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 ε be a nonnegative number. We define

- an **ε-divisor** (approximate divisor) : a divisor of perturbed polynomials $\widehat{p}$ and $\widehat{q}$ satisfying
$$\deg \widehat{p} \leqslant n, \deg \widehat{q} \leqslant m \text{ and } \max(\|p - \widehat{p}\|, \|q - \widehat{q}\|) \leqslant \varepsilon.$$
- an **ε-GCD** (approximate GCD) : an ε-divisor of maximal degree.

Remarks :

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

Definition of ε-primality

Definition :

Two polynomials p and q are **ε-coprime**
if their **ε-GCD** equals 1.

Computation :

- Optimization : algorithm of Karmarkar and Lakshman (1995).
- 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

$$N_\varepsilon(p) = \{\widehat{p} \in \mathbf{C}_n[z] : \|p - \widehat{p}\| \leqslant \varepsilon\}\,.$$

Definition of the ε-pseudozero set :

$$Z_\varepsilon(p) = \{z \in \mathbb{C} : \widehat{p}(z) = 0 \text{ for } \widehat{p} \in N_\varepsilon(p)\}\,.$$

This set is formed by the zeros of polynomials "near p".

Pseudozeros : bibliography

- Mosier (1986) : Definition and study form the ∞-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)
- Stetter (1999) : *numerical polynomial algebra*. Generalisation of the previous works.
- Zhang (2001) : Study of the influence of the basis for the 2-norm (condition number of the evaluation).

Pseudozeros are easily computable

Theorem :
The ε-pseudozeros set satisfies

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

where $\underline{z} = (1, z, \ldots, z^n)$ 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 $\mathbf{C}_n[z]$ and $u \in \mathbf{C}$.

Statement of the problem :

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

We are looking for :

- an expression of p_u ;
- uniqueness of p_u.

Computation of p_u

Let us denote $\underline{u} := (1, u, u^2, \ldots, u^n) \in \mathbf{C}^{n+1}$.
There exists $d \in \mathbf{C}^{n+1}$ satisfying ${}^t d\underline{u} = \|\underline{u}\|_*$ et $\|d\| = 1$.
Let us define the polynomials r and p_u by

$$\begin{aligned} r(z) &= \sum_{k=0}^{n} r_k z^k \quad \text{with} \quad r_k = d_k, \\ p_u(z) &= p(z) - \frac{p(u)}{r(u)} r(z). \end{aligned}$$

$\boxed{p_u \text{ is the nearest polynomial of } p \text{ with root } u.}$

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 $p(z) = 1 + z$

	$\|\cdot\|_1, \quad u = 1$		$\|\cdot\|_\infty, \quad u = 0$	
p_u	$p_1^{(1)}(z) = 0$	$p_1^{(2)}(z) = \frac{1}{3}(1 - z)$	$p_0^{(1)}(z) = z$	$p_0^{(2)}(z) = \frac{1}{2}z$
$p - p_i$	$z - 1$	$\frac{4}{3}z - \frac{2}{3}$	1	$\frac{1}{2}z + 1$
$\|p - p_i\|$	2	2	1	1

Algorithm of computation

Algorithm to draw the ε-pseudozero set :

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

Algorithm of computation

Algorithm to draw the ε-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

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

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.

Complexity of drawing pseudozero set

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

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

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

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

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

Numerical simulation

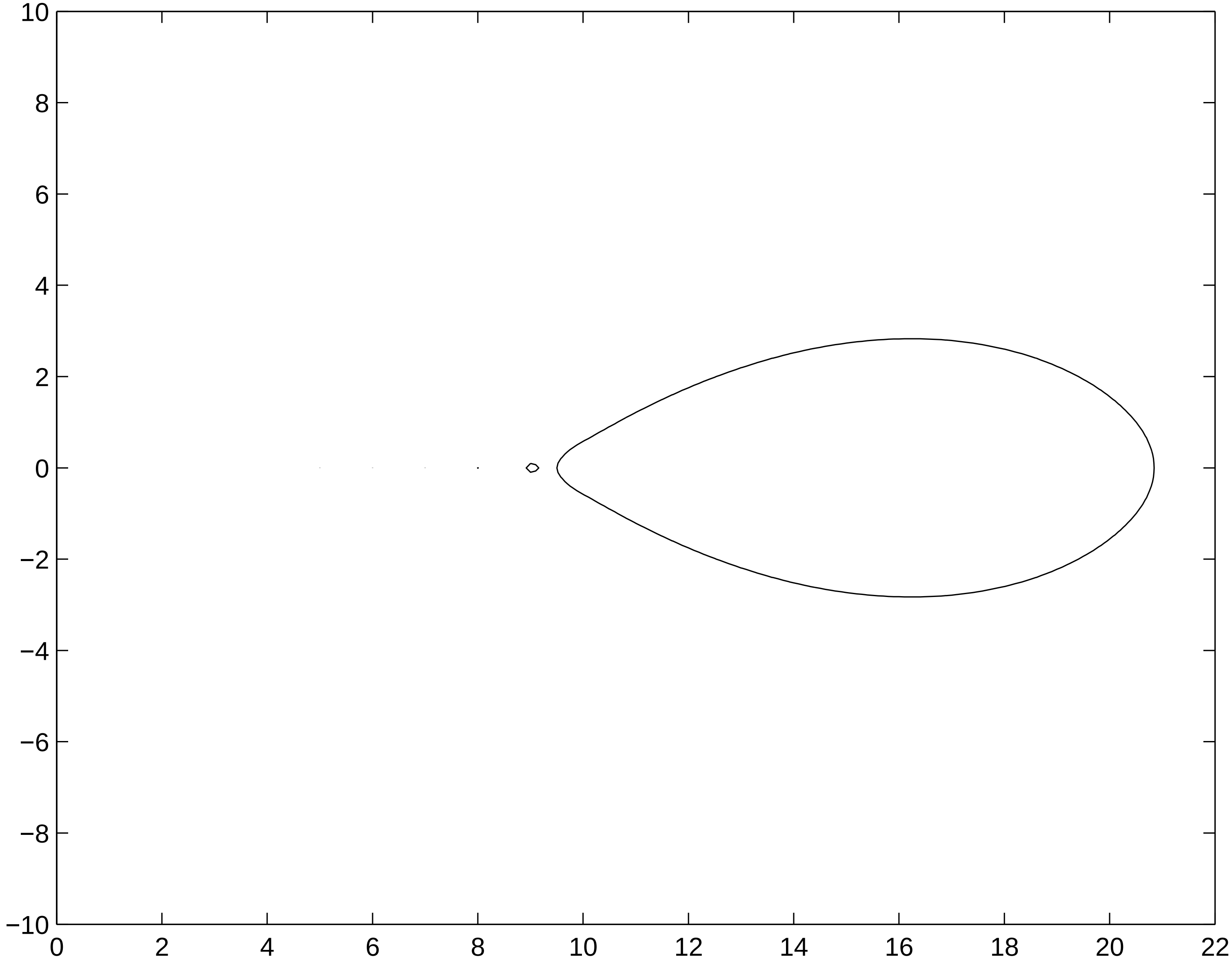
Pseudozero set of the *Wilkinson* polynomial

$$\begin{aligned} W_{20} &= (z-1)(z-2)\cdots(z-20), \\ &= z^{20} - 210z^{19} + \cdots + 20!. \end{aligned}$$

We perturb only the coefficient of z^{19} with $\varepsilon = 2^{-23}$.
One use the weighted-norm $\|\cdot\|_\infty$:

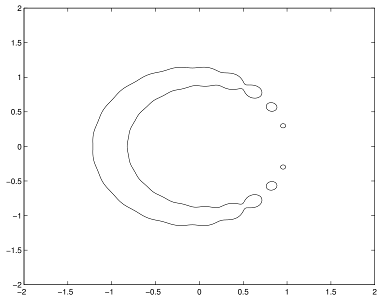
$$\|p\|_\infty = \max_i \frac{|p_i|}{m_i} \text{ with } m_i \text{ non negative}$$

with $m_{19} = 1$, $m_i = 0$ otherwise and the convention $m/0 = \infty$ if $m > 0$ and $0/0 = 0$.

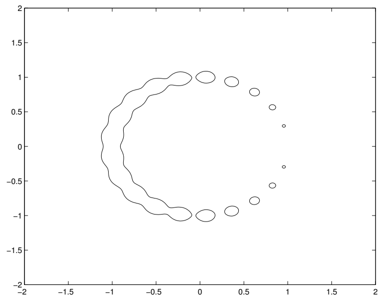

10
8
6
4
2
0
−2
−4
−6
−8
−10
0
2
4
6
8
10
12
14
16
18
20
22

Evolution of ε-pseudozero wrt ε

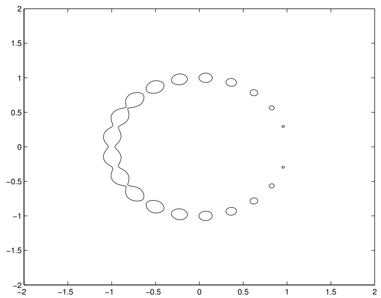
Pseudozero set of the polynomial $p(z) = 1 + z + \cdots + z^{20}$ for different values of ε.



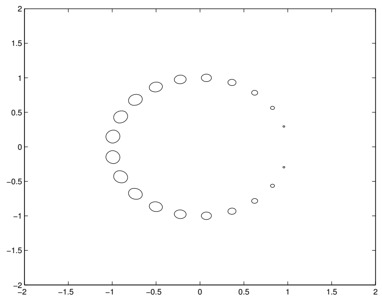
(a) $\varepsilon = 10^{-1}$



(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

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

Algorithm of Beckermann and Labahn (1998).

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

$$\epsilon(p, q) = \inf\{\|(p - \widehat{p}, q - \widehat{q})\| : (\widehat{p}, \widehat{q}) \text{ have a common root and}$$

$$\deg \widehat{p} \leqslant n, \deg \widehat{q} \leqslant m\}.$$

- **Complexity :** in $\mathcal{O}((n + m)^2)$.

Sylvester's Matrix

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

Sylvester criterion : p and q are coprime $\Longleftrightarrow$ the matrix $S(p,q)$ is non singular.

Presentation of the method

$$\boxed{\epsilon(p,q) \geqslant \frac{1}{\|S(p,q)^{-1}\|}}$$

- 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 ε-pseudozero set, we derive that

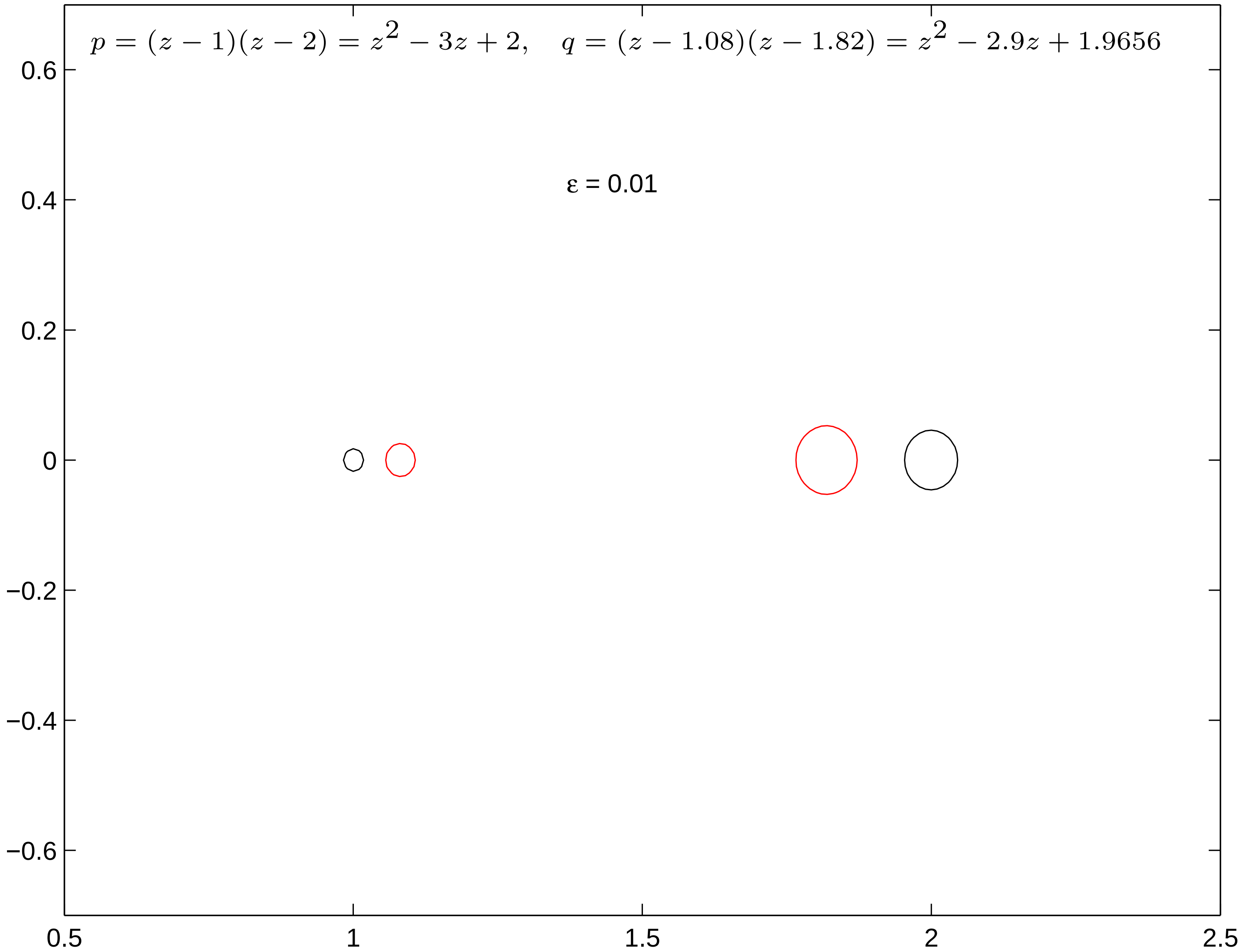
- if the intersection of the ε-pseudozero sets of p and q is empty then the two polynomials are ε-coprime,
- if the intersection is not empty then they are not ε-coprime.

Numerical simulation

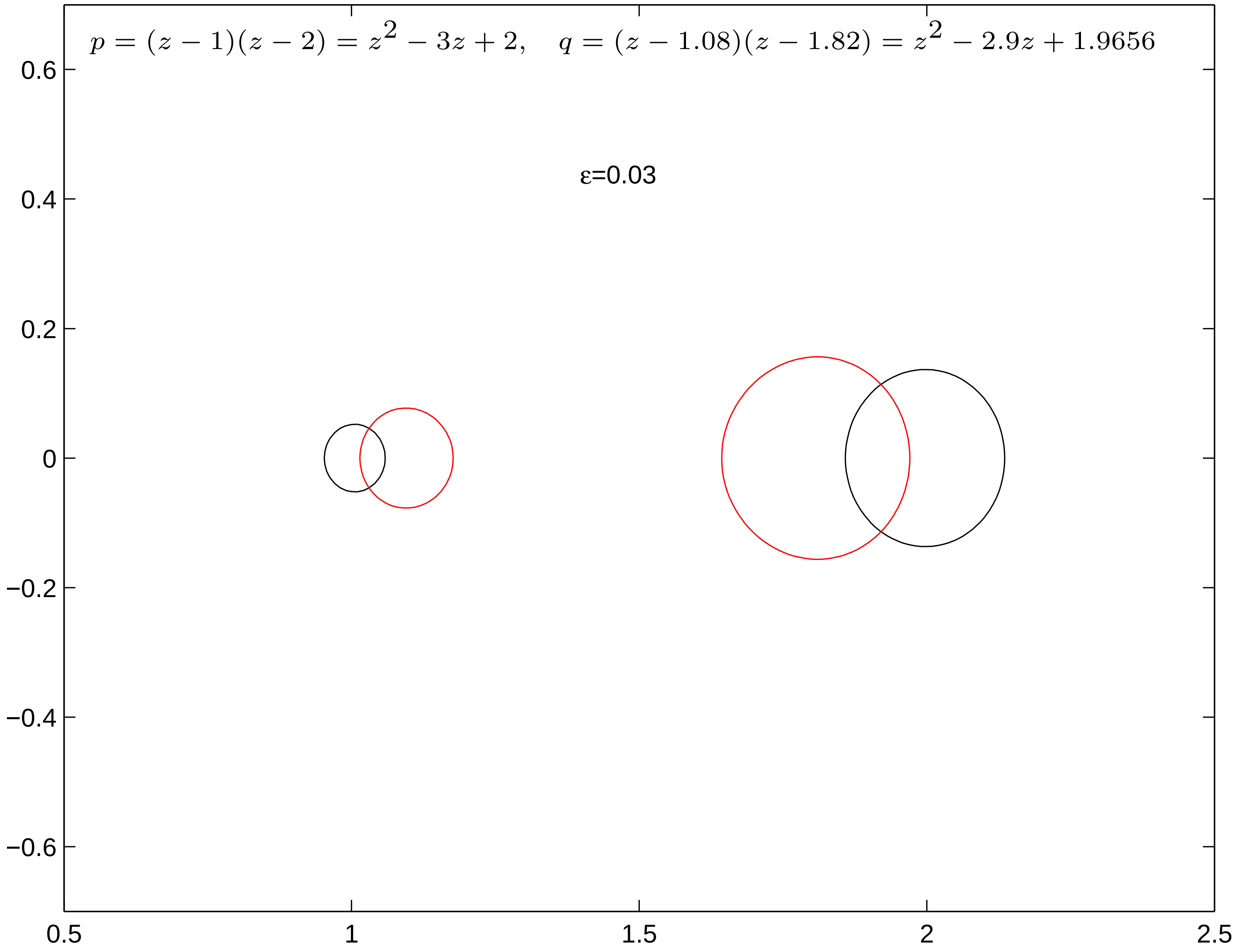
- **Input :** p and q two polynomials.
- **Output :** a graphic.
- **Drawbacks :** qualitative tool.
- **Example in $\|\cdot\|_2$:**

  $p = (z-1)(z-2) = z^2 - 3z + 2$

  $q = (z-1.08)(z-1.82) = z^2 - 2.9z + 1.9656$



$p = (z-1)(z-2) = z^2 - 3z + 2, \quad q = (z-1.08)(z-1.82) = z^2 - 2.9z + 1.9656$
ε = 0.01
0.6
0.4
0.2
0
−0.2
−0.4
−0.6
0.5
1
1.5
2
2.5



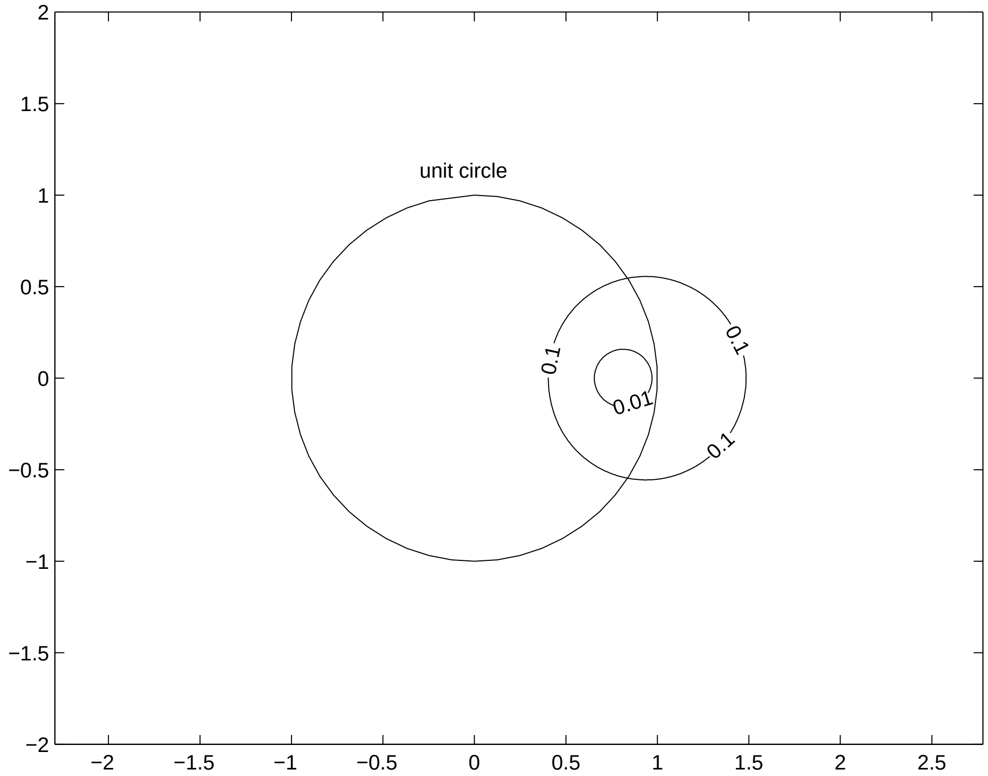
$p = (z-1)(z-2) = z^2 - 3z + 2, \quad q = (z-1.08)(z-1.82) = z^2 - 2.9z + 1.9656$
ε=0.03
0.6
0.4
0.2
0
−0.2
−0.4
−0.6
0.5
1
1.5
2
2.5

Other applications of pseudozeros

Stability on control theory

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

ε-pseudozero set of $p(z) = (z - 0.8)^2$ for $\varepsilon = 0.1$ and $\varepsilon = 0.01$.

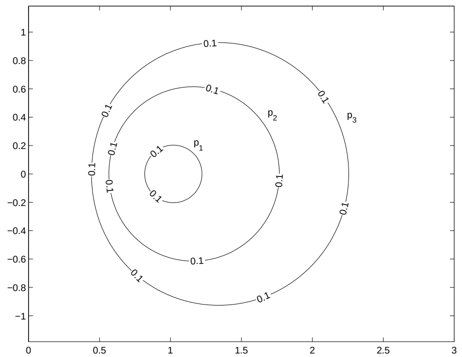


Multiplicity of polynomial roots

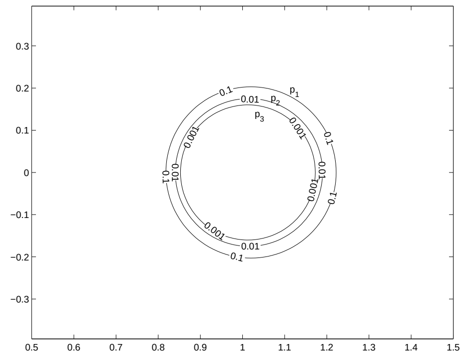
Computation of the ε-pseudozeros of polynomials :

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

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



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



(f) Pseudozero sets $Z_\varepsilon(p_1)$, $Z_{\varepsilon^2}(p_2)$, $Z_{\varepsilon^3}(p_3)$ for $\varepsilon = 10^{-1}$

Conclusion

The pseudozero set provides

1. a better understanding of the effect of coefficients perturbation ;
2. a test for ε-primality of two polynomials ;
3. an application for stability and multiplicity.