантов выбрать в каждой группе коэффициент равно q. В итоге получаем $q^{C_{m-1}}$ вариант. Чтобы длина элемента была равна k, необходимо, чтобы хотя бы один коэффициент при мономах длины k был ненулевым, что даёт нам $q^{C_{k-1}} - 1$ вариант выбора коэффициента при мономах длины k. Суммарное число комбинаций коэффициентов для мономов длин $2 \dots k-1$ равно $q^{C_1} \cdot \dots \cdot q^{C_{k-2}} = q^{\sum_{m=2}^{k-1} C_{m-1}}$.

Итак, мы готовы записать оценку для $S_2^k(q)$.

$$S_2^k(q) \geqslant \underbrace{(q+1)}_{t} \cdot \underbrace{q(q-1)}_{m=1} \cdot \underbrace{q^{\sum_{m=2}^{k-1} C_{m-1}}}_{m=2\dots k-1} \cdot \underbrace{(q^{C_{k-1}} - 1)}_{m=k}$$

Считая, что $C_0 = 1$, можно сократить запись:

$$S_2^k(q) \geqslant (q+1)(q-1) q^{\sum_{m=1}^{k-1} C_{m-1}} (q^{C_{k-1}} - 1).$$

7.3. Формулы для некоторых длин

Используя, полученную формулу запишем оценки для некоторых длин:

$$S_2^2(q) = (q+1)(q-1)q^1(q^1 - 1) = q(q-1)^2(q+1)$$

$$S_2^3(q) = (q+1)(q-1)q^2(q^2 - 1) = q^2(q-1)^2(q+1)^2$$

$$S_2^4(q) \geqslant (q+1)(q-1)q^4(q^5 - 1)$$

$$S_2^5(q) \geqslant (q+1)(q-1)q^9(q^{14} - 1)$$

Для $S_2^2(q)$ и $S_2^3(q)$ равенство обусловлено тем, что вместо признака можно использовать критерий примитивности.

Правая часть полученной оценки в случае длин 2 и 3 совпадает с формулами подсчета таких элементов, полученными ранее А. А. Чеповским в диссертации [5].

8. ПРОГРАММНАЯ РЕАЛИЗАЦИЯ АЛГОРИТМОВ

Ранее для исследования примитивных элементов были реализованы алгоритмы[3] работы с примитивными элементами в свободных неассоциативных алгебрах в системе компьютерной алгебры SageMath. Для небольших конечных полей с помощью теста примитивности были посчитаны примитивные элементы небольших длин. Полученные выше формулы дают те же значения для тех же полей и длин.

Описанное представление позволяет оптимизировать алгоритмы работы с примитивными элементами, заменив ресурсоемкие операции на работу с таблицами: вместо символьного дифференцирования производить транспонирование матриц, упростить умножение элементов алгебр.

8.1. Подсчет количества примитивных элементов длины 4 в свободной неассоциативной алгебре с двумя образующими

Выше мы показали, что если элемент содержит один из мономов вида $x(x(xx))$, $x((xx)x)$, $(x(xx))x$, $((xx)x)x$, то в алгоритме проверки примитивности элемента будут использованы только линейные редукции. Все такие примитивные элементы можно посчитать по полученной выше формуле. Значит, для получения общего числа примитивных элементов длины 4 необходимо посчитать те, которые требуют умножения на нескалярные элементы алгебры $U(A)$ в ходе редукции. Все такие элементы будут содержать мономы вида $(xx)(xx)$.

Найдем частные производные мономов такого вида:

$$\mathcal{D}((\overline{xx})(\overline{xx})) = r_{\overline{xx}} r_{\bar{x}} \mathcal{D}(\bar{x}) + \\ + r_{\overline{xx}} l_{\bar{x}} \mathcal{D}(\bar{x}) + l_{\overline{xx}} r_{\bar{x}} \mathcal{D}(\bar{x}) + l_{\overline{xx}} l_{\bar{x}} \mathcal{D}(\bar{x}).$$

Пронумеруем получившиеся мономы алгебры $U(A)$ по порядку переменной в мономе $(\overline{xx})(\overline{xx})$, по которой при дифференцировании получается $\mathcal{D}(\bar{x})$. Получим $1 : r_{\overline{xx}} r_{\bar{x}}$, $2 : r_{\overline{xx}} l_{\bar{x}}$, $3 : l_{\overline{xx}} r_{\bar{x}}$, $4 : l_{\overline{xx}} l_{\bar{x}}$.

Если таблицу мономов вида $(\overline{xx})(\overline{xx})$ записать в виде

$$\left(\begin{array}{cc|cc} (xx)(xx) & (xx)(xy) & (xy)(xx) & (xy)(xy) \\ (xx)(yx) & (xx)(yy) & (xy)(yx) & (xy)(yy) \\ \hline (yx)(xx) & (yx)(xy) & (yy)(xx) & (yy)(xy) \\ (yx)(yx) & (yx)(yy) & (yy)(yx) & (yy)(yy) \end{array}\right),$$

то, используя введённые обозначения, частные производные $\partial/(\partial x)$ и $\partial/(\partial y)$ можно записать соответственно таблицами:

$$\left(\begin{array}{ccc|c} 1234 & 123 & 134 & 13 \\ 124 & 12 & 14 & 1 \\ \hline 234 & 23 & 34 & 3 \\ 24 & 2 & 4 & \end{array}\right) \text{ и } \left(\begin{array}{ccc|c} & & 4 & 2 \quad 24 \\ & 3 & 34 & 23 \quad 234 \\ \hline 1 & 14 & 12 & 124 \\ 13 & 134 & 123 & 1234 \end{array}\right).$$

Считая, что

• D – таблица коэффициентов, соответствующих мономам в этих таблицах мономов;

• при использовании ее в качестве коэффициентов при частных производных первый индекс указывает на то, к какой производной относится коэффициент (например, d_{1ijk} – коэффициент при некотором мономе $\partial/(\partial x)$, а d_{2ijk} – коэффициент при некотором мономе $\partial/(\partial y)$);

• D^σ – транспонированная таблица коэффициентов, с помощью перестановки σ, то есть $d^\sigma_{i_1i_2i_3i_4} = d_{i_{\sigma(1)}i_{\sigma(2)}i_{\sigma(3)}i_{\sigma(4)}}$;

• из монома $(x_1x_2)(x_3x_4)$ алгебры A получаются следующие мономы алгебры $U(A)$: $r_{x_3x_4}r_{x_2}$, $r_{x_3x_4}l_{x_1}$, $l_{x_1x_2}r_{x_4}$, $l_{x_1x_2}l_{x_3}$, и соответствующие им перестановки (234), (12334), (321), (4321),

получим следующие выражения частных производных группы мономов $(\overline{xx})(\overline{xx})$: $D^{(234)}r_{\overline{xx}}r_{\bar{x}} + D^{(1234)}r_{\overline{xx}}l_{\bar{x}} + D^{(321)}l_{\overline{xx}}r_{\bar{x}} + D^{(4321)}l_{\overline{xx}}l_{\bar{x}}$.

Если примитивный элемент содержит моном вида $(\overline{xx})(\overline{xx})$, частные производные которого требуют редукции, то он не может содержать мономы длины 3. Так как в этом случае в выражения частных производных будут входить мономы вида r_{xx} или l_{xx}, которые могут быть редуцированы только такими же мономами. Итак, примитивный элемент длины 4, не подходящий под условия признака примитивности, имеет вид: $A\bar{x} + B\bar{x}x + D(\overline{xx})(\overline{xx})$.

Также справедливы соотношения для старших мономов, полученные ранее:

$$s^4d_{(x_2x_2)(x_2x_2)} = s^3td_{(x_2x_2)(x_2x_1)} =$$
$$= s^3td_{(x_2x_2)(x_1x_2)} = s^3td_{(x_2x_1)(x_2x_2)} =$$
$$= s^3td_{(x_1x_2)(x_2x_2)} = s^2t^2d_{(x_2x_2)(x_1x_1)} =$$
$$= s^2t^2d_{(x_2x_1)(x_2x_1)} = s^2t^2d_{(x_1x_2)(x_2x_1)} =$$
$$= s^2t^2d_{(x_2x_1)(x_1x_2)} = s^2t^2d_{(x_1x_2)(x_1x_2)} =$$
$$= s^2t^2d_{(x_1x_1)(x_2x_2)} = st^3d_{(x_2x_1)(x_1x_1)} =$$
$$= st^3d_{(x_1x_2)(x_1x_1)} = st^3d_{(x_1x_1)(x_2x_1)} =$$
$$= st^3d_{(x_1x_1)(x_1x_2)} = t^4d_{(x_1x_1)(x_1x_1)}.$$

Исходя из этого получим, что подходящих наборов коэффициентов при таких мономах в каждом поле будет $(q+1)(q-1)$, как уже было показано выше.

Посчитаем для некоторых конечных полей для каждого такого набора число примитивных элементов методами компьютерной алгебры.

С учетом всех приведенных выше рассуждений для подсчета элементов длины 4 в свободных неассоциативных алгебрах с двумя образующими над конечными полями получим следующие алгоритмы.

Алгоритм 1. *Генерация таблиц коэффициентов для мономов длины 4.*

1) подготовить наборы индексов:
   1 – 0000;
   2 – 1000, 0100, 0010, 0001;
   4 – 0111, 1011, 1101, 1110;
   5 – 1111;
   3 – остальные 6 комбинаций;
2) установить значение множителя $t := 0$;
3) если $t > q$, перейти к шагу 12;
4) подготовить таблицы-шаблоны с множителями, поместив t^{k-1} по индексам набора k; если $t = q$, то наоборот, по индексам набора k поместить значение t^{6-k};
5) установить опорное значение $a := 1$;
6) если $a \geqslant q$, перейти к шагу 10;
7) сформировать таблицу коэффициентов как таблицу-шаблон, умноженную на a;
8) увеличить $a := a + 1$;
9) перейти к шагу 6;
10) увеличить $t := t + 1$;
11) перейти к шагу 3;
12) вернуть все сформированные таблицы коэффициентов;
13) завершить алгоритм.

Алгоритм 2. *Генерация таблиц коэффициентов для мономов длин 1 и 2.*

1) подготовить список из 6 нулевых элементов;
2) установить $i := 1$;
3) если $i > 6$ перейти к шагу 11;
4) увеличить элемент i в списке на 1;
5) если значение элемента i меньше q, то перейти к шагу 9;
6) установить элемент i в списке равным 0;
7) увеличить $i := i + 1$;
8) перейти к шагу 3;
9) если в списке есть ненулевые элементы, то сформировать вектор коэффициентов при мономах длины 1 из первых двух элементов списка, матрицу коэффициентов при мономах длины 2 из последних четырех элементов списка;

10) перейти к шагу 2;

11) вернуть все сформированные таблицы коэффициентов;

12) завершить алгоритм.

Алгоритм 3. *Проверка примитивности элементов для заданной таблицы коэффициентов при мономах длины 4.*

Вход: два выражения p_1 и p_2. На каждом этапе редукция описывается следующими шагами:

1) найти коэффициенты k_1 и k_2, не равные одновременно нулю в соответствующих значениях частных производных для старшего монома;

2) в качестве редуцируемого выражения p_1 выбрать то, в котором найден ненулевой коэффициент;

3) вычислить выражение $p_2 := k_1 p_2 + k_2 p_1 \bmod q$;

4) если в выражении p_2 сохранились старшие мономы той же степени, значит редукция невозможна, перейти к шагу 10;

5) найти коэффициенты в соответствующих друг другу группах мономов: k_2 – ненулевые в старших мономах p_2 и k_1 – ненулевые в старших мономах p_1;

6) найти k_2 как $k_1 \times k_2$, в качестве нового значения k_2 выбрать любой ненулевой элемент k_2;

7) произвести редукцию $p_1 := p_2$, $p_2 := k_1 p_2 + k_2 p_1 \bmod q$;

8) если в выражении p_2 сохранились старшие мономы той же степени, значит редукция невозможна, перейти к шагу 10;

9) вернуть p_1, p_2 и завершить алгоритм с кодом УСПЕХ;

10) вернуть исходные выражения, завершить алгоритм с кодом НЕУСПЕХ.

Описанное на шаге 6 алгоритма 3 произведение определим следующим образом. Пусть a – таблица размера $t_1 \times t_2 \times \ldots \times t_\alpha$, b – таблица размера $s_1 \times s_2 \times \ldots \times s_\beta$. Тогда результатом произведения будет таблица $c = a \times b$ размера $t_1 \times t_2 \times \ldots \times t_\alpha \times s_1 \times s_2 \times \ldots \times s_\beta$ такая, что

$$c_{i_1 \ldots i_\alpha j_1 \ldots j_\beta} = a_{i_1 \ldots i_\alpha} \cdot b_{j_1 \ldots j_\beta}.$$

Эта и другие операции с многомерными таблицами реализованы в пакетах NumPy, PyTorch, TensorFlow языка Python. При этом PyTorch и TensorFlow поддерживают вычисления на GPU, что позволяет многократно ускорить обработку больших объёмов данных.

Алгоритм 4. *Подсчет примитивных элементов длины 4.*

1) перебрать простые числа: 2, 3, 5, 7, 11, ...;

2) с помощью **Алгоритма 1** сформировать таблицы коэффициентов при старших мономах по текущему выбранному простому числу;

3) установить счетчик примитивных элементов равным 0;

4) для каждой из таблиц с помощью **Алгоритма 2** сформировать таблицы коэффициентов при остальных мономах;

5) произвести с помощью **Алгоритма 3** редукцию каждого из элементов пока алгоритм возвращает УСПЕХ;

6) если в какой-то момент одно из возвращаемых **Алгоритмом 3** выражений будет ненулевой константой, то элемент примитивен, увеличить счетчик примитивных элементов на 1;

7) вывести по каждому набору коэффициентов старших мономов полученное число примитивных элементов.

В результате работы алгоритма 4 получено, что для каждого набора коэффициентов (вне зависимости от выбранного множителя t и равенства его нулю), число примитивных элементов в простых полях соответственно: $F_2 : 3$, $F_3 : 8$, $F_5 : 24$, $F_7 : 48$, $F_{11} : 120$, ...

Метод неопределённых коэффициентов даёт выражение для этого числа $q^2 - 1$. Тогда общее число примитивных элементов с нередуцируемыми линейно частными производными получится $(q-1)^2(q+1)^2$.

Таким образом, мы получили недостающую часть числа S_2^4:

$$S_2^4 = (q+1)(q-1)q^4(q^5-1) + (q+1)^2(q-1)^2.$$

ИСТОЧНИК ФИНАНСИРОВАНИЯ

При финансовой поддержке Российского научного фонда, грант 22-11-00052.

СПИСОК ЛИТЕРАТУРЫ

1. *Artamonov V.A., Klimakov A.V., Mikhalev A.A., Mikhalev A.V.* Primitive and almost-primitive elements of free algebras of Schreier varieties, Fundam // Prikl. Mat. 2016. V. 21. № 2. P. 3–35.
2. *Kurosh A.G.* Free non-associative algebras and free products of algebras // Mat. Sb. 1947. V. 20. P. 239–262.
3. *Maisuradze M.V.* Software implementation of algorithms for working with primitive elements in free nonassocia-

tive algebras // Intellekt. Sist. Teor. Prilozh. 2021. V. 25. № 4. P. 170–175.
4. *Mikhalev A.A., Mikhalev A.V., Chepovskii A.A., Shampan'er K.* Primitive elements of free associative algebras // Fundam. Prikl. Mat. 2007. V. 13. № 5. P. 171–192.
5. *Chepovskii A.A.* Primitive elements of algebras of Schreier varieties, Cand. Sci. (Phys.-Math.) Dissertation, Moscow: Mosk. Gos. Univ., 2011.
6. *Chepovskii A.A.* Number of primitive elements of lengths 1 and 2 in free non-associative algebras over a finite field // Vestn. Novosib. Gos. Univ. Ser.: Mat., Mekh., Inf. 2011. V. 11. P. 119–122.
7. *Mikhalev A.A., Umirbaev U.U., Yu J.-T.* Automorphic orbits of elements of free non-associative algebras, J. Algebra. 2001. P. 198–223.
8. *Mikhalev A.A., Shpilrain V., Yu J.-T.* Combinatorial Methods: Free Groups, Polynomials, and Free Algebras, New York: Springer, 2004.

PRIMITIVE ELEMENTS OF FREE NON-ASSOCIATIVE ALGEBRAS OVER FINITE FIELDS

© 2024 M. V. Maisuradze[a], A. A. Mikhalev[a]

[a] *Department of Mechanics and Mathematics, Moscow State University, Moscow, 119991 Russia*

The representation of elements of free non-associative algebras as a set of multidimensional tables of coefficients is defined. An operation for finding partial derivatives for elements of free non-associative algebras in the same form is considered. Using this representation, a criterion of primitivity for elements of lengths 2 and 3 in terms of matrix ranks, as well as a primitivity test for elements of arbitrary length, is derived. This test makes it possible to estimate the number of primitive elements in free non-associative algebras with two generators over a finite field. The proposed representation allows us to optimize algorithms for symbolic computations with primitive elements. Using these algorithms, we find the number of primitive elements of length 4 in a free non-associative algebra of rank 2 over a finite field.

Keywords: Schreier variety of linear algebras, free non-associative algebras, primitive elements of free algebras, and free differential calculus in free algebras