On Approximate Irreducibility of Polynomials in Several Variables*

Erich Kaltofen
Department of Mathematics
North Carolina State University
Raleigh, North Carolina 27695-8205 USA
kaltofen@math.ncsu.edu;
http://www.kaltofen.us

John May
Department of Mathematics
North Carolina State University
Raleigh, North Carolina 27695-8205 USA
jpmay@math.ncsu.edu;
http://www.math.ncsu.edu/~jpmay

ABSTRACT

We study the problem of bounding all factorizable polynomials away from a polynomial that is absolutely irreducible. Such separation bounds are useful for testing whether a numerical polynomial is absolutely irreducible, given a certain tolerance on its coefficients. Using an absolute irreducibility criterion due to Ruppert, we are able to find useful separation bounds, in several norms, for bivariate polynomials. We also use Ruppert's criterion to derive new, more effective Noether forms for polynomials of arbitrarily many variables. These forms lead to small separation bounds for polynomials of arbitrarily many variables.

Categories and Subject Descriptors

I.1.2 [**Computing Methodologies**]: Symbolic and Algebraic Manipulation—*Algebraic Algorithms*; G.1.2 [**Mathematics of Computing**]: Numerical Analysis—*Approximation*

General Terms

Algorithms

Keywords

multivariate polynomial factorization, absolute irreducibility, radius of irreducibility, approximate factorization, symbolic/numeric hybrid method, effective Noether irreducibility forms

1. INTRODUCTION

We consider the problem of factoring a bivariate polynomial $f(x,y) \in \mathbb{C}[x,y]$, where the actual coefficients of f are rational real or complex numbers. By introduction of floating point arithmetic or through a physical measurement, the input polynomial f is an approximation of a reducible polynomial $\tilde{f} \in \mathbb{C}[x,y]$, but f itself is irreducible over $\mathbb{C}$; that is, absolutely irreducible. A factorization $\tilde{f} = gh$ is thus an approximate factorization of f.

This problem appears to have first been recognized in [14, concluding remarks], and the optimization version of the problem, namely computing in polynomial time the nearest $\tilde{f}$ that factors, is stated as an open problem in [15, 17]. No polynomial-time algorithm is known today, except when one of the factors g or h is required to have a given constant degree [11]. However, when f is near a factorizable $\tilde{f}$, one can use techniques from numerical analysis, and many researchers have studied this variant [25, 24, 7, 12, 23, 6, 4, 3]. Nagasaka [20] has reversed the problem formulation by giving algorithms that compute a good separation bound for f when f is not near a reducible polynomial. The idea is, more precisely, that one computes a value $B(f) \in \mathbb{R}_{>0}$ such that all $\tilde{f} \in \mathbb{C}[x,y]$ with $\|f - \tilde{f}\| < B(f)$ (and $\deg(\tilde{f}) \le \deg(f)$) must remain absolutely irreducible. If $B(f)$ is not too small, one can then declare f numerically irreducible. The largest possible $B(f)$ constitutes the distance to the nearest factorizable polynomial and can be called the radius of irreducibility. The norm $\|\cdot\|$ is a choice, as different distance measures can lead to different bounds (cf. [10, 11, 26]). We note that Nagasaka's algorithms require that a certain condition on f is satisfied.

Our paper provides an algorithm for computing separation bounds $B(f)$ for an arbitrary irreducible bivariate polynomial f. We combine an absolute irreducibility criterion by Ruppert [21, 22] with the theory of the nearest rank-deficient matrix. Already Gao [8] realized the powerful algorithmic implications of Ruppert's partial differential equation, and with Rodrigues [9] applied it to absolute irreducibility of sparse polynomials modulo p. By using the original Eckart and Young theorem [5] (on complex matrices [27]) we can quickly obtain separation bounds that apply for the Euclidean distance norm on the coefficient vector of f. Our technique, applied to the example polynomial in Nagasaka's paper, produces a bound several times larger than the one he computes. We can give an explicit formula in terms of the smallest singular value of a certain sparse matrix that has integer multiples of the coefficients of f as entries. However, like in [9] further computation can adapt to the possibly sparse structure of f and improve $B(f)$. In order to

[*] This material is based on work supported in part by the National Science Foundation under Grants Nos. CCR-9988177 and ITR/ASC-0113121.

ISSAC'03, August 3–6, 2003, Philadelphia, Pennsylvania, USA.
Copyright 2003 ACM 1-58113-641-2/03/0008 ...$5.00.

generalize our approach to 1- and ∞-norm, we make use of the theory of Moore-Penrose pseudo-inverses. Thus all our algorithms are of polynomial-time complexity.

Aside from the choice of norm, there is the issue of the $\deg(\tilde{f})$. Our bounds limit the degrees in the individual variables, that is $\deg_x(\tilde{f}) \le \deg_x(f)$ and $\deg_y(\tilde{f}) \le \deg_y(f)$ (rectangular polynomials), but allows for $\deg_x(\tilde{f}) < \deg_x(f)$ or $\deg_y(\tilde{f}) < \deg_y(f)$ or both. The latter requires an additional argument. However, we do not allow $\deg_x(\tilde{f}) > \deg_x(f)$, for instance, as there is a reducible polynomial of higher degree arbitrarily close to any given polynomial f, namely $(\epsilon x + 1)f$ with a suitably small choice of ϵ.

We will show that for $x^2 + y^2 - 1$ the nearest factorizable polynomial $\tilde{f}$ whose total degree is bounded by 2 has larger Euclidean distance than the nearest rectangular polynomial. Lastly, our bounds trivially yield a relative error tolerance $B(f)/\|f\|$.

Very small separation bounds were also derived in [16, Section 7] for an arbitrary number of variables. There, the bounds are derived by analyzing the largest changes in the coefficients that keeps a Noether form non-zero. Ruppert's approach can be employed to get smaller, in degree and coefficient size, Noether forms, which via techniques in [16] can be extended to an arbitrary number of variables. This paper derives these new Noether forms for arbitrarily many variables. To our knowledge, these are the most effective known Noether forms. These can be used to find separation bounds for an arbitrary number of variables which are quite small, but better than those in [16].

2. IRREDUCIBILITY TEST

A bivariate polynomial f, with $\deg_x f = m$, and $\deg_y f = n$, can be tested for absolute irreducibility using the following fact due to Ruppert [22].

Fact 1. *Suppose $f \in \mathbb{K}[x,y]$, where $\mathbb{K}$ is an arbitrary field of characteristic 0, then f is absolutely irreducible, that is irreducible over the algebraic closure of $\mathbb{K}$, if and only if there are no non-trivial solutions to*

$$\frac{\partial}{\partial y}\frac{g}{f} = \frac{\partial}{\partial x}\frac{h}{f} \tag{1}$$

where $\deg_x g \le m-1$, $\deg_y g \le n$, $\deg_x h \le m$, *and* $\deg_y h \le n-2$.

Note that the degree bounds are chosen to exclude the solution $g = \partial f/\partial x$, $h = \partial f/\partial y$.

Notice that by using the quotient rule (1) can be rewritten as

$$f\frac{\partial g}{\partial y} - g\frac{\partial f}{\partial y} + h\frac{\partial f}{\partial x} - f\frac{\partial h}{\partial x} = 0 \tag{2}$$

which gives $4mn$ linear equations in the coefficients of g and h. Thus we have a $(4mn) \times (2mn + n - 1)$ matrix $R(f)$, the Ruppert matrix of f, which is full rank if and only if f is absolutely irreducible.

Example 1. Given the polynomial

$$\varphi = c_{2,2}x^2y^2 + c_{2,1}x^2y + c_{1,2}xy^2 + c_{2,0}x^2 + c_{0,2}y^2 + c_{1,1}xy + c_{1,0}x + c_{0,1}y + c_{0,0},$$

the matrix $R(\varphi)$ is 12×9 with zero rows removed (see Figure 1 on page 163). If we specialize to $f = x^2 + y^2 - 1$ we get a 12×9 matrix, with two zero rows which has rank 9 since f is absolutely irreducible. Note that the symmetry of f is not being exploited here. □

Given a matrix $A \in \mathbb{C}^{\mu\times\nu}$ the Frobenius norm will be denoted as $\|A\|_F$ and is equal to the 2-norm of the matrix considered as a vector. That is $\|A\|_F^2 = \sum_{i,j} |A_{i,j}|^2$.

We now state a classic linear algebra theorem by Eckart and Young [5], which is proved for complex matrices in a book by G. W. Stewart [27, Theorem 6.7].

Fact 2. *Let $A \in \mathbb{C}^{\mu\times\nu}$ be a matrix of rank r. If $B \in \mathbb{C}^{\mu\times\nu}$ has rank strictly less than r, then $\|A - B\|_F \ge \sigma(A)$, where $\sigma(A)$ denotes the smallest positive singular value of the matrix A. Furthermore, there exists B of rank $r-1$ so that $\|A - B\|_F = \sigma(A)$.*

Let us now suppose that f is irreducible and both f_Δ and $\tilde{f} = f - f_\Delta$ have the same degrees as f in both variables. Here $\tilde{f}$ denotes the perturbed polynomial and f_Δ the perturbation. Hence $R(f_\Delta)$ and $R(\tilde{f})$ have the same dimensions as $R(f)$, thus $R(f_\Delta) = R(f - \tilde{f})$ is equal to $R(f) - R(\tilde{f})$. If $\tilde{f}$ is factorizable, then $R(\tilde{f})$ must be rank deficient. Because $R(f)$ is of full rank and $R(\tilde{f})$ is rank deficient, Fact 2 implies

$$\|R(f_\Delta)\|_F \ge \sigma(R(f)). \tag{3}$$

Note that the restriction that f_Δ has the same degrees as f is artificial, and we will introduce notation later which will allow f_Δ to have smaller degrees.

It should be noted that although the estimate (3) is sharp for general matrices, due to the structure of the Ruppert matrices, it may be that

$$\min_{\substack{\deg_x(\tilde{f})=m,\deg_y(\tilde{f})=n\\ \operatorname{rank} R(\tilde{f})<2mn+n-1}} \|R(f) - R(\tilde{f})\|_F \gg \sigma(R(f)).$$

Parts of the following lemma and lemma 5 are similar to parts of the proof of Theorem 6 in [9] which are used to bound the norms of the rows of a modified Ruppert matrix.

Lemma 1. *All the entries of $R(f)$ are integer multiples of coefficients of f, or are equal to 0. In fact, if $f = \sum c_{i,j}x^iy^j$, then at most $2mn - m$ multiples of $c_{i,j}$ appear in $R(f)$, and each multiple, $ac_{i,j}$, satisfies: $|a| \le \max\{m,n\}$.*

Proof. First, let $g = \sum u_{i,j}x^iy^j$, and $h = \sum v_{i,j}x^iy^j$ be the polynomials with unknown coefficients in (1). Now, notice that an entry of $R(f)$ is a coefficient of either $u_{s,t}\,x^iy^j$ or $v_{s,t}\,x^iy^j$ in (2). Next, for a given $u_{s,t}\,x^iy^j$, we determine its coefficient. The only terms containing $u_{s,t}$ are $u_{s,t}x^sy^t$ appearing in g, and $t\,u_{s,t}\,x^sy^{t-1}$ appearing in $\partial g/\partial y$. The term $c_{k,l}\,x^ky^l = c_{i-s,j-t+1}x^{i-s}y^{j-t+1}$, appearing in f, and $lc_{k,l}x^ky^{l-1}$ appearing in $\partial f/\partial y$ are the only two terms which will multiply with either of the terms containing $u_{s,t}$ to result in a term containing x^iy^j. Thus, $(t-l)\,c_{k,l}$ is the coefficient of $u_{s,t}\,x^iy^j$, and similarly, $(k-s)\,c_{k,l}$ is the coefficient of $v_{s,t}\,x^iy^j$.

Let us look at how many times a given $c_{k,l}$ can appear in a column of $R(f)$, i.e. how many times it can appear multiplied by a given $u_{s,t}$ or $v_{s,t}$ in (2). It is clear that $c_{k,l}u_{s,t}$ can appear at most twice, once in $f\,\partial g/\partial y$ and once in $g\,\partial f/\partial y$. However, as seen above, these two will both be coefficients of $x^{k+s}y^{l+t-1}$. Hence the only term containing both $c_{k,l}$ and $u_{s,t}$ is $(t-l)\,c_{k,l}\,u_{s,t}\,x^{i-s}y^{j-t-1}$, and similarly, the only term containing both $c_{l,k}$ and $v_{s,t}$ is $(k-s)\,c_{k,l}\,v_{s,t}\,x^{i-s-1}y^{j-t}$.

$$\begin{array}{c|ccccccccc|}
 & u_{0,0} & v_{0,0} & u_{0,1} & u_{1,0} & v_{1,0} & u_{0,2} & u_{1,1} & v_{2,0} & u_{1,2} \\
1 & -c_{0,1} & c_{1,0} & c_{0,0} & 0 & -c_{0,0} & 0 & 0 & 0 & 0 \\
y & -2\,c_{0,2} & c_{1,1} & 0 & 0 & -c_{0,1} & 2\,c_{0,0} & 0 & 0 & 0 \\
x & -c_{1,1} & 2\,c_{2,0} & c_{1,0} & -c_{0,1} & 0 & 0 & c_{0,0} & -2\,c_{0,0} & 0 \\
y^2 & 0 & c_{1,2} & -c_{0,2} & 0 & -c_{0,2} & c_{0,1} & 0 & 0 & 0 \\
xy & -2\,c_{1,2} & 2\,c_{2,1} & 0 & -2\,c_{0,2} & 0 & 2\,c_{1,0} & 0 & -2\,c_{0,1} & 2\,c_{0,0} \\
x^2 & -c_{2,1} & 0 & c_{2,0} & -c_{1,1} & c_{2,0} & 0 & c_{1,0} & -c_{1,0} & 0 \\
xy^2 & 0 & 2\,c_{2,2} & -c_{1,2} & 0 & 0 & c_{1,1} & -c_{0,2} & -2\,c_{0,2} & c_{0,1} \\
x^2y & -2\,c_{2,2} & 0 & 0 & -2\,c_{1,2} & c_{2,1} & 2\,c_{2,0} & 0 & -c_{1,1} & 2\,c_{1,0} \\
x^3 & 0 & 0 & 0 & -c_{2,1} & 0 & 0 & c_{2,0} & 0 & 0 \\
x^2y^2 & 0 & 0 & -c_{2,2} & 0 & c_{2,2} & c_{2,1} & -c_{1,2} & -c_{1,2} & c_{1,1} \\
x^3y & 0 & 0 & 0 & -2\,c_{2,2} & 0 & 0 & 0 & 0 & 2\,c_{2,0} \\
x^3y^2 & 0 & 0 & 0 & 0 & 0 & 0 & -c_{2,2} & 0 & c_{2,1}
\end{array}$$

Figure 1: The matrix of the linear equations in (2) for a symbolic polynomial with degree two in x and y.

Thus, there is only one multiple of $c_{i,j}$ in each column, and $|k-s|, |l-t| \leq \max\{m,n\}$.

Notice that there is not a multiple of $c_{i,j}$ in every column. For $j=0$, $c_{i,0}u_{k,0}$ would have to be a coefficient of $x^{i+k}y^{-1}$, so it does not appear in (2) for any k. Similarly for $i=0$, $c_{0,j}u_{0,l}$ does not appear in (2) for any l. The term $j\,c_{i,j}u_{k,j}x^{i+k}y^{2j-1}$ appears in both $f\,\partial g/\partial y$ and $g\,\partial f/\partial y$, hence cancels, and does not appear in (2). So, a given $c_{i,j}$ does not appear in the columns corresponding to $u_{k,j}$ for any k. Similarly, a given $c_{i,j}$ does not appear in the columns corresponding to $v_{i,l}$ for any l. Therefore, $c_{i,j}$ can appear in at most $2mn-m$ columns. □

As a consequence of the proof of Lemma 1, we see that all the terms containing y^{2n-1} vanish. So in fact the matrix $R(f)$ has dimensions at most $(4mn-2m)\times(2mn+n-1)$ after the zero rows are removed.

Suppose φ is a polynomial with symbolic coefficients with $\deg_x(\varphi)=\deg_x(f)=m$ and $\deg_y(\varphi)=\deg_y(f)=n$. For a perturbation $f_\vartriangle$ with $\deg_x(f_\vartriangle)\leq m$ and $\deg_y(f_\vartriangle)\leq n$ we consider the matrix $R(\varphi)\big|_{\varphi=f_\vartriangle}$, which denotes the Ruppert matrix of φ with the symbolic coefficients set to their values in $f_\vartriangle$. However, notice that $R(\varphi)\big|_{\varphi=f_\vartriangle}$ is only the same as $R(f_\vartriangle)$ if φ has the same degrees as $f_\vartriangle$, and if that is not the case, then Fact 1 does not apply.

Now, applying Lemma 1 to $R(\varphi)\big|_{\varphi=f_\vartriangle}$ we have

$$\begin{aligned}
\|R(\varphi)\big|_{\varphi=f_\vartriangle}\|_F^2 &= \sum_{\substack{1\leq i\leq 4mn\\ 1\leq j\leq 2mn+n-1}} \left|\left(R(\varphi)\big|_{\varphi=f_\vartriangle}\right)_{i,j}\right|^2 \\
&= \sum_{\substack{1\leq i\leq 4mn\\ 1\leq j\leq 2mn+n-1}} |a_{i,j}b_{k_{i,j}}|^2 \\
&\leq \max\{a_{i,j}^2\} \sum_{\substack{1\leq i\leq 4mn\\ 1\leq j\leq 2mn+n-1}} |b_{k_{i,j}}|^2 \\
&\leq (\max\{m,n\})^2(2mn-m)\|f_\vartriangle\|_2^2, \qquad (4)
\end{aligned}$$

where b_k is a coefficient of $f_\vartriangle$ or is zero.

Theorem 1. *If $f\in\mathbb{C}[x,y]$ is irreducible, $\tilde{f}\in\mathbb{C}[x,y]$ does not have greater degree than f in either variable, and*

$$\|f-\tilde{f}\|_2 < \frac{\sigma(R(f))}{\max\{m,n\}\sqrt{2mn-m}},$$

then $\tilde{f}$ is irreducible.

Proof. We begin with the case that $\tilde{f}$ has the same degrees in each variable as f. By (4) applied to $f_\vartriangle = f-\tilde{f}$ we have

$$\begin{aligned}
\|R(f)-R(\tilde{f})\|_F = \|R(\varphi)\big|_{\varphi=f-\tilde{f}}\|_F &= \|R(\varphi)\big|_{\varphi=f_\vartriangle}\|_F \\
&\leq \max\{m,n\}\sqrt{2mn-m}\;\|f_\vartriangle\|_2 \\
&< \sigma(R(f)). \qquad (5)
\end{aligned}$$

Now, since f is irreducible, $R(f)$ is full rank by Fact 1. Hence, Fact 2 with (5) implies that $R(\tilde{f})$ must also be full rank. Thus, $\tilde{f}$ is irreducible, again by Fact 1.

We now assume that $\tilde{f}$ has smaller degree than f. In order to derive a contradiction, let us assume now that $\tilde{f}=gh$ where g,h are non-unit factors, and

$$\|f-\tilde{f}\|_2 < \left(\max\{m,n\}\sqrt{2mn-m}\right)^{-1}\sigma(R(f)).$$

Now we can construct

$$\tilde{\tilde{f}} = (\epsilon\,(x^s+y^t)+g)\,h = \epsilon\,(x^s+y^t)\,h+\tilde{f}$$

with $s=\deg_x(f)-\deg_x(h)$ and $t=\deg_y(f)-\deg_y(h)$, and $\epsilon\in\mathbb{R}_{>0}$ chosen so that

$$\epsilon < \frac{\left(\max\{m,n\}\sqrt{2mn-m}\right)^{-1}\sigma(R(f)) - \|f-\tilde{f}\|_2}{\|(x^s+y^t)h\|_2}.$$

Furthermore, we restrict ϵ so that $\tilde{\tilde{f}}$ has the same degree as f. This is possible because there are at most two values of ϵ which can cause $\epsilon\,(x^s + y^t)\,h + \tilde{f}$ to have lower degree than f, while we have infinite choice for ϵ which satisfy the inequality. Thus, $\tilde{\tilde{f}}$ has the same degree as f, but

$$\begin{aligned}\|f - \tilde{\tilde{f}}\|_2 &\le \|f - \tilde{f}\|_2 + \epsilon\,\|(x^s + y^t)\,h\|_2 \\ &< \left(\max\{m, n\}\sqrt{2mn - m}\right)^{-1} \sigma(R(f)),\end{aligned}$$

which contradicts the first part of the proof. □

Note that this theorem does not hold if we allow the degrees of $\tilde{f}$ to be greater than those of f. For all f and $\epsilon > 0$, $\tilde{f} = (\epsilon\,x + 1)f$ is a polynomial of higher degree than f which is reducible. But,

$$\|\tilde{f} - f\| = \|\epsilon\,x\,f\| = \epsilon\,\|f\|$$

which, by choosing ϵ small enough, can be made arbitrarily small.

In practice, it is possible to get a better denominator than $\max\{m, n\}\sqrt{2mn - m}$ by forming the Ruppert matrix for the polynomial with symbolic coefficients having the same degrees as f, computing the square of its Frobenius norm, and finding the largest coefficient of a $|c_{i,j}|^2$. This can be seen in the following examples.

Example 2. (bounds vs. true distance.) Using the notation of Example 1, consider again the absolutely irreducible polynomial $f = x^2 + y^2 - 1$. Computing $\|R(\varphi)\|_F^2$, we get:

$$\begin{aligned}15\ |c_{0,2}|^2 + 15\ |c_{2,2}|^2 + 15\ |c_{2,0}|^2 + 12\ |c_{1,2}|^2 + 9\ |c_{2,1}|^2 \\ + 6\ |c_{1,1}|^2 + 15\ |c_{0,0}|^2 + 12\ |c_{1,0}|^2 + 9\ |c_{0,1}|^2\,.\end{aligned}$$

The largest coefficient is 15 (the bound predicted in the theorem is 24), and the smallest singular value of $R(f)$ is $\sigma(R(f)) \approx 0.613616017571412930$, so a perturbation which makes f singular must have 2-norm at least $\sigma(R(f))/\sqrt{15} \approx 0.1584349745$.

This polynomial is small enough that it is possible to find the closest factorizable polynomial (with real coefficients, and same *total* degree) by using parametric least squares as in [11]. This involves taking the equation

$$f - (a_1\,x + a_2\,y + a_3)(x + b_1\,y + b_2) = 0 \qquad (6)$$

and considering it as a set of linear equations in a_1, a_2, and a_3. We can write this as a linear system: $Ma = F$, where the matrix M has coefficients in $\mathbb{R}[b_1, b_2]$, and F is a vector of the coefficients of f. Now the residual of the least squares solution of this system,

$$q = \|F - M(M^TM)^{-1}M^TF\|_2,$$

is a rational function in b_1 and b_2. We can find a global minimum of q by taking the partial derivatives of its numerator, q_1 and q_2, and solving $\mathrm{Res}_{b_2}(q_1, q_2) = 0$. Once we have a real solution $b_1 = \alpha_1$, we can solve $\gcd(q_1(\alpha_1, b_2), q_2(\alpha_1, b_2)) = 0$ for corresponding real α_2's. We check all such pairs, and substitute the pair which leads to the smallest residual back into M. We thus obtain a linear system over $\mathbb{R}$, so we can compute the least squares solution. Doing so, we find that closest reducible polynomials *with real coefficients* and total degree 2 are at least distance 1 from f, for example,

$$\tilde{f} = (x - 1)(x + 1).$$

The closest reducible polynomial with degree 2 in x and y is closer. For example, the following $\tilde{f}$ is only distance 0.6727223250 away from f:

$$\tilde{f} = (0.4906834y^2 + 0.8491482x - 0.9073464)(x + 1.214778).$$

Finding the closest factorizable polynomial *with complex coefficients* is computationally more difficult, since each parameter above turns into two parameters, one each for the real and the imaginary parts. □

Example 3. (comparison with [20].) Apply the Theorem 1 to Nagasaka's [20] Example 1:

$$F = (x^2 + yx + 2y - 1)(x^3 + y^2x - y + 7) + 0.2x$$

Here, $R(F)$ is a 47×32 matrix after removing the zero rows. Forming the symbolic polynomial with the same degrees and computing its Frobenius norm, we get:

$$\begin{aligned}&140|c_{0,1}|^2 + 140|c_{0,2}|^2 + 180|c_{0,3}|^2 + 92|c_{1,1}|^2 + 132|c_{1,3}|^2 \\ &+ 68|c_{2,1}|^2 + 92|c_{1,2}|^2 + 68c_{2,2}|^2 + 108|c_{2,3}|^2 + 68|c_{3,1}|^2 \\ &+ 92|c_{4,1}|^2 + 108|c_{3,3}|^2 + 68|c_{3,2}|^2 + 180|c_{5,3}|^2 + 140|c_{5,2}|^2 \\ &+ 132|c_{4,3}|^2 + 140|c_{5,1}|^2 + 92|c_{4,2}|^2 + 108|c_{3,0}|^2 + 108|c_{2,0}|^2 \\ &+ 132|c_{1,0}|^2 + 180|c_{0,0}|^2 + 180|c_{5,0}|^2 + 132|c_{4,0}|^2\end{aligned}$$

The largest coefficient is 180, so by the theorem, a perturbation with 2-norm at least $\sigma(R(F))/\sqrt{180}$ is needed to make F reducible. We compute $\sigma(R(F)) \approx 0.01030023214$, so the bound is 0.0007677339751. The norm $||f||_2 \approx 19.85044080$, and dividing the absolute bound by this gives a relative bound of 0.00003867591571, which is about 7 times better than Nagasaka's relative bound of 0.00000553. □

3. OTHER NORMS

Similar results as those in the previous section can be had for the ∞- and 1-norms of polynomials. First, we need to introduce a few linear algebra concepts. We will write $\|A\|_{p,q}$ for the matrix operator norm defined as $\max_{x \ne 0} \|Ax\|_p/\|x\|_q$ or equivalently as $\max_{\|x\|_q = 1} \|Ax\|_p$. By the definition of the norm, it follows that for all x,

$$\|Ax\|_p \le \|A\|_{p,q}\|x\|_q.$$

When $p = q$ we get the the standard matrix operator norms, some of which can be computed quite easily. The 1-norm for example,

$$\|A\|_1 = \|A\|_{1,1} = \max_j \Big\{ \sum_{i,j} |A_{i,j}| \Big\},$$

the largest absolute column sum. The ∞-norm as well,

$$\|A\|_\infty = \|A\|_{\infty,\infty} = \max_i \Big\{ \sum_{i,j} |A_{i,j}| \Big\},$$

the largest absolute row sum. The height of a matrix can also be represented as one of these norms.

Lemma 2. $\|A\|_{\infty,1} = H(A) = \max_{i,j}\{|A_{i,j}|\}$.

Proof. Clearly $H(A) \le \|A\|_{\infty,1}$ since if z is the unit vector with a 1 in the position of the column containing the entry of largest absolute value, and zeros elsewhere, then $\|Az\|_\infty$ is just the maximum of the absolute values of entries in that column.

Now if $\|x\|_1 = 1$, then

$$\begin{aligned}|(Ax)_i| &\le \sum_j |A_{i,j}||x_j| \\ &\le \max_j\{|A_{i,j}|\} \sum_j |x_j| = \max_j\{|A_{i,j}|\}.\end{aligned}$$

So

$$\|A\|_{\infty,1} = \max_{\|x\|_1=1} \|Ax\|_\infty \le \max_{i,j}\{|A_{i,j}|\} = H(A). \quad \square$$

There seems to be no explicit formula for $\|A\|_{1,\infty}$, but we can get an upper bound which will be useful later.

Lemma 3. $\|A\|_{1,\infty} \le \sum_{i,j} |A_{i,j}|$

Proof. If $\|x\|_\infty = 1$, then

$$\begin{aligned}\|Ax\|_1 &= \sum_i \Big| \sum_j A_{i,j}x_j \Big| \le \sum_i \sum_j |A_{i,j}||x_j| \\ &\le \max_j\{|x_j|\} \sum_{i,j} |A_{i,j}| = \sum_{i,j} |A_{i,j}|.\end{aligned}$$

Notice that the bound is achieved when A has, for example, all positive real entries and it is possible to find small examples which have norm strictly less than the bound. □

Following [1], we will write $A^\dagger$ to indicate the Moore-Penrose pseudo-inverse of A. That is, the unique matrix such that (i) $AA^\dagger A = A$, (ii) $A^\dagger AA^\dagger = A^\dagger$, (iii) $(AA^\dagger)^H = AA^\dagger$ and (iv) $(A^\dagger A)^H = A^\dagger$. For a given matrix B, by B^H we mean the Hermitian (conjugate transpose) of B. In particular, we are interested in the following property of $A^\dagger$ (see [1, p. 9]): if x is in the row space of A then $A^\dagger Ax = x$.

The following is a slight variation of a theorem found in [1, Prop. 10.4.2] which is a generalization of a theorem by Gastinel for invertible matrices [13, p. 775]. This is essentially Fact 2 for operator norms.

Lemma 4. *Suppose A has full rank and A has more rows than columns. If $A - A_\vartriangle$ has lower rank than A, then*

$$\|A_\vartriangle\|_{p,q} \ge 1/\|A^\dagger\|_{q,p}.$$

In this case A^HA is invertible and $A^\dagger = (A^HA)^{-1}A^H$.

Proof. If $A - A_\vartriangle$ is rank deficient, then there is a z so that $(A - A_\vartriangle)z = 0$ or, $Az = A_\vartriangle z$. Also note that since A has full rank, its row space contains all vectors of the appropriate dimension, including z. Now compute:

$$\begin{aligned}\|A_\vartriangle\|_{p,q} &\ge \|A_\vartriangle z\|_p/\|z\|_q = \|Az\|_p/\|z\|_q \\ &= \|Az\|_p/\|A^\dagger Az\|_q \ge \|Az\|_p/(\|A^\dagger\|_{q,p}\|Az\|_p) \\ &= 1/\|A^\dagger\|_{q,p}.\end{aligned}$$

The formula for $A^\dagger$ is classical (see for example [1, Theorem 1.3.2]). □

Note that since $R(f)$ always has more rows than columns, Lemma 4 applies. We still need analog of Lemma 1, however.

Lemma 5. *If $f = \sum c_{i,j}x^iy^j$ then:*

1. *There is at most one multiple of $c_{i,j}$ in each column of $R(f)$.*
2. *There are at most two multiples of $c_{i,j}$ in each row of $R(f)$.*

Proof. The first part is shown in the proof of Lemma 1. For the second part, examine the coefficient of a given x^iy^j in (2):

$$\begin{aligned}&\Big(\sum_{\substack{k+s=i\\ l+t=j-1}} c_{k,l}\,t\,u_{s,t}\Big) - \Big(\sum_{\substack{k+s=i\\ l+t=j-1}} l\,c_{k,l}\,u_{s,t}\Big) \\ &\quad + \Big(\sum_{\substack{k+s=i-1\\ l+t=j}} k\,c_{k,l}\,v_{s,t}\Big) - \Big(\sum_{\substack{k+s=i-1\\ l+t=j}} c_{k,l}\,s\,v_{s,t}\Big).\end{aligned}$$

Clearly, a given $c_{l,k}$ can appear at most four times in the coefficient, once in each sum. But, by looking at the indices, it can be seen that all $u_{s,t}$ and $v_{s,t}$ corresponding to a given $c_{k,l}$ have the same indices. Hence, $c_{k,l}$ appears at most twice in any row of $R(f)$, either as $(t-l)\,c_{k,l}\,u_{s,t}$, or as $(k-s)\,c_{k,l}\,v_{s,t}$. □

Using the previous Lemma 5 and Lemma 1 we can find the following bounds (cf. (4)):

$$\|R(\varphi)\big|_{\varphi=f_\vartriangle}\|_1 \le \max\{m,n\}\|f_\vartriangle\|_1 \tag{7}$$

$$\|R(\varphi)\big|_{\varphi=f_\vartriangle}\|_\infty \le 2\max\{m,n\}\|f_\vartriangle\|_1 \tag{8}$$

$$\|R(\varphi)\big|_{\varphi=f_\vartriangle}\|_{\infty,1} \le \max\{m,n\}\|f_\vartriangle\|_\infty. \tag{9}$$

Theorem 2. *If $f \in \mathbb{C}[x,y]$ is an irreducible polynomial, and $\tilde{f} \in \mathbb{C}[x,y]$ is a factorizable polynomial of equal or lesser degrees, then:*

1. $\|f - \tilde{f}\|_1 \ge (\max\{m,n\}\,\|R(f)^\dagger\|_1)^{-1}$
2. $\|f - \tilde{f}\|_1 \ge (2\max\{m,n\}\,\|R(f)^\dagger\|_\infty)^{-1}$
3. $\|f - \tilde{f}\|_\infty \ge (\max\{m,n\}\,\|R(f)^\dagger\|_{1,\infty})^{-1}$ $\ge (\max\{m,n\}\,\sum_{i,j}|R(f)^\dagger_{i,j}|)^{-1}$

Proof. Begin by assuming that f and $\tilde{f}$ have the same degrees. If there is a constant C so that

$$\|R(\varphi)\big|_{\varphi=f_\vartriangle}\|_{p,q} \le C\|f_\vartriangle\|_r \tag{10}$$

then since $\tilde{f}$ is factorizable, Lemma 4 and (10) imply

$$\begin{aligned}\|R(f)^\dagger\|_{q,p}^{-1} &\le \|R(f) - R(\tilde{f})\|_{p,q} = \|R(\varphi)\big|_{\varphi=f-\tilde{f}}\|_{p,q} \\ &= \|R(\varphi)\big|_{\varphi=f_\vartriangle}\|_{p,q} \le C\|f_\vartriangle\|_r.\end{aligned}$$

Hence,

$$\|f_\vartriangle\|_r = \|f - \tilde{f}\|_r \ge (C\|R(f)^\dagger\|_{q,p})^{-1}.$$

Using (7) for (10) proves part 1 of the theorem. Similarly, (8) and (9) prove parts 2 and 3 respectively. Thus all the parts of the theorem are proven when the degrees are the same. If the degrees of $\tilde{f}$ are smaller, the same argument as used in the proof of Theorem 1 will work here as well. □

In the above theorem, we give 2 bounds for the 1-norm, because the bound in part 2 can be better than the one in part 1. For example, the bound on the 1-norm of $f = x^2y^2 + 0.26y + 1000$ computed as in Example 4 below is better if we use the ∞-norm of its Ruppert matrix.

Notice that this theory does not give any better bound for the 2-norm. However, it can be used to derive Theorem 1 using the matrix 2-norm $||\cdot||_2 = ||\cdot||_{2,2}$. Since for any matrix

A, $||A^\dagger||_2^{-1} = \sigma(A)$, and $||A||_2 \le ||A||_F$. Hence (4) can be used for the bound (10) so if $\tilde{f}$ is reducible,

$$\begin{aligned}\|f-\tilde{f}\|_2 &\ge (\max\{m,n\}\sqrt{2mn-m}\,\|R(f)^\dagger\|_2)^{-1}\\ &= (\max\{m,n\}\sqrt{2mn-m})^{-1}\sigma(R(f)).\end{aligned}$$

We do not give explicit bounds using other matrix p-norms because it seems, in general, difficult to relate the entries of a matrix A to the value of the norm $||A||_{p,q}$.

We add that, unlike the bound in Theorem 1, the bounds in Theorem 2 are rational in the real and imaginary parts of the coefficients of f by virtue of the formula for $R(f)^\dagger$ given in Lemma 4 and the explicit formulas for the 1- and ∞-norms for matrices. Therefore, one may derive bounds using Cramer's rule that depend solely on the degrees of f and $||f||_\infty$ when, for example, the coefficients of f are integers (cf. [16, Section 7]).

Example 4. (example 2 with other norms.) Once again, consider the polynomial $f = x^2 + y^2 - 1$. After computing the pseudo-inverse of $R(f)$, a task which is accomplished easily with the `MatrixInverse` command in Maple version 8, we compute its various norms.

$$\|R(f)^\dagger\|_1 = 5/2,\ \|R(f)^\dagger\|_\infty = 2,\ \|R(f)^\dagger\|_{1,\infty} \le 9.$$

The maximum multiple of an absolute column sum is 2. Observation of a symbolic $R(f)$ shows that the maximum multiple of an absolute row sum is 3, less than the worst case of 4 predicted above, and the maximum multiple of an entry is 2. Hence we get that the ∞-norm of a perturbation of f must be greater than $1/18 \approx 0.05556$, and the 1-norm must be greater than $1/5 = 0.2$ (from the matrix 1-norm), and $1/6 \approx 0.16667$ (from the matrix ∞-norm). □

Example 5. (example 3 with other norms.) We can also compute the bounds on other norms for the polynomial in Example 3. Computing the pseudo-inverse of $R(f)$ we get the norms

$$\|R(f)^\dagger\|_1 \approx 113.598,\quad \|R(f)^\dagger\|_\infty \approx 270.393,$$

$$\|R(f)^\dagger\|_{1,\infty} \le 1192.372.$$

These lead to the bounds:

$$\|f_\triangle\|_1 > 0.001760594950 \text{ and } \|f_\triangle\|_\infty > 0.0001677328901$$

if $f - f_\triangle$ is factorizable. □

We note that the bounds given for the 1-norm in Theorem 2 can be transferred to the 2-norm case via $\|w\|_1 \le \sqrt{d}\,\|w\|_2$ for any $w \in \mathbb{C}^d$. For $\tilde{f} \in \mathbb{C}[x,y]$ we have

$$\begin{aligned}\|f-\tilde{f}\|_2 < \big(&\sqrt{(m+1)(n+1)}\,\max\{m,n\}\times\\ &\min\{\|R(f)^\dagger\|_1, 2\|R(f)^\dagger\|_\infty\}\big)^{-1}\end{aligned} \quad (11)$$

implies $\tilde{f}$ is irreducible. It should be noted that the bound in (11) is almost certainly worse than the bound in Theorem 1. For the polynomial in Examples 3 and 5, (11) yields 0.000359 which is about half as large as the bound derived using Theorem 1. However, as discussed in the paragraph before Example 4, (11) can be used to derive a bound for the 2-norm that depends solely on the degrees and norm of f. Of course, the same applies to the ∞-norm part of Theorem 2, but the bound seems smaller (for Example 3 we obtain 0.000167).

4. SEVERAL VARIABLES

Now we shall derive new Noether irreducibility forms using Fact 1. These new forms will lead to a separation bound for polynomials with more than two variables. Fact 1 applies only to bivariate polynomials, but we can derive forms for polynomials with more variables by first reducing to two variables using the following fact. First, suppose that

$$f = \sum_{e_1+\ldots+e_\eta \le d} c_{e_1,\ldots,e_\eta} x_1^{e_1}\cdots x_\eta^{e_\eta} \in \mathbb{K}[x_1,\ldots,x_\eta],$$

where $\mathbb{K}$ is a field of characteristic 0.

Fact 3. (Lemma 7 in [16]) *Let*

$$L = \mathbb{K}(v_1,\ldots,v_\eta,w_2,\ldots,w_\eta,z_2,\ldots,z_\eta),$$

where $v_1,\ldots,v_\eta,w_2,\ldots,w_\eta,z_2,\ldots,z_\eta$ are indeterminants. The bivariate polynomial

$$\begin{aligned}\hat{f}(x,y) = f(&x+y+v_1, w_2x+z_2y+v_2,\ldots\\ &\ldots, w_\eta x+z_\eta y+v_\eta) \in L[x,y]\end{aligned}$$

is irreducible over the algebraic closure of L if and only if f is irreducible over the algebraic closure of $\mathbb{K}$.

Note that in [16], the substitution for x_1 is $x + v_1$, but the proof follows through using $x + y + v_1$ as given above. The advantage of the latter substitution is that $\deg_x \hat{f} = \deg_y \hat{f} = \operatorname{tdeg} \hat{f} = \operatorname{tdeg} f$ where by tdeg we mean the total degree. This allows us to formulate the following theorem using total degree even though Fact 1 depends on the rectangular degrees.

Theorem 3. (cf. Theorem 7 in [16]) *There exists a finite set of polynomials*

$$\Phi_t \in \mathbb{Z}[\ldots,b_{e_1,\ldots,e_\eta},\ldots] =: E,\ 1 \le t \le T$$

where the $b_{e_1,\ldots,e_\eta}$'s are indeterminants, so that

$$\begin{aligned}&\forall t\colon \Phi_t(\ldots,c_{e_1,\ldots,e_\eta},\ldots) = 0\\ &\qquad\iff f \text{ is not absolutely irreducible or } \operatorname{tdeg} f < d.\end{aligned}$$

Furthermore, for all t,

$$\operatorname{tdeg}\Phi_t \le 2d^2 + d =: D \text{ and}$$

$$\|\Phi_t\|_1 \le (2d)^{4d^2+3d+\eta} =: B. \quad (12)$$

Proof. The proof will closely follow the proof of Theorem 7 in [16]. First, write

$$\varphi = \sum_{e_1+\ldots+e_\eta \le d} b_{e_1,\ldots,e_\eta} x_1^{e_1}\cdots x_\eta^{e_\eta},$$

and

$$\hat{\varphi} = \varphi(x+y+v_1, w_2x+z_2y+v_2,\ldots,w_\eta x+z_\eta y+v_\eta) \in L'[x,y]$$

where $L' = E(v_1,\ldots,v_\eta,w_2,\ldots,w_\eta,z_2,\ldots,z_\eta)$.

Let $\{\Delta_s\}$ be the set of all maximal minors of the matrix $R(\hat{\varphi})$. Define the set

$$\begin{aligned}S := \{\tau \in E \mid\ &\tau \text{ is a coefficient of a term in}\\ &v_1,\ldots,v_\eta,w_2,\ldots,w_\eta,z_2,\ldots,z_\eta \text{ of some } \Delta_s\}.\end{aligned}$$

We shall define the set of irreducibility forms as follows:

$$\{\Phi_t = b_{e_1,\ldots,e_\eta}\tau \in E \mid e_1+\ldots+e_\eta = d,\ \tau \in S\}.$$

Now let us substitute the coefficients of f (the $c_{e_1,\ldots,e_\eta}$'s) for the indeterminants $b_{e_1,\ldots,e_\eta}$. Note that one of our forms $\Phi_t(\ldots, c_{e_1,\ldots,e_\eta}, \ldots) = 0$ if and only if $\tau(\ldots, c_{e_1,\ldots,e_\eta}, \ldots) = 0$ for $\tau \in S$ or $c_{e_1,\ldots,e_\eta} = 0$ for all $e_1+\ldots+e_\eta = d$. The condition $c_{e_1,\ldots,e_\eta} = 0$ for all $e_1+\ldots+e_\eta = d$ holds if and only if f does not have total degree d. Notice, $\tau(\ldots, c_{e_1,\ldots,e_\eta}, \ldots) = 0$ for all $\tau \in S$ if and only if $\Delta_s(\ldots, c_{e_1,\ldots,e_\eta}, \ldots) = 0$. This is true if and only if $R(\hat{\varphi}\big|_{\hat{\varphi}=\hat{f}})$ does not have full rank. Now, if $\operatorname{tdeg} f = d$, then $\deg_x \hat{f} = \deg_x \hat{\varphi} = \deg_y \hat{f} = \deg_y \hat{\varphi} = d$, hence, $R(\hat{f}) = R(\hat{\varphi}\big|_{\hat{\varphi}=\hat{f}})$. Thus, by Fact 1, $R(\hat{f})$ is rank deficient if and only if $\hat{f}$ factors over the algebraic closure of L which is true if and only if f factors over $\mathbb{C}$, by Fact 3.

Now we establish the bounds on Φ_t. Notice that all the coefficients of terms $x^i y^j$ in $\hat{\varphi}$ are linear in the $b_{e_1,\ldots,e_\eta}$'s, hence the entries of $R(\hat{\varphi})$ are also linear in the $b_{e_1,\ldots,e_\eta}$'s by Lemma 1. Thus, any minor of $R(\hat{\varphi})$ will have total degree in the $b_{e_1,\ldots,e_\eta}$'s at most $2d^2+d-1$, the number of columns of $R(\hat{\varphi})$. Therefore the total degree of any Φ_t will be at most $2d^2+d$. To bound the 1-norm, note that each coefficient of $\hat{\varphi}$ has 1-norm at most

$$\binom{d+\eta}{\eta} 3^d =: A \leq (2d)^{d+\eta}.$$

Therefore, a minor of $R(\hat{\varphi})$ has 1-norm at most

$$\begin{aligned} A\,(2d^2+d-1)(2d^2+d-1)! &\leq (2d)^{d+\eta}(2d^2+d-1)^{2d^2+d} \\ &\leq (2d)^{4d^2+3d+\eta} \end{aligned}$$

and $\|\Phi_t\|_1$ must certainly be smaller than this as well. □

The bounds B and D on these new Noether irreducibility forms lead to a separation bound for polynomials with more than two variables. For the following, we will assume that $f \in \mathbb{Z}[x_1, \ldots, x_\eta]$, though similar results can be derived for f which have coefficients in $\mathbb{Z}[\xi]$ where ξ is an algebraic integer over $\mathbb{Q}$.

Fact 4. (Theorem 10 in [16]) *If $\tilde{f} \in \mathbb{C}[x_1, \ldots, x_\eta]$ has the same total degree as f and*

$$\|f - \tilde{f}\|_\infty < 2^{-(d+\eta+1)} D^{-1} B^{-1} (\|f\|_\infty + 1)^{-D}$$

then $\tilde{f}$ is irreducible.

Using the B and D above, we get

$$\|f - \tilde{f}\|_\infty < (2d)^{-(4d^2+4d+2\eta+1)} (\|f\|_\infty + 1)^{-2d^2-d}. \qquad (13)$$

Note that the Noether forms in [16] have bounds

$$D' = 12d^6 \text{ and } B' = (2d)^{12d^7+(12\eta+36)d^6} \qquad (14)$$

which are much larger than the bounds (12), but the forms in [16] apply to fields of positive characteristic as well. The bounds (14) also lead to the much smaller separation bound

$$\|f - \tilde{f}\|_\infty < (2d)^{-(12d^7+29\eta d^6)} (\|f\|_\infty + 1)^{-12d^6}.$$

5. CONCLUDING REMARKS

We have given an efficient algorithm for computing a distance bound that separates an irreducible bivariate polynomial f from a polynomial $\tilde{f}$ that has complex coefficients and factors over the complex numbers. Trivially, our bound also applies when the $\tilde{f}$ is restricted to have real coefficients. However, our approach seems to yield no better bounds in the latter case. Other restrictions for the coefficients of $\tilde{f}$ seem natural, like keeping leading coefficients 1 (monicity) or preserving zero coefficients (sparsity). For those cases we can gain slight improvements in separation (see Example 2). More improvements for sparse polynomials may be obtained by adapting the results in [9] which can be used to further reduce the size of $R(f)$ when f is sparse.

We have generalized Fact 1 to more than two variables, now as a system of partial differential equations. Clearly, our generalization improves on the separation bounds (13) derived for polynomials with more than two variables. These results will be published in the future. It is not clear, however, if they can lead to more effective Noether Forms.

It would be important to have a theory similar to Fact 2 and Lemma 4 for matrices with polynomial entries. In our case, separation from singularity for matrix polynomials applied to the matrix $R(\hat{f})$ in Fact 3 may improve upon the determinantal bound. It seems likely that this would produce more effective Noether forms.

We have also tested an iterative method, similar to the one described in [2], for computing nearby rank-deficient Ruppert matrices. While the iteration converges, it does not necessarily converge to the closest rank-deficient matrix with Ruppert structure. This still might be useful in approximate factoring by using Gao's algorithm [8], but because we can only get a numerically rank-deficient Ruppert matrix, a robust method for computing approximate bivariate GCD's is needed. Our experiments with this can be found at `http://www.math.ncsu.edu/~jpmay/issac03/`.

6. ACKNOWLEDGMENTS

The authors would like to thank the referees whose comments where very useful in improving the final version of this paper.

The authors would also like to acknowledge that the results reported herein were inspired in part by discussions while the authors attended ECCAD 2002 in New York.

7. REFERENCES

[1] Campbell, S. L., and Meyer, Jr., C. D. *Generalized Inverses of Linear Transformations.* Pitman Publ. Ltd., London, 1979.

[2] Chu, M. T., Funderlic, R. E., and Plemmons, R. J. Structured low rank approximation. Paper submitted, 10 pages, 2002.

[3] Corless, R. M., Galligo, A., Kotsireas, I. S., and Watt, S. M. A geometric-numeric algorithm for absolute factorization of multivariate polynomials. In Mora [18], pp. 37–45.

[4] Corless, R. M., Giesbrecht, M. W., van Hoeij, M., Kotsireas, I. S., and Watt, S. M. Towards factoring bivariate approximate polynomials. In Mourrain [19], pp. 85–92.

[5] Eckart, C., and Young, G. The approximation of one matrix by another of lower rank. *Psychometrika 1*, 3 (Sept. 1936), 211–218.

[6] Galligo, A., and Rupprecht, D. Semi-numerical determination of irreducible branches of a reduced space curve. In Mourrain [19], pp. 137–142.

[7] Galligo, A., and Watt, S. A numerical absolute primality test for bivariate polynomials. In *ISSAC 97*

Proc. 1997 Internat. Symp. Symbolic Algebraic Comput. (New York, N. Y., 1997), W. Küchlin, Ed., ACM Press, pp. 217–224.

[8] Gao, S. Factoring multivariate polynomials via partial differential equations. *Math. Comput. 72* (2003), 801–822.

[9] Gao, S., and Rodrigues, V. M. Irreducibility of polynomials modulo p via Newton polytopes. Preprint, 13 pages. Available from `http://www.math.clemson.edu/~sgao/pub.html`. To appear *J. Number Theory*, 2003.

[10] Hitz, M. A., and Kaltofen, E. Efficient algorithms for computing the nearest polynomial with constrained roots. In *Proc. 1998 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'98)* (New York, N. Y., 1998), O. Gloor, Ed., ACM Press, pp. 236–243.

[11] Hitz, M. A., Kaltofen, E., and Lakshman Y. N. Efficient algorithms for computing the nearest polynomial with a real root and related problems. In *Proc. 1999 Internat. Symp. Symbolic Algebraic Comput. (ISSAC'99)* (New York, N. Y., 1999), S. Dooley, Ed., ACM Press, pp. 205–212.

[12] Huang, Y., Wu, W., Stetter, H. J., and Zhi, L. Pseudofactors of multivariate polynomials. In *Internat. Symp. Symbolic Algebraic Comput. ISSAC 2000 Proc. 2000 Internat. Symp. Symbolic Algebraic Comput.* (New York, N. Y., 2000), C. Traverso, Ed., ACM Press, pp. 161–168.

[13] Kahan, W. Numerical linear algebra. *Canadian Math. Bull. 9* (1966), 757–801.

[14] Kaltofen, E. Fast parallel absolute irreducibility testing. *J. Symbolic Comput. 1*, 1 (1985), 57–67. Misprint corrections: *J. Symbolic Comput.* vol. 9, p. 320 (1989).

[15] Kaltofen, E. Polynomial factorization 1987-1991. In *Proc. LATIN '92* (Heidelberg, Germany, 1992), I. Simon, Ed., vol. 583 of *Lect. Notes Comput. Sci.*, Springer Verlag, pp. 294–313.

[16] Kaltofen, E. Effective Noether irreducibility forms and applications. *J. Comput. System Sci. 50*, 2 (1995), 274–295.

[17] Kaltofen, E. Challenges of symbolic computation my favorite open problems. *J. Symbolic Comput. 29*, 6 (2000), 891–919. With an additional open problem by R. M. Corless and D. J. Jeffrey.

[18] Mora, T., Ed. *ISSAC 2002 Proc. 2002 Internat. Symp. Symbolic Algebraic Comput.* (New York, N. Y., 2002), ACM Press.

[19] Mourrain, B., Ed. *ISSAC 2001 Proc. 2001 Internat. Symp. Symbolic Algebraic Comput.* (New York, N. Y., 2001), ACM Press.

[20] Nagasaka, K. Towards certified irreducibility testing of bivariate approximate polynomials. In Mora [18], pp. 192–199.

[21] Ruppert, W. M. Reduzibilität ebener Kurven. *J. reine angew. Math. 369* (1986), 167–191.

[22] Ruppert, W. M. Reducibility of polynomials *f(x,y)* modulo *p*. *J. Number Theory 77* (1999), 62–70.

[23] Sasaki, T. Approximate multivariate polynomial factorization based on zero-sum relations. In Mourrain [19], pp. 284–291.

[24] Sasaki, T., Saito, T., and Hilano, T. Analysis of approximate factorization algorithm I. *Japan J. of Industrial and Applied Mathem. 9*, 3 (Oct. 1992), 351–368.

[25] Sasaki, T., Suzuki, M., Kolář, M., and Sasaki, M. Approximate factorization of multivariate polynomials and absolute irreducibility testing. *Japan J. of Industrial and Applied Mathem. 8*, 3 (Oct. 1991), 357–375.

[26] Stetter, H. J. The nearest polynomial with a given zero, and similar problems. *SIGSAM Bulletin 33*, 4 (Dec. 1999), 2–4.

[27] Stewart, G. W. *Introduction to Matrix Computations*. Academic Press, Inc., New York, 1973.