Regular Chains: Theory and Computation

Paul Vrbik [1]

[1]University of Western Ontario

February 23, 2011

What does it mean to solve a polynomial system?

The pure mathematician says:

For $F \subset \mathbf{k}[x_1, \ldots, x_n]$ find

- a primary decomposition (can be unique) of $\langle F \rangle$ or
- the unique irreducible decomposition of $V(F)$ (the zero set of F in $\overline{\mathbf{k}}^n$).

We don't do this because:

- for practical purposes it's computationally infeasible and
- this decomposition may not be helpful for actually constructing points in $\overline{\mathbf{k}}^n$.

What does it mean to solve a polynomial system?

The computer algebra system constructs:

For $F \subset \mathbf{k}[x_1, \ldots, x_n]$ with $\mathbf{k}$ some effective ring (i.e. $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Q}$),

- a lex Gröbner basis of $\langle F \rangle$.

Elimination theory ensures that we get $\langle G \rangle = \langle g_1, \ldots, g_n \rangle = \langle F \rangle$ such that (crucially):

$$G \cap \mathbf{k}[x_{\ell+1}, \ldots, x_n]$$

is a Gröbner basis of the ℓ-th elimination ideal I_ℓ.

This allows for a kind of back substitution (not guaranteed to be easy).

What does it mean to solve a polynomial system?

But most scientists and engineers need:

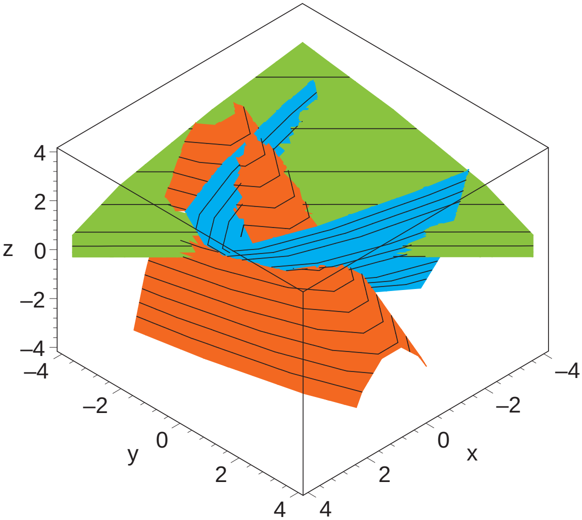
For $F \subset \mathbb{Q}[x_1, \ldots, x_n]$:

- a "useful" description of the points of $V(F)$ whose coordinates are real.

For $F \subset \mathbb{Q}[u_1, \ldots, u_d][x_1, \ldots, x_n]$:

- the real $(x_1, \ldots, x_n)$–solutions from $\mathbb{Q}(u_1, \ldots, u_d)$ (the x_i's are rational functions in the variables $u_1, \ldots, u_d$).

Example of Different Techniques



$$F := \left[\left(x^2 + y + z - 1 \right), \left(x + y^2 - z - 1 \right), \left(x + y + z^2 \right) \right]$$

Maple 15 - Polynomial Ideals

$> with(PolynomialIdeals):$

$> F := \left\langle \left(x^2+y+z-1\right), \left(x+y^2-z-1\right), \left(x+y+z^2\right) \right\rangle:$

$> PrimeDecomposition(F);$

$$\left\langle (z-1), \left(z^2+x+y-1\right), \left(x+y^2+z-1\right), \left(x^2+y+z-1\right) \right\rangle$$

$$\left\langle \left(z^2+2z-1\right), \left(z^2+x+y-1\right), \left(x+y^2+z-1\right), \left(x^2+y+z-1\right) \right\rangle$$

$$\left\langle (y), (z), \left(z^2+x+y-1\right), \left(x+y^2+z-1\right), \left(x^2+y+z-1\right) \right\rangle$$

$$\left\langle (z), (y-1), \left(z^2+x+y-1\right), \left(x+y^2+z-1\right), \left(x^2+y+z-1\right) \right\rangle$$

Maple 15 - Gröbner Basis

$> with(Groebner):$

$> F := \left[\left(x^2 + y + z - 1\right), \left(x + y^2 - z - 1\right), \left(x + y + z^2\right)\right]:$

$> B := Basis(F, plex(x, y, z));$

$$z^6 - 4z^4 + 4z^3 - z^2$$

$$z^4 + 2yz^2 - z^2$$

$$y^2 - z^2 - y + z$$

$$z^2 + x + y - 1$$

$> with(RegularChains):$

$> R := PolynomialRing([x, y, z]):$

$> F := \left[\left(x^2 + y + z - 1\right), \left(x + y^2 - z - 1\right), \left(x + y + z^2\right)\right]:$

$> dec := Triangularize(F, R) : map(Display, dec, R) :$

$$\left[\left\{\begin{array}{c} x - z = 0 \\ y - z = 0 \\ z^2 + 2z - 1 = 0 \end{array}\right., \left\{\begin{array}{c} x = 0 \\ y = 0 \\ z - 1 = 0 \end{array}\right., \left\{\begin{array}{c} x = 0 \\ y - 1 = 0 \\ z = 0 \end{array}\right., \left\{\begin{array}{c} x - 1 = 0 \\ y = 0 \\ z = 0 \end{array}\right.\right]$$

{This is a "triangular" decomposition.}

$> with(RegularChains):$

$> R := PolynomialRing([x, y, z]):$

$> F := \left[\left(x^2 + y + z - 1\right), \left(x + y^2 - z - 1\right), \left(x + y + z^2\right)\right]:$

$> dec := RealRootIsolate(F, R) : map(Display, dec, R) :$

$$\left[\left\{\begin{array}{c} x = [-1, 4] \\ y = [-1, 4] \\ z = [0, 3] \end{array}\right., \left\{\begin{array}{c} x = [-4, 1] \\ y = [-4, 1] \\ z = [-3, 0] \end{array}\right., \left\{\begin{array}{c} x = [0, 0] \\ y = [1, 1] \\ z = [0, 0] \end{array}\right., \left\{\begin{array}{c} x = [0, 0] \\ y = [0, 0] \\ z = [1, 1] \end{array}\right., \left\{\begin{array}{c} x = [1, 1] \\ y = [0, 0] \\ z = [0, 0] \end{array}\right.\right]$$

{Observe that we don't lose the exact solutions from the last slide.}

0-Dimensional Case

The solutions of the last examples are what we classify 0-dimensional (i.e. have finite many solutions).

Definition (Dimension of Triangular Component)

The number of "free variables" of the ideal (i.e. the number of polynomials that are not "algebraic" in some polynomial equation; e.g. $x = 0$ versus $x \neq 0$ or $x > 0$).

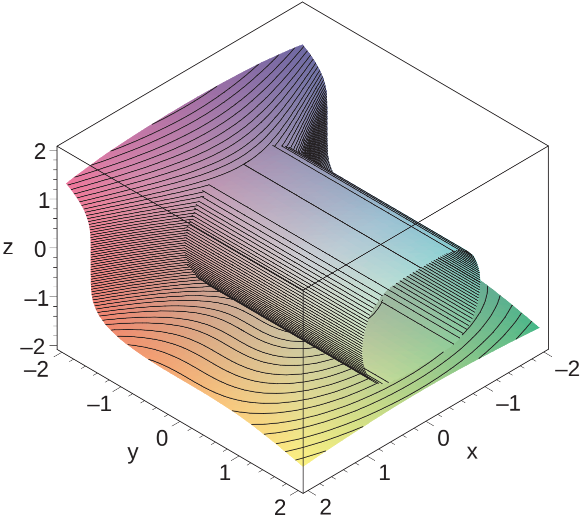
This definition is far from complete. What we really mean by "free" is algebraic independence of $S \subset \{x_1, \ldots, x_n\}$:

$$I \cap \mathbf{K}[S] = \langle 0 \rangle .$$

Example (Free Variables)

For $\mathbf{k}[x, y]$ and $F = \left\langle x^2 + 2x + 1 \right\rangle$ the variable y is free.

Positive-Dimensional Case



$$F := \left[\left(x^2 + y^3 + z^5 \right), \left(x^4 + z^2 - 1 \right) \right]$$

Positive-Dimensional Case

(Like finding a zero dimensional solution where free variables are moved to the coefficient ring.)

$> with(RegularChains):$

$> R := PolynomialRing([x, y, z]):$

$> F := \left[\left(x^2 + y^3 + z^5\right), \left(x^4 + z^2 - 1\right)\right]:$

$> dec := Triangularize(F, R) : map(Display, dec, R) :$

$$\left[\left\{\begin{array}{c} \left(-2x^4 + x^8 + 1\right) z + x^2 + y^2 \\ 10x^{12} - 10x^8 - 5x^{16} + 6x^4 + x^{20} - 1 + 2x^2y^2 + y^4 \end{array}\right.\right]$$

Using the option *output* = *lazard* will actually give you the specialization for $-2x^4 + x^8 + 1$ as well.

Positive-Dimensional Case

To get better information we may restrict the solutions to the real numbers:

$> with(RegularChains):$

$> R := PolynomialRing([x, y, z]):$

$> F := \left[\left(x^2 + y^3 + z^5\right), \left(x^4 + z^2 - 1\right)\right]:$

$> dec := RealTriangularize(F, R) : map(Display, dec, R) :$

$$\left[\begin{cases} z = 0 \\ y + 1 = 0 \\ x - 1 = 0 \end{cases}, \begin{cases} z = 0 \\ y + 1 = 0 \\ x + 1 = 0 \end{cases}, \begin{cases} (-2x^4 + x^8 + 1)z + x^2 = 0 \\ y = 0 \\ x^{12} - 4x^8 + 5x^4 - 1 = 0 \end{cases}, \right.$$

$$\left. \begin{cases} x - 1 = 0 \\ y = 0 \\ z = 0 \end{cases}, \begin{cases} (-2x^4 + x^8 + 1)z + y^3 + x^2 = 0 \\ y^6 + 2x^2y^3 + 10x^{12} - 10x^8 + x^{20} - 5x^{16} + 6x^{16} + 6x^4 - 1 = 0 \\ x < 1 \\ 0 < x + 1 \\ x^{12} - 4x^8 + 5x^4 - 1 \neq 0 \end{cases} \right]$$

Objectives

Many aspects of the theory regular chains were motivated by the following questions:

1. How do we represent (encode) an irreducible component of a variety?
   - And how do we decompose our variety into irreducible components in the first place?
   - Can we avoid finding irreducible components?
2. How can we make this encoding useful for computing points in the affine space?
   - Require that we can back substitute.
   - Require that this back substitution is "well behaved".

Triangular Sets

Definition (notation)

1. Let $\succ$ be an ordering on the variables $\{x_1, \ldots, x_n\}$ and assume that $x_n \succ \cdots \succ x_1$.
2. Let $T = \{T_1, \ldots, T_\ell\} \subset \mathbf{k}[x_1, \ldots, x_n] - \mathbf{k}$.
3. For and $p \in \mathbf{k}[x_1, \ldots, x_n]$ let $\mathrm{mvar}(p)$ (read "main variable") denote the $\succ$-largest x_i such that $\deg(p, x_i) > 0$.

Definition (Triangular Sets)

T is a triangular set if for all $p, q \in T$ with $p \neq q$ we have $\mathrm{mvar}(p) \neq \mathrm{mvar}(q)$.

Or in other words: T is a triangular set if it's T_i's have mutually different $\succ$-largest variable.

Example

$T = \{x_1 - x - 1^2, x_2^2 - x_1, x_1x_3^2 - 2x_2x_3 + 1, (x_2x_3 - 1)x_4 + x_2^2\} \subset \mathbf{P}_4$ is a triangular set because

$$
\begin{aligned}
(x_2x_3 - 1)x_4 + x_2^2 &\in \mathbf{k}[x_1, x_2, x_3, x_4] \\
x_1x_3^2 - 2x_2x_3 + 1 &\in \mathbf{k}[x_1, x_2, x_3] \\
(x_1 - 1)x_2^2 - x_1 &\in \mathbf{k}[x_1, x_2] \\
(x_1 - 1)(x_1 + 1) &\in \mathbf{k}[x_1]
\end{aligned}
$$

(the triangular shape of the polynomial rings as they are written above was the inspiration for the name "triangular" set).

- Triangular sets allow us to back substitute. (Two steps forwards).
- Back substitution isn't guaranteed to be well behaved—consider $(x_1 - 1) = 0$. (One step back).

It's clear that we'll need more restrictions.

Properties of Triangular Sets

Theorem (J.F. Ritt, 1932)

Let $\mathbf{V} \subset \mathbf{k}^n$ *be an irreducible variety and* $F \subset \mathbf{k}[x_1, \ldots, x_n]$ *s.t.* $\mathbf{V} = V(F)$*. Then one can compute a (reduced) triangular set* $T = \langle T_1, \ldots, T_\ell \rangle \subset \langle F \rangle$ *such that*

$$(\forall g \in \langle F \rangle) \ \operatorname{prem}(g, T) = 0.$$

Where

$$\operatorname{prem}(g, T) = \operatorname{prem}(\cdots \operatorname{prem}(\operatorname{prem}(g, T_\ell), T_{\ell-1}) \cdots, T_1)$$

(assuming $\operatorname{mvar}(T_\ell) \succ \cdots \succ \operatorname{mvar}(T_1)$*).*

We get: an ideal membership test for $\langle F \rangle$.

Properties of Triangular Sets

What if we can't get the irreducible components? (Which is typically true because multivariate factorization is expensive in practice).

Theorem (W.T. Wu, 1987)

Let $V \subset \mathbf{k}^n$ be a variety and $F \subset \mathbf{k}[x_1, \ldots, x_n]$ s.t. $V = V(F)$. Then one can compute a (reduced) triangular set $T \subset \langle F \rangle$ such that

$$(\forall g \in F) \ \ \mathrm{prem}(g, T) = 0.$$

We loose: test for $V = \emptyset$.

The stronger restrictions we impose on triangular sets to avoid this will make them regular chains (later).

Addressing the back substitution problem

Vanishing leading terms usually result in bad back substitution.

Definition (Initial)

For $p \in \mathbf{k}[x_1, \ldots, x_n] \setminus \mathbf{k}$ let $\mathrm{init}(p)$ be the leading coefficient (in the usual sense) of p when considered univariate in $\mathrm{mvar}(p)$.

Example

Let $p = (x_1 + x_2)x_3^2 - 2x_2x_3 + 1$.

$$\mathrm{mvar}(p) = x_3$$
$$\mathrm{init}(p) = (x_1 + x_2)$$

Where do the initials vanish?

For a triangular set T let $h_T := \prod_{t \in T} \mathrm{init}(T)$.

The initials will vanish on $V(h_T)$. So, let's get rid of them!

Definition (Geometrically shedding bad initials)

Let

$$W(T) := V(T) \setminus V(h_T).$$

which we call T's quasi-component.

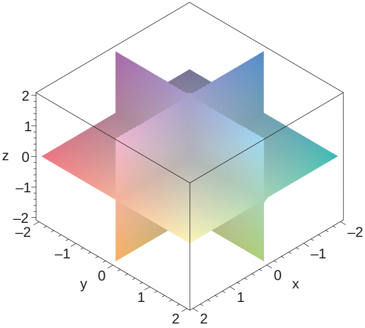
Definition (Algebraically shedding bad initials)

Let

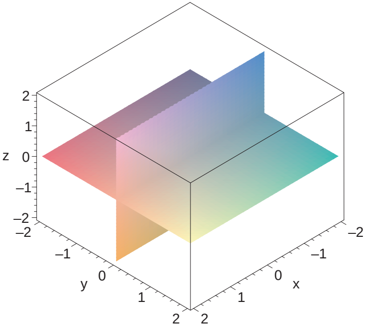
$$\mathrm{sat}(T) := \langle T \rangle : h_T^{\infty} = \left\{ p \in \mathbf{k}[x_1, \ldots, x_n] \,\middle|\, \exists n \in \mathbb{N},\ h^n p \in \langle T \rangle \right\}$$

which we call the saturation ideal of T.

Saturation Ideals Example 1

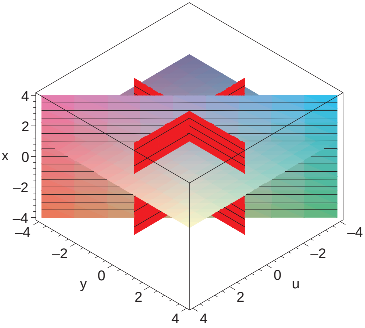


$T = \langle xy, xz \rangle$

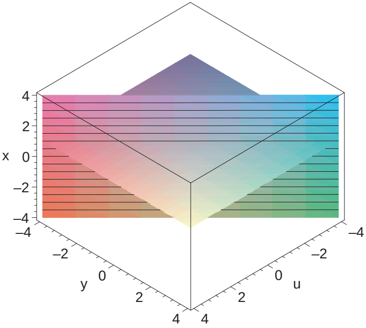


$\mathrm{sat}(T) = \langle y, z \rangle$

Saturation Ideals Example 2



$$T = \langle u, y \rangle \cap \langle y + u, -x + 1 \rangle$$



$$\mathrm{sat}(T) = \langle y + u, -x + 1 \rangle$$

Saturation Ideals Example 3

Example

$\mathrm{sat}(T)$ can be lager than $\langle T \rangle$. For $v \succ u \succ y \succ x$:

$$T = \begin{cases} ux + v \\ vy + u \end{cases}$$

$$\langle T \rangle = \langle u, v \rangle \cap \langle -xy + 1, vy + u \rangle$$

$$\mathrm{sat}(T) = \langle 1 - xy, vy + u \rangle .$$

Relating sat(T) and $W(T)$

Theorem (F. Bouleer, F. Lemaire, MMMM 2006)

We have:

$$\overline{W(T)} = V(\mathrm{sat}(T))$$

and, moreover, if $\mathrm{sat}(T) \neq \langle 1 \rangle$ *then* $\mathrm{sat}(T)$ *is strongly equidimensional.*

Equidimensional: the components of prime decomposition that correspond to $\mathrm{sat}(T)$ are of the same dimension

Strongly Equidimensional: the prime components of $\mathrm{sat}(T)$ have the same set of parameters.

Or, more precisely: If $\dim(\mathrm{sat}(T)) = d$ then $\exists S \subset \{x_1, \ldots, x_n\}$ such that $\#S = d$ and

$$\forall \mathcal{P} \in \mathrm{Ass}\,(\mathrm{sat}(T)) \;\; \mathcal{P} \cap \mathbf{k}[S] = \langle 0 \rangle\,.$$

Regular Chains

Simultaneously discovered by M. Kalkbrener and L. Yan/J. Zhang in 1991.

Definition (Regular Chain)

T is a regular chain if

1. $T = \emptyset$, or
2. $T = T' \cup \{t\}$ with $\mathrm{mvar}(t) \succ \mathrm{mvar}(t')$ for all $t' \in T'$ and
   i. T' is a regular chain, and
   ii. $\mathrm{init}(t)$ is regular (not a zero divisor) modulo $\mathrm{sat}(T')$.

2-ii means that (in the zero dimensionally case) t can be made monic modulo T', fixing the bad back substitution problem.

In higher dimensions we make t monic over some special field of fractions (e.g. $\mathbf{k}(S)[y]$ where $y = \left\{\mathrm{mvar}(t) \,\middle|\, t \in T\right\}$ and $S = \mathbf{x} \setminus y$.)

Properties of Regular Chains

Theorem (Wang 2000, MMM 2000)

For any $F \subseteq \mathbf{k}[x_1, \ldots, x_n]$ *one can compute regular chains* $T_1, \ldots, T_\ell$ *such that*

$$z \in V(F) \iff \exists i \text{ st } z \in W(T_i).$$

Algorithmic Properties of Regular Chains

Definition (Iterated Resultant)

Let $T = T' \cup \{t\}$ be a regular chain with t having largest main variable. For $p \in \mathbf{k}[x_1, \ldots, x_n]$ the iterated resultant is given by

$$\text{res}(\emptyset, p) = p$$

$$\text{res}(T, p) = \begin{cases} p & \text{if } \deg(p, \mathrm{mvar}(t)) = 0 \\ \text{res}\left(T', \text{res}\left(t, p, \mathrm{mvar}(t)\right)\right) & \text{otherwise} \end{cases}$$

Definition (Iterate Pseudo Remainder (revisited))

$\cdots$ the iterated pseudo remainder is given by

$$\mathrm{prem}(p, \emptyset) = p$$

$$\mathrm{prem}(p, T) = \mathrm{prem}(\mathrm{prem}(p, t, \mathrm{mvar}(t)), T')$$

Algorithmic Properties of Regular Chains

Theorem (L. Yang, J. Zhang 1991)

T is a regular chain if and only if

$$\mathsf{res}(T, h_T) \neq 0.$$

(also p is regular modulo $\mathrm{sat}(T)$ if and only if $\mathsf{res}(T, p) \neq 0$.)

Theorem (Aubry, Lazard, MMM)

T is a regular chain if and only if

$$\{p \,|\, \mathrm{prem}(p, T) = 0\} = \mathrm{sat}(T).$$

In a way, these combine to give the technical realization of our "nice back substitution" requirement.

Regular GCD

Definition (Regular GCD)

Let $P, Q \in \mathbb{A}[y]$ be non-constant polynomials with regular leading coefficient.

G is a regular GCD of P, Q if we have:

1. $\mathrm{lc}(G, y)$ is regular in $\mathbb{A}$,
2. $G \in \langle P, Q \rangle \subset \mathbb{A}[y]$,
3. $\deg(G, y) > 0 \Rightarrow \mathrm{prem}(P, G, y) = \mathrm{prem}(Q, G, y) = 0$

(In practice $y = x_n$ and $\mathbb{A} = \mathbf{k}[x_1, \ldots, x_{n-1}] \setminus \mathrm{sat}(T)$ for a regular chain T.)

Also, the existence of this GCD isn't guaranteed. However, we are guaranteed when the regular chain $T = \langle T_1, \ldots, T_\ell \rangle$ the existence of

$$G_i \text{ the regular GCD of } P, Q \bmod \mathrm{sat}(T_i).$$

First Steps Towards Algorithms

Input: $p \in \mathbf{k}[x_1, \ldots, x_n] \setminus \mathbf{k}$ and $T \subseteq \mathbf{k}[x_1, \ldots, x_n]$ a regular chain.

Output: Regular chains $T_1, \ldots, T_d$ such that

$$\overline{W(T) \cap V(p)} = \overline{W(T_1) \cup \cdots \cup W(T_d)}$$

and $W(T) \cap V(p) \subseteq W(T_1) \cup \cdots \cup W(T_d)$.

INTERSECT := proc(F)

$\vdots$

end proc

Input: F a finite set of polynomial of $\mathbf{k}[x_1, \ldots, x_n]$.

Output: Regular Chains $T_1, \ldots, T_d$ such that when
$W = W(T_1) \cup \cdots \cup W(T_d)$ then $\overline{V(F)} = \overline{W}$ and $V(F) \subseteq W$.

```
SOLVE := proc(F)
    C := [∅]; (a list or regular chains)
    while F ≠ ∅ repeat
        choose and remove a polynomial p from F
        C′:=[]
        for T ∈ C repeat
            C′:=concat(intersect(p,T), C′)
        C:=C′
    return C
end proc
```

The Regular Chains Package

1. SemiAlgebraicSetTools and RealTriangularize (real solving)
2. ParametricSystemTools (solving higher dimensional problems as seen as zero dimensional in their parameters)
3. ConstuctibleSetTools (for algebraic geometers)
4. MatrixTools (Paul)
5. FastArithemeticTools (FFT stuff)
6. ChainTools (tool kit)
7. Triangularize (get a triangular decomposition)
8. SamplePoints (retrieve points from the affine space).

Timings

Sys	GL	GS	TL	TK
4corps-1parameter-homog	-	-	-	36.934
8-3-config-Li	108.738	-	25.853	5.968
Alonso-Li	3.476	-	2.192	0.432
Bezier	-	-	-	88.217
Bjork60	62.627	-	-	-
Cheaters-homotopy-easy	2609.543	-	-	0.744
Cheaters-homotopy-hard	3412.281	-	-	0.352
childDraw-1	18.569	-	-	-
childDraw-2	19.301	-	-	-
Cinquin-Demongeot-3-3	63.643	-	7.144	0.640
Cinquin-Demongeot-3-4	-	-	-	3.108
collins-jsc02	-	-	1.556	0.468

Contributions

- 131 exported functions,
- more than 300 internal functions,
- 67,000 lines of MAPLE source code,
- 10,000 lines of test programs,
- 3,000 lines of software development source code (C, LEX, scripts),
- 12,000 lines of documentation,

Acknowledgements

The RegularChains library was originally designed since 1999, by Francois Lemaire (Univ. of Lille, France) and M. Moreno Maza (UWO).

It was integrated in Maple 10 by F. Lemaire, M. Moreno Maza and Yuzhen Xie (UWO).

In Maple 12, contributions were made by Eric Schost, Wenyuan Wu, Yuzhen Xie, MMM (modular algorithms).

In Maple 12, contributions were made by Changbo Chen, Liyun Li, Wei Pan, Yuzhen Xie, MMM (constructible sets and parametric systems).

In Maple 13, contributions were made by Changbo Chen, Frabcois Lemaire, Liyun Li, Xinn Li, Wei Pan, Bican Xia, Rong Xiao, Yuzhen Xie, MMM. (real solving, parametric systems and FFT-based arithmetic).

In Maple 14 and 15, contributions were made by Changbo Chen, Rong Xiao, MMM. (new algorithms for Triangularize and real solving).