Институт по математика и информатика – БАН
Семинар "Алгебра и логика"
23.11.2018 г.

Примитивна дължина и сложност на пресмятанията в алгебрични системи

Веселин Дренски

Нека S е е подмножество в дадена алгебрична система G (например G е полугрупа, група, пръстен или алгебра над поле) и нека Ω е множество от операции в G.

Ние ще обсъждаме въпроса колко операции от Ω са необходими, за да се изрази даден елемент от G чрез елементите на S (и дали въобще е възможно елементът да се изрази чрез S).

Това е важен проблем както за практиката, така и от гледна точка на теория на изчислимостта.

Една от основните задачи на теорията на изчислимостта е да класифицира алгоритмичните проблеми в зависимост от тяхната сложност.

Класът **NP** (недетерминистично полиномиално време) се състои от алгоритмичните проблеми, за които ако имаме кандидат за решение, можем да проверим за полиномиално време дали това е наистина решение. С прости думи това означава, че е лесно да проверим дали нещо е решение на проблема.

Класът **P** се състои от проблеми, за които има алгоритъм, който намира отговора за полиномиално време. Отново с прости думи, лесно е да се намери решение на задачата.

Проблемът P срещу проблема NP

Това е един от най-важните нерешени проблеми в теорията на изчислимостта и в математическата информатика. Въпросът е *дали всеки проблем, чието решение може да бъде проверено бързо (за полиномиално време), може също да бъде решен бързо (отново за полиномиално време).*

Това е един от седемте "Проблеми за наградата на хилядолетието", избрани от Математическия институт "Клей", всеки от които носи награда от 1,000,000 долара за първото коректно решение.

Метод на Гаус за решаване на линейни системи от уравнения

За да решим система от n уравнения с n неизвестни чрез преобразувания по редове привеждаме матрицата на системата в трапецовиден вид, след което намираме неизвестните в обратен ред. Лесно се вижда, че за това са необходими $\mathcal{O}(n^3)$ операции. Аритметичната сложност е добро мерило за времето, необходимо за извършване на пресмятанията, когато времето за извършване на всяка аритметична операция е приблизително едно и също. Така е в случая, когато коефициентите на уравнението са представени чрез плаваща запетая или са от крайно поле.

Когато коефициентите са точно представени цели или рационални числа, при междинните пресмятания числата могат да растат експоненциално. Следователно битовата сложност на метода на Гаус става експоненциална.

Има вариант на метода на Гаус, наречен *алгоритъм на Барайс*, който избягва експоненциалния ръст на междинните резултати и със същата аритметична сложност $\mathcal{O})(n^3)$, има битова сложност $\mathcal{O}(n^5)$.

E. H. Bareiss, *Sylvester's Identity and multistep integer-preserving Gaussian elimination,* Mathematics of Computation **22** (1968), 565-578.

Обратно към задачата – Задача за Chicken McNuggets

През 1979 година Макдоналдс пуска в продажба Chicken McNuggets (хапки от пилешки гърди в златиста, хрупкава панировка със сос по избор).

Първоначално пилешките хапки са пуснати в опаковки от 6, 9 и 20.

(Днес повечето заведения на Макдоналдс в САЩ продават Chicken McNuggets в опаковки от 4, 6, 10, 20, 40 и 50 хапки. В България те се предлагат по 6 и 9, а ако се вземат като меню с картофки и кока-кола – по 5.)

Задача за Chicken McNuggets

Колко пилешки хапки могат да се купят в Макдоналдс, ако се използват само опаковки от $6, 9$ *или* 20 *хапки?*

S.T. Chapman, C. O'Neill, *Factoring in the Chicken McNugget monoid,* arXiv: 1709.01606.

Естествените числа n, които удовлетворяват задачата за Chicken McNuggets се наричат *числа на McNuggets* (McNugget numbers). Очевидно, че за тях съществува наредена тройка (a, b, c) от неотрицателни цели числа такава, че

$$6a + 9b + 20c = n.$$

Отговор

Единствените естествени числа, които не са числа на McNuggets са 1, 2, 3, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 22, 23, 25, 28, 31, 34, 37 и 43. (Това е редицата A065003 (https://oeis.org/A065003) в *Енциклопедията на целочислените редици*, основана от Слоан през 1964 г.)

Числови полугрупи

Ако $a_1, \ldots, a_k \in \mathbb{N}$, то множеството на всички числа от вида

$$n = a_1 z_1 + \cdots + a_k z_k, \quad z_1, \ldots, z_k \in \mathbb{N}_0,$$

е подполугрупа с 0 на адитивната полугрупа $\mathbb{N}_0$. Когато подполугрупата съдържа почти всички (с изключение на краен брой) естествени числа, тя се нарича *числова полугрупа*.

Известно е, че *всяка подполугрупа на* $\mathbb{N}_0$ *се поражда от краен брой числа и притежава единствена минимална система пораждащи.*

Теорема

Ако $a_1, \ldots, a_k \in \mathbb{N}$ *и* $(a_1, \ldots, a_k) = 1$, *то всички достатъчно големи естествени числа се представят във вида*

$$n = a_1 z_1 + \cdots + a_k z_k, \quad z_1, \ldots, z_k \in \mathbb{N}_0.$$

Най-голямото естествено число, което не може да се представи в този вид, се нарича *число на Фробениус*.

Например, числото на Фробениус за числата на McNuggets е равно на 43.

Проблем на Фробениус за монетите

Популярна формулировка:
Коя е най-голямата сума **(числото на Фробениус)**, *която не може да се плати с монети от няколко фиксирани номинала?*

С монети от 5 и 2 пенса могат да се платят всички суми с изключение на 1 и 3 пенса.

Въпреки, че Фробениус никога не е поставял този проблем в явна форма в написан текст, проблемът се приписва на него. Има данни, че той понякога го е споменавал в своите лекции.

J.L. Ramírez Alfonsín, *The Diophantine Frobenius problem,* Oxford Lecture Series in Mathematics and its Applications **30**, Oxford: Oxford University Press, 2005.

Теорема на Силвестър???

Формула за числото на Фробениус е известна само когато монетите са от два взаимно прости номинала a и b. *Тогава то е равно на* $ab - (a + b)$.

Не е ясно, чий е този резултат. Обикновено той се приписва на Силвестър, тъй като през 1884 г. той поставя близка занимателна задача. Но други публикации на Силвестър навеждат на мисълта, че той е знаел за резултата.

MATHEMATICS

FROM

THE EDUCATIONAL TIMES,

WITH ADDITIONAL PAPERS AND SOLUTIONS.

7382. (By Professor Sylvester, F.R.S.) — If p and q are relative primes, prove that the number of integers inferior to pq which cannot be resolved into parts (zeros admissible), multiples respectively of p and q, is

$$\tfrac{1}{2}(p-1)(q-1).$$

[If $p = 4$, $q = 7$, we have $\frac{1}{2}(p-1)(q-1) = 9$; and 1, 2, 3, 5, 6, 9, 10, 13, 17 are the only integers inferior to 28, which are neither multiples of 4 or 7, nor can be made up by adding together multiples of 4 and 7.]

Math. Questions from the Educational Times, 41 (1884), 21.

Solution by W. J. Curran Sharp, M.A.

If the product $(1+x^p+x^{2p}+\ldots+x^{pq})(1+x^q+x^{2q}+\ldots+x^{pq})$ be considered, each term between 1 and x^{pq} corresponds to a number less than pq, and of the form $mp+nq$; also $2x^{pq}$ is the middle term, and the coefficients from each end are the same. Hence twice the number of integers of the form $mp+nq$, and less than pq, is the value of the above product when $x=1$ with four deducted, since the terms involving x^1, x^{pq}, x^{2pq} are not included; and therefore the number of these integers is

$$\tfrac{1}{2}(p+1)(q+1)-2,$$

and the number of those which cannot be put into this form

$$=pq-1-[\tfrac{1}{2}(p+1)(q+1)-2]=\tfrac{1}{2}[pq-p-q+1]=\tfrac{1}{2}(p-1)(q-1).$$

В общия случай не е известна формула за числото на Фробениус, но *при фиксирано количесто от номинали има алгоритъм, който пресмята числото на Фробениус за полиномиално време*.
(**Входните данни** на такъв алгоритъм са логаритмите на номиналите.)

R. Kannan, *Lattice translates of a polytope and the Frobenius problem,* Combinatorica **12** (1992), No. 2, 161-177.

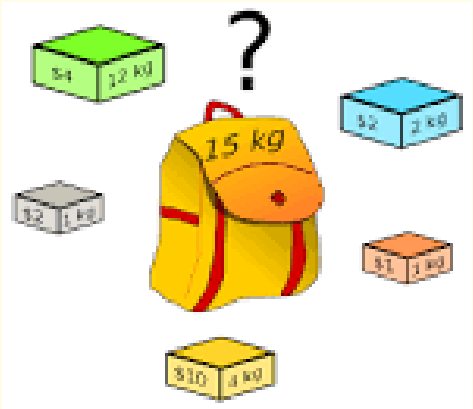
В общия случай не е намерен алгоритъм, който решава задачата за полиномиално време. Този проблем е NP-труден.

J.L Ramírez-Alfonsín, *Complexity of the Frobenius problem,* Combinatorica **16** (1996), No. 1, 143-147.

NP-пълен е алгоритмичен проблем, който е NP и решението на всеки NP-проблем може за полиномиално време да се сведе до решаването на NP-пълния проблем. Проблемът е *NP-труден*, ако знаем, че се изпълнява второто условие, но не знаем дали се изпълнява първото, т.е. решението на всички NP-проблеми се свеждат до неговото решаване, но не знаем дали самият проблем може да се реши за полиномиално време.

В своята статия Рамирес Алфонсин доказва, че *тръгвайки от алгоритъм за решаване на проблема на Фробениус, може да се намери алгоритъм за задача, която е NP-пълна:*

Проблем за раницата (от комбинаторната оптимизация)



Дадено е множество от предмети, всеки от които има тегло и стойност. Да се определи броят на предметите от всеки вид, които да сложим в раницата, така че теглото на предметите в раницата да не е по-голямо от предварително зададеното, а общата им стойност да е колкото се може по-голяма.

Сменяме задачата:

Задача. *Какъв е минималният брой пакети, ако искаме да купим n хапки Chicken McNuggets?*

Решение

Разглеждаме формалния степенен ред

$$f(x,t) = \frac{1}{(1-x^6t)(1-x^9t)(1-x^{20}t)} = \sum f_{np}x^n t^p.$$

Коефициентът f_{np} е равен на броя на начините, по които можем да представим n във вида $n = 6a + 9b + 20c$ и за които $a + b + c = p$.

$$f(x,t) = 1 + x^6t + x^9t + x^{12}t^2 + x^{15}t^2 + x^{18}(t^2 + t^3) + x^{20}t$$
$$+x^{21}t^3 + x^{24}(t^3 + t^4) + x^{26}t^2 + x^{27}(t^3 + t^4)$$
$$+x^{29}t^2 + x^{30}(t^4 + t^5) + x^{32}t^3 + x^{33}(t^4 + t^5)$$
$$+x^{35}t^3 + x^{36}(t^4 + t^5 + t^6) + x^{38}(t^3 + t^4) + x^{39}(t^5 + t^6)$$
$$+x^{40}t^2 + x^{41}t^4 + x^{42}(t^5 + t^6 + t^7) + x^{44}(t^4 + t^5)$$
$$+x^{45}(t^5 + t^6 + t^7) + x^{46}t^3 + x^{47}(t^4 + t^5)$$
$$+x^{48}(t^6 + t^7 + t^8) + x^{49}t^3 + x^{50}(t^5 + t^6) + \cdots$$

Например, можем да купим 47 хапки в 4 пакета или в 5 пакета.

Ако искаме да намерим кои са решенията на системата

$$6a + 9b + 20c = n, \quad a + b + c = p$$

можем да разгледаме формалния степенен ред

$$f(x, t_1, t_2, t_3) = \frac{1}{(1 - x^6 t_1)(1 - x^9 t_2)(1 - x^{20} t_3)} = \sum x^n t_1^a t_2^b t_3^c.$$

Задачата е от полиномиална сложност

За да намерим решенията на уравнението $6a + 9b + 20c = n$,за които $p = a + b + c$ е минимално, е достатъчно да разглеждаме произведението

$$\sum_{6a \leq n} x^{6a} t_1^a \cdot \sum_{9b \leq n} x^{9b} t_2^b \cdot \sum_{20c \leq n} x^{20c} t_3^c.$$

В горния пример A е числова полугрупа, S се състои от единствената минимална система от пораждащи, Ω е операцията събиране. *Представянето на елементите на A с минимален брой събираеми от S може да се намери за полиномиално време.*

Примитивни елементи

Нека A е алгебрична система. *Примитивен елемент* в A е всеки елемент, който принадлежи на минимална пораждаща система на A.

Ранг

Нека G е минимална пораждаща система на A. Всеки елемент $a \in A$ може да се представи във вида $a = f(g_1, \ldots, g_n)$, $\{g_1, \ldots, g_n\} \subseteq G$, където a зависи съществено от всички $g_1, \ldots, g_n$. Минималното n, когато G пробягва всички минимални пораждащи системи на A се нарича *ранг* на a.

Проблем

Как да пресметнем ранга на един елемент в свободната група, свободната алгебра на Ли, свободната асоциативна алгебра, в алгебрата на полиномите и в други свободни обекти в многообразия от алгебрични системи?

По-горе предполагаме, че свободните обекти са с фиксиран краен брой пораждащи.

Отговори

За свободните алгебри на Ли:
А.А. Михалёв, А.А. Золотых, *Ранг элемента свободной* (p)*-супералгебры Ли,* Доклады РАН **334** (1994), No. 6, 690-693.

За свободните групи:
У.У. Умирбаев, *О ранге элементов свободных групп,* Фундаментальная и прикладная математика **2** (1996), No. 1, 313-315.

Проблем

Алгоритмически разрешима ли е задачата да се намери примитивна система, при която се достига рангът на даден елемент? Ако задачата е алгоритмически разрешима, каква е нейната сложност?

Проблем на Бардаков, Шпильрайн и Толстых

V. Bardakov, V. Shpilrain, V. Tolstykh, *On the palindromic and primitive widths of a free group,* J. Algebra **285** (2005), No. 2, 574-585.

Нека A е група, нека S е множеството на примитивните елементи и нека Ω се състои от груповата операция.

Дефиниция. *Примитивната дължина* $\mathrm{plength}(a)$ на $a \in A$ е най-малкото число k такова, че $a = u_1 \cdots u_k$, където $u_1, \ldots, u_k$ са примитивни елементи. Максимумът $\mathrm{pwidth}(A)$ на $\mathrm{plength}(a)$, $a \in A$, се нарича *примитивна ширина* на A.

Проблем. *Да се намери примитивната дължина на елементите на A и примитивната ширина на A.*

Пример

Нека $\mathbb{Z}_{p^n}$ е адитивната група от ред p^n, където p е просто число. Елементът $u \in \mathbb{Z}_{p^n}$ е примитивен тогава и само тогава, когато p не дели u.

Ако p не дели a, то a е примитивен и $\text{plength}(a) = 1$.

Ако p дели a, $a = pa_1$, то $a = (1 + pa_1) + (-1)$. Следователно $\text{plength}(a) = 2$.

A е d-породената свободна група F_d, $d \geq 2$

Теорема. (Бардаков, Шпильрайн и Толстых)

$$\text{pwidth}(F_d) = \infty.$$

V. Bardakov, V. Shpilrain, V. Tolstykh, *On the palindromic and primitive widths of a free group,* J. Algebra **285** (2005), No. 2, 574-585.

Проблем на Ела Айдън

E. Aydın, *Primitive decomposition of elements of the free metabelian Lie algebra of rank two,* Serdica Math. J. **43** (2017), 369-374.

Нека A е алгебра, S – множеството от примитивните елементи, а множеството от операции Ω се състои само от събирането.

Дефиниция. *Адитивната примитивна дължина* $\mathrm{plength}_+(a)$ на $a \in A$ е най-малкото число k такова, че $a = u_1 + \cdots + u_k$, където $u_1, \ldots, u_k$ са примитивни елементи (ако такова k съществува). Максимумът $\mathrm{pwidth}_+(A)$ на $\mathrm{plength}_+(a)$, ако $\mathrm{plength}_+(a)$ е дефинирано за всички $a \in A$, се нарича *адитивна примитивна ширина* на A.

Проблем. *Да се намери адитивната примитивна дължина на елементите на A и адитивната примитивна ширина на A.*

Многообразия от алгебри

Нека K е поле и $K\{X_d\} = K\{x_1, \ldots, x_d\}$ е абсолютно свободната неасоциативна алгебра. (В нея $(x_1x_2)x_3 \neq x_1(x_2x_3)$.)
Нека $V_0 \subset K\{X_\infty\}$.

Дефиниция. Класът $\mathfrak{V}$ от всички (неасоциативни) алгебри R, за които

$$f(r_1, \ldots, r_n) = 0 \text{ за всички } f \in V_0,\ r_1, \ldots, r_n \in R$$

се нарича *многообразие от алгебри*, определено от *полиномните тъждества* от V_0.

Примери

- Многообраизето асоциативните алгебри $\mathfrak{Assoc}$ се определя от тъждеството

$$(x_1x_2)x_3 = x_1(x_2x_3);$$

- Многообразието $\mathfrak{A}$ на асоциативните и комутативните алгебри е подмногообразие на $\mathfrak{Assoc}$, което се определя като подмногообразие от тъждеството

$$x_1x_2 = x_2x_1;$$

- Многообразието $\mathfrak{Lie}$ от алгебрите на Ли се определя от тъждеството за антикомутативност и тъждеството на Якоби, съответно

$$[x_1, x_1] \text{ и } [[x_1, x_2], x_3] + [[x_2, x_3], x_1] + [[x_3, x_1], x_2].$$

(Относително) свободни алгебри в многообразия

Нека $\mathfrak{V}$ е многообразие от алгебри и нека $V \subset K\{X_\infty\}$ е множеството на всички тъждества във $\mathfrak{V}$. Тогава V е идеал в $K\{X_\infty\}$, който е *напълно характеристичен*, т.е. издържа всички ендоморфизми на $K\{X_\infty\}$. С други думи, ако $v(x_1, \ldots, x_n) \in V$ и $u_1, \ldots, u_n \in K\{X_\infty\}$, то $v(u_1, \ldots, u_n)$ също принадлежи на V. Фактор-алгебрите

$$F(\mathfrak{V}) = F_\infty(\mathfrak{V}) = K\{X_\infty\}/V \text{ и } F_d(\mathfrak{V}) = K\{X_d\}/(V \cap K\{X_d\})$$

се наричат *относително свободни алгебри* във $\mathfrak{V}$, съответно от изброим ранг и ранг d.

Алгебрите $F(\mathfrak{V})$ и $F_d(\mathfrak{V})$ имат следното универсално свойство. *Ако R е алгебра от $\mathfrak{V}$, то всяко изображение $X_\infty \to R$ се продължава еднозначно до хомоморфизъм $F(\mathfrak{V}) \to R$. Аналогично свойство е в сила и за $F_d(\mathfrak{V})$.*

Примитивните елементи в $F_d(\mathfrak{V})$ са образите на X_d под действието на автоморфизъм на $F_d(\mathfrak{V})$.

Пример – (относително) свободни нилпотентни алгебри

Нека $\mathfrak{N}$ е многообразие от алгебри, удовлетворяващи всички тъждества от вида $(x_1 \cdots)(\cdots x_n) = 0$ с всевъзможни разположения на скобките.

Едно изображение $\varphi_0 : X_d \to F_d(\mathfrak{N})$ се продължава до автоморфизъм φ на $F_d(\mathfrak{N})$ тогава и само тогава, когато елементите $\varphi_0(X_d)$ са линейно независими по модул $F_d^2(\mathfrak{N})$.

Следователно, *$u \in F_d(\mathfrak{N})$ е примитивен тогава и само тогава, когато не принадлежи на $F_d^2(\mathfrak{N})$.*

Адитивна примитивна дължина в $F_d(\mathfrak{N})$

$$u = \sum_{i=1}^{d} \alpha_i x_i + v, \quad \alpha_i \in K, v \in F_d^2(\mathfrak{N}).$$

Тъй като $x_1 + v$ и $-x_1$ са примитивни и $v = (x_1 + v) + (-x_1)$, то

$$\text{plength}_+(u) = \begin{cases} 1, & \alpha_i \neq 0 \text{ за някое } i = 1, \ldots, d; \\ 2, & \alpha_i = 0, \quad i = 1, \ldots, d. \end{cases}$$

Полиномната алгебра $K[X_d]$

Примитивните елементи в $K[X_d]$ са образите на x_1 под действието на групата $\mathrm{Aut}(K[X_d])$ от автоморфизмите на $K[X_d]$.

Групата $\mathrm{Aut}(K[X_d])$ съдържа подгрупата на *питомните автоморфизми*, породена от *афинните автоморфизми*

$$x_j \to \beta_j + \sum_{i=1}^{d} \alpha_{ij} x_i, \quad \alpha_{ij}, \beta_j \in K, j = 1, \ldots, d,$$

където матрицата (α_{ij}) е обратима, т.е. принадлежи на $GL_d(K)$ и *триъгълните автоморфизми*

$$x_j \to \alpha_j x_j + f_j(x_{j+1}, \ldots, x_d), \quad \alpha_j \neq 0, j = 1, \ldots, d.$$

Теорема (Юнг-ван дер Кулк)

H.W.E. Jung, *Über ganze birationale Transformationen der Ebene,* J. reine und angew. Math. **184** (1942), 161-174.
W. van der Kulk, *On polynomial rings in two variables,* Nieuw Archief voor Wiskunde (3) **1** (1953), 33-41.

- Юнг – за $\mathrm{char}(K) = 0$;
- ван дер Кулк – за произволно поле:

Всички автоморфизми на $K[X_2]$ са питомни.

Автоморфизми на други свободни обекти

Понятието питомен автоморфизъм се дефинира по съответен начин и за други групи и алгебри.

- Нилсен (1924): *Автоморфизмите на свободната група са питомни;*
- Кон (1964): *Автоморфизмите на свободната алгебра на Ли са питомни.*
- Макар Лиманов (1970), Черниакиевич (1971): *Автоморфизмите на свободната асоциативна алгебра* $K\langle X_2\rangle$ *са питомни.*

J. Nielsen, *Die Isomorphismengruppe der freien Gruppen,* Math. Ann. **91** (1924), 169-209.

P. M. Cohn, *Subalgebras of free associative algebras,* Proc. London Math. Soc. (3) **14** (1964), 618-632.

Л. Г. Макар-Лиманов, *Об автоморфизмах свободной алгебры с двумя образующими,* Функц. анализ и его прил. **4** (1970), No. 3, 107-108.

A. J. Czerniakiewicz, *Automorphisms of a free associative algebra of rank* 2, I, II, Trans. Amer. Math. Soc. **160** (1971), 393-401; **171** (1972), 309-315.

Автоморфизъм на Нагата на $K[X_3]$

M. Nagata, *On the Automorphism Group of* $k[x, y]$, Lect. in Math., Kyoto Univ., Kinokuniya, Tokyo, 1972.

$$\begin{aligned} x_1 &\to x_1 - 2(x_2^2 + x_1x_3)x_2 - (x_2^2 + x_1x_3)^2x_3, \\ x_2 &\to x_2 + (x_2^2 + x_1x_3)x_3, \\ x_3 &\to x_3 \end{aligned}$$

Нагата: *Този автоморфизъм е* **див** (т.е. не е питомен), *разглеждан като автоморфизъм на* $(K[x_3])[X_2]$.

Хипотеза на Нагата

Неговият автоморфизъм е **див**, *разглеждан като автоморфизъм на* $K[X_3]$.

Това е една от двете най-важни хипотези за автоморфизмите на полиномните алгебри. Другата хипотеза (от 1939 г., все още нерешена) е:

Хипотеза за якобиана. *Ако матрицата* $J(\varphi) = \left(\frac{\partial \varphi(x_i)}{\partial x_j}\right)$ *на якобиана на един ендоморфизъм* φ *на* $K[X_d]$ *е обратима над* K, *то* φ *е автоморфизъм.*

A. van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture,* Progress in Mathematics, **190**, Birkhäuser Verlag, Basel, 2000.

Теорема на Шестаков-Умирбаев (2002)

Автоморфизмът на Нагата е див, разглеждан като автоморфизъм на $K[X_3]$.

У. У. Умирбаев, И. П. Шестаков, *Подалгебры и автоморфизмы колец многочленов,* Докл. РАН **386** (2002), No. 6, 745-748.

I. P. Shestakov, U. U. Umirbaev, *The Nagata automorphism is wild,* Proc. Natl. Acad. Sci. USA **100** (2003), No. 22, 12561-12563.

I. P. Shestakov, U. U. Umirbaev, *Poisson brackets and two-generated subalgebras of rings of polynomials,* J. Am. Math. Soc. **17** (2004), No. 1, 181-196.

I. P. Shestakov, U. U. Umirbaev, *The tame and the wild automorphisms of polynomial rings in three variables,* J. Am. Math. Soc. **17** (2004), No. 1, 197-227.

Следствие

Ако един автоморфизъм е див като автоморфизъм на $(K[x_3])[X_2]$, *той е див и като автоморфизъм на* $K[X_3]$.

Алгоритъм на Дренски-Ю (2001)

V. Drensky, J.-T. Yu, *Tame and wild coordinates of* $K[z][x, y]$, Trans. Amer. Math. Soc. **353** (2001), 519-537.

Предлага се *алгоритъм, който позволява в полиномиално време да се реши дали даден автоморфизъм на* $K[X_3]$, *който фиксира* x_3, *е див като автоморфизъм на* $(K[x_3])[X_2]$.

Автоморфизъм на Аник на $K\langle X_3\rangle$

Хипотеза. *Автоморфизмът на* $K\langle X_3\rangle$

$$\begin{aligned} x_1 &\to x_1 + x_3(x_1x_3 - x_3x_2), \\ x_2 &\to x_2 + (x_1x_3 - x_3x_2)x_3, \\ x_3 &\to x_3 \end{aligned}$$

е див.

P. M. Cohn, *Free Rings and Their Relations,* 2nd Edition, London Math. Soc. Monographs No. 2, Academic Press, London, 1985, стр. 343.

Теорема на Умирбаев (2007)

Автоморфизмът на Аник е див.

U. U. Umirbaev, *The Anick automorphism of free associative algebras,* J. Reine Angew. Math. **605** (2007), 165-178.

Адитивна примитивна дължина в $K[X_d]$

Теорема (Дренски) *Ако* $d \geq 2$ *и* $f(X_d) \in K[X_d]$, $\deg(f) = n \geq 2$, *то*

$$\operatorname{plength}_+(f) \leq \binom{n+d-1}{d-1}.$$

Идея за докателството за $K[X_2]$

Ако $f(x_1, x_2) \in K[X_2]$ *е примитивен и* $\deg(f) = n > 1$, *то хомогенната компонента от най-висока степен е от вида* $(\alpha_1 x_1 + \alpha_2 x_2)^n$.

Полиномът

$$f(x_1, x_2) = \beta_0 + \beta_1 x_1 + \sum_{i=2}^{n} \xi_i (x_1 + \alpha x_2)^i, \quad \alpha \neq 0,$$

е примитивен.

Фиксираме различни ненулеви елементи $\alpha_0, \alpha_1, \ldots, \alpha_n$ на K и искаме да представим f като линейна комбинация на примитивни полиноми

$$u_0(X_2) = \beta_0 + (\gamma_1 x_1 + \gamma_2 x_2) + \sum_{i=2}^{n} \xi_{0i}(x_1 + \alpha_0 x_2)^i,$$

$$u_p(X_2) = \gamma_{p1} x_1 + \sum_{i=2}^{n} \xi_{pi}(x_1 + \alpha_p x_2)^i, \quad p = 1, \ldots, n,$$

като за u_0 поставяме условието $\gamma_1 x_1 + \gamma_2 x_2$ и $x_1 + \alpha_0 x_2$ да бъдат линейно независими.

Търсим представяне на f във вида

$$f = u_0 + u_1 + \cdots + u_n.$$

За фиксирана степен $i \geq 2$ неизвестните ξ_{pi} са решения на система от линейни уравнения. Тази система винаги има решение, защото редовете на нейната матрица са редове на детерминантата на Вандермонд и следователно са линейно независими.
Лесно можем да подберем коефициентите $\beta_0, \gamma_1, \gamma_2, \gamma_{p1}$, за да изразим афинната част на f чрез афинните части на $u_0, u_1, \ldots, u_n$.

Същата идея за доказателство за $d > 2$

Фиксираме различни ненулеви $\alpha_1, \ldots, \alpha_N$, $N = \binom{n+d-1}{d-1}$, и искаме да представим f като линейна комбинация на

$$\text{афинна част} + \sum_{i=2}^{n} \xi_{pi}(x_1 + \alpha_p x_2 + \alpha_p^{n+1} x_3 + \cdots + \alpha_p^{(n+1)^{p-2}})^i.$$

За фиксирано i неизвесните коефициенти ξ_{pi} са решения на линейна система, която винаги има решение, защото редовете на матрицата са редове на детерминантата на Вандермонд.

Както се вижда, *проблемът за представянето на f като сума на примитивни полиноми е от класа* $\mathbf{P}$.

Свободни метабелеви алгебри на Ли

Нека L_d е d-породената свободна алгебра на Ли. Тя се реализира като най-малкото линейно подпространство на свободната асоциативна алгебра $K\langle X_d\rangle = K\langle x_1, \ldots, x_d\rangle$ (алгебрата на полиномите на d некомутиращи променливи над полето K), което съдържа $X_d = \{x_1, \ldots, x_d\}$ и е затворено относно операцията *комутиране* $[u, v] = uv - vu$.
Подпространството $L'_d = [L_d, L_d]$ е идеал на алгебрата на Ли L_d, наречен *комутаторен идеал*, и е линейната обвивка на комутаторите $[u, v]$, $u, v \in L_d$. По подобен начин дефинираме $L''_d = [L'_d, L'_d]$. Фактор-алгебрата $F_d(\mathfrak{A}^2) = L_d/L''_d$ е *свободната метабелева* (*разрешима от клас* 2) алгебра на Ли.

Примитивни елементи в $F_d(\mathfrak{A}^2)$

Примитивните елементи в $F_d(\mathfrak{A}^2)$ са образите на x_1 под действието на групата $\mathrm{Aut}(F_d(\mathfrak{A}^2))$ от автоморфизмите на $F_d(\mathfrak{A}^2)$.

Групата $\mathrm{Aut}(F_d(\mathfrak{A}^2))$ съдържа подгрупата на *питомните автоморфизми*, породена от *линейните автоморфизми*

$$x_j \to \sum_{i=1}^{d} \alpha_{ij} x_i, \quad j = 1, \ldots, d,$$

където матрицата (α_{ij}) е обратима, т.е. принадлежи на $GL_d(K)$ и *триъгълните автоморфизми*

$$x_j \to \alpha_j x_j + f_j(x_{j+1}, \ldots, x_d), \quad j = 1, \ldots, d.$$

Групата $\mathrm{Aut}(F_d(\mathfrak{A}^2))$ съдържа също *вътрешните автоморфизми* (които са *диви*)

$$x_j \to x_j + [x_j, v], \quad v \in F_d' = [F_d, F_d], j = 1, \ldots, d.$$

Елементите на $F_d'(\mathfrak{A}^2)$ са от вида

$$\sum_i \alpha_i [[x_{i_1}, x_{i_2}], \ldots, x_{i_n}], \quad \alpha_i \in K, i_1 > i_2 \leq \cdots \leq i_n, n \geq 2.$$

Теорема (Ела Айдън)

E. Aydın, *Primitive decomposition of elements of the free metabelian Lie algebra of rank two,* Serdica Math. J. **43** (2017), 369-374.

Нека $f \in F_2(\mathfrak{A}^2)$. Тогава:

- Ако $\deg(f) = 1$, то $\mathrm{plength}_+(f) = 1$;
- Ако $\deg(f) = 2$, то f не може да се представи като сума от примитивни елементи;
- Ако $\deg(f) > 2$, то $\mathrm{plength}_+(f) \leq 3$.

Теорема (Дренски)

Нека $d \geq 3$. Тогава

- $\mathrm{pwidth}_+(F_3(\mathfrak{A}^2)) \leq 6$;
- $\mathrm{pwidth}_+(F_d(\mathfrak{A}^2)) \leq 7$, ако $d \geq 4$.

И в двете теореми представянето като сума от примитивни елементи е ефективно и задачата принадлежи на класа $\mathbf{P}$.

Свободни полинилпотентни алгебри на Ли

Свободната полинилпотентна алгебра на Ли се дефинира като

$$F_d(\mathfrak{N}_c\mathfrak{A}) = L_d/[L_d, l_d]^{c+1}, \quad c \geq 2.$$

Ендоморфизмът φ на $F_d(\mathfrak{N}_c\mathfrak{A})$ е автоморфизъм тогава и само тогава, когато той индуцира автоморфизъм на свободната метабелева алгебра на Ли $F_d(\mathfrak{A}^2)$ (която е хомоморфен образ на $F_d(\mathfrak{N}_c\mathfrak{A})$.)

V. Drensky, *Automorphisms of relatively free algebras,* Comm. Algebra **18** (1990), 4323-4351.

Следствие

Елементът $f \in F_d(\mathfrak{N}_c\mathfrak{A})$ е сума на примитивни елементи тогава и само тогава, когато това свойство се притежава от неговия образ в $F_d(\mathfrak{A}^2)$.

Свободни асоциативни алгебри $K\langle X_d\rangle$, $d \geq 2$

За $d = 2$ всички автоморфизми са питомни и

$$\mathrm{Aut}(K\langle X_2\rangle) \cong \mathrm{Aut}(K[X_2]).$$

Само много специални елементи на $K\langle X_2\rangle$ са суми на примитивни и тогава $plength_+(f) \leq \deg(f) + 1$.

Теорема (Шпильрайн и Ю). *Ако $\alpha x_{i_1} \cdots x_{i_n}$ е моном, който участва в записа на примитивния елемент $u(X_2)$, то мономът $\alpha x_{i_n} \cdots x_{i_1}$ също участва в записа на $u(X_2)$.* С други думи, примитивните елементи са *палиндромни*.

V. Shpilrain, J.-T. Yu, *On generators of polynomial algebras in two commuting or non-commuting variables,* J. Pure Appl. Algebra **132** (1998), No. 3, 309-315.

Нерешени проблеми

- *Да се намерят елементите на* $K\langle X_2\rangle$, *които се представят като сума на примитивни.*
- *Какво става за* $K\langle X_d\rangle$, $d > 2$, *и за* L_d, $d > 2$?
- *Има ли горна граница на* $plength_+(f)$, $f \in K[X_d]$, $d \geq 2$?