On the Complexity of Computing Real Radicals of Polynomial Systems

Mohab Safey El Din[1] Zhi-Hong Yang[2] Lihong Zhi[2]

[1]Sorbonne Université, CNRS, INRIA,
Laboratoire d'Informatique de Paris 6, LIP6, Équipe PolSys

[2]Key Lab of Mathematics Mechanization,
Academy of Mathematics and Systems Science, CAS, China

ISSAC'18, New York, July 16-19

Motivation

Polynomial system solving over the reals: $\boldsymbol{f} = (f_1, \ldots, f_s) \subset \mathbb{Q}[X_1, \ldots, X_n]$

$$\mathbf{V}_{\mathbb{R}}(\boldsymbol{f}) = \{x \in \mathbb{R}^n \mid f_1(x) = 0, \ldots, f_s(x) = 0\}$$

- Numeric computation $\longrightarrow$ reliability issues, especially in the singular case.
- Algebraic computation $\longrightarrow$ $(V = \mathbf{V}_{\mathbb{C}}(\boldsymbol{f}) \longleftrightarrow \sqrt{\langle \boldsymbol{f} \rangle})$
  What if $V \cap \mathbb{R}^n \subset \mathrm{Sing}(V)$?

$$x_1^2 + x_2^2 = 0$$

$\swarrow$ $\qquad$ $\searrow$

$\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$: lines

$$\begin{cases} x_1 + ix_2 = 0 \\ x_1 - ix_2 = 0 \end{cases}$$

$\mathbf{V}_{\mathbb{R}}(\boldsymbol{f})$: point

$$x_1 = x_2 = 0$$

- Dimensions are different.
- $(0,0) \in V$, singular
- $(0,0) \in V \cap \mathbb{R}^n$, smooth!

Example 1 [Everett, Lazard, Lazard, Safey El Din, 2007]

$$
\begin{aligned}
\mathrm{Vor1} =& (\alpha^2+\beta^2+1)a^2\lambda^4 - 2a(2a\beta^2 + ay\beta + a\alpha x - \beta\alpha + 2a + 2a\alpha^2 - \beta\alpha a^2)\lambda^3 \\
&+ (\beta^2 + 6a^2\beta^2 - 2\beta x a^3 - 6\beta\alpha a^3 + 6y\beta a^2 - 6a\beta\alpha - 2a\beta x + 6\alpha x a^2 + y^2a^2 \\
&- 2a\alpha y + x^2a^2 - 2y\alpha a^3 + 6a^2\alpha^2 + a^4\alpha^2 + 4a^2)\lambda^2 \\
&- 2(xa - ya^2 - 2\beta a^2 - \beta + 2a\alpha + \alpha a^3)(xa - y - \beta + a\alpha)\lambda \\
&+ (1+a^2)(xa - y - \beta + a\alpha)^2.
\end{aligned}
$$

Example 1 [Everett, Lazard, Lazard, Safey El Din, 2007]

$$\begin{aligned}\mathrm{Vor1} =&(\alpha^2+\beta^2+1)a^2\lambda^4-2a(2a\beta^2+ay\beta+a\alpha x-\beta\alpha+2a+2a\alpha^2-\beta\alpha a^2)\lambda^3\\&+(\beta^2+6a^2\beta^2-2\beta x a^3-6\beta\alpha a^3+6y\beta a^2-6a\beta\alpha-2a\beta x+6\alpha x a^2+y^2a^2\\&-2a\alpha y+x^2a^2-2y\alpha a^3+6a^2\alpha^2+a^4\alpha^2+4a^2)\lambda^2\\&-2(xa-ya^2-2\beta a^2-\beta+2a\alpha+\alpha a^3)(xa-y-\beta+a\alpha)\lambda\\&+(1+a^2)(xa-y-\beta+a\alpha)^2.\end{aligned}$$

- Real zeros of $\mathrm{Vor1}$ are union of:

$$\begin{cases}a\alpha-ax+\beta-y=0\\ \lambda+1=0\end{cases}\qquad\begin{cases}a\alpha+ax-\beta-y=0\\ \lambda=0\end{cases}\qquad\begin{cases}2\beta\lambda+\beta+y=0\\ a=0\end{cases}$$

Example 1 [Everett, Lazard, Lazard, Safey El Din, 2007]

$$\begin{aligned}\mathrm{Vor1} =&(\alpha^2+\beta^2+1)a^2\lambda^4-2a(2a\beta^2+ay\beta+a\alpha x-\beta\alpha+2a+2a\alpha^2-\beta\alpha a^2)\lambda^3\\&+(\beta^2+6a^2\beta^2-2\beta x a^3-6\beta\alpha a^3+6y\beta a^2-6a\beta\alpha-2a\beta x+6\alpha x a^2+y^2a^2\\&-2a\alpha y+x^2a^2-2y\alpha a^3+6a^2\alpha^2+a^4\alpha^2+4a^2)\lambda^2\\&-2(xa-ya^2-2\beta a^2-\beta+2a\alpha+\alpha a^3)(xa-y-\beta+a\alpha)\lambda\\&+(1+a^2)(xa-y-\beta+a\alpha)^2.\end{aligned}$$

- Real zeros of $\mathrm{Vor1}$ are union of:

$$\begin{cases}a\alpha-ax+\beta-y=0\\ \lambda+1=0\end{cases}\qquad\begin{cases}a\alpha+ax-\beta-y=0\\ \lambda=0\end{cases}\qquad\begin{cases}2\beta\lambda+\beta+y=0\\ a=0\end{cases}$$

- Only one connected component, which is not easy to be seen from $\mathrm{Vor1}$.

Problem

- $\boldsymbol{f} = (f_1, \ldots, f_s) \subset \mathbb{Q}[X_1, \ldots X_n]$.
- $\sqrt[re]{\langle \boldsymbol{f} \rangle}$: the vanishing ideal of $\mathbf{V}_{\mathbb{R}}(\boldsymbol{f})$.
- An ideal I is called real if $I = \sqrt[re]{I}$.
- $D = \max\{\deg f_i, \ldots, \deg f_s\}$.

Input: $\boldsymbol{f} = (f_1, \ldots, f_s)$

Output: irreducible components of $\sqrt[re]{\langle \boldsymbol{f} \rangle}$:

- generators, or
- rational parametrizations.

Example 1 (Continued)

$$\begin{aligned}\mathrm{Vor1} =&(\alpha^2+\beta^2+1)a^2\lambda^4-2a(2a\beta^2+ay\beta+a\alpha x-\beta\alpha+2a+2a\alpha^2-\beta\alpha a^2)\lambda^3\\&+(\beta^2+6a^2\beta^2-2\beta x a^3-6\beta\alpha a^3+6y\beta a^2-6a\beta\alpha-2a\beta x+6\alpha x a^2+y^2a^2\\&-2a\alpha y+x^2a^2-2y\alpha a^3+6a^2\alpha^2+a^4\alpha^2+4a^2)\lambda^2\\&-2(xa-ya^2-2\beta a^2-\beta+2a\alpha+\alpha a^3)(xa-y-\beta+a\alpha)\lambda\\&+(1+a^2)(xa-y-\beta+a\alpha)^2.\end{aligned}$$

Irreducible components of $\sqrt[re]{\langle \mathrm{Vor1}\rangle}$:

$$\begin{aligned}P_1&=\langle a\alpha-ax+\beta-y,\lambda+1\rangle\\P_2&=\langle a\alpha+ax-\beta-y,\lambda\rangle\\P_3&=\langle 2\beta\lambda+\beta+y,a\rangle\end{aligned}$$

Timing: 9 sec.

State of the art

Exact computation:

- Becker, Neuhaus'1993, Neuhaus'1998, Spang'2007
  Using Gröbner bases to compute real radicals for arbitrary polynomial ideals.
  The complexity is $D^{2^{O(n^2)}}$.

Numerical approximations:

- Lasserre, Laurent, Rostalski'2008; Lasserre, Laurent, Mourrain, Rostalski, Trébuchet'2013
  Using SDP relaxations to compute zero-dimensional real radical ideals.
- Ma, Wang, Zhi'2014
  A certificate for computing real radicals using SDP relaxations.
- Brake, Hauenstein, Liddell'2016
  A method based SDP programming for deciding if an ideal is real.

Main Results

$\boldsymbol{f} = (f_1, \ldots, f_s) \subset \mathbb{Q}[X_1, \ldots, X_n]$, $r = \dim\langle \boldsymbol{f} \rangle$, $D = \max\{\deg f_i\}$.

State of the art: $D^{2^{O(n^2)}}$

Smooth case.

A probabilistic algorithm computes generators of irreducible components of $\sqrt[re]{\langle \boldsymbol{f} \rangle}$ using $(snD^n)^{O(1)}$ operations in $\mathbb{Q}$.

General case.

A probabilistic algorithm computes rational parametrizations of irreducible components of $\sqrt[re]{\langle \boldsymbol{f} \rangle}$ using $s^{O(1)}(nD)^{O(nr2^r)}$ arithmetic operations in $\mathbb{Q}$.

Main idea

Simple point criterion [Bochnak, Coste, Roy, 1998]

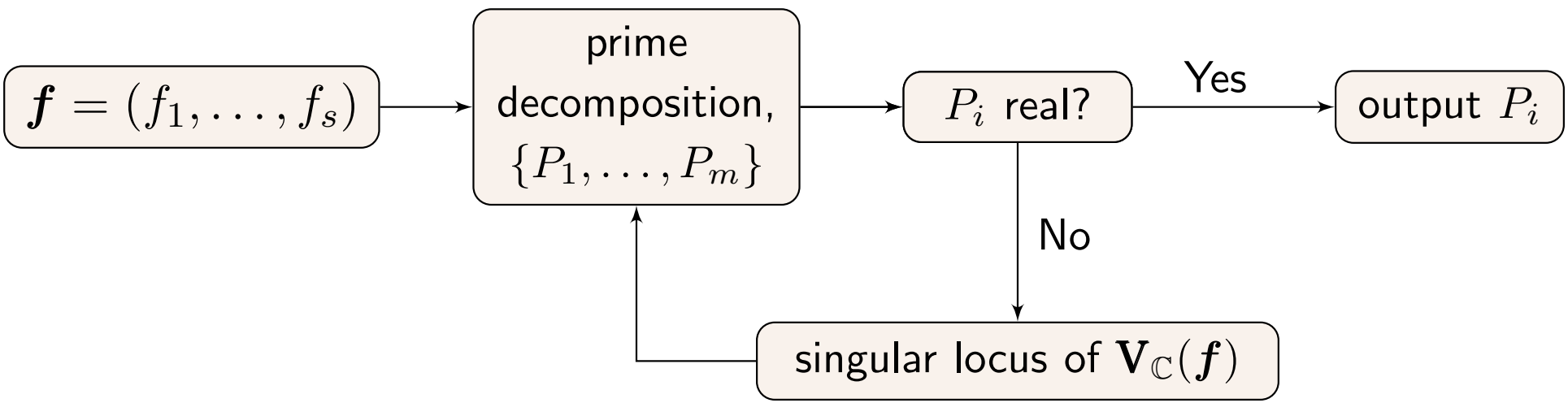
Prime $I = \langle f_1, \ldots, f_s \rangle$ real $\iff \exists x \in \mathbf{V}_{\mathbb{R}}(I)$ s.t. rank $\left(\frac{\partial f_i}{\partial X_j}(x) \right) = n - r$, where $r = \dim I$.

Main idea

Simple point criterion [Bochnak, Coste, Roy, 1998]

Prime $I = \langle f_1, \ldots, f_s \rangle$ real $\iff \exists x \in \mathbf{V}_{\mathbb{R}}(I)$ s.t. rank $\left(\frac{\partial f_i}{\partial X_j}(x) \right) = n - r$, where $r = \dim I$.

Main idea:



Singular point

Singular point [Cox, Little, O'Shea, 1992]

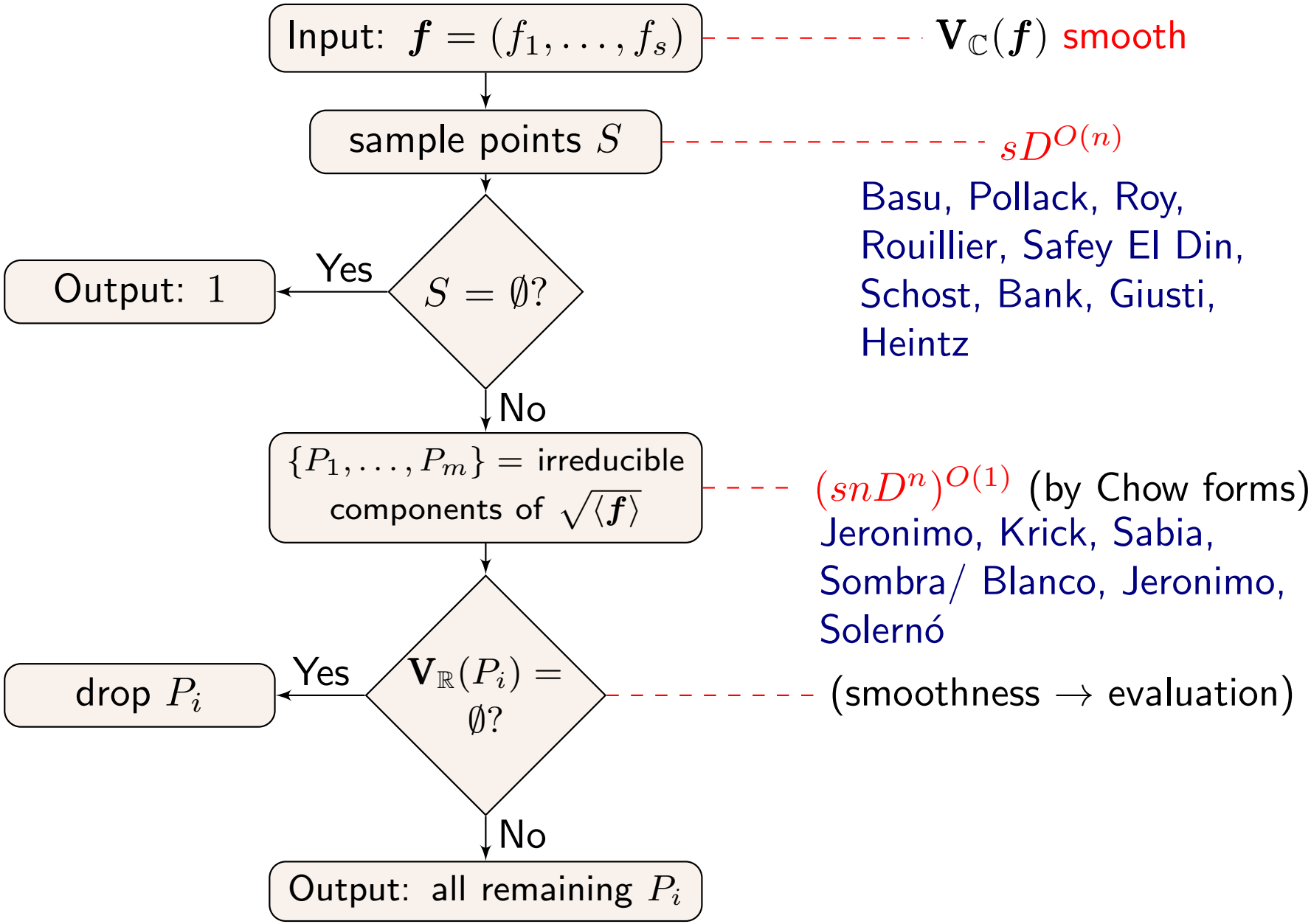
$V \subset \mathbb{C}^n$, $p \in V$, $\mathbf{I}(V) = \langle f_1, \ldots, f_s \rangle$. The *tangent space* of V at p is

$$T_p(V) = \bigcap_{j=1}^{s} \left\{ x \in \mathbb{C}^n \,\middle|\, \sum_{i=1}^{n} \frac{\partial f_j}{\partial X_i}(p) x_i = 0 \right\}.$$

$\dim_p V = \max\{\dim V_i \mid p \in V_i$ irreducible component of $V\}$.

- Smooth Point: $\dim T_p(V) = \dim_p V$.
- Singular Point: $\dim T_p(V) \neq \dim_p V$.
- Singular locus: $\mathrm{Sing}(V) = \{p \in V \mid p$ is a singular point of $V\}$.
- V is smooth if $\mathrm{Sing}(V) = \emptyset$.

Smooth case


Input: $\boldsymbol{f} = (f_1, \ldots, f_s)$
$\mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$ smooth
sample points S
$sD^{O(n)}$
Basu, Pollack, Roy, Rouillier, Safey El Din, Schost, Bank, Giusti, Heintz
$S = \emptyset$?
Yes
Output: 1
No
$\{P_1, \ldots, P_m\}$ = irreducible components of $\sqrt{\langle \boldsymbol{f} \rangle}$
$(snD^n)^{O(1)}$ (by Chow forms)
Jeronimo, Krick, Sabia, Sombra/ Blanco, Jeronimo, Solernó
$\mathbf{V}_{\mathbb{R}}(P_i) = \emptyset$?
Yes
drop P_i
(smoothness $\rightarrow$ evaluation)
No
Output: all remaining P_i

General case

Drop the smoothness assumption on $V = \mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$.

Difficulties: it may happen

- $V \cap \mathbb{R}^n \subset \mathrm{Sing}(V)$;
- ... or even worse, in the singular locus of $\mathrm{Sing}(V)$;

General case

Drop the smoothness assumption on $V = \mathbf{V}_{\mathbb{C}}(\boldsymbol{f})$.

Difficulties: it may happen

- $V \cap \mathbb{R}^n \subset \mathrm{Sing}(V)$;
- ... or even worse, in the singular locus of $\mathrm{Sing}(V)$;

Standard idea: lazy representations for equidimensional components of V.

- equations and inequations.
- Triangular set decompositions (Wu, Lazard, etc.) or rational parametrizations (Giusti, Heintz, Morais, Pardo, etc.)

Rational parametrization

An r-equidimensional variety $V \subset \mathbb{C}^n$ is the Zariski closure of the projection of the following set to $X = (X_1, \ldots, X_n)$:

$$w(T) = 0,\ X_i \frac{\partial w(T)}{\partial T_{r+1}} = v_i(T),\ \frac{\partial w(T)}{\partial T_{r+1}} \neq 0$$

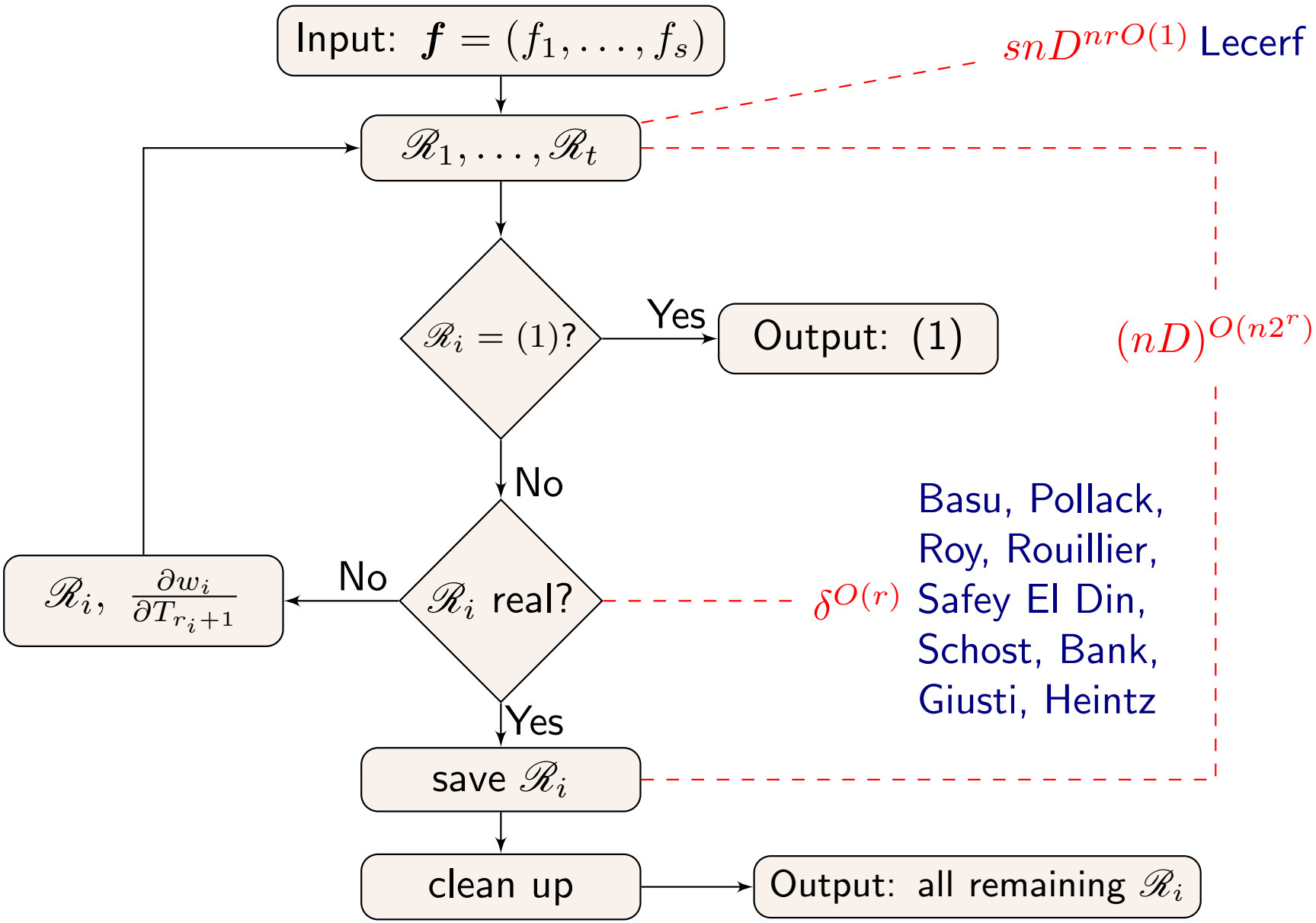
where $T = (T_1, \ldots, T_{r+1})$, $i = 1, \ldots, n$.

A rational parametrization of V:

- $\boldsymbol{\ell} = (\lambda_1, \ldots, \lambda_{r+1})$, generic linear combinations of $X_1, \ldots, X_n$
- polynomials $w, v_1, \ldots, v_n \in \mathbb{Q}[T]$.

Denote $\mathscr{R} = ((w, v_1, \ldots, v_n), \boldsymbol{\ell})$.

General case



Implementation

Combing:

- SINGULAR: operating ideals [Greuel, Pfister].
- Maple: computing sample points RAGlib [Safey El Din] (uses FGb [Faugère] for computing Gröbner bases).

Implementation

Combing:

- SINGULAR: operating ideals [Greuel, Pfister].
- Maple: computing sample points RAGlib [Safey El Din] (uses FGb [Faugère] for computing Gröbner bases).

Examples beyond the reach of the SINGULAR library realrad [Spang].

- (Homotopy-1) 7 variables, degree 7. [Chen, Davenport, May, Moreno Maza, Xia, Xiao]

  $f_1 = x^3y^2 + c_1x^3y + y^2 + c_2x + c_3,\ f_2 = c_4x^4y^2 - x^2y + y + c_5,\ f_3 = c_4 - 1.$

  Timimg: 1 sec.

- (Essential variety) 9 variables, degree 3 [Fløystad, Kileel, Ottaviani]

  $\mathcal{E} = \{M \in \mathbb{R}^{3\times 3} \mid \det(M) = 0,\ 2(MM^T)M - \mathrm{tr}(MM^T)M = 0\}$

  Timing: 800 sec.

Thank you!