The Perron–Frobenius Theorem in Isabelle/HOL

Transferring between Matrix-Representations

René Thiemann

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

Institute of Computer Science
University of Innsbruck

Linear Algebra in Isabelle/HOL, November 15, 2017

Overview

- Certifying Matrix Growth
- Formalization of the Perron–Frobenius Theorem
- Application: Certifying Complexity Proofs

Overview

- Certifying Matrix Growth
- Formalization of the Perron–Frobenius Theorem
- Application: Certifying Complexity Proofs

Matrix Growth

- input: non-negative real matrix

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

- task: decide matrix growth

  how large do values in A^n get for increasing n?

Eigenvalues and eigenvectors

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

$$Av = \lambda v$$

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 λ of A

Remark

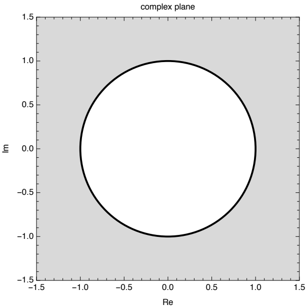
- λ is eigenvalue of A if and only if
  λ is root of characteristic polynomial χ_A

Old 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 χ_A)
2. Compute spectral radius $\rho_A := \max_i |\lambda_i|$
3. Assert $\rho_A \leqslant 1$
4. For each λ_i with $|\lambda_i| = 1$, and Jordan block of A and λ_i with size s_i, assert $s_i \leqslant d + 1$
5. Accept



Example of linear growth

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 χ_A)
2. Compute spectral radius $\rho_A := \max_i |\lambda_i|$
3. Assert $\rho_A \leqslant 1$
4. For each λ_i with $|\lambda_i| = 1$, and Jordan block of A and λ_i with size s_i, assert $s_i \leqslant d + 1$
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. $\chi_A = \frac{(x-1)(8x^3 - 4x^2 - 2x - 1)}{8}$

   $\lambda_1 = 1$

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

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

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

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

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

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

The problem and its solution

- old algorithm 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

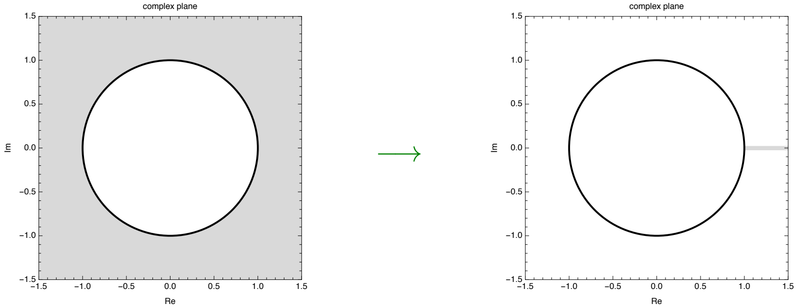
Perron–Frobenius, Part 1

Theorem (Perron–Frobenius)

Let A be a non-negative real matrix

- ρ_A *is an eigenvalue of* A

Consequence



Perron–Frobenius, Part 2

Theorem (Perron–Frobenius)

Let A be a non-negative real and irreducible matrix

- ρ_A *is an eigenvalue of* A
- ρ_A *has multiplicity 1*
- ρ_A *is only eigenvalue with non-negative real eigenvector*
- $\exists f\ k.\ \chi_A = f \cdot (x^k - \rho_A^k) \wedge (f(y) = 0 \longrightarrow |y| < \rho_A)$
- . . .

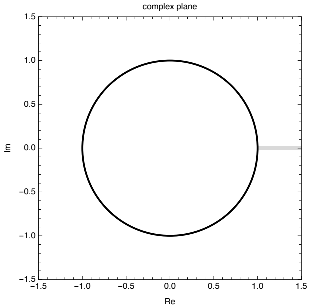
Perron–Frobenius, Part 3

Theorem

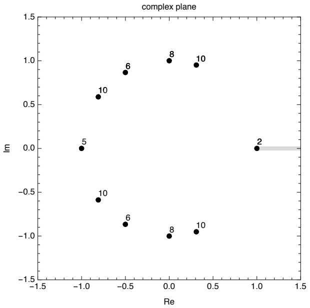
Let A be a non-negative real matrix

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

Consequence



$\longrightarrow$



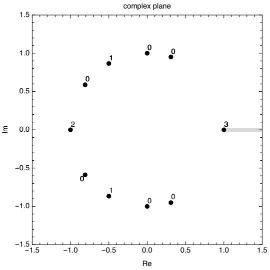
Uniqueness of f and K

Theorem

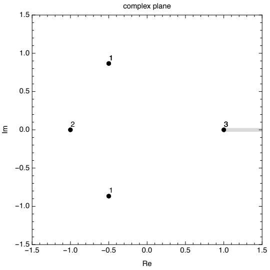
Let A be a non-negative real matrix

- ρ_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 χ_A *computes* f *and* K *for* $\rho_A = 1$

Consequence



$\longrightarrow\ K = \{2, 2, 3\} +$



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

Input: non-negative real matrix A and degree d

Output: Accept or assertion failure.

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

Experiments

large examples ($dim\ A = 21$)

- old: timeouts after 1 hour
- new: finished in fraction of second

matrices of termination competitions 2015–2017 ($2 \leqslant dim\ A \leqslant 5$)

- new algorithm 5x faster

Overview

- Certifying Matrix Growth
- Formalization of the Perron–Frobenius Theorem
- Application: Certifying Complexity Proofs

Part of Paper Proof

Definitions

$$X := \{x \in \mathbb{R}^n \mid x \geq 0, x \neq 0\}$$
$$X_1 := \{x \in X \mid \|x\| = 1\}$$
$$Y := \{(A+I)^n x \mid x \in X_1\}$$
$$r(x) := \min_{j, x_j \neq 0} \frac{(Ax)_j}{x_j}$$
$$r_{max} := \max \{r(y) \mid y \in Y\}$$

Lemmas

- X_1 and Y are compact
- r is continuous on Y
- r_{max} is well-defined (extreme value theorem)
- $r_{max} = \rho_A$
- $\chi'_A(\rho_A) = \sum_i \chi_{B_i}(\rho_A) > 0$ where $B_i = \text{mat-delete } A\ i\ i$

Overview on Formalization

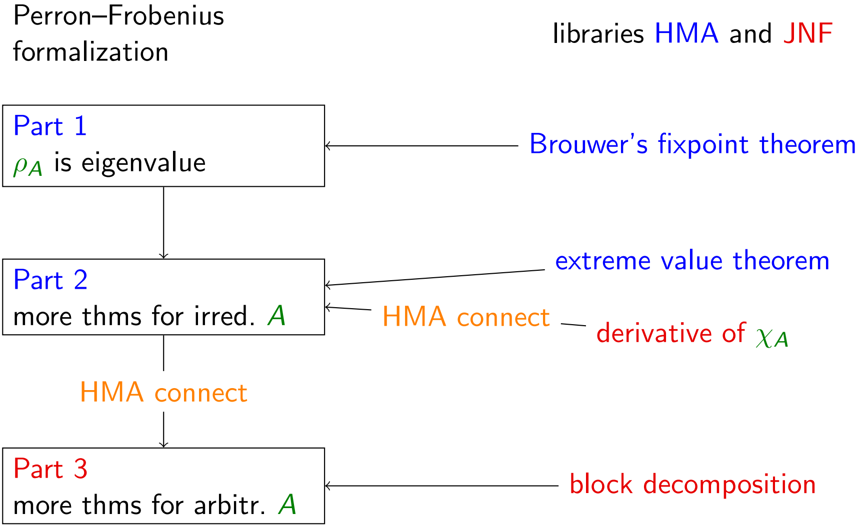
- HMA: Type-based vectors and matrices (ι :: finite $\rightarrow \alpha$)
- JNF: Carrier-based vectors and matrices ($\mathbb{N} \times (\mathbb{N} \rightarrow \alpha)$)

	HMA library	JNF library
compatible dimensions	type-system	explicit carrier
arithmetic, determinants, ...	✓	✓
continuity, compactness, ...	✓	
block-matrices, delete row, ...		✓

- formalization of Perron–Frobenius requires all features

$\Longrightarrow$ develop connection between both worlds: HMA connect

Overview of Formalization



HMA Connect

- main aim: establish connection between JNF and HMA
- tool: transfer
  - define correspondence-relation between vectors, matrices, ...

$$HMA_{vec} :: \mathbb{N} \times (\mathbb{N} \to \gamma) \to (\alpha \to \gamma) \to \text{bool}$$
$$HMA_{vec}\ v\ w = (v = (\text{CARD}(\alpha), \lambda i. w_{\text{from-nat}\ i}))$$

    where from-nat is some bijection between α and $\{0, \ldots, \text{CARD}(\alpha) - 1\} \subseteq \mathbb{N}$

  - prove transfer rules between constants of JNF and HMA

$$(HMA_{mat} \longrightarrow HMA_{mat} \longrightarrow HMA_{mat})\ \text{op} + \text{op} +$$
$$(HMA_{mat} \longrightarrow \text{op} =)\ \text{det}\ \text{det}$$

  - finally transfer complex statements between JNF and HMA

Transferring Theorems from JNF to HMA

- JNF lemma for derivative of characteristic polynomial

$$A \in \text{carrier-mat } n\ n \longrightarrow$$
$$\text{pderiv (charpoly } A) = \sum_{i<n} \text{charpoly (mat-delete } A\ i\ i)$$

- transfer to HMA not yet possible: mat-delete not available
- solution: reformulate lemma

$$A \in \text{carrier-mat } n\ n \longrightarrow \text{monom } 1\ 1 *$$
$$\text{pderiv (charpoly } A) = \sum_{i<n} \text{charpoly (mat-erase } A\ i\ i)$$

- transfer to HMA

$$\text{monom } 1\ 1 * \text{pderiv (charpoly } A) =$$
$$\sum_{i} \text{charpoly (mat-erase } A\ i\ i)$$

Transferring Theorems from HMA to JNF

- Perron–Frobenius Theorem Part 1 (HMA)

  real-non-neg-mat $A \longrightarrow$ eigenvalue A (spectral-radius A)

- transfer to JNF

  $A \in$ carrier-mat (CARD(α)) (CARD(α)) $\longrightarrow$
  real-non-neg-mat $A \longrightarrow$ eigenvalue A (spectral-radius A)

- post-processing with local type definition

  $A \in$ carrier-mat n $n \longrightarrow n \neq 0 \longrightarrow$
  real-non-neg-mat $A \longrightarrow$ eigenvalue A (spectral-radius A)

Overview

- Certifying Matrix Growth
- Formalization of the Perron–Frobenius Theorem
- Application: Certifying Complexity Proofs

Complexity of Term Rewrite Systems

$$\begin{aligned}
\mathsf{sort}(\mathsf{Cons}(x, xs)) &\to \mathsf{insort}(x, \mathsf{sort}(xs)) && \\
\mathsf{sort}(\mathsf{Nil}) &\to \mathsf{Nil} && \\
\mathsf{insort}(x, \mathsf{Cons}(y, ys)) &\to \mathsf{Cons}(x, \mathsf{Cons}(y, ys)) && \mid x \leqslant y \\
\mathsf{insort}(x, \mathsf{Cons}(y, ys)) &\to \mathsf{Cons}(y, \mathsf{insort}(x, ys)) && \mid x \nleqslant y \\
\mathsf{insort}(x, \mathsf{Nil}) &\to \mathsf{Cons}(x, \mathsf{Nil}) &&
\end{aligned}$$

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 of complexity proofs

- check strict decrease in every rewrite step
- bound initial interpretation

$$[\![\mathsf{sort}(\mathsf{Cons}(x_1, \ldots \mathsf{Cons}(x_n, \mathsf{Nil})))]\!] =$$

$$\begin{pmatrix} 3 & 3 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \left(A^n \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix} + \sum_{i<n} A^i \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix} \right) \in \mathcal{O}(n \cdot A^n)$$

$\Longrightarrow$ key analysis: growth of values of A^n depending on n

Further Application: Irreducible Markov chains

- Let A_{ij} encode some probabilities to go from state j to state i

$$A = \begin{pmatrix} 0.3 & 0.8 & 0.2 \\ 0.6 & 0.0 & 0.4 \\ 0.1 & 0.2 & 0.4 \end{pmatrix}$$

- Question: is there stationary distribution: $\exists v.\ v \geq 0 \wedge Av = v$
- Consequence of Perron–Frobenius
  if A is irreducible then stationary distribution is unique

Summary

- formalization of Perron–Frobenius theorem
- HMA connect: combine HMA- and JNF-libraries
  based on transfer + local type definitions
- our application: efficient certifier for complexity proofs
- future application: finite irreducible Markov chains
- AFP 2016: only part 1 of Perron–Frobenius theorem
- AFP 2017: parts 1–3 formalized

  www.isa-afp.org/entries/Perron_Frobenius.html