On the Representation of Constructible Sets

Changbo Chen, Liyun Li, Marc Moreno Maza, Wei Pan, & Yuzhen Xie

ORCCA and Computer Science Department
University of Western Ontario, London, Canada

Introduction

• Constructible sets appear naturally when solving systems of polynomial equations, in particular in presence of parameters.

• The occurrence of redundant components is a normal phenomenon when computing with constructible sets, with both numerical and symbolic methods.

• We investigate efficient algorithms for removing those redundancies and we establish complexity results.

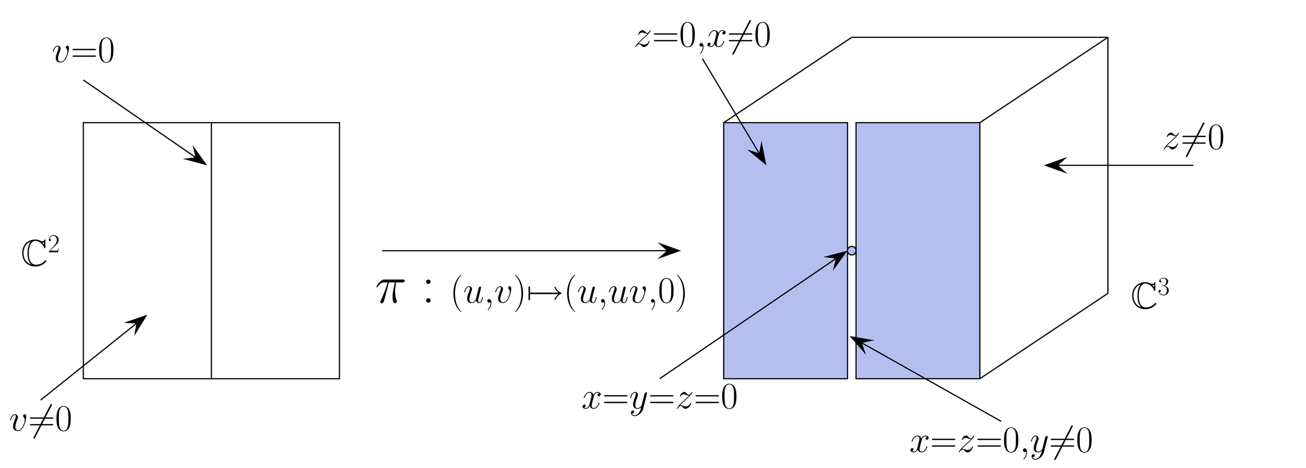
Representation of Constructible Sets

• A constructible set of $\mathbb{C}^n$ is a finite union

$$(A_1 \setminus B_1) \cup \cdots \cup (A_e \setminus B_e)$$

where A_i's and B_i's are algebraic varieties in $\mathbb{C}^n$.

• The image of an algebraic variety under a polynomial map is generally not an algebraic variety, rather a constructible set.



The image of the map π is:

$$\pi(\mathbb{C}^2) = \{\text{xy-plane}\} - \{\text{y-axis}\} + \{\text{origin}\}.$$

It can be encoded uniquely by a **sequence** of algebraic varieties:

$$(\{z = 0\}, \{x = z = 0\}, \{x = y = z = 0\})$$

each of them given by a **Gröbner basis** (a generating set).

• In our library, the above constructible set is represented as

$$\{x = z = 0, y \neq 0\} \cup \{x = y = z = 0\}.$$

Formally, we encode a constructible set C by a list

$$[[T_1, h_1], \ldots, [T_e, h_e]]$$

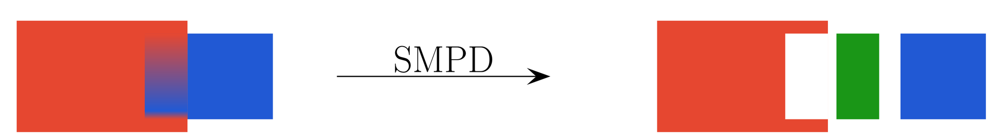
of so-called **regular systems**, where each T_i is a **regular chain** and each h_i is a polynomial regular modulo the saturated ideal of T_i. The points of C are those which cancel *all* polynomials in T_i but not h_i, for some $1 \leq i \leq e$.

Removing Redundancy

• **Within a single constructible set:**

Solution: make the defining regular systems pairwise disjoint (MPD).

• **Among several ones while preserving structure:**



Solution: compute an intersection-free basis by symmetrically making the constructible sets pairwise disjoint (SMPD).

Main Results

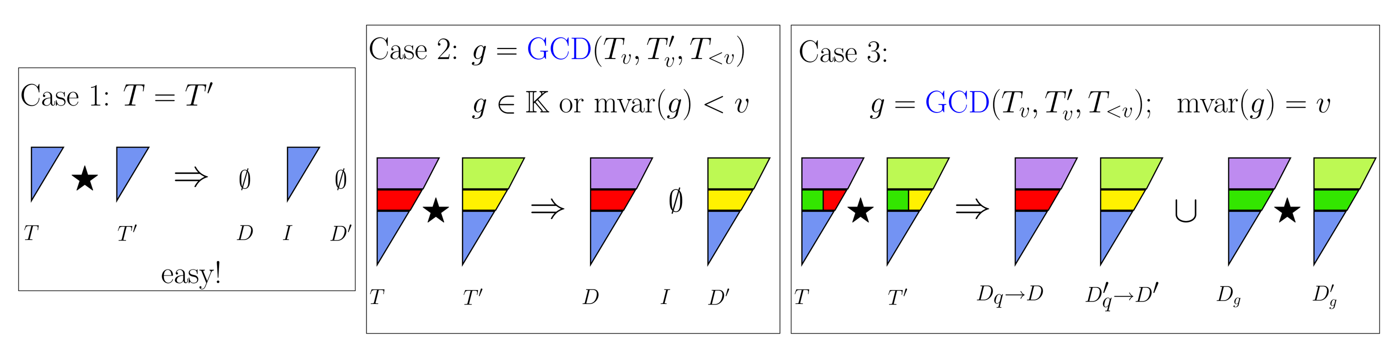
• For practical considerations, we do not rely on asymptotically fast algorithms for polynomial arithmetic (FFT-based). Instead, we assume that our polynomial multiplication and GCD computation rely on classical algorithms running in quadratic time w.r.t. the size of the input data.

• Under some realistic assumptions, we establish quadratic algorithms for the MPD and SMPD operations. These algorithms are available in the ConstructibleSetTools module in the RegularChains library in Maple 12.

The RefinedDifference Operation

• Our algorithms for MPD and SMP reduce to compute the set theoretical difference of two constructible sets. A naive approach (based on elementary logic and standard tools for polynomial systems such as Gröbner bases) is **inefficient** in practice.

• The representation of constructible sets based on regular systems has led us to an efficient algorithm which **exploits the structural properties** (triangular shape) of the input data:



$$\textsc{RefinedDifference}\ (T, T') \to (\underbrace{T \setminus T'}_{D}, \underbrace{T \bigcap T'}_{I}, \underbrace{T' \setminus T}_{D'})$$

Complexity Results

• We consider regular chains with the same set of algebraic variables. This allows us to reduce to computations in dimension zero by means of evaluation/interpolation techniques.

• In the sequel, all regular chains are assumed to be zero-dimensional and squarefree. Consequently, for every regular system $[T, h]$ we have $V(T) \cap V(h) = \emptyset$ and h can be omitted.

• We assume that the base field $\mathbb{K}$ is perfect, for instance $\mathbb{K}$ is $\mathbb{C}$.

• RefinedDifference relies essentially on GCD computations modulo regular chains, as shown by the previous picture.

Lemma 1 Let T be a regular chain of degree δ and let f_1, f_2 be univariate polynomials with respective degrees $d_1 \geq d_2$ and with coefficients in the direct product of fields defined by T. There exists a constant $C > 0$ such that an extended GCD of f_1 and f_2 modulo T can be computed in $O(C^n d_1 d_2 \delta^2)$ operations in $\mathbb{K}$.

Theorem 2 Let $L = \{U_1, \ldots, U_m\}$ be a set of regular chains, with respective degrees $\delta_1, \ldots, \delta_m$. Then a pairwise disjoint representation of L can be computed in $O(C^n \sum_{1 \leq i < j \leq m} \delta_i \delta_j)$ operations in $\mathbb{K}$.

Theorem 3 Given a set $L = \{C_1, \ldots, C_m\}$ of constructible sets, each of which is given by pairwise disjoint regular chains. Let D_i be the number of points in C_i for $1 \leq i \leq m$. An intersection-free basis of L can be computed in $O(C^n \sum_{1 \leq i < j \leq m} D_i D_j)$ operations in $\mathbb{K}$.

Main References

• Our algorithms use the augment refinement method, which was introduced in the 1990's for factor refinement of integers or polynomials over a finite field (Bach, Driscoll and Shallit).

• The complexity analysis uses an inductive process similar to the one of On the complexity of the D5 principle (Dahan, Moreno Maza, Schost & Xie, 2006). This work relies on asymptotically fast algorithms where we rely here on classical ones.

• The Gröbner basis representation of a constructible set was introduced by J. O'Halloran and M. Schoelmoeller in 2002.