Hamburger Beiträge
zur Angewandten Mathematik

A Note on Elimination Polynomials

Klaus Glashoff

Reihe A
Preprint 137
March 1998

Hamburger Beiträge zur Angewandten Mathematik

Reihe A	Preprints
Reihe B	Berichte
Reihe C	Mathematische Modelle und Simulation
Reihe D	Elektrische Netzwerke und Bauelemente
Reihe E	Scientific Computing
Reihe F	Computational Fluid Dynamics and Data Analysis

A Note on Elimination Polynomials

Klaus Glashoff
Universität Hamburg
Fachbereich Mathematik
Bundesstraße 55
D - 20146 Hamburg
Germany
e-mail: glashoff@math.uni-hamburg.de

March, 1998

Abstract. Computation of elimination polynomials by means of primitive polynomial remainder sequences is, in certain cases, an efficient method for the solution of systems of polynomial equations. This has been shown be Kalkbrener ([1991],[1995]). In this paper we relate Kalkbreners theory of elimination sequences the results of Labatie (Netto [1900]), who – in 1835 – presented a complete solution procedure for solving systems of two algebraic equations in two unknowns, implicitely using a different version of elimination sequences.

Keywords: Polynomial remainder sequences, Elimination theory.

1 Introduction

The primitive polynomial remainder sequence (*pprs*) of two multivariate polynomials f_1 and f_2 are of use for the computation of common zeroes of f_1 and f_2. This has been shown by Kalkbrener ([1991], [1995]), who developed the theory of elimination sequences and who applied it to a number of important examples by means of an algorithm implemented in MAPLE. It turns out that his method of computing roots of systems of algebraic equations is very efficient, compared to Groebner-basis-methods, if applied to small size problems, i.e. systems with two or three unknowns.

The method of elimination sequences seems to be a very promising approach which deserves further research in order to enlarge its domain of applicability. Interestingly, the corresponding theory has roots in the mathematics of the early 19'th century: In 1835, Labatie developed a complete triangularization-method for algebraic systens in two unknowns (Netto [1900], p.60-62). In the present paper we are going to connect his results to those of Kalkbrener, thus throwing new light on the definition, properties, and computation of elimination sequences.

In Section 2 we introduce the definition of a primitive polynomial remainder sequence of two primitive polynomials f_1 and f_2 in the variable x_n over the polynomial ring $K[x_1, \ldots, x_{n-1}]$. We then derive some identities relating Bezout-cofactors and the *pprs* (Netto [1900], p.20-22).

In Section 3, we define the so called elimination sequence $\{\epsilon_j\}$ belonging to a *pprs* like Labatie did it for the special case $n = 2$. We then relate this definition to that of Kalkbrener: It turns out that Kalkbreners elimination polynomials $e_j, j = 2, \ldots, k-1$, divide the squarefree forms of those defined by us.

In Section 4, we derive some identities holding between *pprs*, Bezout-cofactors, and the sequence of elimination polynomials. Of special importance is an equality of the form

$$\tilde{q}_i f_1 = \tilde{g}_i f_i - \epsilon_i \tilde{g}_{i-1} f_{i+1} \quad \text{for} \quad i = 2, \ldots, k-1.$$

for certain polynomials $\tilde{q}_i, \tilde{g}_i, \tilde{g}_{i-1}$ (constructable by recursion), where $\tilde{q}_i$ is relatively prime to ϵ_i.

In the concluding Section 5 we derive the necessary and sufficient conditions for the common roots of two polynomials f_1 and f_2. In addition, we relate the product $\prod_{j=2}^{k-1} \epsilon_j$ to $\prod_{j=2}^{k-1} e_j$ and to the Sylvester-resultant of f_1 and f_2. Some of the proofs of this section are not given because the results may be obtained in exactly the same way as Kalkbrener did it for his squarefree variant of the elimination polynomials.

In order to easen the comparison of our results with those of Kalkbrener, we have tried as much as possible to use his notation. But, there are some differences which we shall mention at the appropriate places of this paper. In particular we will rename Kalkbrener's elimination sequence as *K-elimination sequence* in contrast to the *L-elimination sequence* which we define in Section 3.

2 Notation and definitions

Let K be a field and $\bar{K}$ an algebraically closed field which has infinite transcendence degree over K. Let

$$f = \sum_{r=0}^{m} q_r(x_1, \ldots, x_{n-1}) x_n^r$$

be a polynomial in $K[x_1, \ldots, x_n]$ with $q_m \neq 0$. q_m is called the *leading coefficient* of $f, \ell c(f)$. The degree of f in x_n is denoted by $deg(f)$. The content of f, written $cont\ (f)$, is the polynomial $gcd(q_0, \ldots, q_m)$, and the *primitive part* of f, written $pp(f)$, is the polynomial $f/cont(f)$. The polynomial f is *primitive* if $cont(f) = 1$. Let $f, g \in K[x_1, \ldots, x_n]$ be non-zero polynomials. Then there exist polynomials $pquot\,(f, g)$ and $prem\,(f, g)$, called *pseudo-quotient* and *pseudo-remainder* of f and g, such that

$$(\ell c(g))^d \cdot f = \ pquot(f, g) \cdot g + \ prem(f, g)$$

and

$$deg(prem(f, g)) < deg(g),$$

where $d := \max(\{deg(f) - deg(g) + 1, 0\})$ and $deg(0) := -1$. For non-zero primitive polynomials f_1, f_2 in $K[x_1, \ldots, x_n]$ with $deg(f_1 \geq deg(f_2)$, the sequence $f_1, f_2, f_3, \ldots, f_k$ of non-zero polynomials in $K[x_1, \ldots, x_n]$ is called the *primitive polynomial remainder sequence* (abbreviation: *pprs*) of f_1 and f_2 if

$$\begin{aligned} pp(prem(f_{i-2}, f_{i-1})) &= f_i \text{ for } i = 3, \ldots, k \\ \text{and} \quad prem(f_{k-1}, f_k) &= 0. \end{aligned}$$

If the *pprs* $f_1, f_2, \ldots, f_k$ is given, let

$$\begin{aligned} c_i &:= cont(prem(f_{i-1}, f_i)) && \text{for} \quad i = 2, \ldots, k-1, \\ \ell_i &:= \ell c(f_i)^{deg(f_{i-1}) - deg(f_i) + 1} && \text{for} \quad i = 2, \ldots, k \end{aligned}$$

and

$$q_i = pquot(f_{i-1}, f_i).$$

Then, the following relations hold:

$$\begin{array}{rcrcl} \ell_2 \cdot f_1 & = & q_2 \cdot f_2 & + & c_2 \cdot f_3 \\ \ell_3 \cdot f_2 & = & q_3 \cdot f_3 & + & c_3 \cdot f_4 \\ \cdots & & \cdots & & \\ \ell_{k-1} f_{k-2} & = & q_{k-1} f_{k-1} & + & c_{k-1} \cdot f_k \\ \ell_k f_k & = & q_k \cdot f_k & & \end{array} \tag{1}$$

Elimination of f_3 by means of the first two equation of (1) gives

$$\begin{aligned} c_2 c_3 f_4 &= (c_2 \ell_3 + q_3 q_2) f_2 - q_3 \ell_2 f_1, \\ &= g_3 \cdot f_2 + h_3 \cdot f_1 \end{aligned}$$

(where $g_3 = c_2 \ell_3 + q_3 q_2$, $h_3 = -q_3 \ell_2$), i.e. we can express the product $c_2 c_3 f_4$ by an ideal-combination of f_1 and f_2. This may be iterated, and we obtain

Lemma 1. Let us define $c_1 := 1$, and

$$
\begin{aligned}
g_0 &:= 0, \\
g_1 &:= 1, \\
g_i &:= -q_i g_{i-1} + c_{i-1} \ell_i g_{i-2} \qquad \text{for} \quad i = 2, 3, \ldots, k-1
\end{aligned}
\tag{2a}
$$

and

$$
\begin{aligned}
h_0 &= 1, \\
h_1 &= 0, \\
h_i &:= -q_i h_{i-1} + c_{i-1} \ell_i h_{i-2} \qquad \text{for} \quad i = 2, 3 \ldots, k-1.
\end{aligned}
\tag{2b}
$$

Then

$$
\prod_{r=2}^{i-1} c_r f_i = g_{i-1} \cdot f_2 + h_{i-1} \cdot f_1 \qquad \text{for} \quad i = 3, \ldots, k \tag{3}
$$

Proof. (2) is correct for $i = 2$, as by definition

$$
\begin{aligned}
g_2 &= -q_2, \\
h_2 &= \ell_2.
\end{aligned}
$$

Therefore,

$$
c_2 f_3 = g_2 \cdot f_2 + h_2 \cdot f_1
$$

is just the first equation of (1). – In the induction step, we assume (3) for some $i \in \{3, \ldots, k-1\}$. By this assumption and (1),

$$
\begin{aligned}
\prod_{r=2}^{i} c_r f_{i+1} &= \prod_{r=2}^{i-1} c_r (c_i f_{i+1}) = \prod_{r=2}^{i-1} c_r (-q_i f_i + \ell_i f_{i-1}) \\
&= -q_i \prod_{r=2}^{i-1} c_r f_i + \ell_i c_{i-1} \prod_{r=2}^{i-2} c_r f_{i-1} \\
&= -q_i (g_{i-1} f_2 + h_{i-1} f_1) + \ell_i c_{i-1} (g_{i-2} f_2 + h_{i-2} f_1) \\
&= (-q_i g_{i-1} + \ell_i c_{i-1} g_{i-2}) f_2 + (-q_i h_{i-1} + \ell_i c_{i-1} h_{i-2}) f_1 \\
&= g_i f_2 + h_i f_1.
\end{aligned}
$$

Thus, (3) is proved. ■

A simple consequence of Lemma 1 illustrates the usefulness of a *pprs* for the computation of common zeroes of f_1 and f_2. Let $i = k$ in (3):

$$
\prod_{r=2}^{k-1} c_r \cdot f_k = g_{k-1} f_2 + h_{k-1} f_1. \tag{4}
$$

It is well-known that

$$f_k = gcd(f_1, f_2).$$

Let now $\bar{x} = (\bar{x}_1, \ldots, \bar{x}_n)$ be a common zero of f_1 and f_2 which is *not* a zero of f_k. Then, by (4), $(\bar{x}_1, \ldots, \bar{x}_{n-1})$ is a zero of one of the polynomials $c_2, \ldots, c_{k-1}$.

Our aim in the following sections is twofold: First, we are going to sharpen the just mentioned necessary condition for common roots of f_1, f_2 by showing how to cancel certain factors of the c_i. This will lead us to the sequence of *elimination polynomials* $\{\epsilon_2, \epsilon_3, \ldots, \epsilon_{k-1}\} \subset K[x_1, \ldots, x_{n-1}]$, each of which is a factor of the corresponding c_i. We shall derive an identiy like (4) also for the elimination polynomials:

$$\prod_{j=2}^{k-1} \epsilon_j \cdot f_k = g \cdot f_2 + h \cdot f_1.$$

Thus, each common zero $\bar{x} = (\bar{x}_1 \ldots, \bar{x}_n)$ of f_1 and f_2 which is not a zero of f_k is also a zero of one of the elimination polynomials ϵ_j.

In the last section we show how to derive a set of necessary *and sufficient* conditions for the common roots of f_1 and f_2.

3 Elimination Sequences

In this section we are going to define the *L-elimination polynomials* of a given *pprs* just like Labatie did it for bivariate polynomials. Then we show how this sequence of polynomials is related to Kalkbrener's *K-elimination sequence.*

Definition 1. For a given *pprs* $f_1, f_2, f_3, \ldots, f_k$ let

$$\begin{aligned} d_2 &= gcd(\ell_2, c_2), \\ d_3 &= gcd\left(\frac{\ell_2}{d_2} \cdot \ell_3, c_3\right) \\ &\vdots \\ d_{k-1} &= gcd\left(\frac{\ell_2}{d_2} \cdots \frac{\ell_{k-2}}{d_{k-2}} \ell_{k-1}, c_{k-1}\right) \end{aligned} \tag{5}$$

and

$$\varepsilon_i = \frac{c_i}{d_i} \quad \text{for} \quad i = 2, \ldots, k-1. \tag{6}$$

We call $\{\varepsilon_2, \ldots, \varepsilon_{k-1}\}$ the *L-elimination sequence* of $f_1, \ldots, f_2$. The individual polynomials ε_j are the *L-elimination polynomials.*

Definition 2 (Kalkbrener [1991]). Let

$$\begin{aligned}
\hat{p}_i &:= \frac{\prod_{r=2}^{i} c_r}{gcd\left(\prod_{r=2}^{i} c_r, \prod_{r=2}^{i} \ell_r\right)} && \text{for} \quad i = 2, \ldots, k-1 \\
p_i &:= squarefree(\hat{p}_i) \\
e_i &:= \frac{p_i}{gcd\left(p_i, \prod_{r=2}^{i-1} e_r\right)} && \text{for} \quad i = 3, \ldots, k-1 \\
e_2 &:= p_2.
\end{aligned}$$

Here $squarefree(f)$ denotes the squarefree part of $f \in K[x_1, \ldots, x_n]$. – The following Theorem shows the relation between Kalkbrener's *K-elimination polynomials* ε_i and our *L-elimination polynomials* ε_i.

Theorem 1. Let us denote

$$\begin{aligned}
\hat{e}_i &= \frac{\hat{p}_i}{gcd\left(\hat{p}_i, \prod_{r=2}^{i-1} \hat{e}_r\right)} && \text{for} \quad i = 3, \ldots, k-1 \\
\hat{e}_2 &= \hat{p}_2.
\end{aligned}$$

Then the following relations hold true:

$$\begin{aligned}
&(a) \quad \hat{e}_i = \varepsilon_i && \text{for} \quad i = 2, \ldots, k-1, \\
&(b) \quad e_i \text{ devides } squarefree(\varepsilon_i) && \text{for} \quad i = 2, \ldots, k-1.
\end{aligned}$$

Proof of (a). Induction basis:

$$\varepsilon_2 = \frac{c_2}{gcd(\ell_2, c_2)} = \hat{p}_2 = \hat{e}_2.$$

Induction step: $i \in \{3, \ldots, k-1\}$;

$$\begin{aligned}
\hat{e}_i &= \frac{\prod_{r=2}^{i} c_r}{gcd\left(\prod_{r=2}^{i} c_r, \prod_{r=2}^{i} \ell_r\right) \cdot gcd\left(\frac{\prod_{r=2}^{i} c_r}{gcd\left(\prod_{r=2}^{i} c_r, \prod_{r=2}^{i} \ell_r\right)}, \prod_{r=2}^{i-1} \hat{e}_r\right)} \\
&= \frac{\prod_{r=2}^{i} c_r}{gcd\left(\prod_{r=2}^{i} c_r, gcd\left(\prod_{r=2}^{i} c_r, \prod_{r=2}^{i} \ell_r\right) \prod_{r=2}^{i-1} \hat{e}_r\right)} \\
&= \frac{\prod_{r=2}^{i} c_r}{gcd\left(\prod_{r=2}^{i} c_r, gcd\left(\prod_{r=2}^{i} c_r, \prod_{r=2}^{i} \ell_r\right) \cdot \prod_{r=2}^{i-1} \varepsilon_r\right)}
\end{aligned}$$

by the induction hypothesis

$$\varepsilon_r = \hat{e}_r \quad \text{for} \quad r = 2, \ldots, i-1.$$

Now, by Definition 1,

$$
\begin{aligned}
\hat{e}_i &= \frac{\prod_{r=2}^{i} c_r}{\mathrm{gcd}\left(\prod_{r=2}^{i} c_r, gcd\left(\prod_{r=2}^{i} c_r, \prod_{r=2}^{i} \ell_r\right) \prod\limits_{r=2}^{i-1} \frac{c_r}{d_r}\right)} \\
&= \frac{\prod_{r=2}^{i} c_r}{gcd\left(\prod_{r=2}^{i} c_r, gcd\left(c_i \prod_{r=2}^{i-1} \frac{c_r}{d_r}, \ell_i \prod_{r=2}^{i-1} \frac{\ell_r}{d_r}\right) \cdot \prod_{r=2}^{i-1} c_r\right)} \\
&= \frac{\prod_{r=2}^{i} c_r}{\prod_{r=2}^{i-1} c_r \cdot gcd\left(c_i, gcd\left(c_i \prod_{r=2}^{i-1} \frac{c_r}{d_r}, \ell_i \prod_{r=2}^{i-1} \frac{\ell_r}{d_r}\right)\right)}
\end{aligned}
$$

Using the abbreviation

$$\tilde{c}_{i-1} := \prod_{r=2}^{i-1} \frac{c_r}{d_r}$$

and having in mind that

$$gcd(\alpha, gcd(\alpha\beta, \gamma)) = gcd(\alpha, \gamma),$$

we obtain the desired result:

$$
\begin{aligned}
\hat{e}_i &= \frac{c_i}{gcd\left(c_i, gcd\left(c_i \cdot \tilde{c}_{i-1}, \ell_i \cdot \prod_{r=2}^{i-1} \frac{\ell_r}{d_r}\right)\right)} \\
&= \frac{c_i}{gcd\left(c_i, \ell_i \prod_{r=2}^{i-1} \frac{\ell_r}{d_r}\right)} \\
&= \varepsilon_i
\end{aligned}
$$

Proof of (b):
Let us abbreviate $a := \hat{p}_i, b = \prod\limits_{r=2}^{i-1} e_r$ for some fixed $i \in \{2, \ldots, k-1\}$. We show that

$$\frac{squarefree(a)}{gcd(squarefree(a), squarefree(b))} \quad \text{devides } squarefree\left(\frac{a}{gcd(a,b)}\right).$$

Let p be an irreducibel factor of the lhs. Then p divides *squarefree(a)* but not *squarefree(b)* (otherwise, p would have been cancelled). This implies that p does not divide b, and thus is no divisor of $gcd(a, b)$. Therefore, p divides $a/gcd(a, b)$ and, being an irreducibel polynomial, also the squarefree part of $a/gcd(a, b)$. ■

Remark 1. In general, we have

$$e_i \neq squarefree(\varepsilon_i),$$

as may be seen by a simple example:

We denote $x_1 = x, x_2 = y$ and define

$$\begin{aligned} f_1 &= y^3 + 2xy, \\ f_2 &= y^2 + x. \end{aligned}$$

Then the following quantities are easily computed:

$$\begin{array}{lll} \ell_2 = 1, & f_3 = y, & c_2 = x, \\ \ell_3 = 1, & f_4 = 1, & c_3 = x. \\ \varepsilon_2 = e_2 = x, & & e_3 = 1 \neq x = \varepsilon_3. \end{array}$$

Remark 2. Our elimination polynomials ε_j are "in between" e_j and c_j :

$$e_j \quad \text{divides} \quad \varepsilon_j \quad \text{divides} \quad c_j.$$

In the concluding section 5 we shall also prove that – under certain assumptions –

$$\prod_{j=2}^{k-1} e_j \quad \text{divides} \quad \prod_{j=2}^{k-1} \varepsilon_j \quad \text{divides } res(f_1, f_2, x_n),$$

and that $\prod_{j=2}^{k-1} e_j$ is the squarefree form of $\prod_{j=2}^{k-1} \varepsilon_j$.

Kalkbrener gave an equivalent characterization of his *K-elimination sequence* by means of the function $po(\cdot,\cdot)$, where $po(f,g)$ denotes the greatest non-negative integer m such that f^m divides g (f non-constant, g non-zero). This power-function is his main tool for the proofs of the properties of such sequences. Instead of his characterization we shall use our Definition 1 together with Theorem 1 in order to directly obtain the relevant results.

This will require some further identities concerning a *pprs* which we going to derive in the next section.

4 Properties of elimination polynomials

The following Lemma 2 is an immediate consequence of Lemma 1:

Lemma 2. Let the polynomials g_i, h_i $(i = 0, 1, 2, \ldots, k-1)$ be defined as in Lemma 1.

Then,

$$(-1)^{i-1}\ell_i \dots \ell_2 \cdot f_1 = g_i \cdot f_i - c_i g_{i-1} f_{i+1} \tag{7a}$$

and

$$(-1)^{i-1}\ell_i \dots \ell_2 \cdot f_2 = -h_i f_i + c_i h_{i-1} f_{i+1} \tag{7b}$$

for $i = 2, 3, \dots k-1$.

Proof. Multiplication of (2a) by h_{i-1} and (2b) by g_{i-1} and subtraction of the two resulting equalities gives us

$$\begin{aligned} g_i h_{i-1} - g_{i-1} h_i &= -q_i g_{i-1} h_{i-1} + c_{i-1}\ell_i g_{i-2} h_{i-1} \\ &\quad + q_i h_{i-1} g_{i-1} - c_{i-1}\ell_i h_{i-2} g_{i-1} \\ &= -c_{i-1}\ell_i (g_{i-1} h_{i-2} - g_{i-2} h_{i-1}), \end{aligned}$$

for $i = 2, 3, \dots, k-1$. Repeating this process for the rhs of this equation, we obtain

$$\begin{aligned} g_i h_{i-1} - g_{i-1} h_i &= (-1)(-1) c_{i-1}\ell_i c_{i-2}\ell_{i-1}(g_{i-2}h_{i-3} - g_{i-3}h_{i-2}) \\ &\quad \vdots \\ &\quad (-1)^{i-1} c_{i-1} c_{i-2} \dots c_2 \ell_i \ell_{i-1} \dots \ell_2 (g_1 h_0 - g_0 h_1) \\ &= (-1)^{i-1} c_{i-1} c_{i-2} \dots c_2 \ell_i \ell_{i-1} \dots \ell_2 \end{aligned} \tag{8}$$

By (3),

$$c_2 \dots c_{i-1} f_i = g_{i-1} f_2 + h_{i-1} f_1 \tag{9a}$$

$$c_2 \dots c_i f_{i+1} = g_i f_2 + h_i f_1. \tag{9b}$$

Let us multiply the first of these equations by g_i, and the second by g_{i-1}. Then subtraction gives us (using (8)).

$$\begin{aligned} c_2 \dots c_{i-1}(g_i f_i - c_i g_{i-1} f_{i+1}) &= (g_i h_{i-1} - g_{i-1} h_i) f_1 \\ &= (-1)^{i-1} c_{i-1} \dots c_2 \ell_i \dots \ell_2 f_1, \end{aligned}$$

i.e.

$$(-1)^{i-1}\ell_i \dots \ell_2 f_1 = g_i f_i - c_i g_{i-1} f_{i+1}, \quad i = 2, 3, \dots, k-1,$$

which is equ. (7a). In the same manner, we get (7b): Multiply (9a) by h_i, (9b) by h_{i-1} and subtract:

$$\begin{aligned} c_2 \dots c_{i-1}(h_i f_i - c_i h_{i-1} f_{i+1}) &= -(g_i h_{i-1} - g_{i-1} h_i) f_2 \\ &= (-1)^i c_{i-1} \dots c_2 \ell_i \dots \ell_2 f_2, \end{aligned}$$

i.e.

$$(-1)^{i-1}\ell_i \dots \ell_2 f_2 = -h_i f_i + c_i h_{i-1} f_{i+1},$$

which we wanted to prove. ∎

Lemma 3. Let $\{d_2, \dots, d_{k-1}\}$ resp. $\{\varepsilon_2, \dots, \varepsilon_{k-1}\}$ be defined as in (5) resp. (6). Then

(a) g_i and h_i are divisible by $d_2 \cdot d_3 \cdot \ldots \cdot d_i$ for $i = 2, 3, \ldots k$

(b) $$\frac{g_{i-1}}{d_{i-1} \ldots d_2} \cdot f_2 + \frac{h_{i-1}}{d_{i-1} \ldots d_2} . f_1 = \varepsilon_2 \varepsilon_3 \ldots \varepsilon_{i-1} f_i \text{ for } i = 3, \dots, k \qquad (10)$$

Proof. (a): *Induction basis:* For $i = 2$,

$$g_2 = -q_2$$

by Definition (2a). We have to show that $d_2 = gcd(\ell_2, c_2)$ divides q_2: Let d be any common divisor of ℓ_2 and c_2. Then, by the first equation of (1),

$$q_2 \cdot f_2 = \ell_2 f_1 - c_2 f_3,$$

thus d divides $q_2 \cdot f_2$. But, f_2 is primitive, which implies that it is *not* divisible by any polynomial which lies in $K[x_1, \dots, x_{n-1}]$. Thus, d must divide q_2.

Induction step. Lemma 2, (7a) implies

$$(-1)^{i-1} \frac{\ell_i \ell_{i-1} \ldots \ell_2}{d_i d_{i-1} \ldots d_2} f_1 = \frac{g_i}{d_i d_{i-1} \ldots d_2} f_i - \varepsilon_i \frac{g_{i-1}}{d_{i-1} \ldots d_2} f_{i+1} \quad i = 2, 3, \dots, k-1 \qquad (11)$$

By assumption,

$$g_{i-1} \quad \text{is divisible by} \quad d_{i-1} d_{i-2} \ldots d_2.$$

This shows us that both the left hand term of equ. (11) and the second term on the *rhs* of (11) are polynomials in $K[x_1, \dots, x_{n-1}]$. This implies that also

$$g_i f_i / (d_i d_{i-1} \ldots d_2)$$

is a polynomial, i.e., $g_i f_i$ is divisible by the product $d_i \ldots d_2 \in K[x_1, \dots, x_{n-1}]$. As f_i is primitive, $d_i \dots, d_2$ must divide g_i. – Exactly the same arguments lead to the divisibility of h_i by $d_1 d_{i-1} \ldots d_2$.

(b) is a direct consequence of Lemma 1 (3). ■

Now everything is ready to prove the main results: (10) is the "improved version" of (3) we have searched for. The division of both sides of (3) by the appropriate divisor $d_{i-1} \dots, d_2$ will allow us to obtain necessary and sufficient conditions for the solutions of $f_1 = f_2 = 0$ in terms of "simpler" equations involving the elimination polynomials ε_i. This will be performed in the concluding section.

5 Characterization of roots by elimination polynomials

The first theorem gives a necessary condition for the common roots of two primitive polynomials $f_2 1, f_2$.

Theorem 2. Let f_1, f_2 be primitive polynomials in $K[x_1, \ldots, x_n], \{f_1, f_2, f_3, \ldots, f_k\}$ a primitive polynomial remainder sequence, and $\{\varepsilon_2, \ldots, \varepsilon_{k-1}\}$ the corresponding *L-elimination sequence.* Let $a \in \bar{K}^n$ be a common root of f_1 and f_2 . Then $f_k(a) = 0$, or there exists an $i \in \{2, \ldots, k-1\}$ such that

$$\varepsilon_i(a) = 0 \text{ and } (f_i/f_k)(a) = 0 \tag{12}$$

Proof. Let us assume $f_k(a) \neq 0$. By Lemma 3, (10) for $i = k$, it follows that

$$\varepsilon_2(a) e_3(a) \ldots \varepsilon_{k-1}(a) = 0$$

If $i \in \{2, \ldots, k-1\}$ ist the smallest index for which

$$\varepsilon_i(a) = 0,$$

(10) implies

$$0 = \varepsilon_2(a) \ldots \varepsilon_{i-1}(a) f_i(a).$$

By definition of the index i, $\varepsilon_j(a) \neq 0$ for $j \in \{2, \ldots, i-1\}$, and therefore $f_i(a) = 0$. Because of $f_k(a) \neq 0$, this implies $(f_k/f_k)(a) = 0$. ■

Remark. In the case $n = 2$, Labatie proved the following theorem, which – together with Theorem 2, gives a complete characterization of the common roots of two bivariate polynomials

Theorem 3. Let $n = 2$. If, for some $i \in \{2, \ldots, k-1\}$ and some $a \in \bar{K}^n$,

$$\varepsilon_i(a) = 0 \quad \text{and} \quad f_i(a) = 0, \tag{13}$$

then a is a common zero of f_1 and f_2 .

Proof. By (11), it follows from (13) that

$$\left(\frac{\ell_i \ldots \ell_2}{d_i \ldots d_2} f_1 \right) (a) = 0 \tag{14}$$

The first factor of this product, which can be written as

$$\left(\frac{\ell_2}{d_2} \cdot \frac{\ell_3}{d_3} \cdots \frac{\ell_{i-1}}{d_{i-1}} \cdot \ell_i \right) / d_i, \tag{15}$$

is by definition of d_i relatively prime to

$$\varepsilon_i = \frac{c_i}{d_i} \tag{16}$$

(because d_i is the *gcd* of the numerators of (15) and (16)). This implies that (15) and (16) have no common zeroes; i.e.

$$\varepsilon_i(a) = 0 \quad \text{implies} \quad \frac{\ell_i \ldots \ell_2}{d_i \ldots d_2}(a) \neq 0.$$

By means of (14), this implies $f_1(a) = 0$. – In the same manner, we can prove $f_2(a) = 0$. ■

Neither the proof nor the theorem are valid for the general case $n > 2$. Kalkbrener [1995] gave a counterexample for $n = 3$.

Theorem 4. Let $i \in \{2, \ldots, k-1\}$ and $a = (a_1, \ldots a_n) \in K^n$.

If $\varepsilon_i(a) = f_i(a) = 0$ and $f_i(a_1, \ldots a_{n-1}, x_n) \neq 0$,
then $f_1(a) = f_2(a) = 0$.

Proof. Kalkbrener proved this result for his elimination polynomials e_i which, by Theorem 1 (b), divide the squarefree forms of our ε_i. His proof depends on the fact that there is a relation

$$q \cdot f_1 = a_1 f_i + a_2 f_{i+1}, \;\; e_i \text{ divides } a_2, \tag{17a}$$

and e_i and q are relatively prime. For our elimination polynomials ε_i, a corresponding equation follows immediately from (11), which is a direct consequence of Lemma 2, (7a):

$$\tilde{q}_i f_1 = \tilde{g}_i f_i - \varepsilon_i \tilde{g}_{i-1} f_{i+1}, \quad \text{for} \quad i = 2, \ldots, k-1 \tag{17b}$$

Here the definition of $\tilde{q}_i$ and $\tilde{g}_i$ follows by comparison with (11). The rest of Kalkbrenner's proof directly carries over to our case. ■

Theorem 5. Let f_1 and f_2 be relatively prime.

(a) There exist polynomials g and h in $K[x_1, \ldots, x_n]$ such that

$$g f_2 + h f_1 = \prod_{j=2}^{k-1} \varepsilon_j$$

(b) The polynomial $\prod_{j=2}^{k-1} \varepsilon_j$ divides the resultant $res(f_1, f_2, x_n)$.

Proof. (a) follows directly from (4). The proof of (b) can be performed ecactly like Kalkbrener's proof of his Theorem 4 (b), using again (17). ∎

Theorem 6 (Kalkbrener [1991]). Let $\ell c(f_1)$ and $\ell c(f_2)$ be relatively prime. Then

$$\prod_{r=2}^{k-1} e_r = \textit{squarefree}(res(f_1, f_2, x_n))$$

Corollary. If f_1 and f_2 are relatively prime,

$$\prod_{j=2}^{k-1} e_j = \textit{squarefree}(\prod_{j=2}^{k-1} \varepsilon_j)$$

Proof of the Corollary. By Theorem 1 (b) and Theorem 5 (b),

$$\prod_{j=2}^{k-1} e_j \ \textit{divides} \ \prod_{j=2}^{k-1} \varepsilon_i \quad \textit{divides} \quad res(f_1, f_2, x_n).$$

Let p denote an irreducible factor of $\prod_{j=2}^{k-1} \varepsilon_j$. Then, p divides $res\,(f_1, f_2, x_n)$, which by Theorem 6 implies that p divides $\prod_{j=2}^{k-1} e_j$. ∎

References

Gröbner, W. Algebraische Geometrie I. Bibliographisches Institut Mannheim, 1968

Kalkbrener, M. Three contributions to elimination theory.
PhD thesis, Research Institute for Symbolic Computation, Univ. of Linz, Austria, 1991

Kalkbrener, M. Primitive Polynomial Remainder Sequences in Elimination Theory.
Applicable Algebra in Engineering, Communication and Computing 6, 65 - 79, 1995

Netto, E. Vorlesungen über Algebra, Zweiter Band, Teubner, Leibzig, 1900