Testing polynomial primality with pseudozeros

Stef Graillat, Philippe Langlois
University of Perpignan — France

{graillat,langlois}@univ-perp.fr
http://www.univ-perp.fr/~{graillat,langlois}

RNC’5, 5th Conference on Real Numbers and Computers, Lyon, France
September 3–5, 2003
Definition of approximate GCD of polynomials

Classical definition:
Let $p$ and $q$ be two polynomials of degree $n$ and $m$ and let $\varepsilon$ be a nonnegative number. We define

- an $\varepsilon$-divisor (approximate divisor): a divisor of perturbed polynomials $\hat{p}$ and $\hat{q}$ satisfying
  \[ \deg \hat{p} \leq n, \deg \hat{q} \leq m \text{ and } \max(\|p - \hat{p}\|, \|q - \hat{q}\|) \leq \varepsilon. \]
- an $\varepsilon$-GCD (approximate GCD): an $\varepsilon$-divisor of maximal degree.

Remarks:
- $\varepsilon$ measures the uncertainty about the coefficients (representing finite precision).
- Uniqueness of the degree but not of the $\varepsilon$-GCD.
- Dependency with respect to the basis field.

S. Graillat, Ph. Langlois
Definition of $\varepsilon$-primality

Definition :
Two polynomials $p$ and $q$ are $\varepsilon$-coprime if their $\varepsilon$-GCD equals 1.

Computation :
- Sylvester criterion : algorithm COPRIME [Beckermann and Labahn 1998].
- Graphical : pseudozero set.
Outline of the talk

I — Pseudozero set
• Definition and computation
• Nearest polynomial with a given root

II — Pseudozeros and primality
• Presentation of existing algorithms
• Contribution of pseudozero set

III — Other applications of pseudozeros
• Multiplicity of polynomial roots
• Stability in control theory
Pseudozeros: definition, computation and interest
Pseudozero set : definition

**Perturbation :**
Neighborhood of polynomial \( p \)

\[
N_{\varepsilon}(p) = \{ \hat{p} \in \mathbb{C}_n[z] : \| p - \hat{p} \| \leq \varepsilon \}.
\]

**Definition of the \( \varepsilon \)-pseudozero set :**

\[
Z_{\varepsilon}(p) = \{ z \in \mathbb{C} : \hat{p}(z) = 0 \text{ for } \hat{p} \in N_{\varepsilon}(p) \}.
\]

This set is formed by the zeros of polynomials “near \( p \).”
Pseudozeros : bibliography

- Mosier (1986) : Definition and study form the $\infty$-norm.
- Trefethen and Toh (1994) : Study for the 2-norm.
  pseudozeros $\approx$ pseudospectra of the companion matrix.
- Chatelin and Frayssé (1996) : propose a Synthesis in *Lectures on Finite Precision Computations* (SIAM)
- Zhang (2001) : Study of the influence of the basis for the 2-norm (condition number of the evaluation).
Pseudozeros are easily computable

**Theorem:**
The $\varepsilon$-pseudozeros set satisfies

$$Z_\varepsilon(p) = \left\{ z \in \mathbb{C} : |g(z)| := \frac{|p(z)|}{\|z\|_*} \leq \varepsilon \right\},$$

where $z = (1, z, \ldots, z^n)$ and $\| \cdot \|_*$ is the dual norm of $\| \cdot \|$.

The proof needs to know “the” nearest polynomial of $p$ with a given root.
The nearest polynomial with a given root $p_u$

Let $p$ be in $\mathbb{C}_n[z]$ and $u \in \mathbb{C}$.

**Statement of the problem:**

Find a polynomial $p_u \in \mathbb{C}_n[z]$ satisfying $p_u(u) = 0$ and such that if there exists a polynomial $q \in \mathbb{C}_n[z]$ with $q(u) = 0$ then we get $\|p - p_u\| \leq \|p - q\|$.

**We are looking for:**

- an expression of $p_u$;
- uniqueness of $p_u$. 
Computation of $p_u$

Let us denote $u := (1, u, u^2, \ldots, u^n) \in \mathbb{C}^{n+1}$.

There exists $d \in \mathbb{C}^{n+1}$ satisfying $^t du = ||u||_*$ et $||d|| = 1$.

Let us define the polynomials $r$ and $p_u$ by

$$r(z) = \sum_{k=0}^{n} r_k z^k \quad \text{with} \quad r_k = d_k,$$

$$p_u(z) = p(z) - \frac{p(u)}{r(u)} r(z).$$

$p_u$ is the nearest polynomial of $p$ with root $u$. 

S. Graillat, Ph. Langlois
Uniqueness of $p_u$

A sufficient condition for uniqueness:

**Theorem.** *If the norm $\| \cdot \|$ is strictly convex then $p_u$ is unique.*

It is the case, for example, for the norms $\| \cdot \|_p$ for $1 < p < \infty$.

We do not have unicity for $\| \cdot \|_1$ and $\| \cdot \|_{\infty}$. For $p(z) = 1 + z$

<table>
<thead>
<tr>
<th></th>
<th>$| \cdot |_1$, $u = 1$</th>
<th>$| \cdot |_{\infty}$, $u = 0$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p_u$</td>
<td>$p^{(1)}_1(z) = 0$</td>
<td>$p^{(1)}_0(z) = z$</td>
</tr>
<tr>
<td>$p - p_i$</td>
<td>$z - 1$</td>
<td>$\frac{4}{3}z - \frac{2}{3}$</td>
</tr>
<tr>
<td>$|p - p_i|$</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>

$S.\ Graillat, \ Ph.\ Langlois$
Algorithm of computation

Algorithm to draw the $\varepsilon$-pseudozero set:

1. We mesh a square containing all the roots of $p$ ($\text{MATLAB}$ command: `meshgrid`).
2. We compute $g(z) := \frac{|p(z)|}{\|z\|_*}$ for all the nodes $z$ in the grid.
3. We draw the contour level $|g(z)| = \varepsilon$ ($\text{MATLAB}$ commande: `contour`).
Algorithm of computation

Algorithm to draw the $\varepsilon$-pseudozero set:

1. We mesh a square containing all the roots of $p$ (MATLAB command: meshgrid).
2. We compute $g(z) := \frac{|p(z)|}{\|z\|}$ for all the nodes $z$ in the grid.
3. We draw the contour level $|g(z)| = \varepsilon$ (MATLAB commande: contour).

Problems:

- Find a square containing all the roots of $p$ and all the pseudozeros.
- Find a grid step that separates all the roots.
Choice of the grid

Let $p$ be a unitary polynomial of degree $n$ and $\{z_i\}$ the set of its $n$ roots. Let us denote $r = \max_{i=1;\ldots;n} |z_i|$. We have

$$r \leq \max\{1, \sum_{k=1}^{n} |p_k|\}.$$

Let us denote $R := \max\{1, \sum_{i=1}^{n} |p_i| + n\varepsilon\}$. We can prove (in $\| \cdot \|_p$)

$$Z_\varepsilon(p) \subset B(0, R)$$
the closed ball of centre 0 and radix $R$. 

S. Graillat, Ph. Langlois
Complexity of drawing pseudozero set

Let $L$ be the length of the square and $h$ the step of discretization. The evaluation of $g(z) = \frac{|p(z)|}{\|z\|_*}$ needs

- the evaluation of polynomial $p$, that can be done in $O(n)$,
- the computation of the norm of a vector (the complexity depends on the norm).

Let us denote $O(\| \cdot \|_*)$ this complexity. The complexity of the algorithm to draw the pseudozero set is

$$O((L/h)^2(n + \| \cdot \|_*)) .$$

$L$ and $h$ depend on $n$ but also on the polynomial coefficients.
Numerical simulation

Pseudozero set of the *Wilkinson* polynomial

\[ W_{20} = (z - 1)(z - 2) \cdots (z - 20), \]
\[ = z^{20} - 210z^{19} + \cdots + 20!. \]

We perturb only the coefficient of \( z^{19} \) with \( \varepsilon = 2^{-23} \).

One use the weighted-norm \( \| \cdot \|_\infty \) :

\[ \|p\|_\infty = \max_i \frac{|p_i|}{m_i} \text{ with } m_i \text{ non negative} \]

with \( m_{19} = 1, m_i = 0 \) otherwise and the convention \( m/0 = \infty \) if \( m > 0 \) and \( 0/0 = 0 \).
Evolution of \( \varepsilon \)-pseudozero wrt \( \varepsilon \)

Pseudozero set of the polynomial \( p(z) = 1 + z + \cdots + z^{20} \) for different values of \( \varepsilon \).

(a) \( \varepsilon = 10^{-1} \)

(b) \( \varepsilon = 10^{-1.2} \)

(c) \( \varepsilon = 10^{-1.3} \)

(d) \( \varepsilon = 10^{-1.4} \)
Interests of pseudozeros

Pseudozero set provides:

- a qualitative study of polynomials
- a better understanding of the results of polynomial algorithms
- a use of polynomials with coefficients known to a certain accuracy.

Drawback

- the cost
Application of pseudozeros to primality
Algorithm COPRIME

\[ \|p\| = \sum |p_i|, \|(p, q)\| = \max\{\|p\|, \|q\|\} = \max\{\sum |p_i|, \sum |q_i|\}. \]


- **Input**: \( p \) and \( q \) two polynomials.
- **Output**: lower bound of \( \epsilon(p, q) \) defined by

\[
\epsilon(p, q) = \inf \{\|(p - \hat{p}, q - \hat{q})\| : (\hat{p}, \hat{q}) \text{ have a common root and} \]
\[
\deg \hat{p} \leq n, \deg \hat{q} \leq m \}. \]

- **Complexity**: in \( \mathcal{O}((n + m)^2) \).
Sylvester’s Matrix

\[
S(p, q) = \begin{bmatrix}
p_0 & 0 & \cdots & 0 & q_0 & 0 & \cdots & 0 \\
p_1 & p_0 & \cdots & \vdots & q_1 & q_0 & \cdots & \vdots \\
\vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
p_n & \cdots & p_0 & q_m & \cdots & q_0 \\
0 & p_n & p_1 & 0 & q_m & q_1 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & \cdots & 0 & p_n & 0 & \cdots & 0 & q_m 
\end{bmatrix} \in \mathbb{C}^{(n+m) \times (n+m)}.
\]

Sylvester criterion: \( p \) and \( q \) are coprime \( \iff \) the matrix \( S(p, q) \) is non singular.
Presentation of the method

\[ \epsilon(p, q) \geq \frac{1}{\|S(p, q)^{-1}\|} \]

- An estimation of \( \|S(p, q)^{-1}\| \) based on a SVD costs a lot.
- We seek an upper bound of \( \|S(p, q)^{-1}\| \).
Pseudozeros : the algorithm

From the definition of the $\varepsilon$-pseudozero set, we derive that

- if the intersection of the $\varepsilon$-pseudozero sets of $p$ and $q$ is empty then the two polynomials are $\varepsilon$-coprime,
- if the intersection is not empty then they are not $\varepsilon$-coprime.
Numerical simulation

- **Input**: $p$ and $q$ two polynomials.
- **Output**: a graphic.
- **Drawbacks**: qualitative tool.
- **Example in** $\| \cdot \|_2$:

  \[
  p = (z - 1)(z - 2) = z^2 - 3z + 2
  \]

  \[
  q = (z - 1.08)(z - 1.82) = z^2 - 2.9z + 1.9656
  \]
\[ p = (z - 1)(z - 2) = z^2 - 3z + 2, \quad q = (z - 1.08)(z - 1.82) = z^2 - 2.9z + 1.9656 \]
\[ p = (z-1)(z-2) = z^2 - 3z + 2, \quad q = (z - 1.08)(z - 1.82) = z^2 - 2.9z + 1.9656 \]
Other applications of pseudozeros
Stability on control theory

Stability : \(|\text{roots of } p| < 1.\)

\(\varepsilon\)-pseudozero set of \(p(z) = (z - 0.8)^2\) for \(\varepsilon = 0.1\) and \(\varepsilon = 0.01\).
Multiplicity of polynomial roots

Computation of the $\varepsilon$-pseudozeros of polynomials:

$$p_1(z) = z - 1, \quad p_2(z) = (z - 1)^2, \quad p_3(z) = (z - 1)^3,$$

with, respectively, $\varepsilon_1 = \varepsilon$, $\varepsilon_2 = \varepsilon^2$, $\varepsilon_3 = \varepsilon^3$ and $\varepsilon = 10^{-1}$.

(e) $Z_\varepsilon$ of $p_1$, $p_2$, $p_3$ and $\varepsilon = 10^{-1}$

(f) Pseudozero sets $Z_\varepsilon(p_1)$, $Z_\varepsilon(p_2)$, $Z_\varepsilon(p_3)$ for $\varepsilon = 10^{-1}$
Conclusion

The pseudozero set provides
1. a better understanding of the effect of coefficients perturbation;
2. a test for $\varepsilon$-primality of two polynomials;
3. an application for stability and multiplicity.