EXTRACTA MATHEMATICAE Vol. 11, Núm. 3, 475 – 479 (1996)

Un Algoritmo de Descomposición de Funciones Racionales mediante Polinomios Casi-separados *

CESAR ALONSO [1], JAIME GUTIÉRREZ [2] AND TOMÁS RECIO [2]

[1] *Centro de Inteligencia Artifial, Departamento de Matemáticas*
Universidad de Oviedo, 33271-*Oviedo, Spain*
[2] *Departamento de Matemática Estadística y Computación,*
Universidad de Cantabria, 39071-*Santander, Spain*

(Research announcement)

AMS *Subject Class.* (1991): 12Yxx, 14Qxx

Received April 3, 1995

Dado un polinomio f perteneciente a $\mathbb{K}[x]$, determinar si existen otros dos g y h de grado mayor que uno tales que $f(x) = g(h(x)) = g \circ h$, y, en caso de que existan, encontrarlos, es conocido como problema de descomposición para polinomios. Cuando dicha descomposición existe, problemas como la evaluación de f en un punto o la resolución de la ecuación $f = 0$ se pueden resolver de manera más simple.

La generalización del problema de la descomposición al caso de funciones racionales es sin duda un problema más difícil. La descomposición de funciones racionales ha sido estudiada ya en [10] y en [8]. Recientemente, en [11] se presenta el primer algoritmo en tiempo polinomial para la descomposición de funciones racionales. No obstante dicho algoritmo requiere en uno de sus pasos la factorización de un polinomio sobre un cuerpo de funciones algebraicas. El propio Zippel comenta acerca de su algoritmo, que sería muy difícil descomponer funciones racionales de grado superior a 10.

Nosotros presentamos en esta breve nota un algoritmo para la descomposición de funciones racionales siguiendo la idea de Barton&Zippel en [4] para el caso de polinomios. Aunque nuestro algoritmo requiere en principio un número exponencial, en el grado de f, de operaciones en el cuerpo $\mathbb{K}$, resulta en la práctica más eficiente que el de Zippel, pues se pueden descomponer funciones racionales de grado mucho mayor que la cota por él estimada. Finalmente ponemos de manifiesto que el presente trabajo constituye un extracto de una parte de [2] que ha aparecido recientemente.

*Parcialmente subvencionado por TIC-1026-CE y Esprit Bra-POSSO. 6846.

1. Sea $\mathbb{K}$ un cuerpo arbitrario. Denotaremos por $\mathbb{K}(x)$ al cuerpo de las funciones racionales y por S al conjunto de las funciones racionales no constantes. Consideraremos en S la operación de la composición (denotada por $\circ$) respecto de la cual S es un semigrupo con identidad x. El grupo de las unidades en S serán las funciones racionales de la forma $(ax+b)/(cx+d)$ tales que $ad-cb \neq 0$, y su inversa es $(dx-b)/(-cx+a)$.

1.1. Hechas estas consideraciones, diremos que $f \in S$ es indescomponible si no es una unidad y toda expresión de la forma $f = g \circ h$ con g y h en S, implica que ó bien g ó bien h es unidad.

1.2. Una descomposición de f es un conjunto de funciones racionales $f_1, \ldots, f_r \in S$ tales que $f = f_1 \circ \cdots \circ f_r$. A las f_i se les denomina componentes de la descomposición y ésta se dice completa si las componentes son indescomponibles.

1.3. Dos descomposiciones de $f = f_1 \circ \cdots \circ f_r = g_1 \circ \cdots \circ g_s$ se dicen equivalentes, si $r = s$ y existen unidades $u_1, \ldots, u_{r-1}$ tales que : $g_1 = f_1 \circ u_1$, $g_j = u_{j-1}^{-1} \circ f_j \circ u_j$ $(1 < j < r)$ y $g_r = u_{r-1}^{-1} \circ f_r$.

Entre las múltiples propiedades de la descomposición de funciones racionales mencionaremos las siguientes:

(i) El grado es multiplicativo respecto a la composición. Por grado de una función racional entenderemos el máximo de los grados del numerador y denominador de su forma reducida.

(ii) $f \in S$ es una unidad si y sólo si su grado es 1.

(iii) Si $f, h \in S$ y $f = g \circ h$, entonces g está unívocamente determinada por f y h.

(iv) Una función racional de grado primo es indescomponible.

(v) Toda función racional de grado mayor que uno posee una descomposición completa.

(vi) Para toda función racional f existe una unidad u tal que $\overline{f} = u \circ f$ y $\overline{f}(0) = 0$.

2. Como herramienta fundamental en nuestro algoritmo de descomposición de funciones racionales, introducimos el concepto de polinomio casi-separado. Un polinomio en dos variables $a(x,y) \in \mathbb{K}[x,y]$ es casi-separado, si existen otros dos polinomios univariados r, s en $\mathbb{K}[x]$ primos entre sí, tales que

$a(x,y) = r(y)s(x) - r(x)s(y)$. Es fácil ver a partir de esta definición, que un polinomio casi-separado no tiene factores univariados. Como resultado clave para la confección de nuestro algoritmo tenemos:

PROPOSICIÓN 1. *Sea $\mathbb{K}$ un cuerpo arbitrario y sean $f = f_n/f_d, h = h_n/h_d$ dos funciones racionales no constantes y en forma prima en $\mathbb{K}(x)$. Entonces el polinomio en dos variables $h_n(y)h_d(x) - h_n(x)h_d(y)$ divide a $f_n(y)f_d(x) - f_n(x)f_d(y)$ si y sólo si $f = g \circ h$ para alguna función racional $g \in \mathbb{K}(x)$.*

Esta proposición generaliza un resultado análogo para polinomios, que es bien conocido por los especialistas (véase [6], [5], [7] ó [3]). La demostración de esta proposición puede verse en [2].

3. Nuestro algoritmo de descomposición está basado en la proposición 1 enunciada anteriormente. y consta de los siguientes pasos:

ALGORITMO.

INPUT: $f = f_n/f_d \in \mathbb{K}(x)$.

OUTPUT: Una descomposición completa de $f = g_1 \circ \cdots \circ g_s$.

D1. [Inicialización] Sean $\overline{g}_0(x) = x$, $i = 1$, $\quad \overline{g}_i(x) = \dfrac{\overline{g}_{in}(x)}{\overline{g}_{id}(x)}$.

D2. [Factorización] Factorizar $f_n(y)f_d(x) - f_n(x)f_d(y)$ sobre $\mathbb{K}[y,x]$ en componentes irreducibles:

$$a_0(y,x) = y - x,\ a_1(y,x),\ a_2(y,x), \ldots, a_r(y,x)\,.$$

D3. [Búsqueda de candidatos] Encontrar el polinomio casi-separado de grado mínimo, que sea producto de $a_j(y,x)$'s y múltiplo de $\overline{g}_{(i-1)n}(y)\overline{g}_{(i-1)d}(x) - \overline{g}_{(i-1)n}(x)\overline{g}_{(i-1)d}(y)$. Denotemos este polinomio por:

$$\overline{g}_{in}(y)\overline{g}_{id}(x) - \overline{g}_{in}(x)\overline{g}_{id}(y)\,.$$

D4. [Determinación de componentes a izquierda] Planteamos y resolvemos un sistema lineal cuyas indeterminadas serán los coeficientes de la función racional $g_i(x)$ tal que:

$$\overline{g}_i(x) = g_i(\overline{g}_{i-1}(x))\,.$$

D5. Si $\overline{g}_i(x) = f(x)$, entonces $f(x) = g_i(x) \circ \cdots \circ g_1(x)$. En otro caso incrementamos i en una unidad y repetimos todo desde D3.

Un análisis detallado de este algoritmo es bastante difícil, especialmente si lo confrontamos con la experiencia práctica. En el caso peor el algoritmo es exponencial en el grado de la función racional f. No obstante, en la práctica parece que la mayor parte del tiempo se emplea en el paso D2.

Presentamos ahora un ejemplo de la implementación en el paquete de cálculo simbólico Maple V de nuestro algoritmo, realizado en un Macintosh Centrix 650. Obsérvese que se descomponen de manera efectiva funciones racionales de grado superior a la cota estimada por Zippel.

EJEMPLO 2.

INPUT:

$$f(x) = \frac{x^{24} + x^{16} + x^8 + 1}{x^8(x^8 + 2x^4 + 1)}$$

OUTPUT:

$$\left[\frac{2x^2 - 1}{x^2(2x - 1)}, \frac{x^2}{2x^2 - 1}, \frac{x^2}{2x^2 - 1}, \frac{-x}{x^2 + 1}\right]$$

Computing time: 202.58 s. Words: 1017233.

4. Entre las múltiples aplicaciones de la descomposición de funciones racionales, queremos hacer hincapié en una aplicación muy particular: el cálculo de subcuerpos de $\mathbb{K}(x)$. Dado $f = f_n/f_d \in \mathbb{K}(x)$, estamos interesados en encontrar todos los cuerpos intermedios $\mathbb{F}$, con $\mathbb{K}(f) \subset \mathbb{F} \subset \mathbb{K}(x)$. Este es un clásico problema de Álgebra como se menciona en [9]. Sabemos que hay sólo un número finito de dichos cuerpos intermedios, ya que es conocido, aplicando el teorema de Luroth, que cada uno de ellos está generado por una función racional $h(x)$ en $\mathbb{K}(x)$. Así pues $f = g \circ h$, con lo que las componentes a derecha de f llevan a generadores de estos cuerpos intermedios. Existen solamente un número finito de componentes a derecha de f ya que, según se puso de manifiesto en la proposición 1, cada una de ellas viene determinada por un factor casi-separado del polinomio $f_n(y)f_d(x) - f_n(x)f_d(y)$.

Consideremos la función racional del ejemplo 2,

$$f(x) = \frac{x^{24} + x^{16} + x^8 + 1}{x^8(x^8 + 1 + 2x^4)}.$$

Existen ocho cuerpos entre $\mathbb{K}(x)$ y $\mathbb{K}(f(x))$. Dichos cuerpos están generados por las siguientes funciones racionales:

$$\left\{\frac{x}{1 - x^2}, x^2, \frac{-x}{1 + x^2}, \frac{-x^2}{1 + x^4}, x^4, \frac{x^2}{1 - x^4}, \frac{-x^4}{1 + x^8}, \frac{x^4(1 + x^4)}{1 - x^{12}}\right\}.$$

Mediante la proposición 1 aplicada dos a dos a los generadores de los cuerpos intermedios del ejemplo anterior, podemos computar la relación de orden entre ellos dada por la inclusión (observar que si $f = g \circ h$, entonces $\mathbb{K}(f) \subset \mathbb{K}(h)$). Obtenemos así el retículo ordenado de todos los cuerpos intermedios. A partir de dicho retículo, podemos obtener todas las descomposiciones completas no equivalentes de la función f. En el caso que nos ocupa se puede ver que f posee seis descomposiciones no equivalentes.

Todos estos cálculos se han realizado utilizando el paquete FRAC consistente en una serie de procedimientos implementados en Maple V (véase [3] y también [1]).

Bibliografía

[1] Alonso, C., Gutiérrez, J., Recio, T., FRAC: A Maple package for computing in the rational function field $\mathbb{K}(x)$, en "Proc. of Maple Summer Workshop and Symposium", Troy, New York. Birkhauser, 1994, 107–115.

[2] Alonso, C., Gutiérrez, J., Recio, T., A rational function decomposition algorithm by near-separated polynomials, *J. of Simbolic Computation* **19** (1995), 527–544.

[3] Alonso, C., "Análisis, Implementacián y Desarrollo de Algoritmos para la Manipulacián de Variedades Paramétricas", Tesis Doctoral, Universidad de Cantabria, Santander, 1994.

[4] Barton, R., Zippel, R., Polynomial decomposition algorithms, *J. of Symbolic Computation* **1** (1985), 159–168.

[5] Dorey, M.D., Whaples, G., Prime and composite polynomials, *J. of Algebra* **28** (1974), 88–101.

[6] Evyatar, A., Scott, D., On polynomials in a Polynomial, *Bull. London Math. Society* **4** (1972), 176–178.

[7] Fried, M.D., Macrae, R., On curves with separated variables, *Math. Ann.* **180** (1969), 220–226.

[8] Fried, M.D., Arithmetic properties of functions fields (II), The generalized Schur problem, *Acta Arithmetica* **XXV** (1974), 225–258.

[9] Helmke, U., The variety of subfields of $\mathbb{K}(x)$, *Comm. in Algebra* **18** (11) (1990), 3775–3789.

[10] Ritt, F., Prime and composite polynomials, *Trans. Amer. Math. Society* **23** (1922), 51–66.

[11] Zippel, R., Rational function decomposition, en "Proc. of ISSAC-91", edit. S. Watt, ACM Press, N.Y., 1991, 1–6.