Записки научных
семинаров ПОМИ
Том 439, 2015 г.

Х. Д. Икрамов

КАК ПРОВЕРИТЬ КОНГРУЭНТНОСТЬ ЗАДАННЫХ КВАДРАТНЫХ МАТРИЦ?

1. Пусть A и B – квадратные матрицы порядка n с элементами из поля $\mathbf{Q}$ или $\mathbf{Q}(i)$ (поля рациональных гауссовых чисел). Как проверить возможное подобие этих матриц над $\mathbf{C}$?

Классический критерий подобия матриц A и B – это тождество их жордановых форм. Однако построение жордановой формы предполагает предварительное вычисление собственных значений. Хорошо известно, что собственные значения матрицы порядка n ($n > 4$) в общем случае нельзя найти посредством конечного алгоритма, использующего лишь арифметические операции и радикалы.

И все же проверить, будут ли A и B подобны, можно с помощью конечного числа арифметических операций, не прибегая к радикалам. Вычислительный процесс с этими свойствами, – конечность и использование только арифметических операций, – будем называть *рациональным*.

Опишем один из возможных рациональных алгоритмов для проверки подобия заданных матриц A и B. (О других рациональных подходах к этой задаче см. [1, §3.4].) Пусть

$$(\lambda - \lambda_1)^{s_1}, (\lambda - \lambda_2)^{s_2}, \ldots, (\lambda - \lambda_k)^{s_k}$$

и

$$(\lambda - \mu_1)^{t_1}, (\lambda - \mu_2)^{t_2}, \ldots, (\lambda - \mu_l)^{t_l}$$

суть элементарные делители A и B над полем $\mathbf{C}$. Сопоставим паре (A, B) однородное матричное уравнение

$$AX - XB = 0. \tag{1}$$

Ключевые слова: конгруэнции, каноническая форма, подобие, жорданова форма, коквадрат.

Формула для числа $N_{A,B}$ линейно независимых решений этого уравнения выведена в [2, гл. VIII, §1]:

$$N_{A,B} = \sum_{i=1}^{k} \sum_{j=1}^{l} \delta_{ij},$$

где δ_{ij} обозначает степень наибольшего общего делителя многочленов $(\lambda - \lambda_i)^{s_i}$ и $(\lambda - \mu_j)^{t_j}$.

Наряду с $N_{A,B}$ рассмотрим числа $N_{A,A}$ и $N_{B,B}$, дающие размерности подпространств матриц, перестановочных соответственно с A и B:

$$AX - XA = 0, \qquad BX - XB = 0.$$

В [3] сформулирован следующий критерий подобия: $n \times n$-матрицы A и B подобны тогда и только тогда, когда они имеют один и тот же характеристический многочлен и

$$N_{A,A} = N_{B,B} = N_{A,B}. \tag{2}$$

Хотя формально все эти три числа определяются через элементарные делители заданных матриц, их можно найти посредством рациональных вычислений. Рассмотрим, к примеру, число $N_{A,B}$. Матричное уравнение (1) можно интерпретировать как систему из n^2 линейных однородных уравнений относительно n^2 элементов неизвестной матрицы X. Матрицей коэффициентов этой системы является так называемая кронекерова разность матриц A и B:

$$A \otimes I_n - I_n \otimes B^T.$$

Составив эту разность и вычислив ее ранг $r_{A,B}$, получим требуемую в (2) характеристику

$$N_{A,B} = n^2 - r_{A,B}.$$

Диксон [4] указал, что первое условие сформулированного выше критерия (о совпадении характеристических многочленов) излишне. Он же отметил, что равенства (2) можно заменить единственным соотношением

$$r_{A,B}^2 = r_{A,A} r_{B,B}.$$

Описанный алгоритм заодно объясняет причину введенного ограничения на природу элементов заданных матриц: проверки на точное равенство нулю промежуточных результатов метода, вообще говоря, невозможны для матриц с произвольными комплексными или вещественными элементами.

Итак, подобие между A и B (или его отсутствие) можно установить посредством рациональной процедуры. В данной заметке нас интересует, останется ли этот вывод справедливым, если вместо подобий рассматривать матричные преобразования другого типа, а именно *конгруэнции*. Существуют два типа конгруэнтных преобразований комплексных матриц. Это, во-первых, *-конгруэнции, т.е. преобразования вида

$$A \mapsto Q^* A Q, \tag{3}$$

и, во-вторых, T-конгруэнции

$$A \mapsto Q^T A Q. \tag{4}$$

В обеих формулах (3) и (4) Q – произвольная невырожденная матрица.

Вопрос о проверке конгруэнтности заданных матриц будет исследован в предположении, что эти матрицы невырожденны. При таком ограничении проверка T-конгруэнтности сводится к проверке подобия сопутствующих матриц (см. раздел 2). В случае *-конгруэнций ситуация значительно сложнее, и рациональную процедуру для проверки *-конгруэнтности нам удается предложить лишь при некотором дополнительном ограничении. Это ограничение связано с видом канонической формы матриц относительно *-конгруэнций. Оно формулируется в разделе 3; там же описан рациональный алгоритм, проверяющий выполнение этого условия.

2. Сопоставим (невырожденным) матрицам A и B их *коквадраты* C_A и C_B. Так названы в [1, §4.5] матрицы

$$C_A = A^{-T} A \quad \text{и} \quad C_B = B^{-T} B. \tag{5}$$

Там же (см. [1, теорема 4.5.27]) находим следующее утверждение.

Теорема 1. *Для конгруэнтности невырожденных $n \times n$-матриц A и B необходимо и достаточно, чтобы были подобны их коквадраты C_A и C_B.*

Отсюда следует, что проверка T-конгруэнтности матриц A и B может быть осуществлена посредством такой двухшаговой (и рациональной) процедуры:

(i) Построить коквадраты C_A и C_B в соответствии с (5).

(ii) Проверить подобие матриц C_A и C_B, используя, например, рациональный алгоритм, описанный в разделе 1.

3. В случае *-конгруэнций мы также привлекаем коквадраты матриц A и B. Вместо (5) они определяются теперь формулами

$$C_A = A^{-*}A \quad \text{и} \quad C_B = B^{-*}B. \tag{6}$$

Если квадратная матрица M подвергается конгруэнции

$$M \to \tilde{M} = X^* M X,$$

то

$$M^{-1} \to \tilde{M}^{-1} = X^{-1} M^{-1} X^{-*}$$

и

$$S_M = M^{-*}M \to S_{\tilde{M}} = X^{-1} S_M X,$$

т.е. коквадрат матрицы M претерпевает подобие, задаваемое той же матрицей X. Неудивительно поэтому, что каноническая форма матрицы M относительно конгруэнций тесно связана с жордановой формой ее коквадрата.

Связь эта такова. В канонической форме невырожденной матрицы M, представляющей собой блочно-диагональную матрицу, могут присутствовать диагональные блоки только двух типов. Это, во-первых, ганкелевы матрицы вида

$$\Delta_k = \lambda \begin{pmatrix} & & & 1 \\ & & \cdots & i \\ & 1 & \cdots & \\ 1 & i & & \end{pmatrix}, \tag{7}$$

где $|\lambda| = 1$, а индекс k указывает порядок матрицы, и, во-вторых, блоки четной размерности

$$H_{2k}(\mu) = \begin{pmatrix} 0 & I_k \\ J_k(\mu) & 0 \end{pmatrix}. \tag{8}$$

Здесь $J_k(\mu)$ – жорданова клетка с числом μ на главной диагонали, а относительно μ можно без ограничения общности считать, что $|\mu| > 1$.

Легко проверить, что коквадратом матрицы (8) является прямая сумма

$$J_k(\mu) \oplus J_k(\mu)^{-*}.$$

Отсюда можно вывести, что блоки вида (8) в канонической форме матрицы M находятся во взаимно однозначном соответствии с парами жордановых клеток вида

$$J_k(\mu) \oplus J_k(\bar{\mu}^{-1})$$

в жордановой форме ее коквадрата.

Коквадрат матрицы (7), где $\lambda = e^{i\phi}$, – это верхнетреугольная теплицева матрица с числом $e^{2i\phi}$ на главной диагонали и числом $2ie^{2i\phi}$ на первой наддиагонали (см. [5, задача 4.5.P15]). Такая матрица подобна жордановой клетке $J_k(\lambda^2)$.

Блоки вида (7) также находятся во взаимно однозначном соответствии с жордановыми клетками вида $J_k(\lambda^2)$ в жордановой форме коквадрата.

Соотношения между канонической формой M и жордановой формой матрицы C_M можно описать так:

(i) знание канонической формы матрицы M однозначно определяет жорданову форму ее коквадрата;

(ii) жорданова форма J коквадрата C_M *не* определяет однозначно каноническую форму матрицы M, если C_M имеет собственные значения, по модулю равные единице.

Второе соотношение заставляет нас наложить на матрицы A и B следующее ограничение: их коквадраты не должны иметь собственных значений с модулем 1. Будем называть это ограничение условием 2, имея в виду, что условием 1 была невырожденность обеих матриц.

Если условие 2 выполнено, то теорема из предыдущего раздела сохраняет справедливость. Остается в силе и предложенный там алгоритм проверки конгруэнтности. Разумеется, коквадраты вычисляются теперь по формулам (6) и речь идет о *-конгруэнтности.

Остается обсудить вопрос о том, можно ли с помощью рациональной процедуры проверить условие 2. Для определенности будем говорить о матрице A.

Нам потребуется минимальный многочлен $a(\lambda)$ коквадрата $C_A = A^{-*}A$. Его можно найти, например, так: строится последовательность натуральных степеней C_A^k до тех пор, пока очередная матрица C_A^m не станет впервые линейной комбинацией предыдущих степеней

$$I, C_A, C_A^2 \dots, C_A^{m-1}.$$

Если при этом

$$C_A^m = a_1 C_A^{m-1} + a_2 C_A^{m-2} + \dots + a_{m-1} C_A + a_m I,$$

то

$$a(\lambda) = \lambda^m - a_1\lambda^{m-1} - a_2\lambda^{m-2} - \dots - a_{m-1}\lambda - a_m. \qquad (9)$$

Этот метод вычисления минимального многочлена, по всей видимости, не является оптимальным. Однако очевидно, что он рационален в принятом нами смысле.

Прямой подстановкой $\lambda = -i$ в (9) выясним, не является ли точка $-i$ корнем $a(\lambda)$. Если $a(-i) = 0$, то условие 2 для матрицы A нарушено и проверка конгруэнтности A и B выбранным нами способом невозможна.

Пусть $a(-i) \neq 0$. Выполним в (9) замену переменного

$$\lambda = \frac{z-i}{z+i},$$

переводящую единичную окружность плоскости λ в вещественную ось на плоскости z. Эта замена превращает $a(\lambda)$ в рациональную функцию

$$\phi(z) = \frac{f(z)}{(z+i)^m},$$

где $f(z)$ – многочлен степени m. Отсутствие у $a(\lambda)$ корней с модулем 1 транслируется в условие: $f(z)$ не должен иметь вещественных корней.

Представим в алгебраической форме

$$f_j = g_j + ih_j \tag{10}$$

каждый коэффициент многочлена

$$f(z) = f_0 z^m + f_1 z^{m-1} + \cdots + f_{m-1} z + f_m.$$

Представления (10) определяют многочлены с вещественными коэффициентами

$$g(z) = g_0 z^m + g_1 z^{m-1} + \cdots + g_{m-1} z + g_m$$

и

$$h(z) = h_0 z^m + h_1 z^{m-1} + \cdots + h_{m-1} z + h_m.$$

Хотя бы один из них имеет степень m.

Ясно, что вещественное число x тогда и только тогда будет корнем многочлена f, когда x является общим корнем многочленов g и h и, следовательно, корнем их наибольшего общего делителя. Поэтому следующий шаг нашей процедуры – это вычисление НОД(g, h), для чего можно использовать алгоритм Евклида, который также рационален.

Если многочлены g и h оказались взаимно простыми, наша проверка закончена: $f(z)$ не имеет вещественных корней, а матрица C_A не имеет собственных значений, по модулю равных единице.

Предположим теперь, что многочлен $d(z) = \text{НОД}(g, h)$ имеет положительную степень. Нужно выяснить, есть ли у этого многочлена вещественные корни.

Если d – многочлен нечетной степени, то хотя бы один вещественный корень у него имеется. В этом случае наша проверка снова закончена, но теперь итог отрицателен: для матрицы A требуемое условие не выполнено.

Пусть теперь d – многочлен четной степени r. Существование у него вещественных корней или их отсутствие можно установить, например, с помощью метода Якоби. Обозначим через $z_1, \ldots, z_r$ корни многочлена d, а через s_l – степенные суммы этих корней:

$$s_l = z_1^l + z_2^l + \cdots + z_r^l, \quad l = 0, 1, 2, \ldots .$$

Хорошо известно, что суммы s_l $(1 \leqslant l < r)$ могут быть выражены через коэффициенты многочлена d, а, начиная с индекса r, эти суммы связаны линейным рекуррентным соотношением порядка r.

Составим квадратичную форму

$$J = \sum_{i,j=0}^{r-1} s_{i+j} x_i x_j .$$

Пусть π и ν – положительный и отрицательный индексы инерции этой формы. Согласно теореме Якоби, многочлен $d(z)$ имеет $\pi - \nu$ различных вещественных корней. (Напомним, что разность $\pi - \nu$ называется сигнатурой формы J.)

Итак, если $\pi \neq \nu$, то вещественных корней $f(z)$ не имеет, а условие 2 для матрицы A выполнено. Проверка для A закончена, и можно перейти к аналогичной проверке для B.

В заключение отметим, что условие 2 не является искусственным. Для любой эрмитовой матрицы H ее коквадрат есть единичная матрица, все собственные значения которой равны единице. Между тем *-конгруэнтны лишь те эрмитовы матрицы, что имеют одинаковые индексы инерции.

Литература

1. Х. Д. Икрамов, *О конечных спектральных процедурах в линейной алгебре.* — Программирование (1994), No. 1, 56–69.
2. Ф. Р. Гантмахер, *Теория матриц.* Наука, М., 1966.

3. M. A. Gauger, C. I. Byrnes, *Characteristics free, improved decidability criteria for the similarity problem.* — Linear and Multilinear Algebra **5** (1977), 153–158.
4. J. D. Dixon, *An isomorphism criterion for modules over a principal ideal domain.* — Linear and Multilinear Algebra **8** (1979), 69–72.
5. R. A. Horn, C. R. Johnson, *Matrix Analysis. Second edition.* Cambridge University Press, Cambridge, 2012.

Ikramov Kh. D. How to check whether given square matrices are congruent.

Let A and B be square nonsingular n-by-n matrices with entries being rational or rational Gaussian numbers. We describe a method for verifying whether these matrices are congruent. The method uses a finite number of arithmetic operations (and, in the complex case, conjugation operations).

Московский государственный университет
Ленинские горы,
119991 Москва, Россия
E-mail: ikramov@cs.msu.su

Поступило 4 сентября 2015 г.