Change of order for regular chains in positive dimension

Xavier Dahan⋆, Xin Jin†, Marc Moreno Maza†, and Éric Schost†

⋆: LIX, École polytechnique, 91128 Palaiseau, France.
†: ORCCA, University of Western Ontario, London, Canada.

ISSAC, Genova, July 9-12th, 2006.

Motivation and examples

We describe an algorithm for changing the order of regular chains⋆ in positive dimension.

Example: invariant theory. Polynomials $P(X,Y)$ invariant under $(X,Y) \mapsto (-X,-Y)$ can be written in terms of

$$S = X^2,\ T = Y^2,\ U = XY.$$

To rewrite an invariant polynomial, it helps to obtain the expression of X and Y in term of S, T, U. This is done by changing the order in the input system

$$\left|\begin{array}{l} \mathbf{S} - X^2 \\ \mathbf{T} - Y^2 \\ \mathbf{U} - XY \end{array}\right. \quad \text{for} \quad \mathbf{S} > \mathbf{T} > \mathbf{U} > \mathbf{X} > \mathbf{Y}$$

$$\text{to} \quad \left|\begin{array}{l} S\,\mathbf{Y} - UX \\ \mathbf{X}^2 - S \\ \mathbf{U}^2 - ST \end{array}\right. \quad \text{for} \quad \mathbf{Y} > \mathbf{X} > \mathbf{U} > \mathbf{S} > \mathbf{T}.$$

This is also an example of an implicitization problem.

Main result. Let C be a regular chain, whose saturated ideal⋆ is prime.

We give a probabilistic algorithm, of complexity polynomial in the size of input (degree, complexity of evaluation) and output (number of monomials), and in the degree of the quasi-component⋆ of C.

Let d be the maximum degree in C, let n be the number of variables. If all random choices are made uniformly in a finite set Γ, the probability of failure is at most $\frac{2n(3d^n+n^2)d^{2n}}{|\Gamma|}$.

Specificities. We use a small set of well-defined subroutines.

- change of order in dimension zero;
- Newton-Hensel lifting.

Definition (regular chain, quasi-component)

Let X be n ordered variables.
Let $C = C_1, \ldots, C_s$ be in $k[X]$, with main variables $X_{\ell_1} < \cdots < X_{\ell_s}$.

- the initial h_i is the leading coefficient of C_i in X_{ℓ_i};
- the ith saturated ideal is $\mathrm{Sat}_i = \langle C_1, \ldots, C_i \rangle : (h_1 \cdots h_i)^\infty$;
- C is a regular chain if h_i is regular mod Sat_i for all i;
- the quasi-component is the zero-set of Sat_n.

Basic setup

Let V be an irreducible variety of dimension r, defined by polynomials in $k[X] = k[X_1, \ldots, X_n]$.

Free / algebraic variables. A set Y of r variables $Y_1, \ldots, Y_r$ is free if the image

$$(x_1, \ldots, x_n) \in V \mapsto (y_1, \ldots, y_r)$$

is dense. Then, the generic points of V can be described by a regular chain

$$\left|\begin{array}{l} T_s(Y, Z_1, \ldots, Z_s) \\ \vdots \\ T_1(Y, Z_1) \end{array}\right. \quad \text{with } Z = (Z_1, \ldots, Z_s) = X - Y$$

(algebraic variables)

Data structure. If Y are free variables, we represent V by

$$y = (y_1, \ldots, y_r) \in k^r, \quad \left|\begin{array}{l} T_s(y, Z_1, \ldots, Z_s) \\ \vdots \\ T_1(y, Z_1) \end{array}\right.$$

Specialize and lift paradigm: intermediate computations are done in dimension 0 and 1.

Exchange property. Let Y and Y' be sets of free variables, and let $v \in Y - Y'$. Then, there exists $w \in Y' - Y$ such that $Y - v + w$ is free.

This means that the sets of free variables form a matroid⋆, the coordinate matroid of V.

Algorithmically, given $T_1(y, Z_1), \ldots, T_s(y, Z_1, \ldots, Z_s)$, we use a subroutine called Swap:

1. change of order in T to put w as last variable; [dim. 0]
2. lift v in T; [dim. 1]
3. specialize w at a random value. [dim. 0]

Definition (matroid)

Let X be a finite set.
A matroid over X is a collection $B(M)$ of subsets of X with the same cardinality r and satisfying the exchange property:
For all Y and Y' in $B(M)$, for every $v \in Y - Y'$ there exists $w \in Y' - Y$ such that $Y - v + w$ is in $B(M)$.

Algorithm

Input.

- A regular chain T_{in}, whose saturated ideal I is prime.
- A target order $\succ$ on the variables.

Output.

- A regular chain T_{out} for the order $\succ$, with saturated ideal I.

Step 1. Determine a sequence of exchanges.

Prop. For a generic $\alpha \in V$, the coordinates matroids of (i) the variety V and (ii) the tangent space $T_\alpha V$ coincide.

Prop. The algebraic variables in T_{out} are the maximal set of algebraic variables for a suitable lexicographic order.

Then, using linear algebra in the Jacobian matrix at α, we can find by a greedy algorithm a sequence of exchanges:

$Y_0 = Y_{\mathsf{in}}$ (free variables of T_{in})
➥ $Y_1 = Y_0 - v_0 + w_0$
…
➥ $Y_N = Y_{N-1} - v_{N-1} + w_{N-1}$ (free variables of T_{out})

Step 2. Apply the exchanges to the triangular sets.

T_0 (specialization of T_{in})
➥ $T_1 = \mathsf{Swap}(T_0, v_0, w_0)$
…
➥ $T_N = \mathsf{Swap}(T_{N-1}, v_{N-1}, w_{N-1})$ (specialization of T_{out})

Step 3. Lift all free variables in T_N.

Implementation. This algorithm is implented in the `RegularChains` Maple package.

References

Regular chains Aubry, Kalkbrener, Lazard, Moreno Maza, Lemaire-Moreno Maza-Xie (`RegularChains`), …

Lifting / specialization Giusti, Heintz, Lecerf, Pardo *et al.*

Change of order Faugère-Gianni-Lazard-Mora, Collart-Kalkbrener-Mall (Gröbner walk), Boulier-Lemaire-Moreno Maza (Pardi)

Implicitization Buzé, Chardin, Cox, D'Andrea, Jouanolou, Khetan, …