A Conjectura de Lehmer

Rui Soares Barbosa

2º ano - Ciências da Computação
Universidade do Minho

1 de Janeiro de 1970

- Contexto
- A Medida de Mahler
- O Problema de Lehmer
- Explorações Computacionais
- Limites Teóricos

- Contexto
- A Medida de Mahler
- O Problema de Lehmer
- Explorações Computacionais
- Limites Teóricos

contexto

$\boxed{\text{Procura de primos grandes}}$

1916/18 - Pierce considerou a sequência de inteiros

$$\Delta_n = \prod_{i=1}^{d} (\alpha_i^n - 1)$$

onde os α_i são raízes de um polinómio em $\mathbb{Z}[x]$.

contexto

Pretendia procurar primos nos factores de Δ_n.

De facto,

- os divisores de Δ_n satisfazem condições estritas
- $m \mid n \Rightarrow \Delta_m \mid \Delta_n$

pelo que $\frac{\Delta_p}{\Delta_1}$ (p primo) seriam bons candidatos . . .

contexto

exemplo: Mersenne

$$p(x) = x + 2$$

- $p(x) = 0$ sse $x = 2$
- $\Delta_n = 2^n - 1$ (números de Mersenne)
- $\frac{\Delta_p}{\Delta_1} = \frac{2^p - 1}{2^1 - 1} = 2^p - 1$ (forma dos primos de Mersenne)

De facto, os maiores primos encontrados são primos de Mersenne.

contexto

1933 - Lehmer estudou o crescimento da sucessão (Δ_n)

$$\lim_{n\to\infty} \frac{|\Delta_{n+1}|}{|\Delta_n|} = \lim_{n\to\infty} \frac{\prod |\alpha_i^{n+1} - 1|}{\prod |\alpha_i^n - 1|}$$

$$\lim_{n\to\infty} \frac{|\alpha_i^{n+1} - 1|}{|\alpha_i^n - 1|} = \max\{1, |\alpha_i|\}$$

e introduziu a medida

$$M(p) := |a_d| \prod_{i=1}^{d} \max\{1, |\alpha_i|\}$$

de forma que $\Delta_n \sim M(p)^n$

- Contexto
- A Medida de Mahler
- O Problema de Lehmer
- Explorações Computacionais
- Limites Teóricos

M(p) como medida de complexidade de polinómios

Consideramos polinómios em $\mathbb{Q}[x]$ (ou $\mathbb{Z}[x]$)

$$p(x) = a_d x^d + ... + a_0 = a_d \prod_{i=1}^{d} (x - \alpha_i)$$

onde $a_i \in \mathbb{Q}$ (ou $\mathbb{Z}$) (coeficientes) e $\alpha_i \in \mathbb{C}$ (raízes).

polinómios

Os números que são raízes de polinómios não nulos de $\mathbb{Q}[x]$ dizem-se algébricos.

observação

A um número algébrico α corresponde um único polinómio mínimo p t.q.:

- $p(\alpha) = 0$
- $p \in \mathbb{Z}[x]$ com coeficiente primos entre si
- p é irredutível em $\mathbb{Q}[x]$

Notas: $f(\alpha) = 0 \Rightarrow p \mid f$
As raízes de p dizem-se raízes conjugadas
São invariantes sob $z = a + bi \to \bar{z} = a - bi$
(z e $\bar{z}$ têm o mesmo polinómio irredutível
$x^2 - 2ax + a^2 + b^2$ em $\mathbb{R}[x] \supset \mathbb{Q}[x]$)

propriedades da medida de Mahler

- $M(pq) = M(p)M(q)$

propriedades da medida de Mahler

- $M(pq) = M(p)M(q)$
- $M(p) = M(-p)$

propriedades da medida de Mahler

- $M(pq) = M(p)M(q)$
- $M(p) = M(-p)$
- $M(p) = M(p^\star)$

Definição (polinómio recíproco)

$$p^\star(x) = x^d p(1/x)$$

exemplo

$$\begin{aligned} p(x) &= x^4 + 3x^3 - 5x^2 + 0x + 7 \\ p^\star(x) &= x^4 \left(\frac{1}{x^4} + 3\frac{1}{x^3} - 5\frac{1}{x^2} + 0\frac{1}{x^1} + 7 \right) \\ &= 1 + 3x - 5x^2 + 0x^3 + 7x^4 \end{aligned}$$

propriedades

$$
\begin{aligned}
p(x) &= \sum_{j=0}^{d} a_j x^j = a_d \prod_{i=1}^{d} (x - \alpha_i) \\
&= a_d \sum_{j=0}^{d} \sum_{\{i_1,\ldots,i_{d-j}\} \subset \{1,\ldots,d\}} (-1)^{d-j} \alpha_{i_1} \ldots \alpha_{i_{d-j}} x^j
\end{aligned}
$$

propriedades

$$
\begin{aligned}
p(x) &= \sum_{j=0}^{d} a_j x^j = a_d \prod_{i=1}^{d} (x - \alpha_i) \\
&= a_d \sum_{j=0}^{d} \sum_{\{i_1,\ldots,i_{d-j}\} \subset \{1,\ldots,d\}} (-1)^{d-j} \alpha_{i_1} \ldots \alpha_{i_{d-j}} x^j
\end{aligned}
$$

Logo,

$$
\begin{aligned}
a_j &= a_d \sum_{\{i_1,\ldots,i_{d-j}\} \subset \{1,\ldots,d\}} (-1)^{d-j} \alpha_{i_1} \ldots \alpha_{i_{d-j}} \\
\Rightarrow \quad & \\
|a_j| &\leq |a_d| \binom{d}{j} \prod_{i=0}^{d} max\{1, |\alpha_1|\}
\end{aligned}
$$

propriedades

Desigualdade da Norma

$$|a_j| < \binom{n}{j} M(p)$$

consequência

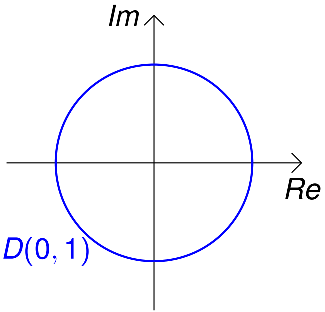
$$\{p \in \mathbb{Z}[x] \mid grau(p) \leq D, M(p) < M\}$$

é finito para quaisquer $D \in \mathbb{N}_0$ e $M \in \mathbb{R}$.

$$M(p) := |a_d| \prod_{i=1}^{d} \max\{1, |\alpha_i|\} \geq 1$$

observação

$M(p)$ é o produto dos zeros fora do disco unitário.

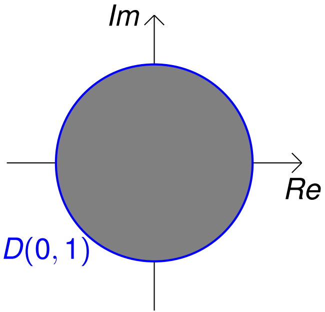


propriedades da medida de Mahler

$$M(p) := |a_d| \prod_{i=1}^{d} \max\{1, |\alpha_i|\} \geq 1$$

observação

$M(p)$ é o produto dos zeros fora do disco unitário.
$M(p) = 1$ quando todas as raízes α de p tiverem módulo < 1



$\boxed{\text{os polinómios mais "simples"} \ldots}$

Uma raíz n-ésima ζ da unidade satisfaz

$$\zeta^n = 1$$

$$\zeta_k = e^{k\frac{2\pi}{n}i} \quad k = 1, \ldots, n$$

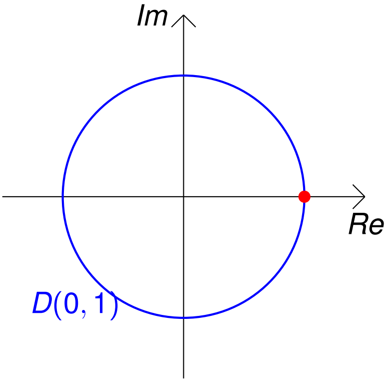
polinómios ciclotómicos

$\boxed{\text{os polinómios mais "simples" \ldots}}$

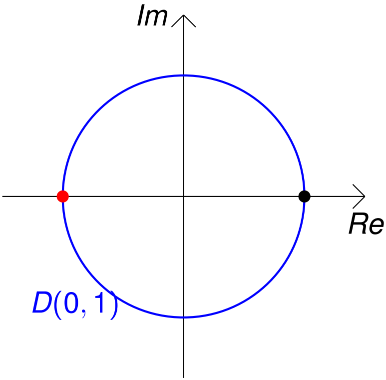
Uma raíz n-ésima ζ primitiva da unidade satisfaz

$$\begin{cases} \zeta^n = 1 \\ \zeta^m \neq 1 \quad \forall m, 0 < m < n \end{cases}$$

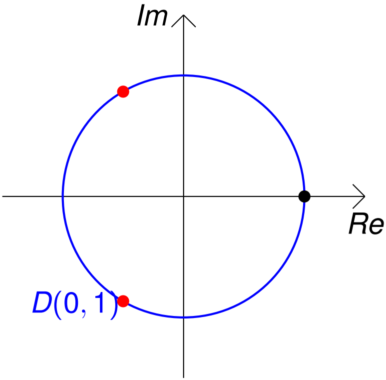
$$\zeta_k = e^{k\frac{2\pi}{n}i} \quad k = 1, \ldots, n,\ gcd(k,n) = 1$$



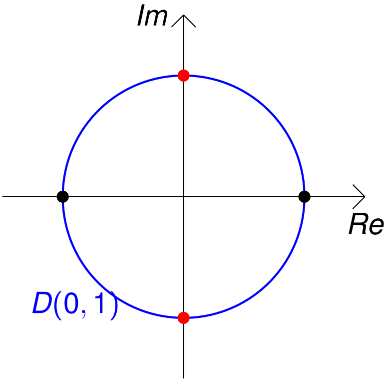
$$\begin{cases} \zeta^1 = 1 \\ \zeta^m \neq 1 \quad (0 < m < 1) \end{cases}$$



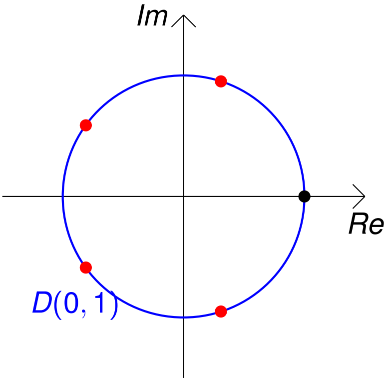
$$\begin{cases} \zeta^2 = 1 \\ \zeta^m \neq 1 \quad (m = 1) \end{cases}$$



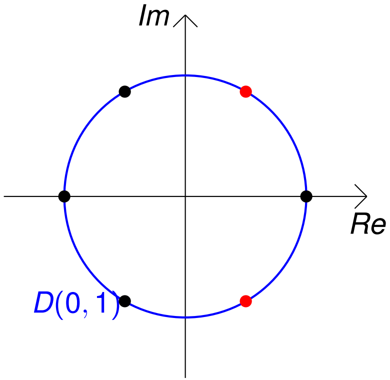
$$\begin{cases} \zeta^3 = 1 \\ \zeta^m \neq 1 \quad (m = 1, 2) \end{cases}$$



$$\begin{cases} \zeta^4 = 1 \\ \zeta^m \neq 1 \quad (m = 1, 2, 3) \end{cases}$$



$$\begin{cases} \zeta^5 = 1 \\ \zeta^m \neq 1 \quad (m = 1, 2, 3, 4) \end{cases}$$



$$\begin{cases} \zeta^6 = 1 \\ \color{red}{\zeta^m \neq 1 \quad (m = 1, 2, 3, 4, 5)} \end{cases}$$

As raízes primitivas têm o mesmo polinómio mínimo

$$\Phi_n(x) = \prod_{\zeta_k primitiva} (x - \zeta_k) = \begin{cases} x - 1 & \text{se } n = 1 \\ \dfrac{x^n - 1}{\prod\limits_{m|n} \Phi_m(x)} & \text{se } n > 1 \end{cases}$$

observação

$$M(\Phi_n) = \prod |\zeta_k| = 1$$

Esta medida é mínima.

polinómios ciclotómicos

observação

$$M(\Phi_n) = \prod |\zeta_k| = 1$$

Esta medida é mínima.

Questão

Que outros polinómios têm medida mímima?

exemplos

- x, pois a sua única raiz é 0.
- produtos de polinómios já conhecidos de medida 1.

observação

$$M(\Phi_n) = \prod |\zeta_k| = 1$$

Esta medida é mínima.

Questão

Que outros polinómios têm medida mímima?

exemplos

- x, pois a sua única raiz é 0.
- produtos de polinómios já conhecidos de medida 1.

Em geral, $p = x^a \Phi_{b_1} \dots \Phi_{b_r}$, com $a, r, b_i \in \mathbb{N}_0$

...

teorema de Kronecker

...

Haverá outros?

Teorema (Kronecker)

Não!

$M(p) = 1$ *sse* *p é produto de ciclotómicos e potências de x.*

ou seja,

$M(p) = 1$ *sse* *as raízes de p são raízes da unidade ou zero.*

Demonstração.

Seja $p \in \mathbb{Z}[x]_d$ com raízes α_i tal que $M(p) = 1$.
Consideremos de novo $p_k = a_d^k \prod (x - \alpha_i^k)$.

$$
\begin{aligned}
& M(p_k) = 1 \\
\Rightarrow\ & |a_{j(k)}| \leq \binom{d}{j} && \text{(desigualdade da norma)} \\
\Rightarrow\ & \{f_k | k \in \mathbb{N}\} \ \text{ é finito} \\
\Rightarrow\ & \{\beta | \exists k, f_k(\beta) = 0\} \ \text{ é finito} \\
\Rightarrow\ & \forall i, \exists r > s, \alpha_i^r = \alpha_i^s \\
\Rightarrow\ & \forall i,\ \alpha_i = 0 \vee \alpha^{r-s} = 1
\end{aligned}
$$

$\square$

- Contexto
- A Medida de Mahler
- O Problema de Lehmer
- Explorações Computacionais
- Limites Teóricos

contexto

1933 - Lehmer estudou o crescimento da sucessão (Δ_n)

...

$$\Delta_n = \prod_{i=1}^{d} (\alpha_i^n - 1)$$

$$\lim_{n \to \infty} \frac{|\alpha_i^{n+1} - 1|}{|\alpha_i^n - 1|} = \max\{1, |\alpha_i|\}$$

e introduziu a medida de Mahler de forma que $\Delta_n \sim M(p)^n$.

contexto

1933 - Lehmer estudou o crescimento da sucessão (Δ_n) e introduziu a medida de Mahler de forma que $\Delta_n \sim M(p)^n$.

Observou que

- menor crescimento reduz factores extra ($\neq \Delta_m$).
- pelo que potencialmente se encontram mais primos se $M(p)$ pequeno.

Lehmer -1933

"The following problem arises immediately. If ϵ is a positive quantity, to find a polynomial of the form

$$f(x) = x^r + a_{r-1}x^{r-1} + ... + a_0$$

where the a's are integers, such that the absolute value of the product of those roots of f which lie outside the unit circle, lies between 1 and $1 + \epsilon$.
This problem, in interest in itself, is especially important for our purposes. Whether or not the problem has a solution for $\epsilon < 0.176$ we do not know"

o problema de Lehmer

Problema

Dado $\epsilon > 0$ arbitrário, existe $p \in \mathbb{Z}[x]$ tal que $1 < M(p) < 1 + \epsilon$?

Conjectura

Não

polinómio mínimo

encontrado por Lehmer:

$$\ell(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1$$

$$M(\ell) = 1.176280818$$

Ainda não ultrapassado.

sinfonia de Mahler (opus 1.1762...)

A medida de Mahler e o problema de Lehmer surgem em muitas áreas aparentemente não relacionadas da matemática:

- teoria de números transcendentes

desigualdades úteis no estudo de números transcendentes (área onde Mahler a aplicou)

sinfonia de Mahler (opus 1.1762...)

A medida de Mahler e o problema de Lehmer surgem em muitas áreas aparentemente não relacionadas da matemática:

- teoria de números transcendentes
- factorização de polinómios

se a conjectura de Lehmer for verdadeira, existe um limite ao número de factores não ciclotómicos de um polinómio dependente dos seus coeficientes.

sinfonia de Mahler (opus 1.1762...)

A medida de Mahler e o problema de Lehmer surgem em muitas áreas aparentemente não relacionadas da matemática:

- teoria de números transcendentes
- factorização de polinómios
- sistemas dinâmicos

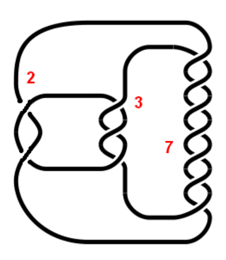
entropia de automorfismos ergódicos

a conjectura de Lehmer é falsa sse existem automorfismos em K^n ergódicos e com entropia arbitrariamente pequena

sinfonia de Mahler (opus 1.1762...)

A medida de Mahler e o problema de Lehmer surgem em muitas áreas aparentemente não relacionadas da matemática:

- teoria de números transcendentes
- factorização de polinómios
- sistemas dinâmicos
- teoria de nós



os polinómios de Alexander são um invariante de nó.
A medida mínima de polinómios de enlaces de “pretzel” é $M(\ell(x)) = 1.176\ldots$ - “pretzel”-(2,3,7).

sinfonia de Mahler (opus 1.1762...)

A medida de Mahler e o problema de Lehmer surgem em muitas áreas aparentemente não relacionadas da matemática:

- teoria de números transcendentes
- factorização de polinómios
- sistemas dinâmicos
- teoria de nós
- funções-L e curvas elípticas

Existem relações entre a medida de Mahler para polinómios de várias variáveis e o valor de séries-L.

Para $M(p) < 2$, temos $|a_j| \leq 2\binom{d}{j}$.
Assim, a_j tem $4\binom{d}{j} + 1$ possibilidades.

exemplo (grau=4)

número de polinómios a procurar (exaustivamente):

$$\underbrace{4\binom{4}{4}}_{a_4}\underbrace{\left(4\binom{4}{3}+1\right)}_{a_3}\underbrace{\left(4\binom{4}{2}+1\right)}_{a_2}\underbrace{\left(4\binom{4}{1}+1\right)}_{a_1}\underbrace{\left(4\binom{4}{0}+1\right)}_{a_0} = 144500$$

medidas mínimas para cada $\mathbb{Z}[x]_d$

d	nº pols	polinómio	M(p)
1	20	$x-2$	2
2	180	x^2-x-1	1.618...
3	3380	x^3+0x^2-x+1	1.324...
4	144500	$x^4-x^3+0x^2+0x-1$	1.380...
5	14826420	$x^5-x^4+x^3+0x^2-x+1$	1.349...
10	1.8×10^{23}	$\ell(x)$	1.176...

Lehmer-1933

"We have not made an examination of all 10th degree symmetric polynomials, but a rather intensive search has failed to reveal a better polynomial than

$$x^{10}+x^9-x^7-x^6-x^5-x^4-x^3+x+1, \Omega = 1.176280818$$

All efforts to find a better equation of degree 12 and 14 have been unsuccessful."

medidas mínimas para cada $\mathbb{Z}[x]_d$

Estratégias de pesquisa

- $M(p^\star) = M(p)$, $M(-p) = M(p)$

medidas mínimas para cada $\mathbb{Z}[x]_d$

Estratégias de pesquisa

- $M(p^\star) = M(p)$, $M(-p) = M(p)$
- 1980 - Boyd: limites optimizados

Limites Optimizados

Se $M(p) < M$, $|a_j| \leq \binom{d}{j} + \binom{d-2}{j-1}(M^2 + M^{-2} - 2)$

- $\mathcal{O}(C^{d^2})$
- pesquisa exaustiva até $d \leq 24$, $M = 1.3$
- exemplo: $d = 10$

medidas mínimas para cada $\mathbb{Z}[x]_d$

Estratégias de pesquisa

- $M(p^\star) = M(p)$, $M(-p) = M(p)$
- 1980 - Boyd: limites optimizados
- 1989 - Boyd: Altura 1

Altura 1

$p \in \mathbb{Z}[x]$ com $M(p) < 2 \Rightarrow \exists g \in \mathbb{Z}[x], H(fg) = 1$

- $\mathcal{O}(C^d)$
- pesquisa até $d \leq 40$ (encontrou anteriores)

medidas mínimas para cada $\mathbb{Z}[x]_d$

Estratégias de pesquisa

- $M(p^\star) = M(p)$, $M(-p) = M(p)$
- 1980 - Boyd: limites optimizados
- 1989 - Boyd: Altura 1
- 1998 - Mossinghoff, Pinner, Vaaler: Perturbações

Produtos de ciclotómicos perturbados

encontrar produto de Φs e peturbar o coeficiente do meio (± 1)

- $\mathcal{O}(C^{\sqrt{d}})$
- pesquisa até $d \leq 64$ (encontrou $> 80\%$ dos anteriores)

- Contexto
- A Medida de Mahler
- O Problema de Lehmer
- Explorações Computacionais
- Limites Teóricos
  - Limites Globais
  - Limites Restritos

limites globais

$$M(p) > 1 + R(d)$$

- 1971 - Blanksby e Montgomery: $R(d) = \frac{1}{52d \log 6d}$
- 1978 - Stewart: $R(d) = \frac{1}{10^4 d \log d}$

limites globais

$$M(p) > 1 + R(d)$$

- 1971 - Blanksby e Montgomery: $R(d) = \frac{1}{52d \log 6d}$
- 1978 - Stewart: $R(d) = \frac{1}{10^4 d \log d}$
- 1979 - Dobrowolski: $R(d) = \frac{1}{1200} \left(\frac{\log \log d}{\log d} \right)^3$ (com $d \geq 2$).
- idem (assimptótico) $R(d) = (1 - \epsilon) \left(\frac{\log \log d}{\log d} \right)^3$
- 1982 - Cantor e Strauss: $R(d) = (2 - \epsilon) \left(\frac{\log \log d}{\log d} \right)^3$
- 1983 - Louboutin: $R(d) = (\frac{9}{4} - \epsilon) \left(\frac{\log \log d}{\log d} \right)^3$
- 1996 - Voutier: $R(d) = \frac{1}{4} \left(\frac{\log \log d}{\log d} \right)^3$ (com $d \geq 2$)

limites globais

$$M(p) > 1 + R(d)$$

Mas...

Em qualquer caso,

$$\lim_{d \to \infty} R(d) = 0$$

Problema de Lehmer ainda em aberto...

polinómio recíproco

Recordemos que...

$$p^\star(x) = x^d p(1/x)$$

Definição (polinómio recíproco)

p diz-se recíproco quando $p = p^\star$.

observação

Se p recíproco,

- $a_j = a_{d-j}$ (coeficientes simétricos)
- Se $p(\alpha) = 0 \Rightarrow p(1/\alpha) = 0$ (raízes estáveis sob $z \to 1/z$)

M(p) é mínimo quando os zeros são raízes da unidade.

Vamos considerar números algébricos “próximos” destas.

números de Pisot e de Salem

Definição (Número de Pisot-Vijayaraghavan)

inteiro algébrico real $\alpha > 1$ tal que todos as raízes conjugadas α' satisfazem $|\alpha'| < 1$

exemplo (Número de Ouro)

$\varphi = \frac{1+\sqrt{5}}{2} > 1$
polinómio mínimo: $x^2 - x - 1$
$\varphi' = \frac{1+\sqrt{5}}{2} = \frac{-1}{\varphi}$. Logo, $|\varphi'| < 1$.
φ é PV.

números de Pisot e de Salem

Definição (Número de Pisot-Vijayaraghavan)

inteiro algébrico real $\alpha > 1$ tal que todos as raízes conjugadas α' satisfazem $|\alpha'| < 1$

observação

O polinómio mínimo de um número de Pisot α é não recíproco (se $d > 2$), já que

- Como $d > 2$, existem duas raízes α_0, α_1 de módulo < 1.
- $1/\alpha_0$ e $1/\alpha_1$ são raízes de $p^\star$
- $|1/\alpha_0|, |1/\alpha_1| > 1$
- $p \neq p^\star$

números de Pisot e de Salem

Definição (Número de Salem)

inteiro algébrico real $\alpha > 1$ tal que todos as raízes conjugadas α' satisfazem $|\alpha'| \leq 1$ e pelo menos um satisfaz $|\beta| = 1$

números de Pisot e de Salem

Definição (Número de Salem)

inteiro algébrico real $\alpha > 1$ tal que todos as raízes conjugadas α' satisfazem $|\alpha'| \leq 1$ e pelo menos um satisfaz $|\beta| = 1$

observação

O polinómio mínimo de um n. de Salem α é recíproco, já que

- Existe β raíz de p no disco unitário.
- $1/\beta$ é o conjugado de β, logo são raízes conjugadas.
- β é raíz de p e $p^\star$
- Como p é pol. min. de β, $p^\star = kp$ ($k \in \mathbb{Z}$)
- $k = \pm 1$, pois os coeficientes são os mesmos ($gcd = 1$).
- Se $k = -1$, p(1)=-p(1), então p(1)=0: impossível!

números de Pisot e de Salem

Definição (Número de Salem)

inteiro algébrico real $\alpha > 1$ tal que todos as raízes conjugadas α' satisfazem $|\alpha'| \leq 1$ e pelo menos um satisfaz $|\beta| = 1$

observação

- Os conjugados de α Salem são estáveis sob $z \to 1/z$
- Um inteiro algébrico α é Salem sse $1/\alpha$ é seu conjugado e todos os outros conjugados têm módulo 1.

mínimo para polinómios não recíprocos

Teorema (Smyth (1971))

Se $p \in \mathbb{Z}[x]$ é não recíproco e $p(0) \neq 0$, então

$$M(p) \geq M(x^3 - x - 1) = 1.3247 = \theta$$

onde θ é a solução real do polinómio acima.

observação

θ é o mínimo número de Pisot.

Versão enfraquecida

Considerar $\sqrt{\frac{5}{4}}$ em vez de θ.

mínimo para polinómios não recíprocos

Definição (funções de Blaschke)

Para cada $\alpha \in \mathbb{C}$, definimos

$$B_\alpha : \mathbb{C} \to \mathbb{C}$$
$$z \mapsto \frac{z-\alpha}{1-\bar{\alpha}z} = -\frac{z-\alpha}{\bar{\alpha}(z-(1/\bar{\alpha}))}$$

A um conjunto $\{\alpha_j | 1 \leq j \leq r\}$ associamos a função de Blaschke:

$$B = \prod_{j=1}^{r} B_{\alpha_j}$$

propriedades

Se $|\alpha| < 1$, B_α é holomórfica numa vizinhança de $D(0, 1)$

$|B_\alpha(z)| = 1$ para $|z| = 1$

mínimo para polinómios não recíprocos

Sejam

- p - polinómio irredutível não recíproco (mod. raízes $\neq 0, 1$)
- $a_0, a_d = \pm 1$ (como $M(f) < 2$)
- α_i - raízes de p com módulo < 1.
- β_i - raízes de p com módulo > 1.
- B - f. de Blaschke dos α_i
- $B^\star$ - f. de Blaschke dos $1/\beta_i$ (zeros de $f^\star$ com mod. < 1).

Então,

$$\frac{B}{p} = \frac{C\prod(z-\alpha_i)}{\prod\bar{\alpha}_i(z-\frac{1}{\bar{\alpha}_i})\prod(z-\alpha_i)\prod(z-\beta_i)}$$

$$\frac{B^\star}{p^\star} = \frac{C^\star\prod(z-\frac{1}{\beta_i})}{\prod\frac{1}{\beta_i}(z-\bar{\beta}_i)\prod(z-\frac{1}{\alpha_i})\prod(z-\frac{1}{\beta_i})}$$

Então,

$$\frac{B}{p} = \frac{C\prod(z-\alpha_i)}{\prod\bar{\alpha}_i(z-\frac{1}{\bar{\alpha}_i})\prod(z-\alpha_i)\prod(z-\beta_i)}$$

$$\frac{B^\star}{p^\star} = \frac{C^\star\prod(z-\frac{1}{\beta_i})}{\prod\frac{1}{\beta_i}(z-\bar{\beta}_i)\prod(z-\frac{1}{\alpha_i})\prod(z-\frac{1}{\beta_i})}$$

$$\boxed{z \longrightarrow \bar{z}}$$

Então,

$$\frac{B}{p} = \frac{C \prod (z - \alpha_i)}{\prod \bar{\alpha}_i (z - \frac{1}{\bar{\alpha}_i}) \prod (z - \alpha_i) \prod (z - \beta_i)}$$

$$\frac{B^\star}{p^\star} = \frac{C^\star \prod (z - \frac{1}{\beta_i})}{\prod \frac{1}{\beta_i} (z - \bar{\beta}_i) \prod (z - \frac{1}{\alpha_i}) \prod (z - \frac{1}{\beta_i})}$$

$\boxed{z \longrightarrow \bar{z}}$

De facto,

$$\frac{B}{p} = \frac{B^\star}{p^\star}$$

mínimo para polinómios não recíprocos

expansão em série de Taylor:

$$
\begin{aligned}
B &= c_0 + c_1 z + c_2 z^2 + \dots + c_k x^k + \dots \\
B^\star &= d_0 + d_1 z + d_2 z^2 + \dots + d_k x^k + \dots \\
t = p/p^\star &= t_0 + t_1 z + t_2 z^2 + \dots + t_k x^k + \dots
\end{aligned}
$$

mínimo para polinómios não recíprocos

expansão em série de Taylor:

$$\begin{aligned} B &= c_0 + c_1 z + c_2 z^2 + \ldots + c_k x^k + \ldots \\ B^\star &= d_0 + d_1 z + d_2 z^2 + \ldots + d_k x^k + \ldots \\ t = p/p^\star &= t_0 + t_1 z + t_2 z^2 + \ldots + t_k x^k + \ldots \end{aligned}$$

$$c_k = \frac{B^{(k)}(0)}{k!} \quad d_k = \frac{B^\star\ (k)(0)}{k!} \quad t_k = \frac{(p/p^\star)^{(k)}(0)}{k!}$$

mínimo para polinómios não recíprocos

$$c_k = \frac{B^{(k)}(0)}{k!} \quad d_k = \frac{B^{\star\,(k)}(0)}{k!} \quad t_k = \frac{\frac{p}{p^\star}^{(k)}(0)}{k!}$$

$$B = \frac{B^\star p}{p^\star} \quad B^{(k)}(0) = \sum \binom{k}{j} B^{\star\,(j)} t^{(k-j)}$$

observação

$$\begin{aligned} p(0), p^\star(0), t_0 &= \pm 1 \\ |c_0| &= |B(0)| = \left| B^\star \frac{p}{p^\star}(0) \right| = |B^\star(0)| = |d_0| \end{aligned}$$

mínimo para polinómios não recíprocos

$$c_k = \frac{B^{(k)}(0)}{k!} \quad d_k = \frac{B^{\star\,(k)}(0)}{k!} \quad t_k = \frac{\frac{p}{p^\star}^{(k)}(0)}{k!}$$

$$B = \frac{B^\star p}{p^\star} \quad B^{(k)}(0) = \sum \binom{k}{j} B^{\star\,(j)} t^{(k-j)}$$

observação

$$\begin{aligned} p(0), p^\star(0), t_0 &= \pm 1 \\ |c_0| &= |B(0)| = \left| B^\star \frac{p}{p^\star}(0) \right| = |B^\star(0)| = |d_0| \\ &= |B^\star(0)| = \left| \frac{\prod \frac{-1}{\beta_i}}{\prod \frac{-1}{\beta_i}(-\beta)} \right| \end{aligned}$$

mínimo para polinómios não recíprocos

$$c_k = \frac{B^{(k)}(0)}{k!} \quad d_k = \frac{B^{\star\,(k)}(0)}{k!} \quad t_k = \frac{\frac{p}{p^\star}^{(k)}(0)}{k!}$$

$$B = \frac{B^\star p}{p^\star} \quad B^{(k)}(0) = \sum \binom{k}{j} B^{\star\,(j)} t^{(k-j)}$$

observação

$$\begin{aligned} p(0), p^\star(0), t_0 &= \pm 1 \\ |c_0| &= |B(0)| = \left|B^\star \frac{p}{p^\star}(0)\right| = |B^\star(0)| = |d_0| \\ &= |B^\star(0)| = \left|\frac{\prod \frac{-1}{\beta_i}}{\prod \frac{-1}{\beta_i}(-\beta)}\right| = \left|\frac{-1}{\prod \beta_i}\right| = \frac{1}{M(p)} \end{aligned}$$

mínimo para polinómios não recíprocos

$$c_k = \frac{B^{(k)}(0)}{k!} \quad d_k = \frac{B^{\star\,(k)}(0)}{k!} \quad t_k = \frac{\frac{p}{p^\star}^{(k)}(0)}{k!}$$

$$B = \frac{B^\star p}{p^\star} \quad B^{(k)}(0) = \sum \binom{k}{j} B^{\star\,(j)} t^{(k-j)}$$

observação

$p/p^\star$ não é constante. Seja $k \geq 1$ mínimo com $t_k \neq 0$.

$$c_k = t_0 d_k + t_k d_0$$

mínimo para polinómios não recíprocos

$$c_k = t_0 d_k + t_k d_0 \Leftrightarrow c_k - t_0 d_k = t_k d_0$$

Se $|c_k|, |d_k| < \frac{|t_k||c_0|}{2}$,

$$\begin{aligned} |t_k||c_0| &= |c_k - t_0 d_k| \\ &\leq |c_k| + |t_0||d_k| \\ &= |c_k| + |d_k| \\ &< |t_k||c_0| \end{aligned}$$

Logo,

$$|c_k| \geq \frac{|t_k||c_0|}{2} \text{ ou } |d_k| \geq \frac{|t_k||c_0|}{2}$$

$$|c_k| \geq \frac{|t_k||c_0|}{2} \text{ ou } |d_k| \geq \frac{|t_k||c_0|}{2}$$

resultado

Se $B = c_0 + c_1 x + \ldots + c_k x^k + \ldots$ é função de Blaschke,

$$|c_0|^2 + |c_1|^2 + \ldots + |c_k|^2 + \ldots = 1$$

Donde,

$$1 \geq c_0^2 + c_k^2$$

$$|c_k| \geq \frac{|t_k||c_0|}{2} \text{ ou } |d_k| \geq \frac{|t_k||c_0|}{2}$$

resultado

Se $B = c_0 + c_1 x + \ldots + c_k x^k + \ldots$ é função de Blaschke,

$$|c_0|^2 + |c_1|^2 + \ldots + |c_k|^2 + \ldots = 1$$

Donde,

$$1 \geq c_0^2 + c_k^2 \geq c_0^2 + \frac{|t_k|^2 c_0^2}{4} = c_0^2 \left(1 + \frac{|t_k|^2}{4}\right)$$

$$|c_k| \geq \frac{|t_k||c_0|}{2} \text{ ou } |d_k| \geq \frac{|t_k||c_0|}{2}$$

resultado

Se $B = c_0 + c_1 x + \ldots + c_k x^k + \ldots$ é função de Blaschke,

$$|c_0|^2 + |c_1|^2 + \ldots + |c_k|^2 + \ldots = 1$$

Donde,

$$1 \geq c_0^2 + c_k^2 \geq c_0^2 + \frac{|t_k|^2 c_0^2}{4} = c_0^2 \left(1 + \frac{|t_k|^2}{4}\right)$$

$$M(p)^2 \geq 1 + \frac{|t_k|^2}{4}$$

$$M(p) \geq \left(1 + \frac{|t_k|^2}{4}\right)^{1/2} \geq \sqrt{\frac{5}{4}} = 1.118\ldots$$

mínimo para polinómios recíprocos

- O teorema de Smyth aplica-se a qualquer polinómio irredutível de grau ímpar

- Se p recíproco, é invariante sob $z \to 1/z$.
- Como o grau é ímpar, existe raíz $\alpha = 1/\alpha$.
- $\alpha = \pm 1$
- $p = x + 1$ ou $p = x - 1$; $M(p) = 1$.

mínimo para polinómios recíprocos

- O teorema de Smyth aplica-se a qualquer polinómio irredutível de grau ímpar
- 2007 - Borwein, Dobrowolski, Mossinghoff

Teorema

Se p é um polinómio com coeficiente ímpares, irredutível, não ciclotómico e $p(0) \neq 0$, então

$$M(p) \geq 5^{1/4} = 1.495\ldots$$

mínimo para polinómios recíprocos

- O teorema de Smyth aplica-se a qualquer polinómio irredutível de grau ímpar
- 2007 - Borwein, Dobrowolski, Mossinghoff
- Não se sabe se existe um número de Salem mínimo. O menor <u>conhecido</u> é 1.176 (raiz de $\ell(x)$)

trabalho futuro