Change of Ordering for Regular Chains in Positive Dimension

X. Dahan*, X. Jin†, M. Moreno Maza†, É. Schost*

† University of Western Ontario, London, Ontario, Canada.
* École polytechnique, 91128 Palaiseau, France.

{dahan,schost}@lix.polytechnique.fr
{xjin5,moreno}@csd.uwo.ca

Abstract

We discuss changing the variable ordering for a regular chain in positive dimension. This quite general question has applications going from implicitization problems to the symbolic resolution of some systems of differential algebraic equations.

We propose a modular method, reducing the problem to dimension zero and using Newton-Hensel lifting techniques. The problems raised by the choice of the specialization points, the lack of the (crucial) information of what are the free and algebraic variables for the new ordering, and the efficiency regarding the other methods are discussed. Strong hypotheses (but not unusual) for the initial regular chain are required. Change of ordering in dimension zero is taken as a subroutine.

We report on an implementation of our method realized in Maple within the `RegularChains` library.

1 Introduction

Change of variable ordering and, more generally, change of variables, is a fundamental technique in many areas of mathematics. Discovering a good change of variables for a given problem may lead to dramatic simplifications. This is a well-known fact in physics, for instance. Conversely, implementing a target change of variables may lead to difficult computational questions, inducing for instance expression swell: this is the case when replacing x by $x + 1000$ in a univariate polynomial such as $1 + x + \cdots + x^{20}$.

In this paper, we discuss this second computational challenge. We consider an input system of polynomial equations

$$P_1(X_1, \ldots, X_n) = \cdots = P_m(X_1, \ldots, X_n) = 0 \tag{1}$$

with coefficients in a field $\mathbb{K}$ and with zero set $V \subset \overline{\mathbb{K}}^n$, where $\overline{\mathbb{K}}$ is an algebraic closure of $\mathbb{K}$. We consider also an invertible change of variables $(X_1, \ldots, X_n) \longmapsto (U_1, \ldots, U_n)$ given by another set of polynomial equations

$$U_1 = F_1(X_1, \ldots, X_n), \ldots, U_n = F_n(X_1, \ldots, X_n) \tag{2}$$

with coefficients in $\mathbb{K}$. We are interested in describing the zero set V by means of the variables $(U_1, \ldots, U_n)$ instead of the variables $(X_1, \ldots, X_n)$. A quite common type of change

of variables is a change of variable ordering; in this case $(U_1, \ldots, U_n)$ is just a permutation of $(X_1, \ldots, X_n)$.

In order to propose an efficient computational solution, we shall transform our problem twice. First, we assume that the system of equations (1) has a particular shape. To be precise, see Section 2, we assume that $P_1, \ldots, P_m$ is a regular chain whose saturated ideal is prime. This assumption is matched by many practical situations, for instance those arising from implicitization problems. Moreover, without this assumption, developing a computational solution which would be more efficient than any general procedure for solving systems of equations is, as far as know, an unsolved question. Our assumption implies that the system of equations (1) has a triangular shape in the following sense. Let us order the variables $X_1 < \cdots < X_n$ and let v_j be the greatest variable occurring in P_j, for all $1 \leq j \leq m$; then we have $v_1 < \cdots < v_m$.

Second, we observe that the computation of a change of variables reduces to that of a change of variable ordering. Indeed, defining

$$P_{m+1} = U_1 - F_1(X_1, \ldots, X_n), \ldots, P_{m+n} = U_n - F_n(X_1, \ldots, X_n) \tag{3}$$

the polynomial set $P_1, \ldots, P_m, P_{m+1}, \ldots, P_{m+n}$ is a regular chain for the variable ordering $X_1 < \cdots X_n < U_1 < \cdots < U_n$; moreover its saturated ideal is prime. We shall see that one can compute a regular chain $q_1, \ldots, q_m, q_{m+1}, \ldots, q_{n+m}$ for the variable ordering $U_1 < \cdots < U_n < X_1 < \cdots X_n$. The polynomials $q_1, \ldots, q_m$ form a regular chain representing the zero set V by means of the variables $U_1, \ldots, U_n$. To summarize, the algorithms presented here have the following characteristics.

Input: a *regular chain* $C = C_1, \ldots, C_s$ in the polynomial ring $\mathbb{K}[X_1, \ldots, X_n]$ (for some ordering $\mathcal{R}$ on the variables $X_1, \ldots, X_n$) and a second ordering $\overline{\mathcal{R}}$ on $X_1, \ldots, X_n$.

Output: a regular chain $\overline{C} = \overline{C}_1, \ldots, \overline{C}_s$ for the second ordering $\overline{\mathcal{R}}$, such that C and $\overline{C}$ have the same *saturated ideal*.

Conditions: the saturated ideal of C is a prime.

Example 1 *In this paper, we shall use the following driving example from invariant theory. Consider the set of polynomials P in $\mathbb{Q}[X_1, X_2]$ such that $P(X_1, X_2) = P(-X_1, -X_2)$. Classical invariant theory tells us that any such polynomial P can be written as a polynomial in X_1^2, X_2^2 and X_1X_2; natural questions to ask are whether such a representation is unique, and how to perform the rewriting. To solve these problems, we are led to introduce the system of polynomial equations*

$$\left| \begin{array}{lcl} \pi_1 & = & X_1^2 \\ \pi_2 & = & X_2^2 \\ \sigma & = & X_1X_2 \end{array} \right. \quad or \quad \left| \begin{array}{lcl} \pi_1 - X_1^2 & = & 0 \\ \pi_2 - X_2^2 & = & 0 \\ \sigma - X_1X_2 & = & 0 \end{array} \right. ,$$

the new variables' names coming from the fact that π_1, π_2 and σ are respectively called Primary and Secondary invariants in the invariant literature.

This input describes π_1, π_2 and σ in terms of X_1, X_2. To answer the questions above, we wish to reverse the dependencies, so as to rewrite X_1 and X_2 in terms of π_1, π_2, σ. This is done by applying an algorithm for change of variable ordering, yielding

$$\left|\begin{array}{lcl} \pi_1 X_2 - \sigma X_1 &=& 0 \\ X_1^2 - \pi_1 &=& 0 \\ \sigma^2 - \pi_1\pi_2 &=& 0 \end{array}\right. \quad or \quad \left|\begin{array}{lcl} X_2 &=& \frac{\sigma}{\pi_1} X_1 \\ X_1^2 &=& \pi_1 \\ \sigma^2 &=& \pi_1\pi_2 \end{array}\right. .$$

In this form, we observe the relation $\sigma^2 = \pi_1\pi_2$ between our basic invariants, which establishes that the representation cannot be unique. Furthermore, the new form of the system can be used as a set of rewriting rules, so as to obtain a canonical form for any invariant polynomial.

Many solutions exist to treat our problems, including Gröbner bases [4, 8] and resultant/GCD computations [2]. The complexity of these methods is hard to control, as the following situation shows: suppose that the sets of free variables are the same for the input and output orders, and that the algebraic variables have to be permuted. Then, the problem can be handled by zero-dimensional change-of-ordering over a rational function field; it seems however difficult to control the degrees of the expressions met in the indeterminate steps. One specificity of our approach consists in the use of modular methods, so as to keep under control the size of all expressions met during the computations.

2 Problem statement and main ideas of our approach

Define $X = \{X_1, \ldots, X_n\}$ and let $\mathcal{R}$ be a total ordering on X. Every non-constant polynomial $P \in \mathbb{K}[X]$ is viewed as a univariate one w.r.t. its greatest variable; then, the *initial* of P is its leading coefficient. Let $C = C_1, \ldots, C_s$ be non-constant polynomials in $\mathbb{K}[X]$ with respective (pairwise distinct) main variables $v_1 < \cdots < v_s$. We recall below the notion of a *saturated ideal* and a *regular chain* and refer the reader to [9, 1, 3] for more detail.

- For all $1 \leq i \leq s$ the *saturated ideal* of $C_1, \ldots, C_i$ is the ideal $\langle C_1, \ldots, C_i\rangle : (h_1 \cdots h_i)^\infty$ where h_i is the initial of C_i .
- The set C is a *regular chain* if for all $2 \leq i \leq s$ the initial h_i is regular modulo the *saturated ideal* of $C_1, \ldots, C_{i-1}$.

Let $\mathcal{P} \subset \mathbb{K}[X]$ be a prime ideal of dimension d and let C be a regular chain for $\mathcal{R}$ with $\mathcal{P}$ as saturated ideal. (Note that C has $n - d$ elements.) Given a new variable ordering $\overline{\mathcal{R}}$, we aim at computing from C a regular chain $\overline{C}$ for $\overline{\mathcal{R}}$ with $\mathcal{P}$ as saturated ideal.

Example 2 *The following* implicitization problem *provides a second example. Consider $\mathcal{R} = x > y > z > s > t$ and $\overline{\mathcal{R}} = t > s > z > y > x$. The polynomial system below*

$$\left|\begin{array}{l} x - t^3 \\ y - s^2 - 1 \\ z - s\,t \end{array}\right.$$

is a regular chain C for $\mathcal{R}$; let $\mathcal{P}$ be its saturated ideal, which is simply in this example the ideal generated by C; then, $\mathcal{P}$ is prime. For the ordering $\overline{\mathcal{R}}$

$$\left|\begin{array}{l} s\,t - z \\ (x\,y + x)s - z^3 \\ z^6 - x^2y^3 - 3x^2y^2 - 3x^2y - x^2 \end{array}\right.$$

is a regular chain $\overline{C}$ with $\mathcal{P}$ as saturated ideal. One can view C as the parametric equations of an irreducible variety V. The last equation in $\overline{C}$ is its implicit equation. Hence, changes of variable ordering are a tool for solving implicitization problems [5].

The key point of our approach is to reduce to the dimension zero case, that is when $s = n$, isolating this particular case as the central one. In order to achieve this reduction, we transform the input regular chain by a sequence of elementary changes of variable orders in dimension zero. We use matroid theory to compute this sequence of intermediate variable orders, as described in Section 3. We rely on several known techniques, notably lifting techniques and rational reconstruction [12]. In Section 4 we present our algorithm and show how all these tools interact together. We have implemented this algorithm within the `RegularChains` library in MAPLE [10], as illustrated in Section 5.

3 A tool from combinatorics: matroid theory

Matroid theory [13] plays a central role in our approach. We review in this section the notion of a *matroid* and we define that of the *coordinate matroid of an irreducible variety*. The proofs our statements are not reported here and rely on results appearing in [1, 3, 5, 9, 13].

Definition 1 *A* matroid *M over a finite set X is given by a non-empty family $B(M)$ of subsets of X with the same cardinality r and satisfying the* exchange property*: for all $e, f \in B(M)$, for every $v \in e - f$ there exists $w \in f - e$ such that $e - v + w \in B(M)$ holds.*

The elements of $B(M)$ are called the bases of M and r is its rank. The family of the $X - e$, for all $e \in B$, is the set of the bases of a matroid M^*, the dual matroid *of M.*

Example 3 *Consider a $m \times n$ matrix A over a field $\mathbb{K}$. Let X be the set of the columns of A and let $B(A)$ be the set all $e \subseteq X$ such that the columns of e are linearly independent and e is maximal w.r.t. inclusion. Then, the elements of $B(A)$ are the bases of a matroid over X. Matroids arising from this construction are called* linear *over $\mathbb{K}$.*

Let $V \subset \overline{\mathbb{K}}^n$ be an irreducible algebraic variety defined over a field $\mathbb{K}$. Let X be a set of n variables. let $\mathcal{P}$ be the prime ideal of $\mathbb{K}[X]$ consisting of the polynomials that vanish at every point of V. Let d be the dimension of V with $0 < d < n$ and define $s = n - d$.

Definition 2 *Let $B(X)$ be the family of the subsets $Y \subseteq X$ such that $\mathcal{P} \cap \mathbb{K}[Y]$ is the trivial ideal and Y is maximal w.r.t. inclusion. The family $B(X)$ is the collection of the bases of a rank d matroid on X, denoted by $\mathcal{M}_{\text{coord}}(V)$ and that we call the* coordinate matroid of V.

Theorem 1 *Let Y be a subset of X with cardinal d. Then, the set Y is a basis of $\mathcal{M}_{\text{coord}}(V)$ if and only if there exists a regular chain $C = C_1, \ldots, C_s$ with $\mathcal{P}$ as saturated ideal in $\mathbb{K}[X]$ and $X - Y$ as set of algebraic variables.*

We consider the variable order $\overline{\mathcal{R}} = X_1 < \cdots < X_n$. Let $\overline{C} = \overline{C}_1, \ldots, \overline{C}_s$ be a regular chain for $\overline{\mathcal{R}}$ and with $\mathcal{P}$ as saturated ideal in $\mathbb{K}[X]$. Let B_1 and B_2 be two distinct bases of $\mathcal{M}^*_{\text{coord}}(V)$, the dual of $\mathcal{M}_{\text{coord}}(V)$. Then, we write $B_1 <_{\text{lex}} B_2$ if the largest element (w.r.t. $\overline{\mathcal{R}}$) of $(B_1 - B_2) \cup (B_2 - B_1)$ belongs to B_2.

Theorem 2 *The set of the algebraic variables of $\overline{C}$ is the maximum basis of $\mathcal{M}^*_{\text{coord}}(V)$ for the ordering $<_{\text{lex}}$.*

Let $\text{Jac}(C)$ be the Jacobian matrix of C, our input regular chain. Let $\mathbb{L}$ be the field extension defined by $\mathcal{P}$, that is the total ring of fractions of $\mathbb{K}[X]/\mathcal{P}$. The columns of $\text{Jac}(C)$ are indexed by the variables of X.

Theorem 3 *The linear matroid over X defined by $\text{Jac}(C)$, regarded as a matrix with coefficients in $\mathbb{L}$, is equal to $\mathcal{M}^*_{\text{coord}}(V)$.*

Corollary 1 *Using a greedy algorithm, taking $\text{Jac}(C)$ as input, one can compute the maximum basis of $\mathcal{M}^*_{\text{coord}}(V)$ for the ordering $<_{\text{lex}}$.*

The algorithm underlying the previous corollary involves linear algebra over the function field $\mathbb{L}$. In practice, we specialize the non-algebraic variables of C before applying this algorithm, so as to reduce to linear algebra over finite extensions of $\mathbb{K}$.

4 Main result and algorithm

Assume that $\mathbb{K}$ is a **perfect field** and let $C = C_1, \ldots, C_s$ be a regular chain in $\mathbb{K}[X_1, \ldots, X_n]$ for some ordering $\mathcal{R}$ on the variables $X_1, \ldots, X_n$. Let d be such that $\deg C_i \leq d$ holds for all i. Suppose that the saturated ideal of $C_1, \ldots, C_s$ is prime and that the characteristic of $\mathbb{K}$ is greater than d^n. Let finally $\overline{\mathcal{R}} = X_1 < \cdots < X_n$ be a second ordering on the variables.

Theorem 4 *A regular chain $\overline{C}$ for $\overline{\mathcal{R}}$, such that C and $\overline{C}$ have the same saturated ideal, can be computed by a probabilistic algorithm of complexity polynomial in the input size, output size, and degree of the underlying variety. Suppose that non-algebraic variables of C at a random point y in a box Γ^{n-s}. Then the probability of failure is at most*

$$\frac{2n(3d^n + n^2)d^{2n}}{|\Gamma|}.$$

We give a sketch of the algorithm

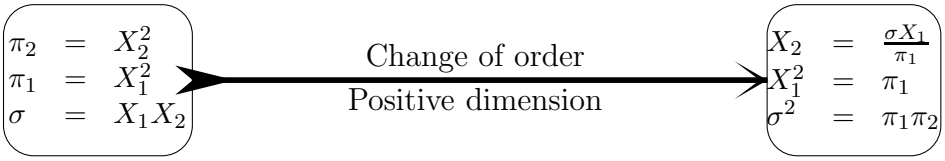
1. Specialize the non-algebraic variables of C at a random point y.
2. Compute $\text{Jac}(C)$ and specialize it at y.
3. Compute the elements $v_1, \ldots, v_p, w_1, \ldots, w_p \in X$ such that $B_{i+1} = B_i + v_i - w_i$ defines a sequence of bases of $\mathcal{M}_{\text{coord}}(V)$, with $v_i \notin B_i$ and $w_i \in B_i$, starting at B_0 the set of non-algebraic variables of C and ending at B_ℓ, the set of non-algebraic variables of $\overline{C}$.
4. For $i = 1, \ldots, \ell$ repeat:
   (a) in dimension zero, change the regular chain from the variable ordering given by B_i to the variable ordering given by B_i by putting w_i as least variable,

(b) lift v_i,

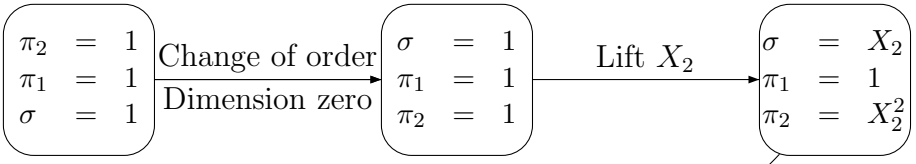
(c) specialize w_i.

5. Lift all the non-algebraic variables that are still specialized.

We illustrate the algorithm with our driving example introduced in Section 1.



Step 1.



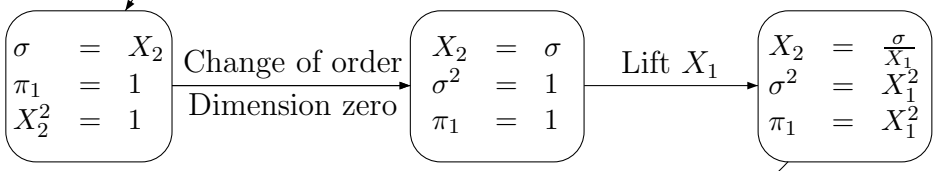
variables π_2, π_1, σ with $X_1 \leftarrow 1, X_2 \leftarrow 1$

variables σ, π_1, π_2 with $X_1 \leftarrow 1, X_2 \leftarrow 1$

variables $\sigma, \pi_1, \pi_2, X_2$ with $X_1 \leftarrow 1$

Specialization $\pi_2 \leftarrow 1$

Step 2.



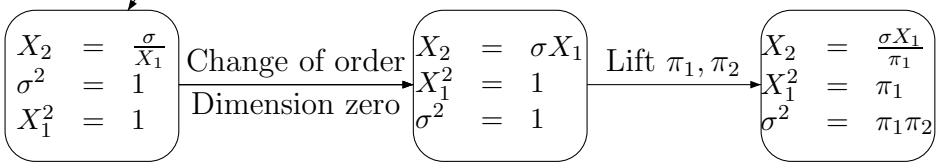
variables σ, π_1, X_2 with $X_1 \leftarrow 1, \pi_2 \leftarrow 1$

variables X_2, σ, π_1 with $X_1 \leftarrow 1, \pi_2 \leftarrow 1$

variables X_2, σ, π_1, X_1 with $\pi_2 \leftarrow 1$

Specialization $\pi_1 \leftarrow 1$

Step 3.



variables X_2, σ, X_1 with $\pi_1 \leftarrow 1, \pi_2 \leftarrow 1$

variables X_2, X_1, σ with $\pi_1 \leftarrow 1, \pi_2 \leftarrow 1$

variables $X_2, X_1, \sigma, \pi_1, \pi_2$

5 Change of ordering with `RegularChains` in MAPLE

Now, we solve our driving example with the MAPLE implementation of our algorithm, based on the `RegularChains` library. The changes of variable ordering in dimension zero are performed by the `Triangularize` command which implements the TRIADE algorithm of [11] and which is not a procedure specialized for this purpose. This is, therefore, a place for improvement in our current implementation.

```
> R := PolynomialRing([P1,P2,S,X2,X1]);
                              R := polynomial_ring

> F := [P1-X1^2, P2-X2^2, S-X1*X2];
                                    2         2
                      F := [P1 - X1 , P2 - X2 , S - X1 X2]

> rc := Chain(ListTools[Reverse](F),Empty(R),R);
                               rc := regular_chain

> R2 := PolynomialRing([X1,X2,S,P2,P1]);
                              R2 := polynomial_ring

> rc2 :=ChangeOfOrdering(rc, R, R2);
                               rc2 := regular_chain

> Equations(rc2, R2);
                             S X2          2   2
                      [X1 - ----, -P2 + X2 , S  - P2 P1]
                             P2
```

Finally, we solve the implicitization problem in Example 2. We observe that the solution provided by our implementation is different and has larger coefficients than the solution reported in Example 2 and computed by the `Triangularize` command. Indeed, our current implementation computes strongly normalized regular chains. However, we plan to integrate the techniques described in [6, 7] in order to produce regular chains with smaller coefficients.

```
> R := PolynomialRing([x,y,z,s,t]);
                              R := polynomial_ring

> F := [x-t^3, y-s^2-2, z-s*t];
                                    3       2
                       F := [x - t , y - s  - 2, z - s t]

> rc := Chain(ListTools[Reverse](F),Empty(R),R);
                               rc := regular_chain
```

```
> R2 := PolynomialRing([t,s,z,y,x]);
                              R2 := polynomial_ring

> rc2 :=ChangeOfOrdering(rc, R, R2);
                               rc2 := regular_chain

> Equations(rc2, R2);
                                        4
                                       z
      [t - ------------------------------------------------------------,
                                                                    2
           245980980 (1/61495245 x - 1/61495245 x y + 1/245980980 y  x)

                         3
                        z
    s - ----------------------------------,
        245490 (-1/122745 x + 1/245490 x y)

      2  3      2  2       2        2    6
    -x  y  + 6 x  y  - 12 x  y + 8 x  + z ]
```

6 Conclusion

As mentioned above, there are many available solutions for performing our task of change of order. The main contribution of this article is to present an algorithm driven by straightforward geometric considerations, where most of the work is reduced to a few central problems: lifting techniques for regular chains, and change of order in dimension zero. Hence, on the practical side, as remarked in the previous section, some work is required to improve on these specific tasks.

References

[1] P. Aubry, D. Lazard and M. Moreno Maza. On the theories of triangular sets. *J. Symb. Comp.*, 28:105–124, 1999.

[2] F. Boulier, F. Lemaire and M. Moreno Maza. PARDI !. In *ISSAC'01*, pages 38–47, ACM Press, 2001.

[3] F. Boulier, F. Lemaire and M. Moreno Maza. Well known theorems on triangular systems and the D5 principle. In *Transgressive Computing 2006*, University of Granada, Spain, 2006.

[4] S. Collart, M. Kalkbrener and D. Mall. Converting bases with the Gröbner walk. *J. Symb. Comp.*, 24(3-4):465–470, 1997.

[5] D. Cox, J. Little and D. O'Shea. *Ideals, varieties, and algorithms*. Springer-Verlag, 2nd ed., 1997.

[6] X. Dahan and É. Schost. Sharp estimates for triangular sets. In *ISSAC'04*, pages 103–110, ACM Press, 2004.

[7] X. Dahan, M. Moreno Maza, É. Schost, W. Wu and Y. Xie. Lifting techniques for triangular decompositions. In *ISSAC'05*, pages 108–115, ACM Press, 2005.

[8] J.-C. Faugère, P. Gianni, D. Lazard and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *J. Symb. Comp.*, 16(4):329–344, 1993

[9] M. Kalkbrener. A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. *J. Symb. Comp.*, 15:143–167, 1993.

[10] F. Lemaire, M. Moreno Maza and Y. Xie. The `RegularChains` library. In *Maple Conference 2005*, pages 355–368, I. Kotsireas Ed., 2005.

[11] M. Moreno Maza. On triangular decompositions of algebraic varieties. MEGA-2000 Conference, Bath, 2000.

[12] É. Schost. Degree bounds and lifting techniques for triangular sets. In *ISSAC'02*, pages 238–245, ACM Press, 2002.

[13] D. J. A. Welsh. *Matroid theory*. Academic Press, 1976, London.