Change of order for regular chains in positive dimension

X. Dahan[⋆], X. Jin[†], M. Moreno Maza[†], É. Schost[†]

[⋆] LIX, École polytechnique (France),
[†] ORCCA University of Western Ontario (Canada)

AGGM'06, Barcelona, Spain.

September, 6, 2006.

Overview

- **Goal:** changing lexicographic orders of polynomial systems.
- **Which systems:** regular chains in positive dimension.
- **Toy example:**

$$\left| \begin{array}{l} x - \frac{1-t^2}{1+t^2} \\ y - \frac{2t}{1+t^2} \end{array} \right. \quad \to \quad \left| \begin{array}{c} t + \frac{x}{y} - \frac{1}{y} \\ x^2 + y^2 - 1 \end{array} \right.$$

  Many other similar implicitization examples.
- **How:** by a modular algorithm, reducing to perform most operations in dimension 0.
- **Tools:** a few basic routines (linear algebra, Newton-Hensel lifting).

A driving example from invariant theory

Polynomials $P(X_1, X_2)$ invariant under $(X_1, X_2) \mapsto (-X_1, -X_2)$, can be rewritten in terms of:

$$P_1 = X_1^2\ , \quad P_2 = X_2^2\ , \quad S = X_1 X_2.$$

To rewrite an invariant polynomial, obtaining the expressions of X_1 and X_2 in terms of P_1, P_2, S is relevant.

This is done by changing the order in the input system.

Initial order :		Target order :
$P_1 > P_2 > S > X_1 > X_2$		$X_2 > X_1 > S > P_1 > P_2$
$P_1 - X_1^2$		$S X_2 - P_1 X_1$
$P_2 - X_2^2$	$\xrightarrow[\text{order}]{\text{Change of}}$	${X_1}^2 - P_1$
$S - X_1 X_2$		$S^2 - P_1 P_2$

More examples: implicitization, ranking conversions

- For $\mathcal{R} = x > y > z > s > t$ and $\overline{\mathcal{R}} = t > s > z > y > x$ we have:

$$\mathsf{convert}(\begin{cases} x - t^3 \\ y - s^2 - 1 \\ z - s\,t \end{cases}, \mathcal{R}, \overline{\mathcal{R}}) \quad = \quad \begin{cases} s\,t - z \\ (x\,y + x)s - z^3 \\ z^6 - x^2y^3 - 3x^2y^2 - 3x^2y - x^2 \end{cases}$$

- For $\mathcal{R} = \cdots > v_{xx} > v_{xy} > \cdots > u_{xy} > u_{yy} > v_x > v_y > u_x > u_y > v > u$ and $\overline{\mathcal{R}} = \cdots u_x > u_y > u > \cdots > v_{xx} > v_{xy} > v_{yy} > v_x > v_y > v$ we have:

$$\mathsf{convert}(\begin{cases} v_{xx} - u_x \\ 4\,u\,v_y - (u_x\,u_y + u_x\,u_y\,u) \\ u_x^2 - 4\,u \\ u_y^2 - 2\,u \end{cases} \mathcal{R}, \overline{\mathcal{R}}) \quad = \quad \begin{cases} u - v_{yy}^2 \\ v_{xx} - 2\,v_{yy} \\ v_y\,v_{xy} - v_{yy}^3 + v_{yy} \\ v_{yy}^4 - 2\,v_{yy}^2 - 2\,v_y^2 + 1 \end{cases}$$

Previous work

Arbitrary dimension.

Collart - Kalkbrener - Mall: Gröbner walk (1997).

Boulier - Lemaire - Moreno Maza: PARDI ! (2001).

Dimension zero.

Faugère - Gianni - Lazard - Mora (1993).

Díaz Toca - González Vega (2001).

Pascal - Schost (2006).

Implicitization.

Cox, Curves, surfaces and syzygies (2003).

Busé - Chardin, homological methods (2005).

D'Andrea - Khetan, resultant formalism.

Regular chains (1/2)

Consider ordered variables $\mathbf{X} = X_1 > \cdots > X_n$.

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

For $i \leq s$, the initial h_i is the leading coefficient of C_i in X_{ℓ_i}.

The saturated ideal is $\mathrm{Sat}_i(\mathbf{C}) = (C_1, \ldots, C_i) : (h_1 \ldots h_i)^\infty$.

$\mathbf{C}$ is a regular chain if h_i is regular mod $\mathrm{Sat}_i(\mathbf{C})$ for all i.

The quasi-component $W(\mathbf{C}) := V(\mathbf{C}) \setminus V(h_1 \cdots h_{\ell_s})$ satisfies $\overline{W(\mathbf{C})} = V(\mathrm{Sat}_n(\mathbf{C}))$.

The algebraic variables are those which appear as main variables. The other ones ar
free.

Example

$$\left| \begin{array}{l} C_2 = (X_1 + X_2){X_3}^2 + X_3 + 1 \\ C_1 = {X_1}^2 + 1. \end{array} \right. , \text{ with } \left| \begin{array}{l} \mathsf{mvar}(C_2) = X_3 \\ \mathsf{mvar}(C_1) = X_1 \end{array} \right. .$$

Regular chains (1/2)

Consider ordered variables $\mathbf{X} = X_1 > \cdots > X_n$.

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

For $i \leq s$, the initial h_i is the leading coefficient of C_i in X_{ℓ_i}.

The saturated ideal is $\mathrm{Sat}_i(\mathbf{C}) = (C_1, \ldots, C_i) : (h_1 \ldots h_i)^\infty$.

$\mathbf{C}$ is a regular chain if h_i is regular mod $\mathrm{Sat}_i(\mathbf{C})$ for all i.

The quasi-component $W(\mathbf{C}) := V(\mathbf{C}) \setminus V(h_1 \cdots h_{\ell_s})$ satisfies $\overline{W(\mathbf{C})} = V(\mathrm{Sat}_n(\mathbf{C}))$.

The algebraic variables are those which appear as main variables. The other ones ar free.

Example

$$\left| \begin{array}{l} C_2 = (X_1 + X_2) X_3^2 + X_3 + 1 \\ C_1 = X_1^2 + 1. \end{array} \right. , \quad \text{with } \mathsf{init}(C_2) = h_2 = X_1 + X_2$$

Regular chains (1/2)

Consider ordered variables $\mathbf{X} = X_1 > \cdots > X_n$.

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

For $i \leq s$, the initial h_i is the leading coefficient of C_i in X_{ℓ_i}.

The saturated ideal is $\mathrm{Sat}_i(\mathbf{C}) = (C_1, \ldots, C_i) : (h_1 \ldots h_i)^\infty$.

$\mathbf{C}$ is a regular chain if h_i is regular mod $\mathrm{Sat}_i(\mathbf{C})$ for all i.

The quasi-component $W(\mathbf{C}) := V(\mathbf{C}) \setminus V(h_1 \cdots h_{\ell_s})$ satisfies $\overline{W(\mathbf{C})} = V(\mathrm{Sat}_n(\mathbf{C}))$.

The algebraic variables are those which appear as main variables. The other ones ar

free.

Example

$$\left| \begin{array}{l} C_2 = (X_1 + X_2)X_3^2 + X_3 + 1 \\ C_1 = X_1^2 + 1. \end{array} \right. , \qquad \begin{array}{l} \mathrm{Sat}_1(C_1, C_2) = (C_1) : h_1 = (C_1) \\ \mathrm{Sat}_2(C_1, C_2) = (C_1, C_2) : (X_1 + X_2)^\infty \end{array}$$

Regular chains (1/2)

Consider ordered variables $\mathbf{X} = X_1 > \cdots > X_n$.

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

For $i \leq s$, the initial h_i is the leading coefficient of C_i in X_{ℓ_i}.

The saturated ideal is $\mathrm{Sat}_i(\mathbf{C}) = (C_1, \ldots, C_i) : (h_1 \ldots h_i)^\infty$.

$\mathbf{C}$ is a regular chain if h_i is regular mod $\mathrm{Sat}_i(\mathbf{C})$ for all i.

The quasi-component $W(\mathbf{C}) := V(\mathbf{C}) \setminus V(h_1 \cdots h_{\ell_s})$ satisfies $\overline{W(\mathbf{C})} = V(\mathrm{Sat}_n(\mathbf{C}))$.

The algebraic variables are those which appear as main variables. The other ones ar

free.

Example

$$\left| \begin{array}{l} C_2 = (X_1 + X_2)X_3^2 + X_3 + 1 \\ C_1 = X_1^2 + 1. \end{array} \right. , \qquad \begin{array}{l} h_2 = X_1 + X_2 \text{ is not a zero} - \text{divisor} \\ \text{ in } k[X_1, X_2]/(X_1^2 + 1). \end{array}$$

Regular chains (1/2)

Consider ordered variables $\mathbf{X} = X_1 > \cdots > X_n$.

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

For $i \leq s$, the initial h_i is the leading coefficient of C_i in X_{ℓ_i}.

The saturated ideal is $\mathrm{Sat}_i(\mathbf{C}) = (C_1, \ldots, C_i) : (h_1 \ldots h_i)^\infty$.

$\mathbf{C}$ is a regular chain if h_i is regular mod $\mathrm{Sat}_i(\mathbf{C})$ for all i.

The quasi-component $W(\mathbf{C}) := V(\mathbf{C}) \setminus V(h_1 \cdots h_{\ell_s})$ satisfies $\overline{W(\mathbf{C})} = V(\mathrm{Sat}_n(\mathbf{C}))$.

The algebraic variables are those which appear as main variables. The other ones ar free.

EXAMPLE

$$\left| \begin{array}{l} C_2 = (X_1 + X_2)X_3^2 + X_3 + 1 \\ C_1 = X_1^2 + 1. \end{array} \right. , \qquad W(\mathbf{C}) = V(\mathbf{C}) \setminus V(X_1 + X_2).$$

Regular chains (1/2)

Consider ordered variables $\mathbf{X} = X_1 > \cdots > X_n$.

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

For $i \leq s$, the initial h_i is the leading coefficient of C_i in X_{ℓ_i}.

The saturated ideal is $\mathrm{Sat}_i(\mathbf{C}) = (C_1, \ldots, C_i) : (h_1 \ldots h_i)^\infty$.

$\mathbf{C}$ is a regular chain if h_i is regular mod $\mathrm{Sat}_i(\mathbf{C})$ for all i.

The quasi-component $W(\mathbf{C}) := V(\mathbf{C}) \setminus V(h_1 \cdots h_{\ell_s})$ satisfies $\overline{W(\mathbf{C})} = V(\mathrm{Sat}_n(\mathbf{C}))$.

The algebraic variables are those which appear as main variables. The other ones are free.

EXAMPLE

$$\left| \begin{array}{l} C_2 = (X_1 + X_2)X_3^2 + X_3 + 1 \\ C_1 = X_1^2 + 1. \end{array} \right. , \qquad X_1, X_3 \text{ are algebraic}, X_2 \text{ is free.}$$

Regular chains (2/2)

The regular chains are simple data structures, well-suited to describe the generic points of varieties of positive dimension.

In positive dimension, lexicographic Gröbner bases become complicated to understand. Modular algorithms become harder to design.

References:

- Lazard. A new method for solving... (1991)
- Kalkbrener. Generalized Euclidean algorithm... (1993)
- Moreno Maza. On triangular decompositions... (2000)
- Lemaire - Moreno Maza - Xie. The `RegularChains` library. (2005)

Specialization and lift paradigm (1/2)

Technique relying on the Hensel lifting (p-adic lifting), or the Newton operator (variables lifting, like in this work).

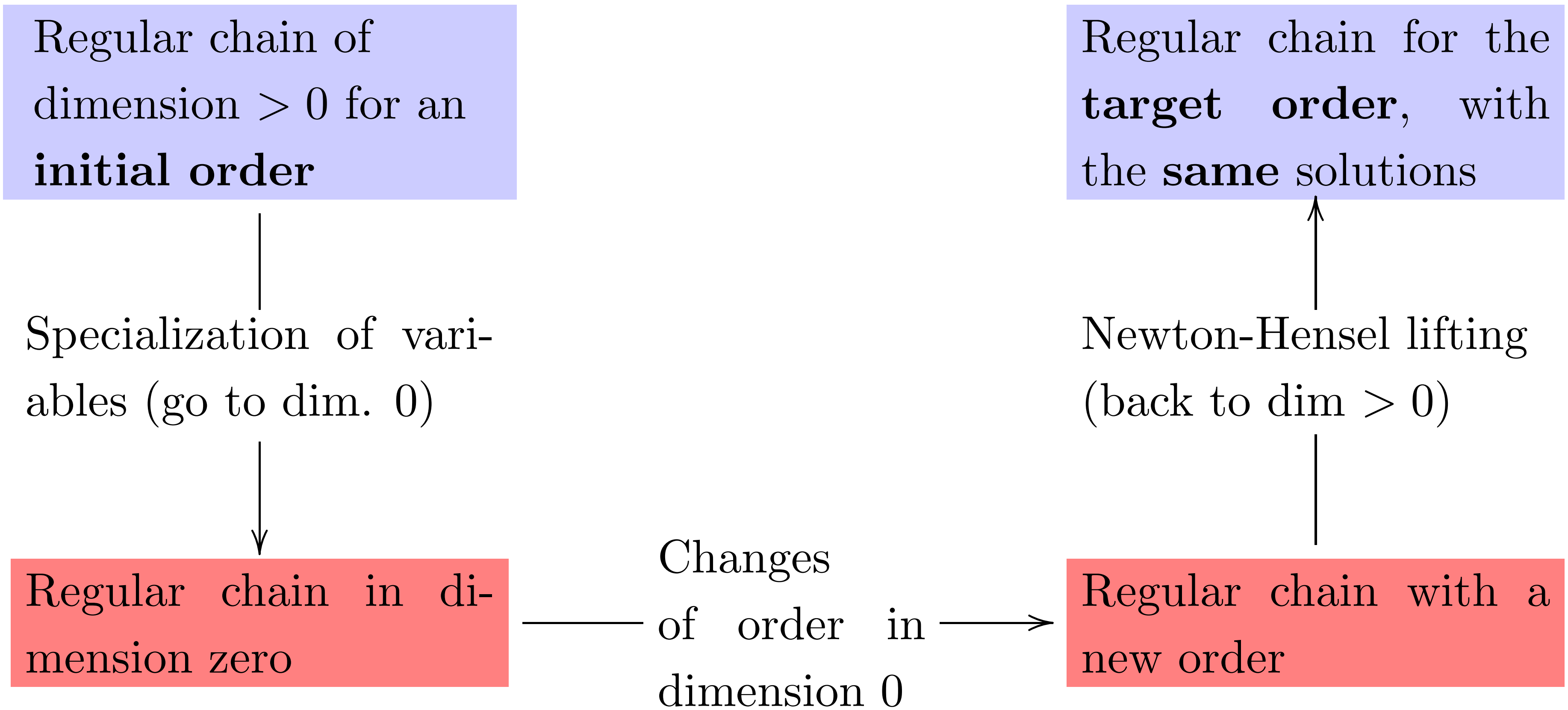
Principle:

- Specialize the free variables at a generic point † ...
- reach dimension 0 where the main computations are done (for a lower cost) ...
- and finally use Newton-Hensel techniques to recover the free variables (move up again to positive dimension).

† the non-generic point are in a closed subset of the variety. The conditions defining this closed set depend on the problem considered.

Many previous versions (for gcd, factorization, Gröbner bases, ...) Our approach follows Giusti *et al.*, Schost, and Dahan *et al.*

Specialization and lift paradigm (2/2)



Main algorithm

Main problem:	algebraic/free variables for the initial order	$\neq$	algebraic/free variables for the target order

Need to swap some free variables and algebraic ones.

To do this by staying close to dimension 0, we need to perform several times the following loop:

- change of order in dimension 0.
- lift a relevant variable v_i (go to dimension 1)
- specialize another variable w_i (back to dimension 0)

Problem: Find the sequence of couples of variables (v_i, w_i) to specialize and to lift

Solution: Linearization of the problem through the tangent space of a generic poin

The algorithm on the example

Initial order :

$$P_1 > P_2 > S > X_1 > X_2$$

$$\left| \begin{array}{c} P_1 - X_1^2 \\ P_2 - X_2^2 \\ S - X_1 X_2 \end{array} \right.$$

Algebraic variables :

$$P_1 > P_2 > S$$

$$\xrightarrow[\text{order}]{\text{Change of}}$$

Target order :

$$X_2 > X_1 > S > P_1 > P_2$$

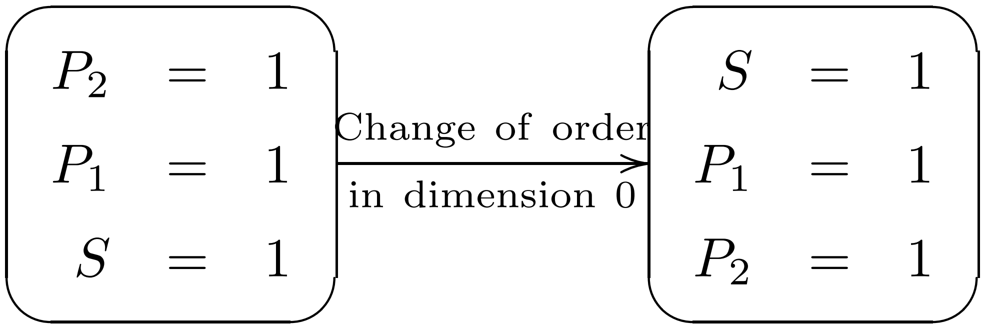
$$\left| \begin{array}{c} S X_2 - P_1 X_1 \\ {X_1}^2 - P_1 \\ S^2 - P_1 P_2 \end{array} \right.$$

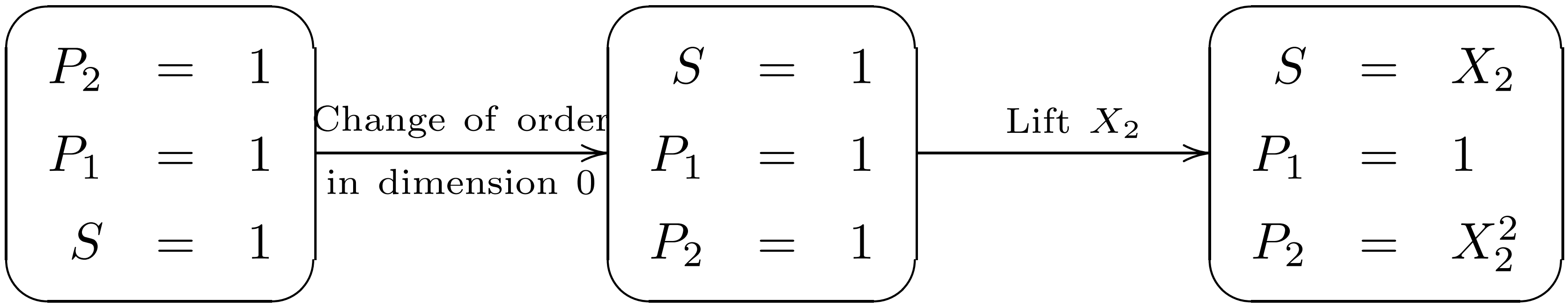
Algebraic variables :

$$X_2 > X_1 > S$$

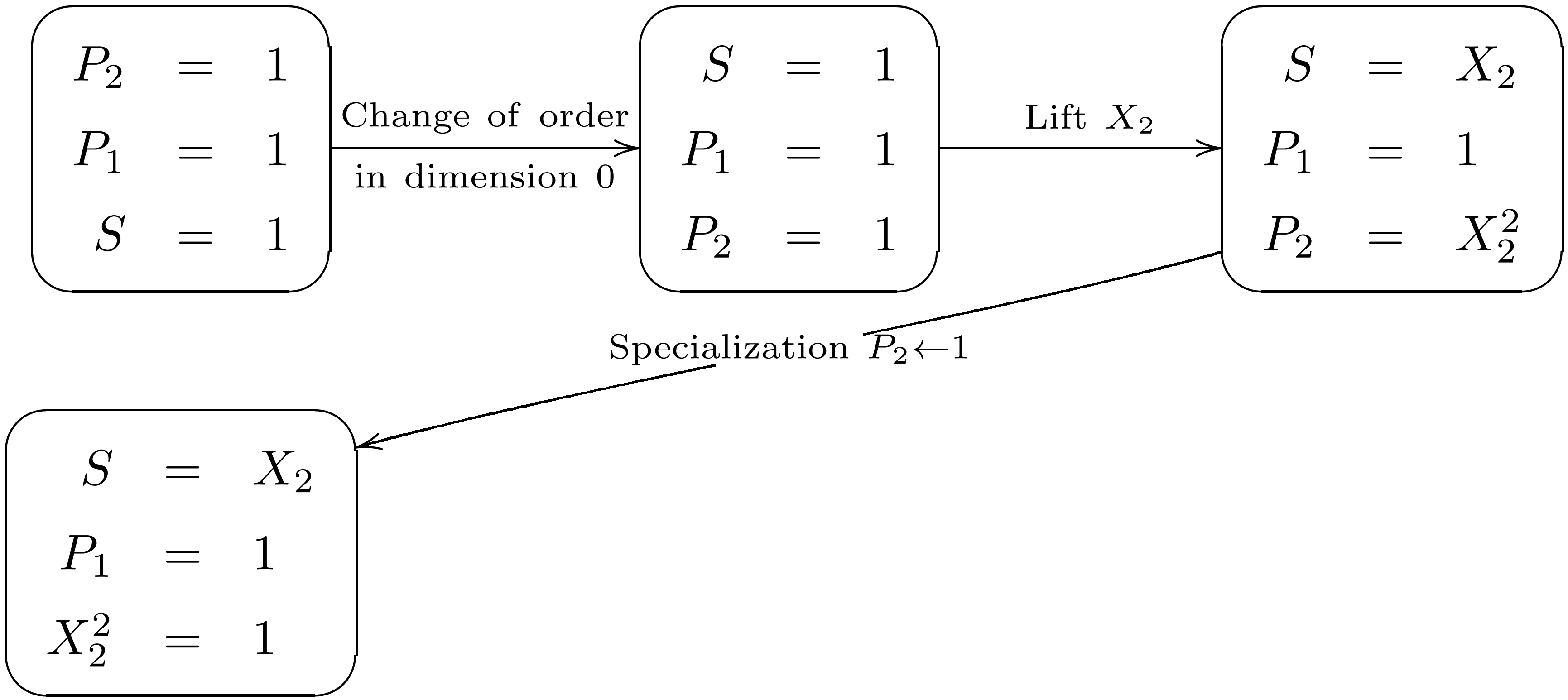
- **Step 1** (more details later): determine that we will exchange (X_2, P_2) and (X_1, P_1).
- **Step 1.5:** Specialize the free variables at $(1, 1)$.
- **Step 2:** do the work in dimension 0 and 1.
- **Step 3:** move up to dimension 2.

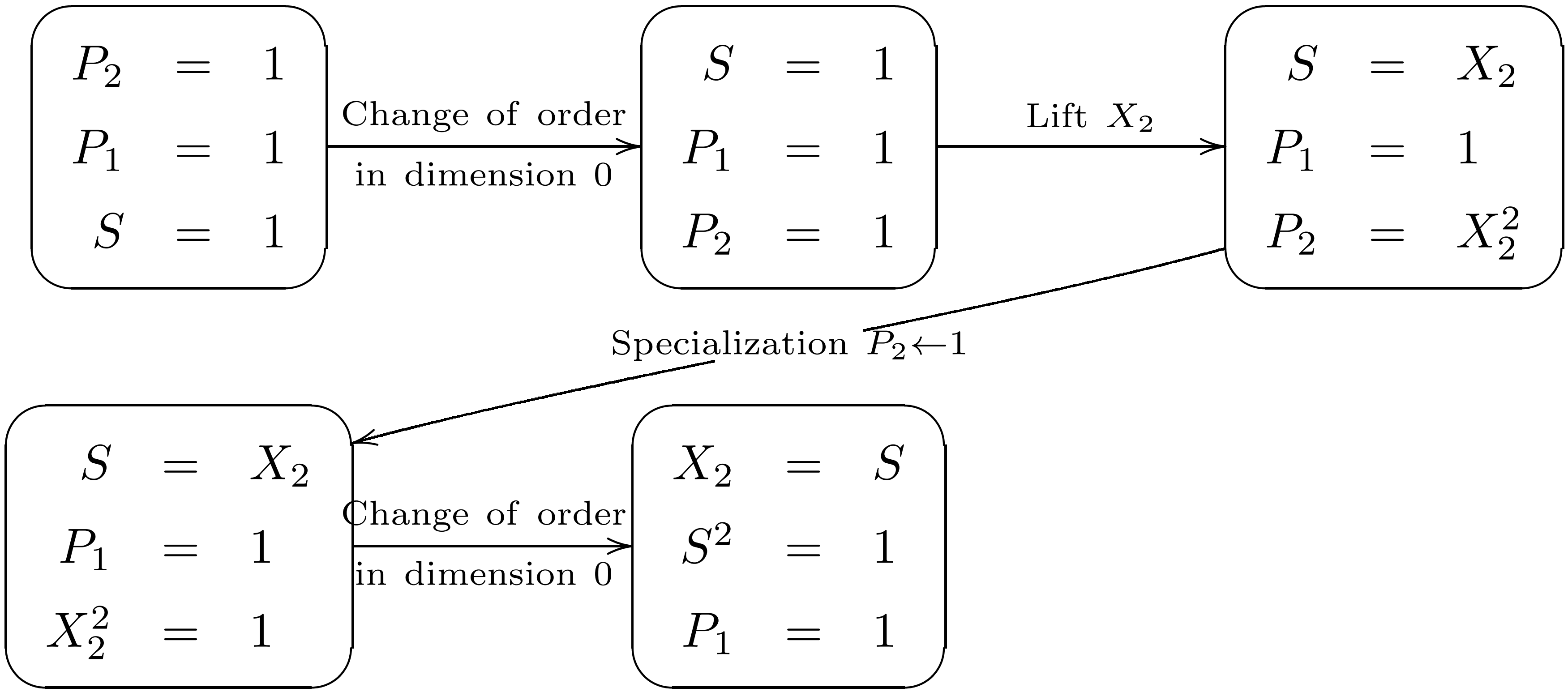
$$
\begin{aligned}
P_2 &= 1 \\
P_1 &= 1 \\
S &= 1
\end{aligned}
$$


$P_2 = 1$
$P_1 = 1$
$S = 1$
Change of order
in dimension 0
$S = 1$
$P_1 = 1$
$P_2 = 1$

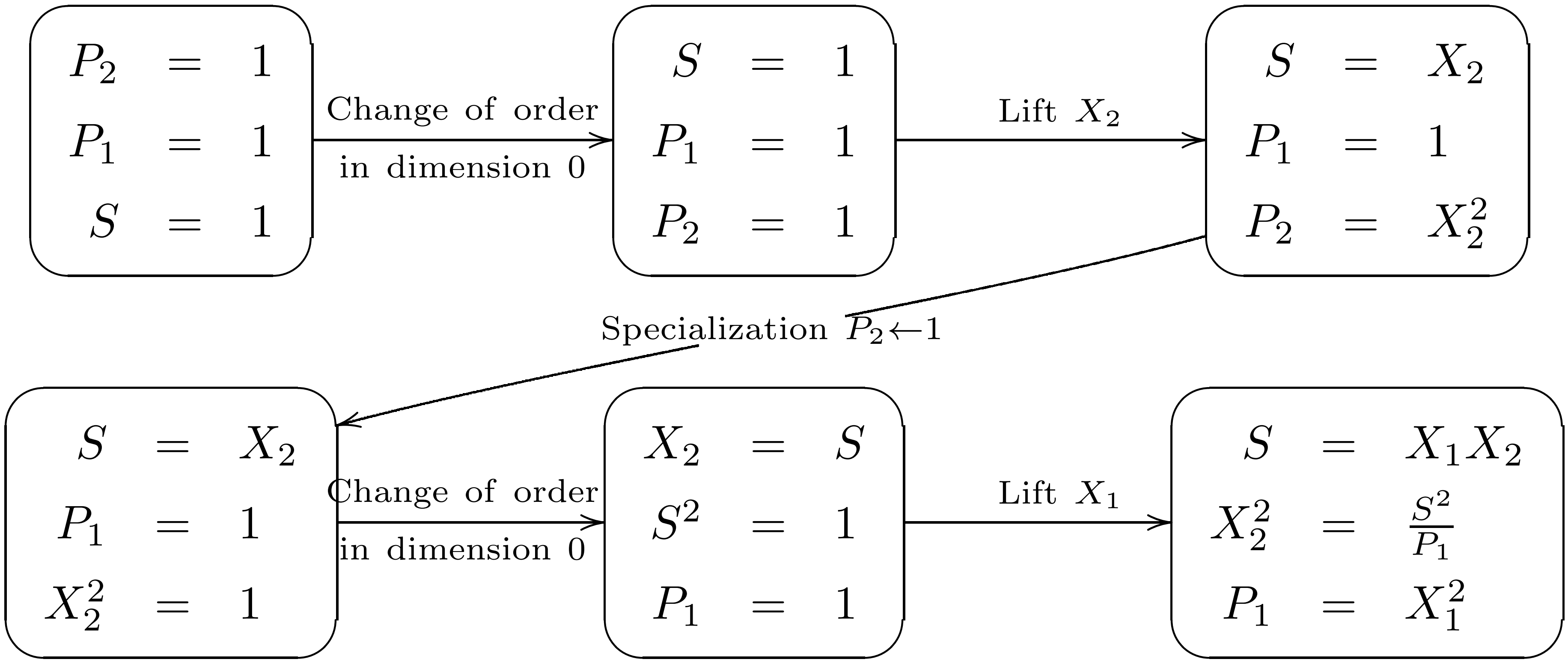


$P_2 = 1$
$P_1 = 1$
$S = 1$
Change of order
in dimension 0
$S = 1$
$P_1 = 1$
$P_2 = 1$
Lift X_2
$S = X_2$
$P_1 = 1$
$P_2 = X_2^2$

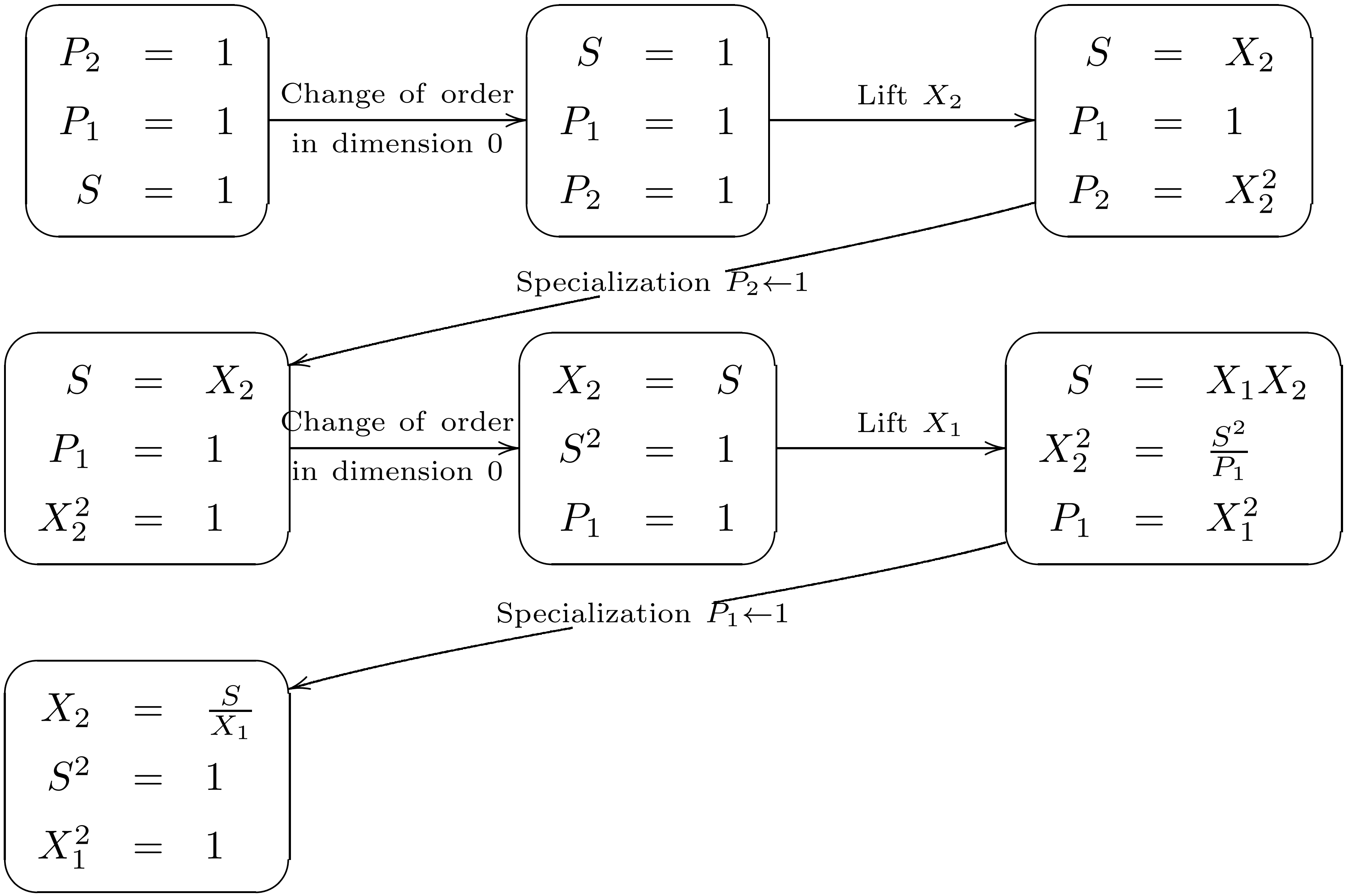

$P_2 = 1$
$P_1 = 1$
$S = 1$
Change of order
in dimension 0
$S = 1$
$P_1 = 1$
$P_2 = 1$
Lift X_2
$S = X_2$
$P_1 = 1$
$P_2 = X_2^2$
Specialization $P_2 \leftarrow 1$
$S = X_2$
$P_1 = 1$
$X_2^2 = 1$

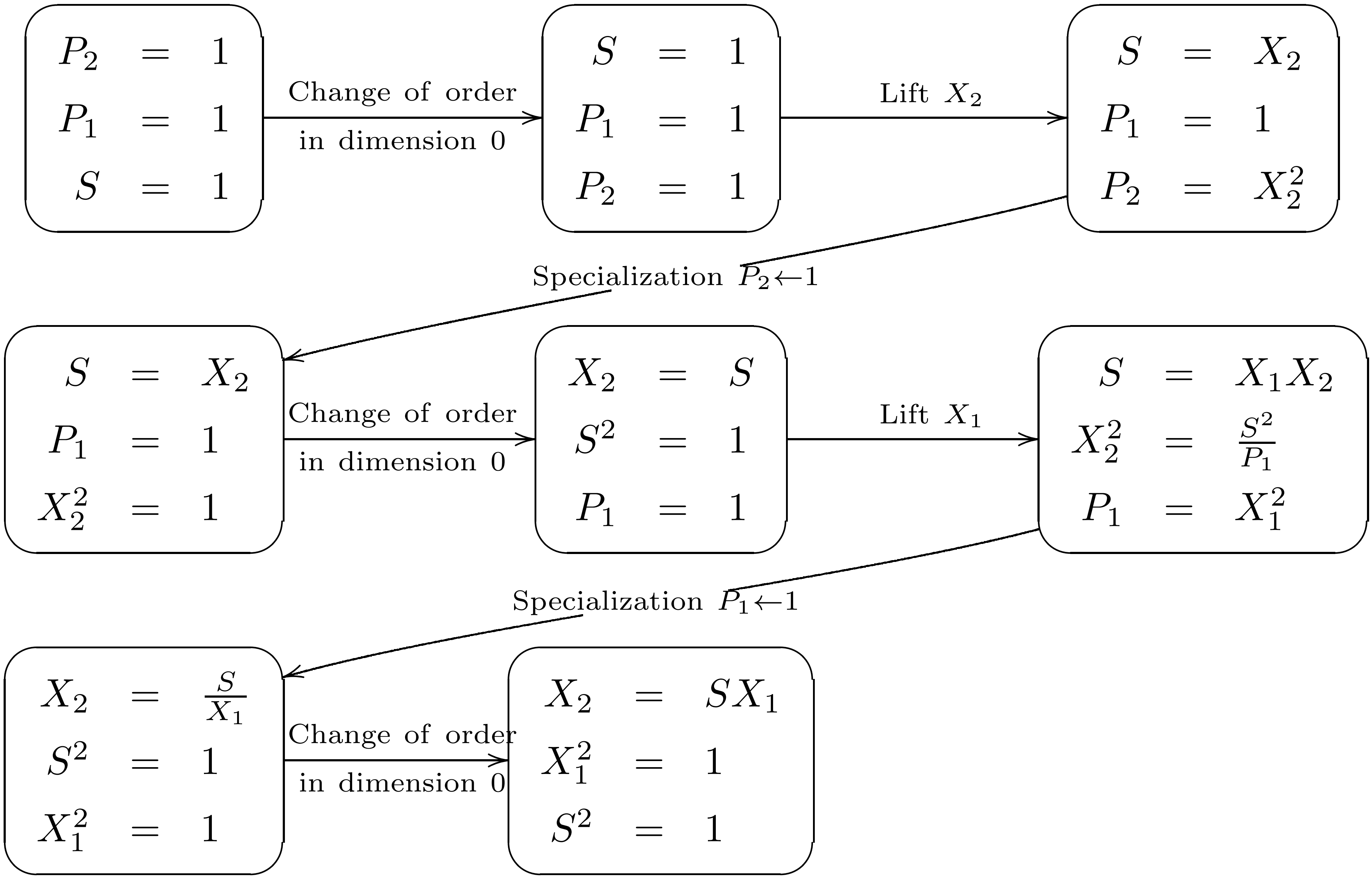


P2 = 1
P1 = 1
S = 1
Change of order
in dimension 0
S = 1
P1 = 1
P2 = 1
Lift X2
S = X2
P1 = 1
P2 = X2^2
Specialization P2←1
S = X2
P1 = 1
X2^2 = 1
Change of order
in dimension 0
X2 = S
S^2 = 1
P1 = 1

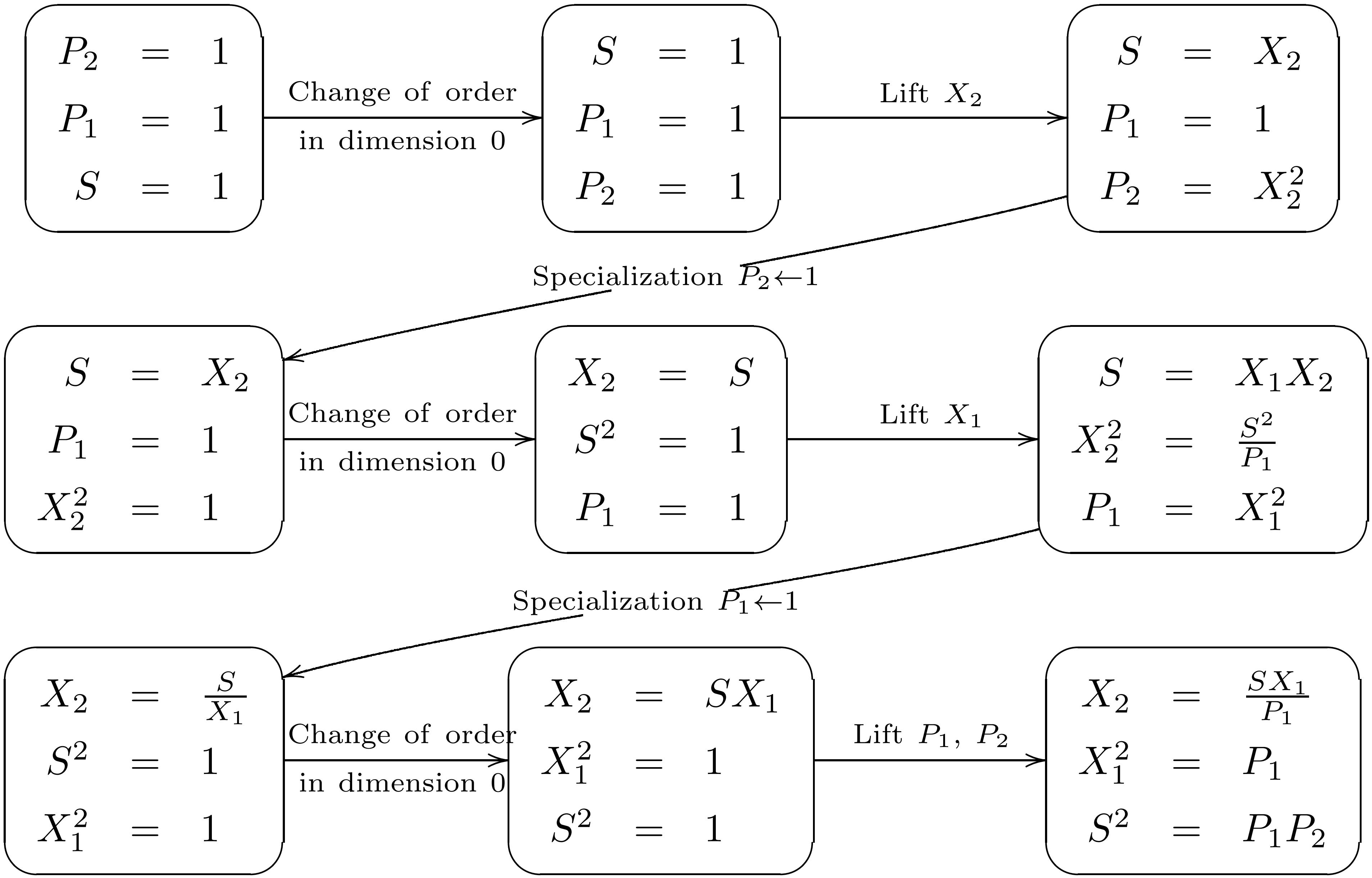


$P_2 = 1$
$P_1 = 1$
$S = 1$
Change of order
in dimension 0
$S = 1$
$P_1 = 1$
$P_2 = 1$
Lift X_2
$S = X_2$
$P_1 = 1$
$P_2 = X_2^2$
Specialization $P_2 \leftarrow 1$
$S = X_2$
$P_1 = 1$
$X_2^2 = 1$
Change of order
in dimension 0
$X_2 = S$
$S^2 = 1$
$P_1 = 1$
Lift X_1
$S = X_1 X_2$
$X_2^2 = \frac{S^2}{P_1}$
$P_1 = X_1^2$


$P_2 = 1$
$P_1 = 1$
$S = 1$
Change of order
in dimension 0
$S = 1$
$P_1 = 1$
$P_2 = 1$
Lift X_2
$S = X_2$
$P_1 = 1$
$P_2 = X_2^2$
Specialization $P_2 \leftarrow 1$
$S = X_2$
$P_1 = 1$
$X_2^2 = 1$
Change of order
in dimension 0
$X_2 = S$
$S^2 = 1$
$P_1 = 1$
Lift X_1
$S = X_1 X_2$
$X_2^2 = \frac{S^2}{P_1}$
$P_1 = X_1^2$
Specialization $P_1 \leftarrow 1$
$X_2 = \frac{S}{X_1}$
$S^2 = 1$
$X_1^2 = 1$



$P_2 = 1$
$P_1 = 1$
$S = 1$
Change of order in dimension 0
$S = 1$
$P_1 = 1$
$P_2 = 1$
Lift X_2
$S = X_2$
$P_1 = 1$
$P_2 = X_2^2$
Specialization $P_2 \leftarrow 1$
$S = X_2$
$P_1 = 1$
$X_2^2 = 1$
Change of order in dimension 0
$X_2 = S$
$S^2 = 1$
$P_1 = 1$
Lift X_1
$S = X_1 X_2$
$X_2^2 = \frac{S^2}{P_1}$
$P_1 = X_1^2$
Specialization $P_1 \leftarrow 1$
$X_2 = \frac{S}{X_1}$
$S^2 = 1$
$X_1^2 = 1$
Change of order in dimension 0
$X_2 = S X_1$
$X_1^2 = 1$
$S^2 = 1$



$P_2 = 1$, $P_1 = 1$, $S = 1$
Change of order in dimension 0
$S = 1$, $P_1 = 1$, $P_2 = 1$
Lift X_2
$S = X_2$, $P_1 = 1$, $P_2 = X_2^2$
Specialization $P_2 \leftarrow 1$
$S = X_2$, $P_1 = 1$, $X_2^2 = 1$
Change of order in dimension 0
$X_2 = S$, $S^2 = 1$, $P_1 = 1$
Lift X_1
$S = X_1 X_2$, $X_2^2 = \frac{S^2}{P_1}$, $P_1 = X_1^2$
Specialization $P_1 \leftarrow 1$
$X_2 = \frac{S}{X_1}$, $S^2 = 1$, $X_1^2 = 1$
Change of order in dimension 0
$X_2 = S X_1$, $X_1^2 = 1$, $S^2 = 1$
Lift P_1, P_2
$X_2 = \frac{S X_1}{P_1}$, $X_1^2 = P_1$, $S^2 = P_1 P_2$

Finding what variables to exchange (1/2)

Let M be the set of all possible choices for the algebraic variables

- We know one element m_{init} in M: those corresponding to the input regular chain.
- There is an m_{final} that corresponds to the output regular chain.
- We want to find a sequence

$$m_{\text{init}} = m_0 \to m_1 \to \cdots \to m_N = m_{\text{final}}$$

where m_i and m_{i+1} differ only by one entry.

Finding what variables to exchange (2/2)

Let $\mathbf{C} = C_1, \ldots, C_s$ be the input regular chain.

Prop. A set of s variables is in M if and only if the corresponding submatrix of the Jacobian of C has full rank.

Prop. The set m_{final} is the maximal element in M for a lexicographic order induced by the target order on the variables.

Prop. The set m_{final} can be computed by a greedy algorithm which relies only on testing appartenance to M.

Technically, all these propositions require that $\mathbf{C}$ defines a prime saturated ideal. A proofs then use the fact that M defines a matroid.

In dimension 0

Easier problem, which mainly reduces to suitable linear algebra operations.

0. Gröbner basis computation

- Bucherberger
- Faugère

1. Change of order for Gröbner bases

- FGLM
- Gröbner Walk

2. Specialized algorithms

- Pardi
- Díaz Toca / González Vega - Pascal / Schost

Work involved

Step 1. Determining the variables to exchange.

- Linear algebra modulo a zero-dimensional regular chain.

Step 2. Work in dimension 0 / 1

- Newton-Hensel lifting:
  - operations modulo a regular chain ...
  - ... with power series coefficients and
  - univariate rational function reconstruction

Step 3. Lifting all free variables.

- Newton-Hensel lifting with multivariate power series coefficients.
- Rational reconstruction of multivariate functions.

Complexity results

Let **C** be a regular chain whose saturated ideal is **prime**.

Theorem 1. There exists a probabilistic algorithm, of complexity polynomial in the following quantities:

- the number of variables n
- complexity of evaluation of the inputs
- degree of the quasi-component $W(\mathbf{C})$
- o number of monomials with n variables in the degree of the output

Theorem 2. Let d the maximum degree of the input, n the number of variables, if all the random values are made uniformly in a finite set Γ, then the probability of failure is at most:

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

Conclusion and future work

A simple modular algorithm for changing of order in positive dimension.

Complexity study, estimation of probability of success.

Implementation submitted for Maple 11 integration.

Todo:

- remove the primality assumption;
- improve the code
  - Newton-Hensel lifting in several variables
  - rational reconstruction in several variables
  - use alternative normalization for the output to decrease the coefficient size