ELSEVIER Journal of Pure and Applied Algebra 121 (1997) 217–222

JOURNAL OF
PURE AND
APPLIED ALGEBRA

A note on separated factors of separated polynomials

Cesar Alonso *, Jaime Gutierrez, Tomas Recio

Departamento de Matemáticas, Estadística y Computación, Facultad de Ciencias, Universidad de Cantabria, Santander 39071, Spain

Communicated by M.-F. Roy; received 30 November 1993; revised 1 February 1996

Abstract

By introducing the concept of near-separated polynomial we extend to rational functions a theorem of Fried and MacRae (1969) concerning separated factors of separated polynomials. Our result allows to solve several problems about the decomposition of rational functions by means of factorization of bivariate polynomials. © 1997 Elsevier Science B.V.

1991 Math. Subj. Class.: 12E20, 12E25, 12F12

1. Introduction and main result

The goal of this note is to prove the following elementary result.

Theorem 1. *Let* $\mathbb{K}$ *be an arbitrary field and let* $f(X) = f_n(X)/f_d(X)$, $g(X) = g_n(X)/g_d(X)$, $f_1(X) = f_{1n}(X)/f_{1d}(X)$, *and* $g_1(X) = g_{1n}(X)/g_{1d}(X)$ *be non-constant rational functions in* $\mathbb{K}(X)$, *given in prime form. Then* $f_{1n}(X)g_{1d}(Y) - g_{1n}(Y)f_{1d}(X)$ *divides* $f_n(X)g_d(Y) - g_n(Y)f_d(X)$ *in* $\mathbb{K}[X,Y]$ *if and only if there exists a rational function* $h(X) = h_n(X)/h_d(X)$, *in* $\mathbb{K}(X)$ *such that* $f(X) = h(f_1(X))$ *and* $g(X) = h(g_1(X))$.

This theorem is a verbatim generalization of the same result obtained by Fried and MacRae [6] in 1969, there restricted to the case where f, g, f_1, and g_1 are polynomials in $\mathbb{K}[X]$. Recently, Fried has considered Corollary 5 of our result in the context of the construction of exceptional covers [5]. Moreover, our motivation for Theorem 1 comes from its applications to the decomposition of rational functions (see Corollaries 5, 7, 8).

* Corresponding author.

[1] Partially supported by CICyT PB 89/0379/C02/01, Esprit Bra-POSSO. 6846 and TIC 1026 CE.

PII S0022-4049(96)00131-4

For a survey on the rational function decomposition problem and its applications to parametric varieties, see [1, 2, 8]. Roughly speaking, our result allows to translate basic issues in the decomposition problem of univariate rational functions to the much better studied case of algorithms for factoring bivariate polynomials.

Although our result has an elementary proof, it seems that it has been ignored by several authors working in the functional decomposition problem. In fact, the analogous result for the polynomial case was the key for the first polynomial decomposition algorithm [4], but this approach was not followed in the earlier studies of the more difficult rational decomposition case. Surprisingly, a particular version of our theorem turned out to be the key for a practical rational function decomposition algorithm [1, 2].

Definition 2. A non-constant polynomial $f(X,Y)$ in $\mathbb{K}[X,Y]$ is *near-separated* if there exist non-zero polynomials $r(x)$, $u(X)$ in $\mathbb{K}[X]$ and $s(Y)$, $t(Y)$ in $\mathbb{K}[Y]$, such that $r(X)$ (respectively, $s(Y)$) is not a constant times $u(X)$ (respectively, $s(Y)$ is not a constant times $t(Y)$) and if we can express $f(X,Y)$ in the form $r(X)s(Y)-t(Y)u(X)$. The list $[r(X),s(Y),t(Y),u(X)]$ is called a *representation* of $f(X,Y)$. In the particular case that we have $f(X,Y)=r(X)s(Y)-r(Y)s(X)$ we will say that $f(X,Y)$ is a *symmetric* near-separated polynomial.

Remark 3. For instance, the polynomial

$$x^3y+x^3+y^5-y-y^5x-4\,y^2x^3-4\,y^2x+8\,y^2-x$$

is near-separated, admitting a representation as

$$(-1+x)((x^2+x)(y+1-4\,y^2)-y^5+y-8\,y^2)).$$

On the other hand, it is easy to see that the polynomial X^n+XY+Y^n is not near-separated for any $n\in\mathbb{N}$. Below (Corollary 6) we will sketch an algorithm to decide if a polynomial is near-separated and, in the affirmative case, to construct a representation.

2. Proof of the main result and corollaries

We will give now, in the following lemma, some basic properties of the near-separated polynomials.

Lemma 4. (i) *Every univariate factor, on the X variable alone, of a near-separated polynomial is a factor of $r(X)$ and $u(X)$. Likewise, it is a factor of $s(Y)$ and $t(Y)$ if it only depends on the Y variable.*

(ii) *Given $f(X,Y)$ near-separated, there exists a near-separated polynomial, without univariate factors, $\bar{f}(X,Y)$, such that $\bar{f}(X,Y)$ divides $f(X,Y)$. We will call such polynomial $\bar{f}(X,Y)$ primitive near-separated.*

If $f(X,Y)$ is symmetric near-separated then:

(iii) *$(X-Y)$ is a factor of $f(X,Y)$. Moreover, if char $(\mathbb{K})$ is zero, then $(X-Y)$ is a simple factor.*

Proof. (i) Let $f(X,Y)=r(X)s(Y)-t(Y)u(X)$ and $v(X)$ univariate factor of $f(X,Y)$. Then $f(X,Y)=g(X,Y)v(X)$. Let α be a root of $v(X)$ in the algebraic closure $\overline{\mathbb{K}}$ of $\mathbb{K}$. It is trivial that if α is a root of $r(X)$ or of $u(X)$ then it will be also a root of the other. Assume then that $r(\alpha)$ and $u(\alpha)$ are non-zero. Then we have $r(\alpha)/u(\alpha)=t(Y)/s(Y)$. Thus, $t(Y)$ and $s(y)$ are associated (i.e. equal except for multiplication times a constant) in $\overline{\mathbb{K}}[Y]$ and then in $\mathbb{K}[Y]$. We arrive then to a contradiction with the definition of near-separated polynomial. The case of a factor depending only on Y is the same.

(ii) Observe that given a near-separated polynomial $f(X,Y)=r(X)s(Y)-t(Y)u(X)$, we can remove its univariated factors dividing by the GCD of $r(X)$ and $u(X)$ and by the GCD of $s(Y)$ and $t(Y)$ (respectively $d_1(X)$ and $d_2(Y)$) obtaining a new near-separated polynomial $\bar{f}(X,Y)$ that is primitive in $\mathbb{K}[X][Y]$ and also in $\mathbb{K}[Y][X]$.

(iii) The first part is trivial. Now let *char*$(\mathbb{K})$ be equal to zero and suppose that $(X-Y)^2$ divides $f(X,Y)$. Doing the change $Z=X-Y$, we have that $Z=0$ is a double root of $r(Z+Y)s(Y)-r(Y)s(Z+Y)$. Deriving with respect to Z and making $Z=0$, we obtain $r'(Y)/s'(Y)=r(Y)/s(Y)$, and this is not possible because *char*$(\mathbb{K})$ is zero. □

Using these lemmas we are able to prove our main result. We will assume that all rational functions given in the hypothesis of Theorem 1 are such that numerators and denominators do not have common factors (i.e. they are in prime form).

Proof of Theorem 1. Suppose that such a rational function $h(X)=h_n(X)/h_d(X)$ exists. We consider

$$h(f_1(X))-h(g_1(Y))=\frac{h_n(f_1(X))h_d(g_1(Y))-h_d(g_1(Y))h_d(f_1(X))}{h_d(f_1(X))h_d(g_1(Y))}.$$

We observe that $X-Y$ divides $h_n(X)h_d(Y)-h_d(X)h_n(Y)$. So, we have

$$h(f_1(X))-h(g_1(Y))=\frac{(f_1(X)-g_1(Y))m(f_1(X),g_1(Y))}{h_d(f_1(X))h_d(g_1(Y))}$$

with $m(X,Y)\in\mathbb{K}[X,Y]$. Now, operating as usual in the above expression and multiplying by a suitable power of $f_{1d}(X)$ and $g_{1d}(Y)$ we get

$$\frac{(f_{1n}(X)g_{1d}(Y)-g_{1n}(Y)f_{1d}(X))n(X,Y)}{u(X)v(Y)}$$

with numerator and denominator relatively prime. On the other hand, we have

$$h(f_1(X))-h(g_1(Y))=f(X)-g(Y)=\frac{f_n(X)g_d(Y)-g_n(Y)f_d(X)}{f_d(X)g_d(Y)},$$

also with numerator and denominator relatively prime. So, we conclude that $f_{1n}(X)g_{1d}(Y) - g_{1n}(Y)f_{1d}(X)$ divides $f_n(X)g_d(Y) - g_n(Y)f_d(X)$ in $\mathbb{K}[X,Y]$.

Conversely, let us now suppose that $f_{1n}(X)g_{1d}(Y) - g_{1n}(Y)f_{1d}(X) = a(X,Y)$ divides $f_n(X)g_d(Y) - g_n(Y)f_d(X)$. Following Fried and MacRae's ideas (see [6]) we consider $\mathbb{K}[\alpha,\beta] = \mathbb{K}[X,Y]/(a(X,Y))$. First, note that α and β are transcendental over $\mathbb{K}$ since no polynomial in one variable alone can be a multiple of $a(X,Y)$. Moreover, if there exists $b(X), c(X,Y)$ in $\mathbb{K}[X,Y]$ such that $b(\alpha)c(\alpha,\beta) = 0$ in $\mathbb{K}[\alpha,\beta]$, then $b(X)c(X,Y) = a(X,Y)d(X,Y)$. Since $a(X,Y)$ has no univariate factors by Lemma 4(i), it follows that $b(X)$ divides $d(X,Y)$ and then $c(\alpha,\beta)$ is zero. This reasoning allows us to conclude that no non-constant element of $\mathbb{K}[\alpha]$ or of $\mathbb{K}[\beta]$ is zero divisor in $\mathbb{K}[\alpha,\beta]$. Now let M be the multiplicative set of $\mathbb{K}[\alpha,\beta]$ generated by the non-zero elements of $\mathbb{K}[\alpha]$ and $\mathbb{K}[\beta]$; and consider the quotient ring with respect to M, $\mathbb{K}[\alpha,\beta]_M$. Then $\mathbb{K}[\alpha,\beta]_M$ contains $\mathbb{K}(\alpha)$ and $\mathbb{K}(\beta)$. We consider $\mathbb{F} = \mathbb{K}(\alpha) \cap \mathbb{K}(\beta)$. This intersection field is not reduced to $\mathbb{K}$, since $f_{1n}(X)g_{1d}(Y) - g_{1n}(Y)f_{1d}(X) = 0$ in $\mathbb{K}[\alpha,\beta]$ and thus $f_1(\alpha) = g_1(\beta) \neq 0$ is included in $\mathbb{F}$. As $\mathbb{F}$ is contained in $\mathbb{K}(\alpha)$ and in $\mathbb{K}(\beta)$ and these fields are of transcendence degree one, we can apply Lüroth theorem to find some generator w such than $\mathbb{F} = \mathbb{K}(w)$. Next we claim that $f_1(\alpha) = w' = g_1(\beta)$ is also a Lüroth generator. For let $w = F(\alpha) = G(\beta)$, where again $F = F_n/F_d, G = G_n/G_d$ is a representation without common factors. Now $f_{1n}(X)g_{1d}(Y) - g_{1n}(Y)f_{1d}(X)$ divides $F_n(X)G_d(Y) - G_n(Y)F_d(X)$ since $F_n(\alpha)G_d(\beta) - G_n(\beta)F_d(\alpha) = 0$. It follows that $\max\{\deg(f_{1n}), \deg(f_{1d})\} \leq \max\{\deg(F_n), \deg(F_d)\}$. One checks then that each maximum is also the degree of the algebraic extensions $[\mathbb{K}(\alpha):\mathbb{K}(w')]$, $[\mathbb{K}(\alpha):\mathbb{K}(w)]$, respectively. But $\mathbb{K}(w') \subseteq \mathbb{K}(w)$, and thus we must have that the degrees are actually equal and the claim follows. Since, by hypothesis, $f_n(X)g_d(Y) - f_d(X)g_n(Y)$ is a multiple of $f_{1n}(X)g_{1d}(Y) - g_{1n}(Y)f_{1d}(X)$, we have $f(\alpha) = g(\beta) \in \mathbb{F}$. Therefore, there is some h such that $f(X) = h(f_1(X))$ and $g(X) = h(g_1(X))$. □

Applying this result to the particular case when $f = g$ and $f_1 = g_1$, yields the following corollary [2]. Remark that this result also clarifies the approach hidden behind Netto's proof of Lüroth theorem (cf. [7]), that, in our terminology, proceeds by reducing the computation of the field generator to GCD computations with near-separated polynomials.

Corollary 5. *Let $\mathbb{K}$ be an arbitrary field and let $f(X) = f_n(X)/f_d(X)$ be a non-constant rational function in $\mathbb{K}(X)$. with g.c.d.$(f_n(X), f_d(X)) = 1$. Then, there are two rational functions $g(X), h(X) = h_n(X)/h_d(X)$ in $\mathbb{K}(X)$ such that $f(X) = g(h(X))$ if and only if the symmetric near-separated polynomial $h_n(X)h_d(Y) - h_n(Y)h_d(X)$ divides $f_n(X)f_d(Y) - f_n(Y)f_d(X)$.*

Given a primitive near-separated polynomial $f(X,Y)$, every representation is associated with two rational functions in prime form f_n/f_d, g_n/g_d, such that $f = f_n(X)g_d(Y) - g_n(Y)f_d(X)$. In general, there are several pairs of rational functions that might correspond with the same primitive near-separated polynomial (for instance, think of f_n/f_d,

g_n/g_d and f_d/f_n, $-g_d/-g_n$). Corollary 6(i) addresses this point. A trivial generalization to non-primitive polynomials also holds. Corollary 6(ii) will be used for testing if a polynomial is near-separated and for constructing one representation.

Corollary 6. (i) (*Uniqueness of representation*) *Given two representations of a primitive near-separated polynomial* $f(X,Y)$, *as*

$$r_1(X)s_1(Y) - t_1(Y)u_1(X) = r_2(X)s_2(Y) - t_2(Y)u_2(X),$$

there is $U(X) = (aX+b)/(cX+d)$, *and* $\mathbb{K}(X)$ *such that* $U(r_1(X)/u_1(X)) = r_2(X)/u_2(X)$ *and* $U(t_1(X)/s_1(X)) = t_2(X)/s_2(X)$. *Conversely, composing in this way any given primitive representation with a linear transformation* U, *yields another primitive representation of* f.

(ii) *In every representation of a near-separated polynomial* $f(X,Y) = r(X)s(Y) - t(Y)u(X)$, *it holds*: $\max\{\deg(r), \deg(u)\} = \deg_x f(X,Y)$ *and* $\max\{\deg(t), \deg(s)\} = \deg_y f(X,Y)$.

Proof. (i) Notice that if $r_1(X)s_1(Y) - t_1(Y)u_1(X)$ and $r_2(X)s_2(Y) - t_2(Y)u_2(X)$ are associated, then, since they both divide each other, applying Theorem 1 we will obtain that $\mathbb{K}(r_1(X)/u_1(X)) = \mathbb{K}(r_2(X)/u_2(X))$ and $\mathbb{K}(t_1(X)/s_1(X)) = \mathbb{K}(t_2(X)/s_2(X))$, and that there is a common field automorphism U that transforms one couple of rational functions into the other. Conversely if $U(r_1(X)/u_1(X)) = r_2(X)/u_2(X)$ and $U(t_1(X)/s_1(X)) = t_2(X)/s_2(X)$, then $r_2(X)s_2(Y) - t_2(Y)u_2(X) = (ad-bc)(r_1(X)s_1(Y) - t_1(Y)u_1(X))$. Then dividing the numerator and denominator of $U(X)$ by a suitable constant we can obtain $ad - bc = 1$.

(ii) Assume that f is primitive. Let $f(X,Y) = r(X)s(Y) - t(Y)u(X)$. If $\deg(r) \neq \deg(u)$ the proof is trivial.Otherwise, if $\deg(r) = \deg(u) > \deg_x f$, the highest degree X-terms must cancel, but this implies that $s(y)$ and $t(y)$ are associated, contradicting the assumption of primitivity. The same reasoning holds for the degree in Y. The non-primitive case follows easily. □

Thus, in order to check if a given polynomial $f(x,y)$ is near separated we can proceed as follows. First we extract all univariate factors (in X and in Y) of f. What remains is now tested for being primitive near-separated. Let us assume, then, that f has no univariate factors. Using the above corollary and composing with a unit, we can always suppose that a near-separated polynomial has a representation of the type $rs - tu$, either with $r(0) = 0$, $t(0) = 0$, or with $r(0) \neq 0$, $u(0) = 0$, $t(0) = 0$. In the first case (that corresponds to $f(0,0) = 0$) we can take $-t(Y) = f(0,Y)$, $r(X) = f(X,0)$) and we determine the remaining polynomials by solving a linear system (that is compatible if and only if f is near-separated). In the second case, $f(X, 0) = r(X)$, $s(Y) = f(0,Y)/r(0)$ and we consider $f - rs = g(X,Y)$. Then g must be $t(Y)u(X)$. Let α be a constant such that $X - \alpha$ does not divide $g(X,Y)$ (a small modification of this procedure is required here for the case of a finite field, in some extreme circumstances). Take then $t(Y) = g(\alpha, Y)$ and $u(X) = g(X,Y)/t(Y)$. This final operation must yield a polynomial if and only if the given f is near-separated. Remark that the fact of being near-separated is independent of the base field, i.e. it is near-separated over $\mathbb{K}$ if and only if it is near-separated in an extension field of $\mathbb{K}$. On the other hand, Corollaries 5 and 8 (below) depend on the base field (since we must find some factors and then check if they are near-separated, see [2]), but not Corollary 7 (since we must find common factors and then apply the decision procedure outlined above, cf. [3]).

The following corollaries give necessary and sufficient conditions for a pair of rational functions to have a common right (respectively, left) component with respect to functional composition. The first corollary follows by applying Corollary 5 to the rational functions f, g. The second corollary is a direct consequence of Theorem 1.

Corollary 7. *Let $\mathbb{K}$ be an arbitrary field and let $f(X) = f_n(X)/f_d(X)$, $g(X) = g_n(X)/g_d(X)$ be rational functions in prime forms. Then $f(X)$ and $g(X)$ have a right common component for the composition if and only if $f_n(X)f_d(Y) - f_n(Y)f_d(X)$ and $g_n(X)g_d(Y) - g_n(Y)g_d(X)$ have a common factor primitive symmetric near-separated of the form $h_n(X)h_d(Y) - h_n(Y)h_d(X)$. If it is the case, $h(X) = h_n(X)/h_d(X)$ will be the common component.*

Corollary 8. *Under the same conditions of the above corollary, $f(X)$ and $g(X)$ have a left common component for the composition if and only if $f_n(X)g_d(Y) - g_n(Y)f_d(X)$ has a primitive near-separated divisor.*

References

[1] C. Alonso, J. Gutierrez and T. Recio, FRAC: a Maple package for computing in the rational function field $\mathbb{K}(X)$, in: R.J. Lopez, Ed., Maple V: Mathematics and its Applications (Birkhauser, Basel, 1994) 107–115.

[2] C. Alonso, J. Gutierrez and T. Recio, A rational function decomposition algorithm by near-separated polynomials, J. Symbolic Comput., to appear.

[3] C. Alonso, J. Gutierrez and T. Recio, Reconsidering algorithms for real parametric curves, AAECC 6 (1995) 345–352.

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

[5] M. Fried, Global Construction of Exceptional Covers, Contemporary Mathematics, Vol. 168 (American Mathematical Society, Providence, RI, 1994) 69–100.

[6] M. Fried and R. MacRae, On curves with separated variables, Math. Ann. 180 (1969) 220–226.

[7] A. Schinzel, Selected Topics on Polynomials (Univ. Michigan Press, Ann Arbor, 1982).

[8] R. Zippel, Rational function decomposition, Proc. ISSAC'91 (ACM Press, New York, 1991).