A Perron–Frobenius Theorem for Jordan Blocks for Complexity Proving

Jose Divasón U. La Rioja, Spain
Sebastiaan Joosten U. Twente, the Netherlands
René Thiemann U. Innsbruck, Austria
Akihisa Yamada NII, Japan

Main result

Theorem (due to René Thiemann):

If $A \in \mathbb{R}_{\geq 0}^{n \times n}$ is a non-negative real square matrix, then one of the largest Jordan blocks of A has the spectral radius ρ_A as the eigenvalue.

Proof

Very nontrivial, but believe it, it's formalized in Isabelle/HOL.

Complexity analysis

- What's the complexity of function sort?

```
sort (x :: xs)     = insert x (sort xs)
sort Nil           = Nil
insert x (y :: ys) = x :: y :: ys        when x <= y
insert x (y :: ys) = y :: insert x ys    when x > y
insert x Nil       = x :: Nil
```

Polynomial interpretation method

Find monotone polynomials $[\![sort]\!] : \mathbb{N} \to \mathbb{N}$, $[\![::]\!] : \mathbb{N} \to \mathbb{N} \to \mathbb{N}$, ..., s.t.

$$[\![sort\ (x :: xs) > insert\ x\ (sort\ xs)]\!]$$
$$[\![sort\ nil > nil]\!]$$
$$[\![insert\ x\ (y :: ys) > x :: y :: ys]\!]$$
$$[\![insert\ x\ (y :: ys) > y :: insert\ x\ ys]\!]$$
$$[\![insert\ x\ nil > x :: nil]\!]$$

Theorem:
If such interpretations exist, then the program terminates, and the runtime is $O\left([\![sort\ \left(x_1 :: (\ldots :: (x_k :: nil)\ )\right)]\!]\right)$

Polynomial runtime demands
$x\ [\![::]\!]\ y = f\ x + y$

Matrix interpretation method

Find affine maps $[\![sort]\!] : \mathbb{N}^n \to \mathbb{N}^n$, $[\![::]\!] : \mathbb{N}^n \to \mathbb{N}^n \to \mathbb{N}^n$, ..., s.t.

$$
\begin{aligned}
&[\![sort\ (x :: xs) && > insert\ x\ (sort\ xs)]\!] \\
&[\![sort\ nil && > nil]\!] \\
&[\![insert\ x\ (y :: ys) && > x :: y :: ys]\!] \\
&[\![insert\ x\ (y :: ys) && > y :: insert\ x\ ys]\!] \\
&[\![insert\ x\ nil && > x :: nil]\!]
\end{aligned}
$$

$$
\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} > \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} \Leftrightarrow \begin{matrix} x_1 > y_1 \\ x_2 \geq y_2 \\ x_3 \geq y_3 \end{matrix}
$$

Theorem:

If such interpretations exist, then the program terminates, and the runtime is $O\left(\left\| [\![sort\ (x_1 :: (\ldots :: (x_k :: nil)\ ))]\!] \right\|\right)$

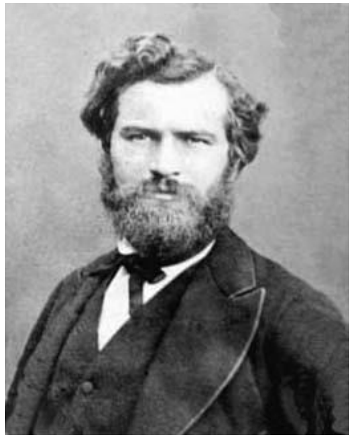
Runtime via matrix power

- Let $[\![sort]\!]\ x = Sx + s$, $x\ [\![::]\!]\ y = Cx + \boldsymbol{A}y + c$, $[\![nil]\!] = n$.

  Then $[\![sort\ (x_1 :: \cdots :: x_k :: nil)]\!]$
  $$= S \cdot \left(Cx_1 + \boldsymbol{A}Cx_2 + \cdots \boldsymbol{A}^{k-1}Cx_k + \boldsymbol{A}^k n\right) + \alpha$$
  $$\in O\left(k \cdot \left\|\boldsymbol{A}^k\right\|\right)$$
- So, if $\left\|\boldsymbol{A}^k\right\| \in O\left(k^d\right)$, runtime is $O\left(k^{d+1}\right)$

Jordan Normal Form precisely gives $\boldsymbol{A}^k$

Jordan normal form (JNF)



- Example:
  - $J = \begin{bmatrix} 2 & 1 & & & & \\ & 2 & 1 & & & \\ & & 2 & & & \\ & & & 3 & 1 & \\ & & & & 3 & \\ & & & & & 4 \end{bmatrix}$

Jordan blocks, generally $\begin{bmatrix} \lambda & 1 & & \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{bmatrix}$

Theorem:

Every square matrix has a JNF (over $\mathbb{C}$), i.e. $A = P\,J\,P^{-1}$

Note: $A^k = P\,J\,P^{-1}\,P\,J\,P^{-1} \cdots P\,J\,P^{-1} = P\,J^k\,P^{-1}$

Power of JNF

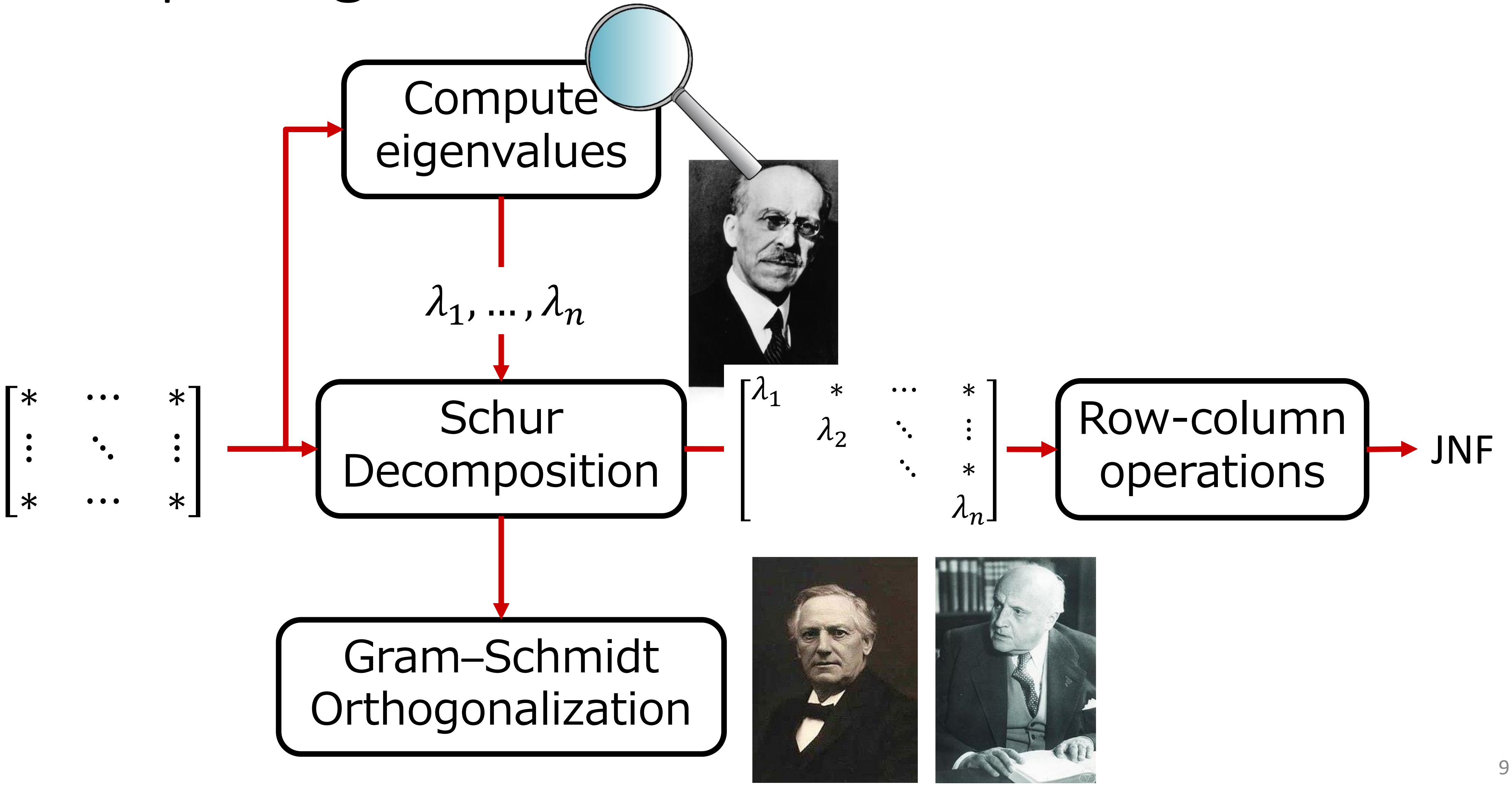
- Example:

$$J^k = \begin{bmatrix} \boxed{\begin{matrix} 2 & 1 & \\ & 2 & 1 \\ & & 2 \end{matrix}}^{k} & & \\ & \boxed{\begin{matrix} 3 & 1 \\ & 3 \end{matrix}}^{k} & \\ & & \boxed{4}^{k} \end{bmatrix}^k = \begin{bmatrix} 2^k & 2^{k-1}k & 2^{k-3}k(k-1) & & & \\ & 2^k & 2^{k-1}k & & & \\ & & 2^k & & & \\ & & & 3^k & 3^{k-1}k & \\ & & & & 3^k & \\ & & & & & 4^k \end{bmatrix}$$

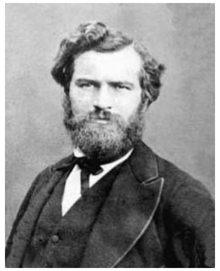
Lemma:

$$\overbrace{\begin{bmatrix} \lambda & 1 & & \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{bmatrix}}^{\text{size } n}{}^{k} = \begin{bmatrix} \binom{k}{0}\lambda^k & \binom{k}{1}\lambda^{k-1} & \cdots & \binom{k}{n-1}\lambda^{k-n-1} \\ & \binom{k}{0}\lambda^k & \cdots & \binom{k}{n-2}\lambda^{k-n-2} \\ & & \ddots & \vdots \\ & & & \binom{k}{0}\lambda^k \end{bmatrix}$$

Computing JNFs (following [Piziak & Odell '07])



Computing eigenvalues



$A \in \mathbb{Z}^{n \times n}$ → **Gauss–Jordan elimination**

↓ characteristic polynomial $\chi_A \in \mathbb{Z}[x]$

Polynomial factorization

$$\chi_A = f_1 \cdot \cdots \cdot f_m \in \mathbb{Z}[x]$$

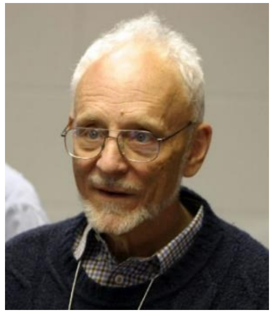
$\deg f_i \leq 2$ → **High-school math** → $\lambda_1, \ldots, \lambda_j \in \mathbb{C}$

→ **Algebraic number representation** → $\lambda_{j+1}, \ldots, \lambda_n \in \mathbb{C}$

Polynomial factorization

$f \in \mathbb{Z}[x]$

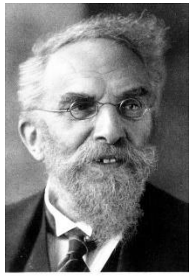
find prime → p → Berlekamp factorization



s.t. coprime p (lead_coeff f), (f mod p) is square free

$$f \equiv g_1 \cdot \cdots \cdot g_l \pmod{p}$$

factor bound → k → Hensel lifting



All Isabelle-formalized, but highly involved and expensive to run!

LLL reconstruction

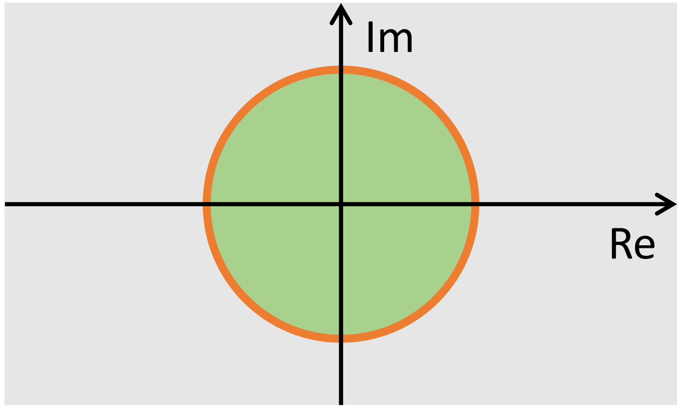
$$f = f_1 \cdot \cdots \cdot f_m \in \mathbb{Z}[x]$$

Power of Jordan blocks, revisited

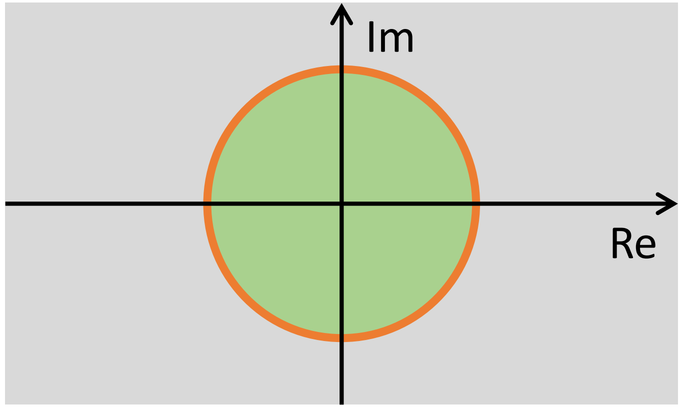
Lemma:

$$\begin{bmatrix} \lambda & 1 & & \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{bmatrix}^k = \begin{bmatrix} \binom{k}{0}\lambda^k & \binom{k}{1}\lambda^{k-1} & \cdots & \binom{k}{n-1}\lambda^{k-n-1} \\ & \binom{k}{0}\lambda^k & \cdots & \binom{k}{n-2}\lambda^{k-n-2} \\ & & \ddots & \vdots \\ & & & \binom{k}{0}\lambda^k \end{bmatrix}$$

- Observation
  - $|\lambda| > 1$ … **EXPTIME**
  - $|\lambda| = 1$ … **need care**
  - $|\lambda| < 1$ … **don't-care**



Checking polynomial growth



input: $A \in \mathbb{N}^{n\times n}, d \in \mathbb{N}$

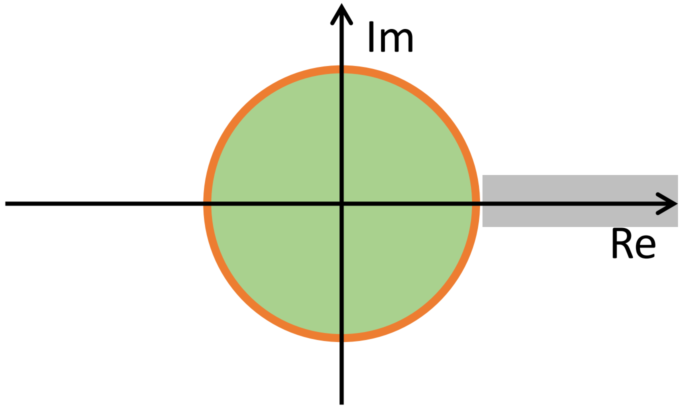
output: accept if $|A^k| \in \mathcal{O}(k^d)$

1. compute all eigenvalues Λ
2. reject (EXPTIME) if $\boldsymbol{\rho_A = \max_{\lambda\in\Lambda}|\lambda| > 1}$
3. compute JNF for each $\boldsymbol{\lambda \in \Lambda}$ **s.t.** $\boldsymbol{|\lambda| = 1}$

Theorem (Perron–Frobenius, basic):
If $A \in \mathbb{R}_{\geq 0}^{n\times n}$ then ρ_A is an eigenvalue of A.
(i.e., $\chi_A(\rho_A) = 0$)

Checking polynomial growth

input: $A \in \mathbb{N}^{n \times n}, d \in \mathbb{N}$
output: accept if $|A^k| \in \mathcal{O}(k^d)$



1. reject (EXPTIME) if χ_A has root in $(1, \infty)$
2. compute **all eigenvalues** Λ
3. compute JNF for each $\boldsymbol{\lambda \in \Lambda}$ **s.t.** $|\boldsymbol{\lambda}| = \mathbf{1}$

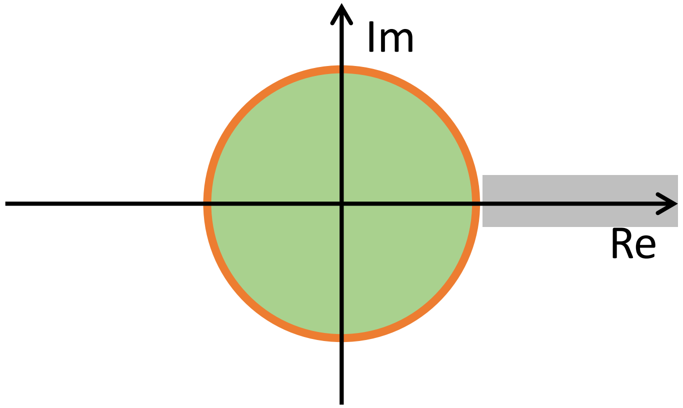
Theorem (Perron–Frobenius, more):
If $A \in \mathbb{R}_{\geq 0}^{n \times n}$ then

$$\chi_A(\lambda) = f(\lambda) \cdot \prod_{i \in I} (\lambda^i - \rho_A^i)$$

with $f(\lambda) = 0 \Longrightarrow |\lambda| < \rho_A$

Checking polynomial growth

input: $A \in \mathbb{N}^{n \times n}$, $d \in \mathbb{N}$
output: accept if $|A^k| \in \mathcal{O}(k^d)$



1. reject (EXPTIME) if χ_A has root in $(\mathbf{1}, \infty)$
2. compute **all eigenvalues** Λ
3. compute JNF for each **$\lambda \in \Lambda$ s.t. $|\lambda| = 1$**

Theorem (Perron–Frobenius, more):

If $A \in \mathbb{R}_{\geq 0}^{n \times n}$ and $\rho_A \leq 1$ then

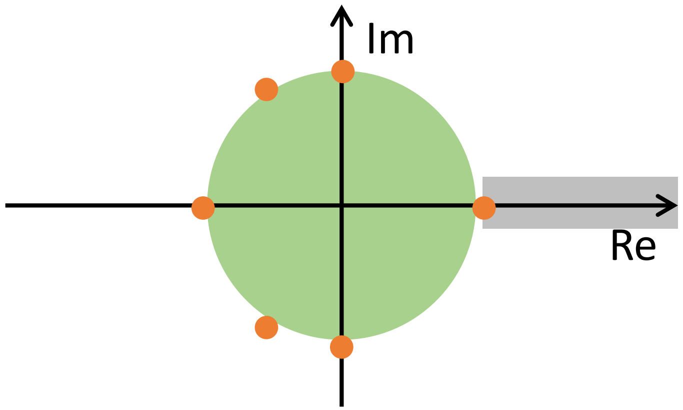
$$\chi_A(\lambda) = f(\lambda) \cdot \prod_{i \in I} (\lambda^i - 1)$$

with $f(\lambda) = 0 \Longrightarrow |\lambda| < 1$

concerned eigenvals are roots of unity!

Checking polynomial growth

input: $A \in \mathbb{N}^{n \times n}$, $d \in \mathbb{N}$
output: accept if $|A^k| \in \mathcal{O}(k^d)$



1. reject (EXPTIME) if χ_A has root in $(\mathbf{1}, \infty)$
2. compute **all eigenvalues** Λ
3. compute JNF for ***i*-th root of unity** up to some i

Theorem (Perron–Frobenius, more):

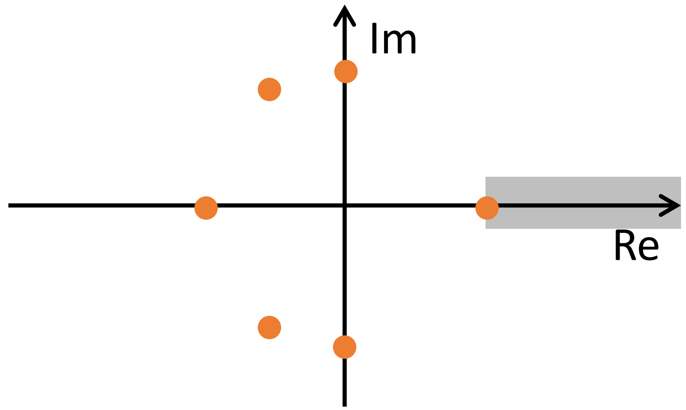
If $A \in \mathbb{R}_{\geq 0}^{n \times n}$ and $\rho_A \leq 1$ then

$$\chi_A(\lambda) = f(\lambda) \cdot \prod_{i \in I} (\lambda^i - 1)$$

with $f(\lambda) = 0 \Longrightarrow |\lambda| < 1$ **can be ignored!**

Checking polynomial growth

input: $A \in \mathbb{N}^{n \times n}$, $d \in \mathbb{N}$
output: accept if $|A^k| \in \mathcal{O}(k^d)$



1. reject (EXPTIME) if χ_A has root in $(1, \infty)$

2. compute JNF for ***i*-th root of unity** up to some i
   - 1,
   - -1,
   - $\frac{-1+\sqrt{3}\mathbb{i}}{2}, \frac{-1-\sqrt{3}\mathbb{i}}{2}$
   - …

not very nice!

Power of JNF, revisited

- Example:

$$J^k = \begin{bmatrix} \begin{bmatrix} \lambda_1 & 1 & \\ & \lambda_1 & 1 \\ & & \lambda_1 \end{bmatrix}^k & & \\ & \begin{bmatrix} \lambda_2 & 1 \\ & \lambda_2 \end{bmatrix}^k & \\ & & [\lambda_3]^k \end{bmatrix}^k$$

Only the largest Jordan block matter...

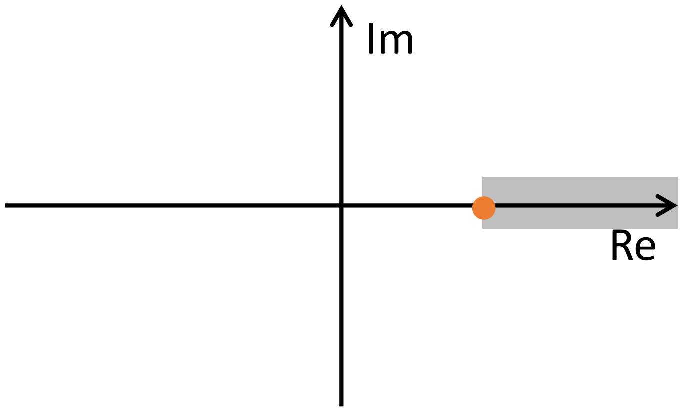
Lemma: If $|\lambda| = 1$ then

$$\underbrace{\begin{bmatrix} \lambda & 1 & & \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{bmatrix}}_{\text{size } n}^k \in \mathcal{O}\left((n-1)^k\right)$$

Theorem (Perron–Frobenius–Thiemann):
If $A \in \mathbb{R}_{\geq 0}^{n \times n}$, then one of the largest Jordan Blocks of A has ρ_A as the eigenvalue.

Finally!

input: $A \in \mathbb{N}^{n \times n}$, $d \in \mathbb{N}$
output: accept if $|A^k| \in \mathcal{O}(k^d)$



1. reject (EXPTIME) if χ_A has root in $(\mathbf{1}, \infty)$

2. compute JNF for eigenvalue **1**

Corollary:
For $A \in \mathbb{R}_{\geq 0}^{n \times n}$, $\|A^k\| \in \mathcal{O}(k^d)$ iff
- no eigenvalue in $(1, \infty)$ and
- the Jordan block of A for eigenvalue 1 is of size at most $d + 1$.

Conclusion

- Contribution
  - a very nontrivial Perron–Frobenius style theorem
  - all formalized in IsaFoR, implemented in CeTA
  - On 6,690 matrices from past TermComps, x5 speed up in certification.
- Future work
  - Utilize in complexity analysis (not only certification)?