ISSAC 2003

On Approximate Irreducibility of Polynomials in Several Variables

John May
Joint work with: Erich Kaltofen

North Carolina State University

http://www.kaltofen.us
http://www.math.ncsu.edu/~jpmay

This talk is sponsored by a TATA ECCAD'02 Award

Problem [Nagasaka ISSAC'02]

Given $f \in \mathbb{C}[x,y]$, irreducible, compute "large" $\varepsilon > 0$,
such that $\forall \tilde{f}, \deg \tilde{f} \leq \deg f : \|f - \tilde{f}\| < \varepsilon \Longrightarrow \tilde{f}$ is irreducible.

Problem [Nagasaka ISSAC'02]

Given $f \in \mathbb{C}[x,y]$, irreducible, compute "large" $\varepsilon > 0$,
such that $\forall \tilde{f}, \deg \tilde{f} \le \deg f : \|f - \tilde{f}\| < \varepsilon \Longrightarrow \tilde{f}$ is irreducible.

Problem depends on choice of norm $\|\cdot\|$,
choice of degree.

For $f = x^2 + y^2 - 1$, the 2-norm, and total degree:

$$\tilde{f} = (x-1)(x+1), \|f - \tilde{f}\|_2 = 1.$$

Problem [Nagasaka ISSAC'02]

Given $f \in \mathbb{C}[x,y]$, irreducible, compute "large" $\varepsilon > 0$, such that $\forall \tilde{f}, \deg \tilde{f} \leq \deg f : \|f - \tilde{f}\| < \varepsilon \Longrightarrow \tilde{f}$ is irreducible.

Problem depends on choice of norm $\|\cdot\|$,

choice of degree.

For rectangular degrees we get closer to $f = x^2 + y^2 - 1$:

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

$$= 0.596072y^2 + 0.849148x^2 + 0.490683xy^2 + 0.124180x - 1.102225,$$

$$\|f - \hat{f}\|_2 \approx 0.6727223.$$

Problem [Nagasaka ISSAC'02]

Given $f \in \mathbb{C}[x,y]$, irreducible, compute "large" $\varepsilon > 0$, such that $\forall \tilde{f}, \deg \tilde{f} \leq \deg f : \|f - \tilde{f}\| < \varepsilon \Longrightarrow \tilde{f}$ is irreducible.

Our results apply to the coefficient 1-, 2- and ∞-norms, and the rectangular bi-degree $\deg f = (m,n)$.

New results make it possible to use total degree instead.

Problem [Nagasaka ISSAC'02]

Given $f \in \mathbb{C}[x,y]$, irreducible, compute "large" $\varepsilon > 0$, such that $\forall \tilde{f}, \deg \tilde{f} \le \deg f : \|f - \tilde{f}\| < \varepsilon \Longrightarrow \tilde{f}$ is irreducible.

Degree bound is important:
$(1+\delta x) f$ is reducible but for $\delta < \varepsilon / \|f\|$,

$$\|(1+\delta x) f - f\| = \|\delta x f\| = \delta \|f\| < \varepsilon$$

Ruppert's Theorem

$f \in \mathbb{K}[x,y]$, $\deg f = (m,n)$.

$\mathbb{K}$ is a field, algebraically closed, and characteristic 0.

Theorem. f is reducible $\iff \exists g, h \in \mathbb{K}[x,y]$, non-zero,

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

$$\deg g \leq (m-2, n)\,, \deg h \leq (m, n-1).$$

Ruppert's Theorem

$f \in \mathbb{K}[x,y]$, $\deg f = (m,n)$.

$\mathbb{K}$ is a field, algebraically closed, and characteristic 0.

Theorem. f is reducible $\iff \exists g,h \in \mathbb{K}[x,y]$, non-zero,

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

$$\deg g \leq (m-2,n)\,,\, \deg h \leq (m,n-1).$$

Bounds on the degrees of g and h eliminate the solution $g = \frac{\partial f}{\partial x}$, $h = \frac{\partial f}{\partial y}$.

Ruppert's Theorem

$f \in \mathbb{K}[x,y]$, $\deg f = (m,n)$.

$\mathbb{K}$ is a field, algebraically closed, and characteristic 0.

Theorem. f is reducible $\iff \exists g,h \in \mathbb{K}[x,y]$, non-zero,

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

$$\deg g \leq (m-2,n), \deg h \leq (m,n-1).$$

The PDE can be rewritten as

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

Ruppert's Theorem

$f \in \mathbb{K}[x,y]$, $\deg f = (m,n)$.

$\mathbb{K}$ is a field, algebraically closed, and characteristic 0.

Theorem. f is reducible $\iff \exists g,h \in \mathbb{K}[x,y]$, non-zero,

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

$$\deg g \le (m-2,n)\,,\ \deg h \le (m,n-1).$$

The PDE leads to a set of equations linear in the coefficients of g and h.

Ruppert's Theorem

$f \in \mathbb{K}[x, y]$, $\deg f = (m, n)$.

$\mathbb{K}$ is a field, algebraically closed, and characteristic 0.

Theorem. f is reducible $\iff \exists g, h \in \mathbb{K}[x, y]$, non-zero,

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

$$\deg g \leq (m-2, n), \deg h \leq (m, n-1).$$

The PDE leads to a set of equations linear in the coefficients of g and h.

Given f the PDE gives a matrix $R(f)$.

$R(f)$ is rank deficient $\iff$ f has nontrivial factors.

Structure of $R(f)$ for a generic degree 2 f

$$\begin{bmatrix}
-c_{0,1} & c_{1,0} & c_{0,0} & 0 & -c_{0,0} & 0 & 0 & 0 & 0 \\
-2c_{0,2} & c_{1,1} & 0 & 0 & -c_{0,1} & 2c_{0,0} & 0 & 0 & 0 \\
-c_{1,1} & 2c_{2,0} & c_{1,0} & -c_{0,1} & 0 & 0 & c_{0,0} & -2c_{0,0} & 0 \\
0 & c_{1,2} & -c_{0,2} & 0 & -c_{0,2} & c_{0,1} & 0 & 0 & 0 \\
-2c_{1,2} & 2c_{2,1} & 0 & -2c_{0,2} & 0 & 2c_{1,0} & 0 & -2c_{0,1} & 2c_{0,0} \\
-c_{2,1} & 0 & c_{2,0} & -c_{1,1} & c_{2,0} & 0 & c_{1,0} & -c_{1,0} & 0 \\
0 & 2c_{2,2} & -c_{1,2} & 0 & 0 & c_{1,1} & -c_{0,2} & -2c_{0,2} & c_{0,1} \\
-2c_{2,2} & 0 & 0 & -2c_{1,2} & c_{2,1} & 2c_{2,0} & 0 & -c_{1,1} & 2c_{1,0} \\
0 & 0 & 0 & -c_{2,1} & 0 & 0 & c_{2,0} & 0 & 0 \\
0 & 0 & -c_{2,2} & 0 & c_{2,2} & c_{2,1} & -c_{1,2} & -c_{1,2} & c_{1,1} \\
0 & 0 & 0 & -2c_{2,2} & 0 & 0 & 0 & 0 & 2c_{2,0} \\
0 & 0 & 0 & 0 & 0 & 0 & -c_{2,2} & 0 & c_{2,1}
\end{bmatrix}$$

Generalizations

Gao 2000: Counting Factors

Changes the degree bound: $\deg g \le (m-1, n)$

linearly indep. solutions to the PDE = # factors of f

Requires squarefreeness: $\mathrm{GCD}(f, \frac{\partial f}{\partial x}) = 1$

Generalizations

Gao 2000: Counting Factors

Changes the degree bound: $\deg g \leq (m-1, n)$

linearly indep. solutions to the PDE = # factors of f

Requires squarefreeness: $\mathrm{GCD}(f, \frac{\partial f}{\partial x}) = 1$

Gao and Rodrigues 2002: Sparse Version

If (g, h) is a solution to the PDE, then $P(xg) \subseteq P(f)$, $P(yh) \subseteq P(f)$, where P is the Newton polytope for the term degree pairs.

Generalizations

May 2003: Multivariate Version

$f \in \mathbb{C}[x, y_1, \ldots, y_k]$ is irreducible $\iff \exists g, h_i, 1 \le i \le k$:

$$\frac{\partial}{\partial y_i}\frac{g}{f} - \frac{\partial}{\partial x}\frac{h_i}{f} = 0, \forall 1 \le i \le k$$

$$\deg g \le \deg f, \quad \deg h_i \le \deg f, \forall 1 \le i \le k,$$

$$\deg_x g \le (\deg_x f) - 2, \quad \deg_{y_i} h_i \le (\deg_{y_i} f) - 1, \forall 1 \le i \le k.$$

Distance to the Nearest Reducible Polynomial

For a fixed norm and factor degree:

The problem can be solved by finding the distance to the nearest reducible polynomial [cf. Hitz et al. ISSAC’99].

Distance to the Nearest Reducible Polynomial

For a fixed norm and factor degree:

The problem can be solved by finding the distance to the nearest reducible polynomial [cf. Hitz et al. ISSAC'99].

We can find a lower bound on the radius of irreducibility by:

1. Separating $R(f)$ from rank deficient matrices then
2. relating the norm of $R(f)$ to the norm of f.

Some Linear Algebra

Generalized operator norm of a matrix:

$$\|A\|_{p,q} = \max_{x \neq 0} \|Ax\|_p \big/ \|x\|_q$$

This include all standard operator norms as well as the height of a matrix $H(A) = \|A\|_{\infty,1}$.

Some Linear Algebra

Generalized operator norm of a matrix:

$$\|A\|_{p,q} = \max_{x \neq 0} \|Ax\|_p \big/ \|x\|_q$$

Theorem. Suppose $A \in \mathbb{C}^{\nu \times \mu}$ has full rank and A has more rows than columns. If $A - A_\Delta$ has lower rank than A, then

$$\|A_\Delta\|_{p,q} \geq 1 \big/ \|A^\dagger\|_{q,p}$$

where $A^\dagger = (A^H A)^{-1} A^H$.

Some Linear Algebra

Generalized operator norm of a matrix:

$$\|A\|_{p,q} = \max_{x \neq 0} \|Ax\|_p / \|x\|_q$$

Theorem. Suppose $A \in \mathbb{C}^{\nu \times \mu}$ has full rank and A has more rows than columns. If $A - A_\Delta$ has lower rank than A, then

$$\|A_\Delta\|_{p,q} \geq 1 / \|A^\dagger\|_{q,p}$$

where $A^\dagger = (A^H A)^{-1} A^H$.

If $p = q = 2$, then $\|A^\dagger\|_{q,p}^{-1} = \sigma(A)$, smallest singular value of A.

Structure of $R(f)$

Facts about $R(f)$ where $f = \sum c_{i,j} x^i y^j$:

- All the entries of $R(f)$ are integer multiples of coefficients of f or zero.
- Every multiple in $R(f)$, $ac_{i,j}$, satisfies: $|a| \leq \max\{m,n\}$
- There are at most $2mn - m$ multiples of $c_{i,j}$ in the entries of $R(f)$
- There is at most one multiple of $c_{i,j}$ in each column
- There are at most two multiples of $c_{i,j}$ in each row

Structure of $R(f)$ for a generic degree 2 f

$$\begin{bmatrix}
-c_{0,1} & c_{1,0} & c_{0,0} & 0 & -c_{0,0} & 0 & 0 & 0 & 0 \\
-2c_{0,2} & c_{1,1} & 0 & 0 & -c_{0,1} & 2c_{0,0} & 0 & 0 & 0 \\
-c_{1,1} & 2c_{2,0} & c_{1,0} & -c_{0,1} & 0 & 0 & c_{0,0} & -2c_{0,0} & 0 \\
0 & c_{1,2} & -c_{0,2} & 0 & -c_{0,2} & c_{0,1} & 0 & 0 & 0 \\
-2c_{1,2} & 2c_{2,1} & 0 & -2c_{0,2} & 0 & 2c_{1,0} & 0 & -2c_{0,1} & 2c_{0,0} \\
-c_{2,1} & 0 & c_{2,0} & -c_{1,1} & c_{2,0} & 0 & c_{1,0} & -c_{1,0} & 0 \\
0 & 2c_{2,2} & -c_{1,2} & 0 & 0 & c_{1,1} & -c_{0,2} & -2c_{0,2} & c_{0,1} \\
-2c_{2,2} & 0 & 0 & -2c_{1,2} & c_{2,1} & 2c_{2,0} & 0 & -c_{1,1} & 2c_{1,0} \\
0 & 0 & 0 & -c_{2,1} & 0 & 0 & c_{2,0} & 0 & 0 \\
0 & 0 & -c_{2,2} & 0 & c_{2,2} & c_{2,1} & -c_{1,2} & -c_{1,2} & c_{1,1} \\
0 & 0 & 0 & -2c_{2,2} & 0 & 0 & 0 & 0 & 2c_{2,0} \\
0 & 0 & 0 & 0 & 0 & 0 & -c_{2,2} & 0 & c_{2,1}
\end{bmatrix}$$

2-Norm of $R(f)$ and a Lower Bound

Structure of $R(f)$ leads to relationships between the norms of $R(f)$ and the norms of f:

$$\|R(f)\|_2 \leq \|R(f)\|_{Frob} \leq \max\{m,n\}\sqrt{2mn-n}\,\|f\|_2$$

2-Norm of $R(f)$ and a Lower Bound

Structure of $R(f)$ leads to relationships between the norms of $R(f)$ and the norms of f:

$$\|R(f)\|_2 \leq \|R(f)\|_{Frob} \leq \max\{m,n\}\sqrt{2mn-n}\,\|f\|_2$$

Theorem.
If $f \in \mathbb{C}[x,y]$ is irreducible, $\tilde{f} \in \mathbb{C}[x,y]$ is factorizable, and $\deg \tilde{f} \leq \deg f$ then:

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

Lower Bound

Suppose:

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

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

f is irreducible $\Rightarrow R(f)$ is full rank. So $\|R(f) - R(\tilde{f})\|_{Frob} < \sigma(R(f)) \Rightarrow R(\tilde{f})$ is full rank $\Rightarrow \tilde{f}$ is irreducible.

Other Norms of $R(f)$

Other relationships between the norms of $R(f)$ and the norms of f: lead to other Theorems:

	If $\tilde{f}$ factors, then
$\|R(f)\|_1 \leq \max\{m,n\}\|f\|_1$	$\|f-\tilde{f}\|_1 \geq (\max\{m,n\}\,\|R(f)^\dagger\|_1)^{-1}$
$\|R(f)\|_\infty \leq 2\max\{m,n\}\|f\|_1$	$\|f-\tilde{f}\|_1 \geq (2\max\{m,n\}\,\|R(f)^\dagger\|_\infty)^{-1}$
$\|R(f)\|_{\infty,1} \leq \max\{m,n\}\|f\|_\infty$	$\|f-\tilde{f}\|_\infty \geq (\max\{m,n\}\,\sum_{i,j}\|R(f)^\dagger_{i,j}\|)^{-1}$

Example 1

$f = x^2 + y^2 - 1,$

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

Computing $\|R(\varphi)\|^2_{Frob}$, we get:

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

The largest coefficient is 15 (vs. theoretical bound 24), and the smallest singular value of $R(f)$ is $\sigma(R(f)) \approx 0.613616$, so f is at least distance $\sigma(R(f))/\sqrt{15} \approx 0.1584349$ from a reducible polynomial.

Example 2 [Nagasaka priv. commun. 2003]

$f = (-0.769142u^6 - 0.791975u^2 + 0.535324u + 0.828448)x^4 + (-0.653187u^3 + 0.320409u^2 + 0.103376u + 0.475811)x^3 + (0.996342u^5 + 0.755931u - 0.941103)x^2 + (0.169204u^5 - 0.243435u)x - 0.838000u^6 - 0.214451u + 0.209513$

$R(f)$ is 88×53.

Largest coefficient of $\|R(\varphi)\|_{Frob}$ is 514 vs. the theoretical bound of 848.

Our lower bound (2-norm): 0.04326727713

Nagasaka's lower bound: 0.00001128558364

Challenge Problems:

`http://www.math.ncsu.edu/˜jpmay/issac03/challenge.html`