Computational Logic

# The Perron–Frobenius Theorem for Certification of Complexity Proofs

René Thiemann

joint work with Jose Divasón, Sebastiaan Joosten, Ondřej Kunčar, and Akihisa Yamada

Institute of Computer Science
University of Innsbruck

Master Seminar 1, November 8, 2017

# Overview

- Introduction
- Certifying Matrix Growth
- Proofs
- Formalization

# Overview

- Introduction
- Certifying Matrix Growth
- Proofs
- Formalization

# Certification Approach

- Take input problem, e.g., Boolean formula
- Analyse using automated untrusted tools, e.g., run SAT-solver
- Obtain answer (SAT/UNSAT) + certificate
- Check certificate by trusted tool (trusted = formal proof)
  - Certification can be easy
    positive answer of SAT-solver with assignment $x, \neg y, \neg z, \ldots$
  - Certification can be hard or expensive
    "there is no satisfying assignment", DRAT, ...

# Complexity of Term Rewrite Systems

$$\begin{aligned}
\mathsf{sort}(\mathsf{Cons}(x, xs)) &\to \mathsf{insort}(x, \mathsf{sort}(xs)) \\
\mathsf{sort}(\mathsf{Nil}) &\to \mathsf{Nil} \\
\mathsf{insort}(x, \mathsf{Cons}(y, ys)) &\to \mathsf{Cons}(x, \mathsf{Cons}(y, ys)) && \mid x \leqslant y \\
\mathsf{insort}(x, \mathsf{Cons}(y, ys)) &\to \mathsf{Cons}(y, \mathsf{insort}(x, ys)) && \mid x \not\leqslant y \\
\mathsf{insort}(x, \mathsf{Nil}) &\to \mathsf{Cons}(x, \mathsf{Nil})
\end{aligned}$$

Aim: bound on maximal number of rewrite steps starting from

$$\mathsf{sort}(\mathsf{Cons}(x_1, \ldots \mathsf{Cons}(x_n, \mathsf{Nil})))$$

# Running automated complexity tool

Running TCT on TRS yields $\mathcal{O}(n^2)$ + certificate

$$[\![\mathsf{sort}]\!](xs) = \begin{pmatrix} 3 & 3 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \cdot [\![xs]\!]$$

$$[\![\mathsf{insort}]\!](x, xs) = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \cdot [\![xs]\!] + \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix}$$

$$[\![\mathsf{Cons}]\!](x, xs) = \underbrace{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}}_{A} \cdot [\![xs]\!] + \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}$$

$$[\![\mathsf{Nil}]\!] = \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix}$$

# Certification — part 1

Obtain strict decrease in every rewrite step:

$$[\![\mathsf{sort}(\mathsf{Cons}(x, xs))]\!] = \begin{pmatrix} 3 & 3 & 3 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \cdot [\![xs]\!] + \begin{pmatrix} 3 \\ 2 \\ 2 \end{pmatrix} \begin{matrix} > \\ \geq \\ \geq \end{matrix} \begin{pmatrix} 3 & 3 & 3 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \cdot [\![xs]\!] + \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix} = [\![\mathsf{insort}(x, \mathsf{sort}(xs))]\!]$$

# Certification — part 2

Bound initial interpretation:

$$[\![\mathsf{sort}(\mathsf{Cons}(x_1, \dots \mathsf{Cons}(x_n, \mathsf{Nil})))]\!] = \begin{pmatrix} 3 & 3 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \left( A^n \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix} + \sum_{i<n} A^i \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} \right) \in \mathcal{O}(n \cdot A^n)$$

Key analysis: growth of values of $A^n$ depending on $n$

# Overview

- Introduction
- Certifying Matrix Growth
- Proofs
- Formalization

# Eigenvalues and eigenvectors

Matrix $A$ has eigenvector $v \neq 0$ with eigenvalue $\lambda$ if

$$Av = \lambda v$$

Remark

- $\lambda$ is eigenvalue of $A$ if and only if
  $\lambda$ is root of characteristic polynomial $\chi_A$

Consequences

- $A^n v = \lambda^n v$
- $|A^n v| = |\lambda|^n |v|$
- if $|\lambda| > 1$ then $A^n$ grows exponentially

**Theorem**

*$A^n$ grows polynomially if and only if*
*$|\lambda| \leqslant 1$ for all eigenvalues $\lambda$ of $A$*

# Jordan blocks

Matrix $A$ has Jordan normal form $J = PAP^{-1}$

$$J = \begin{pmatrix} J_1 & 0 & \dots & 0 \\ 0 & J_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & J_k \end{pmatrix} \qquad J_i = \begin{pmatrix} \lambda_i & 1 & 0 & \dots & 0 \\ 0 & \lambda_i & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \lambda_i & 1 \\ 0 & \dots & \dots & 0 & \lambda_i \end{pmatrix}$$

Remarks

- the $\lambda_i$s are precisely the eigenvalues of $A$
- $\chi_A = \chi_J = \prod_{i=1}^{k}(x - \lambda_i)^{s_i}$ where $s_i$ = size of Jordan block $J_i$
- $J$ is unique up to permutation of blocks

Consequences

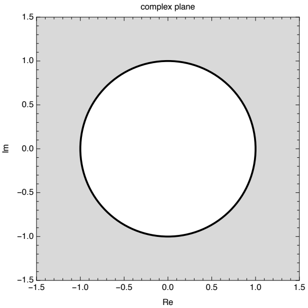
- $A^n = P^{-1}J^nP$, so $A$ and $J$ have same growth rate
- $J_i^n \in \Theta(n^{s_i-1}|\lambda_i|^n)$
- if $\max_i |\lambda_i| = 1$ then $A^n \in \Theta(n^{s-1})$ where $s = \max_{|\lambda_i|=1} s_i$

# Basic certification algorithm for $A^n \in \mathcal{O}(n^d)$

Input: Matrix $A$ and degree $d$

Output: Accept or assertion failure.

1. Compute all eigenvalues $\lambda_1, \ldots, \lambda_n$ of $A$ (all complex roots of $\chi_A$)
2. Compute spectral radius $\rho_A := \max_i |\lambda_i|$
3. Assert $\rho_A \leqslant 1$
4. For each $\lambda_i$ with $|\lambda_i| = 1$, and Jordan block of $A$ and $\lambda_i$ with size $s_i$, assert $s_i - 1 \leqslant d$
5. Accept



# Example insertion sort

Input: Matrix $A$ and degree $d$

Output: Accept or assertion failure.

1. Compute all eigenvalues $\lambda_1, \dots, \lambda_n$ of $A$ (all complex roots of $\chi_A$)
2. Compute spectral radius $\rho_A := \max_i |\lambda_i|$
3. Assert $\rho_A \leqslant 1$
4. For each $\lambda_i$ with $|\lambda_i| = 1$, and Jordan block of $A$ and $\lambda_i$ with size $s_i$, assert $s_i - 1 \leqslant d$
5. Accept

$$\text{Input: } A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}, d = 1$$

1. $\lambda_1 = 1, \lambda_2 = 0$
2. $\rho_A = 1$

4. $s_1 - 1 = 2 - 1 \leqslant 1 = d$

# Another example

Input: $A = \frac{1}{2}\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$

1. $\chi_A = \dfrac{(x-1)\,(8x^3 - 4x^2 - 2x - 1)}{8}$

$$\lambda_1 = 1$$

$$\lambda_2 = (\text{root } \#1 \text{ of } f_1)$$

$$\lambda_3 = (\text{root } \#1 \text{ of } f_2) + (\text{root } \#1 \text{ of } f_3)\mathrm{i}$$

$$\lambda_4 = (\text{root } \#1 \text{ of } f_2) + (\text{root } \#2 \text{ of } f_3)\mathrm{i}$$

$$f_1 = 8x^3 - 4x^2 - 2x - 1$$

$$f_2 = 32x^3 - 16x^2 + 1$$

$$f_3 = 1024x^6 + 512x^4 + 64x^2 - 11$$

# The problem and its solution

- algorithm 1 requires precise calculations ($|\lambda_i| = 1$)
- precise calculations with algebraic numbers are expensive
- aim: avoid explicit computation of eigenvalues
- solution: apply the Perron–Frobenius theorem

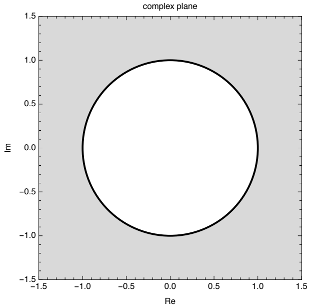
# Perron–Frobenius, Part 1

## Theorem (Perron–Frobenius)

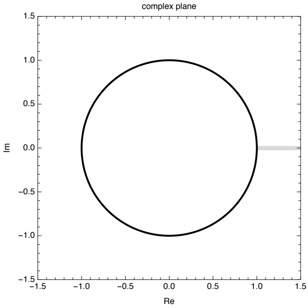
*Let $A$ be a non-negative real matrix*

- $\rho_A$ *is an eigenvalue of* $A$

## Consequence




$\longrightarrow$



# Perron–Frobenius, Part 2

**Theorem (Perron–Frobenius)**

*Let $A$ be a non-negative real and irreducible matrix*

- $\rho_A$ *is an eigenvalue of* $A$
- $\rho_A$ *has multiplicity 1*
- $\exists f\ k.\ \chi_A = f \cdot (x^k - \rho_A^k) \wedge (f(y) = 0 \longrightarrow |y| < \rho_A)$
- $\ldots$

Consequence

- non-negative real and irreducible matrices have constant or exponential growth

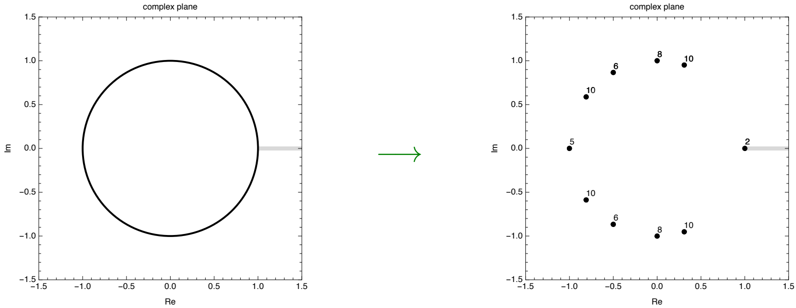
# Perron–Frobenius, Part 3

## Theorem

*Let $A$ be a non-negative real matrix*

- $\rho_A$ *is an eigenvalue of* $A$
- $\exists f\ K.\ \chi_A = f \cdot \prod_{k \in K}(x^k - \rho_A^k) \wedge (f(y) = 0 \longrightarrow |y| < \rho_A)$

## Consequence



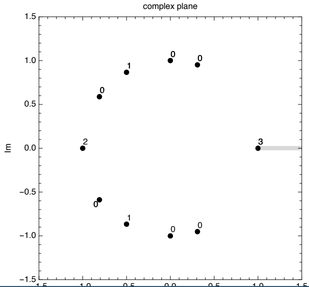
# Uniqueness of f and K

**Theorem**

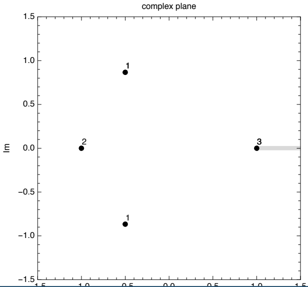
*Let $A$ be a non-negative real matrix*

- $\rho_A$ *is an eigenvalue of* $A$
- $\exists! f\, K.\ \chi_A = f \cdot \prod_{k \in K}(x^k - \rho_A^k) \wedge (f(y) = 0 \longrightarrow |y| < \rho_A)$
- decompose $\chi_A$ *computes* $f$ *and* $K$ *for* $\rho_A = 1$

## Consequence




$\xrightarrow{K=\{2,2,3\}}$



# New certification algorithm

Input: non-negative matrix $A$ and degree $d$

Output: Accept or assertion failure.

1. Assert that $\chi_A$ has no real roots in $(1, \infty)$ via Sturm's method
2. Compute $K$ via decompose $\chi_A$
3. If $|K| - 1 \leqslant d$ then accept
4. Check the Jordan blocks for eigenvalue 1, i.e., assert that each Jordan block of $A$ and 1 has size $s \leqslant d + 1$
5. If $\dim A \leqslant 4$ then accept
6. For each $k \in \{2, \ldots, \max K\}$ do
   - $m_k := |\{k' \in K.\ k \text{ divides } k'\}|$
   - If $m_k - 1 > d$ then check the Jordan blocks for all primitive roots of unity of degree $k$
7. Accept

# Experiments

- input: $d = 0$ and matrix $A$ of dimension 21 with

$$\chi_A = \frac{4096x^{21} - 8192x^{20} + \ldots + 152x^6 - x^4 - 9x^3 + 1}{4096}$$

- basic certification algorithm
  - factor $\chi_A = \frac{(x+1)(x^2+1)(x^2+x+1)\cdot\left((x-1)(64x^7-64x^6+4x^3-1)\right)^2}{4096}$
  - compute norms of roots of $64x^7 - 64x^6 + 4x^3 - 1$
  - timeout after 1 hour
- new certification algorithm
  - apply Sturm's method
  - decompose $\chi_A = (x^3 - 1) \cdot (x^4 - 1) \cdot f$, $K = \{3, 4\}$
  - only check Jordan block of eigenvalue 1
  - finished within fraction of a second
- matrices of termComp (dim $A \leqslant 5$): new algorithm 5x faster

# Improvements in Automation

- new certification runs in polynomial time for $\dim A \leqslant 5$

$\Longrightarrow$ there exists polynomial time SAT/SMT-encoding

$\Longrightarrow$ possibility to encode desired degree when searching for matrix interpretation

# Overview

- Introduction
- Certifying Matrix Growth
- Proofs
- Formalization

# Perron–Frobenius Theorem

- Parts 1 and 2 are well-studied
- New part 3: if $A$ is real non-negative matrix, then
  $\exists f\, K.\ \chi_A = f \cdot \prod_{k \in K}(x^k - \rho_A^k) \wedge (f(y) = 0 \longrightarrow |y| < \rho_A)$

## Proof by induction on the dimension of A.

- If $A$ is irreducible, then apply part 2 and set $K = \{k\}$
- If $\dim\ A = 1$ then result is trivial: $f = 1$, $K = \{1\}$
- Otherwise,

$$\pi(A) = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix}$$

  where $\pi$ is a permutation of rows and columns

$\Longrightarrow$ $B$ and $D$ are real non-negative matrices, $\chi_A = \chi_B \cdot \chi_D$

$\Longrightarrow$ apply induction hypothesis and perform case analysis:
$\rho_B = \rho_D \vee \rho_B < \rho_D \vee \rho_B > \rho_D$

# Largest Jordan blocks

Step 5 of new algorithm (if $\dim A \leqslant 4$ then accept) requires

## Theorem

*If $A$ is non-negative real matrix, $\dim A \leqslant 4$ and $\rho_A \leqslant 1$ then for every JB with $|\lambda| = 1$ there exists JB of 1 which is at least as large*

## Proof.

- Let there be JB with $\lambda \neq 1$, $|\lambda| = 1$ and size $s$ such that all JBs of 1 are smaller than $s$

$\Longrightarrow$ $s > 1$ since $\rho_A = 1$ is eigenvalue

$\Longrightarrow$ $\chi_A = (x^2 - 1)^2$

$$\Longrightarrow \pi(A) = \begin{pmatrix} B & C \\ 0 & D \end{pmatrix} = \begin{pmatrix} 0 & a & c & d \\ \frac{1}{a} & 0 & e & f \\ 0 & 0 & 0 & b \\ 0 & 0 & \frac{1}{b} & 0 \end{pmatrix} \text{ for } \begin{array}{cc} a, b & > 0 \\ c, d, e, f & \geq 0 \end{array}$$

# Proof continued

- $\pi(A) = PJP^{-1}$ and $h = 0 \longrightarrow g = 0$ for

$$g = \frac{-abe + af + bc - d}{2b}$$

$$h = \frac{abe + af + bc + d}{2a}$$

$$J = \begin{pmatrix} -1 & g & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & h \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$P = \begin{pmatrix} \frac{1}{2} & \frac{-a}{2} & \frac{abe+af-bc-d}{8b} & \frac{abe+af-bc-d}{8} \\ 0 & 0 & \frac{1}{2} & \frac{-b}{2} \\ \frac{1}{a} & 1 & \frac{abe-af+bc-d}{2ab} & 0 \\ 0 & 0 & \frac{1}{b} & 1 \end{pmatrix}$$

# Largest Jordan blocks

**Theorem**

*If $A$ is non-negative real matrix, $\dim A \leqslant 4$ and $\rho_A \leqslant 1$ then for every JB with $|\lambda| = 1$ there exists JB of 1 which is at least as large*

**Conjecture**

If $A$ is non-negative real matrix and $\rho_A \leqslant 1$ then for every JB with $|\lambda| = 1$ there exists JB of 1 which is at least as large

- with conjecture it would suffice to only consider JB for 1
- no violation of conjecture among billions of tested matrices
- no idea how to prove it

# Overview

# Overview on Formalization

- Carrier-based matrices ($\mathbb{N} \times \mathbb{N} \times (\mathbb{N} \to \mathbb{N} \to \alpha)$) for part 3
  - permits decomposition of matrices into smaller ones
- Type-based matrices ($\iota$ :: finite $\to \iota \to \alpha$) for part 1
  - continuity of matrix operations, Brouwer's fixpoint theorem
- Combination for part 2
  - proof requires continuity as well as decomposition
  - transfer, local type definitions
    (see paper or master seminar 2 in SS 2016)

# Summary

- efficient algorithm for certifying polynomial growth of $A^n$ for non-negative real matrices
- conjecture on largest Jordan blocks for further simplification
- permits SAT/SMT encoding for $\dim A \leqslant 5$
- soundness based on Perron–Frobenius theorem
- Isabelle formalization available in archive of formal proofs
- further application: unique solutions of Markov chains