

ПРИМЕНЕНИЕ КОНЕЧНОГО ПОЛЯ ПО МОДУЛЮ ПРОСТОГО ЧИСЛА ДЛЯ ВЫЧИСЛЕНИЯ БАЗИСА ГРЁБНЕРА

А. Е. Руденок¹⁾, М. Н. Василевич²⁾

¹⁾ Белорусский государственный университет,
пр. Независимости, 4, 220030, г. Минск, Беларусь, roudenok@bsu.by

²⁾ Белорусский государственный университет,
пр. Независимости, 4, 220030, г. Минск, Беларусь, vasilmn@bsu.by

Рассматривается идеал фокусных величин системы дифференциальных уравнений, называемой системой Куклеса. Для нахождения многообразия этого идеала вычисляется его базис Грёбнера. Вычисление этого базиса в кольце многочленов над полем вещественных чисел представляет большие вычислительные трудности. Показано, как их можно преодолеть, используя вместо кольца многочленов $R[x]$ кольцо многочленов $Z_p[x]$, где Z_p – конечное поле, p – простое число.

Ключевые слова: система Куклеса; идеал ляпуновских величин; базис Грёбнера; конечное поле; модульная арифметика.

Система Куклеса [1] представляет собой систему вида

$$\dot{x} = -y, \quad \dot{y} = x(1 - Ax - Kx^2) - 3xy(B + Lx) + (A - U - Mx)y^2 - Ny^3, \quad (1)$$

где A, B, C, K, L, M, N – вещественные константы.

С 1944 года в течение шестидесяти лет стояла проблема о различении центра и фокуса особой точки $O(0,0)$ этой системы. Для решения этой задачи строится идеал из многочленов над полем рациональных чисел. Эти многочлены называются ляпуновскими величинами [2, с.108]. После их построения находится многообразие этого идеала, которое называется многообразием центра. Это многообразие можно найти, например, вычислением результатов многочленов, составляющих идеал. Этот способ применялся на ранних этапах развития информационных технологий. Современный уровень информационных технологий позволил применять для решения этой задачи базисы Грёбнера, которые были известны с 1965 года [3], но практически не применялись вплоть до 1988 года (версия Wolfram Mathematica 1.0).

Решение задачи о различении центра и фокуса для системы Куклеса было дано независимо Ллойдом и Пирсоном [4] и Садовским [5, 6] с использованием различных методов.

В работе [4] многообразие центра было получено вычислением результатов ляпуновских величин и с использованием суперкомпьютеров Cray-2 вычислительных центров Manchester Computing Centre и Minnesota Supercomputer Center.

В статье [6] приведена программа для ляпуновских величин в пакете Mathematica 4.1. Следует заметить, что в [5] эта программа приведена с опечатками, которые нами исправлены.

```
{z1,z2}={-y, x-A x^2-K x^3-3 B x y-3 L x^2 y+A y^2-U y^2-M x y^2-N y^3};
u=x^2+y^2+Sum[Sum[p[j,i-j]*x^j*y^(i-j),{j,0,i}],{i,3,16}];
D[u,x]*z1+D[u,y]*z2-Sum[g[i-1](x^2+y^2)^i,{i,2,8}];
CoefficientList[%/.{x->x*s,y->y*s},s];
Do[w[i]=CoefficientList[w[i],y]/.x->1,{i,3,16}];
Do[t[2*i+1]=Solve[Table[w[2*i+1][[j]]==0,{j,1,2*i+2}],Table[p[j,2*i+1-j],{j,0,2*i+1}]]][[1]],{i,1,7}]
```

```

Do[t[2*i+2]=Solve[Table[w[2*i+2][[j]]==0,{j,1,2*i+3}],Union[Table[p[j,2*i+2-j],
{j,1,2*i+2}],{g[i]}]][[1]],{i,1,7}]
Do[p[0,2*j]=0,{j,2,7}]
Do[Do[g[i]=Expand[g[i]/.t[2*i+3-j]],{j,1,2*i}],{i,1,7}]
Do[g[i]=Factor[g[i]],{i,1,7}]

```

Используя эту программу А.П. Садовский вычислил первые шесть ляпуновских величин системы Куклеса. Многообразие идеала, образованное этими многочленами он нашел с помощью результатов. Необходимо отметить сложность вычислений этих результатов, степени которых достигали 996.

Во всех этих работах авторам не удалось найти базис Грёбнера идеала. Впервые его вычислил А.Е. Руденко (см. монографию [2], с. 138). В монографии [2] А.П. Садовский построил идеал, образующие которого состоят из 7 ляпуновских величин. Сам базис Гребнера содержит 57 многочленов. Громоздкость этого базиса не позволила найти непосредственно из него многообразие центра.

Ниже мы приведем идеал J , образованный из первых шести ляпуновских величин системы (1) [7]. Первые три члена идеала J состоят из полиномов:

$$1) ABK - ABM - 6B^2N - 3KN - MN + 2A^2BU + 6B^3U + 7BKU + 3BMU - 2ANU + 3ABU^2 - 3NU^2;$$

$$2) 6A^3BK + 15AB^3K + 11ABK^2 - 6A^3BM - 15AB^3M - 3ABKM - 6ABM^2 - 36A^2B^2N - 90B^4N - 14A^2KN - 93B^2KN - 12K^2N - 2A^2MN - 45B^2MN - 11KMN - 3M^2N + 6ABN^2 - 6N^3 + 12A^4BU + 66A^2B^3U + 90B^5U + 54A^2BKU + 153B^3KU + 56BK^2U + 32A^2BMU + 75B^3MU + 47BKMU + 15BM^2U - 12A^3NU - 6AB^2NU + 10AKNU + 12AMNU + 96BN^2U + 8A^3BU^2 + 15AB^3U^2 - 22ABKU^2 - 15ABMU^2 - 8A^2NU^2 - 135B^2NU^2 - 59KNU^2 - 30MNU^2 - 30A^2BU^3 + 15BKU^3 + 30ANU^3;$$

$$3) 45A^5BK + 240A^3B^3K + 315AB^5K + 158A^3BK^2 + 450AB^3K^2 + 159ABK^3 - 45A^5BM - 240A^3B^3M - 315AB^5M - 35A^3BKM - 150AB^3KM + 20ABK^2M - 101A^3BM^2 - 240AB^3M^2 - 74ABKM^2 - 45ABM^3 - 270A^4B^2N - 1440A^2B^4N - 1890B^6N - 91A^4KN - 1290A^2B^2KN - 3105B^4KN - 157A^2K^2N - 1350B^2K^2N - 99K^3N - A^4MN - 720A^2B^2MN - 1575B^4MN - 155A^2KMN - 1200B^2KMN - 114K^2MN - 46A^2M^2N - 360B^2M^2N - 64KM^2N - 15M^3N + 66A^3BN^2 - 180AB^3N^2 - 21ABKN^2 - 255ABMN^2 - 42A^2N^3 - 990B^2N^3 - 153KN^3 - 75MN^3 + 90A^6BU + 750A^4B^3U + 2070A^2B^5U + 1890B^7U + 499A^4BKU + 2970A^2B^3KU + 4365B^5KU + 1004A^2BK^2U + 3150B^3K^2U + 735BK^3U + 381A^4BMU + 1860A^2B^3MU + 2205B^5MU + 985A^2BKMU + 2760B^3KMU + 824BK^2MU + 479A^2BM^2U + 840B^3M^2U + 416BKM^2U + 105BM^3U - 90A^5NU + 36A^3B^2NU + 810AB^4NU + 86A^3KNU + 624AB^2KNU - 44AK^2NU + 68A^3MNU + 1740AB^2MNU + 502AKMNU + 240AM^2NU + 1098A^2BN^2U + 6030B^3N^2U + 3237BKN^2U + 1635BMN^2U + 90AN^3U - 19A^5BU^2 - 162A^3B^3U^2 - 315AB^5U^2 - 420A^3BKU^2 - 1098AB^3KU^2 - 266ABK^2U^2 - 387A^3BMU^2 - 1260AB^3MU^2 - 873ABKMU^2 - 420ABM^2U^2 + 19A^4NU^2 - 1836A^2B^2NU^2 - 5985B^4NU^2 - 1053A^2KNU^2 - 6204B^2KNU^2 - 916K^2NU^2 - 618A^2MNU^2 - 3150B^2MNU^2 - 972KMNU^2 - 315M^2NU^2 - 1335ABN^2U^2 - 495N^3U^2 - 386A^4BU^3 - 1050A^2B^3U^3 + 65A^2BKU^3 + 420B^3KU^3 - 59BK^2U^3 - 210A^2BMU^3 + 386A^3NU^3 + 1890AB^2NU^3 + 1184AKNU^3 + 840AMNU^3 + 1260BN^2U^3 + 315A^3BU^4 - 525ABKU^4 - 315A^2NU^4 + 210KNU^4.$$

Остальные три образующих идеала J мы не приводим из-за их громоздкости, в частности, степень шестого члена идеала равна $\{6, 6, 7, 7, 12, 13\}$ по переменным $\{K, M, N, U, A, B\}$ соответственно и состоит из 9097 слагаемых.

Мы вычисляли базис Грёбнера этого идеала в кольце многочленов над полем вещественных чисел. Даже использование процессора Intel 14-го поколения (5.6 ГГц) и пакета Mathematica 14 потребовали длительных вычислений (12 дней). Можно преодолеть эти трудности,

используя вместо кольца многочленов $R[x]$ кольцо многочленов $Z_p[x]$, где Z_p – конечное поле, p – простое число. Мы использовали $p = 100003$. Удивительно, что вычисление базиса Грёбнера таким способом заняло 3 часа. Первый член вычисленного базиса в кольце многочленов $Z_p[x]$ имеет вид:

$$A^5U^6(100002N+BU)(A^2+25003B^2)(A+14241B)^3(A+85762B)^3 \times \\ \times (A^3B^3+2AB^5+100000A^2B^2N+99999B^4N+3ABN^2+100002N^3) \times \\ \times (A^5+4A^3B^2+4AB^4+2A^4U+12A^2B^2U+16B^4U+A^3U^2)$$

Для восстановления базиса в кольце многочленов $R[x]$ мы использовали алгоритм [8, 9], который восстанавливает числа из модульной арифметики в обычную арифметику:

Algorithm Rational Reconstruction (RR).

Input: Integers m, u, N, D with $m > u \geq 0$, $N, D > 0$ and $2ND < m$.

Output: Either $n, d \in \mathbb{Z}$ s.t. $|n| \leq N$, $0 < d \leq D$, $\gcd(n, d) = 1$, and $n/d \equiv u \pmod{m}$, or FAIL implying no such rational n/d exists.

Set $(r_0, t_0) = (m, 0)$.

Set $(r_1, t_1) = (u, 1)$.

While $r_1 > N$ do

 Set $q = \lfloor r_0/r_1 \rfloor$

 Set $(r_0, r_1) = (r_1, r_0 - q r_1)$.

 Set $(t_0, t_1) = (t_1, t_0 - q t_1)$.

Set $(n, d) = (r_1, t_1)$.

If $d < 0$ then set $(n, d) = (-n, -d)$.

If $d \leq D$ and $\gcd(n, d) = 1$ then output (n, d) .

Otherwise output FAIL.

Восстановленный с помощью этого алгоритма первый член базиса в кольце многочленов $R[x]$ имеет вид:

$$A^5U^6(-N+BU)(A^2+9/4B^2)(A+21/316B)^3(A-21/316B)^3 \times \\ \times (A^3B^3+2AB^5-3A^2B^2N-4B^4N+3ABN^2-N^3) \times \\ \times (A^5+4A^3B^2+4AB^4+2A^4U+12A^2B^2U+16B^4U+A^3U^2)$$

Библиографические ссылки

1. Куклес И.С. О некоторых случаях отличия фокуса от центра // Докл. АН СССР. 1944. Т. 42. № 5. С. 208-211.
2. Садовский А.П. Полиномиальные идеалы и многообразия. Минск: БГУ, 2008.
3. Buchberger B. Ein Algorithmus zum auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. PhD thesis. Innsbruck, 1965.
4. Lloyd N. G., Pearson J. M. Computing centre conditions for certain cubic systems // J. Comp. Appl. Math. 1992. V. 40. № 3. P. 323-336.
5. Садовский А. П. Решение проблемы центра и фокуса для кубической системы нелинейных колебаний // Дифференц. уравнения. 1997. Т. 33. № 2. С. 236-244.
6. Садовский А. П. Кубические системы нелинейных колебаний с семью предельными циклами // Дифференц. уравнения. 2003. Т. 39. № 4. С. 472-481.
7. Руденок А. Е., Василевич М. Н. О базисе Грёбнера идеала ляпуновских величин системы Куклеса // Дифференц. уравнения. 2023. Т. 59. № 2. С. 170-182.
8. Wang P. S., Guy M. J. T., Davenport J. H. P-adic Reconstruction of Rational Numbers. SIGSAM Bulletin. 1982. V. 16. № 2. P. 2-3.
9. Monagan M. B. Maximal quotient rational reconstruction: an almost optimal algorithm for rational reconstruction // Proceedings of the 2004 International Symposium on Symbolic and Algebraic Computation. 2004. P. 243-249.