Publication LIFL 2001–09 LIFL 2001–09

Well known theorems on triangular systems

François Boulier, François Lemaire and Marc Moreno Maza

novembre 2001

LABORATOIRE D'INFORMATIQUE FONDAMENTALE DE LILLE
UPRES–A 8022
UNIVERSITÉ DES SCIENCES ET TECHNOLOGIES DE LILLE
U.F.R. I.E.E.A. Bât. M3 – 59655 VILLENEUVE D'ASCQ CEDEX
Tél. (+33) 3 20 43 47 24 – Télécopie (+33) 3 20 43 65 66 – E-mail
direction@lifl.fr

Well known theorems on triangular systems

François Boulier, François Lemaire and Marc Moreno Maza

novembre 2001

The two theorems given in the first section are not new but their proofs are. The theorems given in the second section are all more or less known and not difficult.

1 Triangular systems

1.1 The unmixedness theorem

Consider a triangular system C of the ring $R = k[t_1, \ldots, t_m, x_1, \ldots, x_n]$ where $x_1 < \cdots < x_n$ denote the leaders of the elements of C and $t_1, \ldots, t_m$ the other indeterminates. In the sequel, h denotes either the product of the initials *or* the product of the separants of the elements of C. Denote $\mathfrak{A} = (C) : h^\infty$. This subsection is entirely dedicated to the proof of the following theorem.

Theorem 1 *If $\mathfrak{p}$ is an associated prime of $\mathfrak{A}$ then we have $\dim \mathfrak{p} = m$ and $\mathfrak{p} \cap k[t_1, \ldots, t_m] = (0)$. In particular, non zero elements of $k[t_1, \ldots, t_m]$ are non zero divisors in $R/\mathfrak{A}$.*

Introduce a new indeterminate x_{n+1}, the polynomial $f = h\, x_{n+1} - 1$, the ring $R' = R[x_{n+1}]$, the triangular subset $C' = C \cup \{f\}$ of R' and the ideal $\mathfrak{A}' = (C')$.

Proposition 1 *If $\mathfrak{p}'$ is an associated prime of $\mathfrak{A}'$ then we have $\dim \mathfrak{p}' = m$ and $\mathfrak{p}' \cap k[t_1, \ldots, t_m] = (0)$.*

Proof By lemma 1, the ideal $\mathfrak{U}'$ has dimension m. It is generated by $n+1$ elements in a polynomial ring in $m+n+1$ indeterminates over a field. By Macaulay's theorem [10, vol. 2, chap. VII, theorem 26], every associated prime of $\mathfrak{U}'$ has dimension m. By lemma 1 again, $\mathfrak{p}' \cap k[t_1, \ldots, t_m] = (0)$ for each associated prime of $\mathfrak{U}'$. $\square$

Lemma 1 *The dimension of $\mathfrak{U}'$ is m. Moreover, if $\mathfrak{p}'$ is an associated prime of $\mathfrak{U}'$ of dimension m then $\mathfrak{p}' \cap k[t_1, \ldots, t_m] = (0)$.*

Proof Let $\mathfrak{p}'$ be an associated prime of $\mathfrak{U}'$.

Assume h is the product of the initials of the elements of C. Then none of these initials lies in $\mathfrak{p}'$. Thus the quantities $x_1, \ldots, x_{n+1}$ depend algebraically on $t_1, \ldots, t_m$ over k modulo $\mathfrak{p}'$.

Assume h is the product of the separants of the elements of C. Let $p_\ell = a_d\, x_\ell^d + \cdots + a_1\, x_\ell + a_0$ be any element of C' (for $1 \leq \ell \leq n+1$). Since its separant $s_\ell = d\, a_d\, x_\ell^{d-1} + \cdots + a_1$ does not lie in $\mathfrak{p}'$, at least one of the coefficients $a_d, \ldots, a_1$ does not lie in this ideal. Thus the quantities $x_1, \ldots, x_{n+1}$ depend algebraically on $t_1, \ldots, t_m$ over k modulo $\mathfrak{p}'$.

We have proven that, in both cases, $x_1, \ldots, x_{n+1}$ depend algebraically on $t_1, \ldots, t_m$ over k modulo $\mathfrak{p}'$, hence, first, that $\dim \mathfrak{p}' \leq m$ (whence $\dim \mathfrak{U}' \leq m$), second, that if $\dim \mathfrak{p}' = m$ then $\mathfrak{p}' \cap k[t_1, \ldots, t_m] = (0)$.

Now, any m–uple $(\bar{t}_1, \ldots, \bar{t}_m)$, taken in a universal extension of k, which does not annihilate h, can be prolonged to a zero of $\mathfrak{U}'$. Therefore $\mathfrak{U}'$ has an associated prime $\mathfrak{p}'$ such that $\dim \mathfrak{p}' \geq m$ whence $\dim \mathfrak{U}' \geq m$. Thus $\dim \mathfrak{U}' = m$. $\square$

Consider the two ring homomorphisms

$$R \xrightarrow{\phi} R[h^{-1}] \simeq R'/(f) \xleftarrow{\psi} R'.$$

The ring isomorphism between $R[h^{-1}]$ and $R'/(f)$ is classical (see [5, Exercise 2.2, page 79]). The homomorphism ϕ is the localization at h hence ϕ^{-1} is the intersection with R. The homomorphism ψ is factoring by (f).

Proposition 2 proves that the associated primes of $\mathfrak{U}'$ are in one to one correspondence with the associated primes of $\mathfrak{U}$. Let $\mathfrak{p}'$ be an associated prime of $\mathfrak{U}'$ and $\mathfrak{p}$ be the corresponding associated prime of $\mathfrak{U}$. The ideals $h^{-1}\mathfrak{p}$ and $\mathfrak{p}'/(f)$ are the same. Hence the field of fractions of $(R'/(f))/(\mathfrak{p}'/(f))$ is isomorphic to $R'/\mathfrak{p}'$ for $f \in \mathfrak{p}'$ and is isomorphic to $R/\mathfrak{p}$ for $h \notin \mathfrak{p}$. Thus by proposition 1 the indeterminates $t_1, \ldots, t_m$ provide a transcendence basis of $R/\mathfrak{p}$ over k and the theorem is proven.

Proposition 2 *Let $\mathfrak{p}'_i$ $(1 \leq i \leq r)$ be the associated primes of $\mathfrak{U}'$. Then $\mathfrak{p}'_i/(f) \cap R$ $(1 \leq i \leq r)$ are the associated primes of $\mathfrak{U}$.*

Proof Let $\mathfrak{q}'$ be a primary ideal of R' with associated prime $\mathfrak{p}'$.

There is a one to one correspondence between the ideals of $R'/(f)$ and the ideals of R' which contain (f). This correspondence maps prime ideals to prime ideals (see [7, chap. 2, proposition 1.3]).

Thus $\mathfrak{p}'/(f)$ is prime and is equal to the radical of $\mathfrak{q}'/(f)$.

Moreover, $\mathfrak{q}'/(f)$ is primary. Proof. Let a, $b \in R'$ be such that $ab \in \mathfrak{q}'/(f)$ and $a \notin \mathfrak{p}'/(f)$. Since $f \in \mathfrak{q}'$, $\mathfrak{p}'$ we have $ab \in \mathfrak{q}'$ and $a \notin \mathfrak{p}'$. Thus $b \in \mathfrak{q}'$ hence $b \in \mathfrak{q}'/(f)$ and the claim is proven.

Therefore, if $\mathfrak{q}'_1 \cap \cdots \cap \mathfrak{q}'_r$ is an irredundant primary decomposition of $\mathfrak{U}'$ then $\mathfrak{q}'_1/(f) \cap \cdots \cap \mathfrak{q}'_r/(f)$ is an irredundant primary decomposition of $\mathfrak{U}'/(f)$ and $\mathfrak{p}'_1/(f), \ldots, \mathfrak{p}'_r/(f)$ are its associated primes.

With respect to the ring homomorphism ϕ (localization at h), a contracted ideal $\mathfrak{A}$ of R is an ideal such that $\mathfrak{A} : h^\infty = \mathfrak{A}$ by [10, vol. 1, chap. IV, par. 10, theorem 15].

The ideal $\mathfrak{U}$ is a contracted ideal. It is the contraction of $\mathfrak{U}'/(f)$ (for $\mathfrak{U}'/(f)$ and $\mathfrak{U}^e$ are generated by a same basis: C).

Thus, by [10, vol. 1, chap. IV, par. 10, theorem 17], the associated primes of $\mathfrak{U}$ are the contractions of the associated primes of $\mathfrak{U}'/(f)$. □

1.1.1 Comments

The proof is much inspired of the key argument involved in the proof of Lazard's lemma by Sally Morrison [8, 9]: using the Macaulay theorem to prove first that the nonzero elements of $k[t_1, \ldots, t_m]$ are nonzero divisors modulo $\mathfrak{U}$. Our proof is conducted differently than that of Sally Morrison (who does not consider the ideal[1] $(C) : I_C^\infty$): we apply the very same argument to $(C) : I_C^\infty$ and to $(C) : S_C^\infty$.

This is an advantage of our variant.

Sally Morrison wrote a different proof than that given in [3, lemma 2] because she thought that an important argument was missing. Let's consider the following example. Take $\mathfrak{A} = (x, yz)$ in the ring $R = k[x, y, z]$ for the ordering $x < y < z$. The quotient ring $R/\mathfrak{A}$ can be obtained by constructing

$$R_1 = k[x]/(x), \quad R_2 = R_1[y], \quad R_3 = R_2[z]/(yz).$$

[1] It is a tradition to denote I_C the set of the initials of C and S_C the set of its separants.

Clearly, y is a nonzero divisor in R_2 but a zero divisor in R_3. This phenomenon does not actually arise for ideals of the form $(C):I_C^\infty$ or $(C):S_C^\infty$ i.e. it suffices (for such ideals) to verify that an indeterminate is a non zero divisor at step i to prove that it is a non zero divisor modulo the whole ideal. This property is implicitly used in the proof of [3, lemma 2] but cannot be considered as obvious.

It is also implicitly used in the proof of [2, theorem 5.1]. Notice by the way that this theorem implies our theorem 1. Philippe Aubry gave another proof (which seems correct to us) in [1, théorème 4.6.1], based on the properties of regular sequences in Cohen–Macaulay rings (the unmixedness property of the ideal $(C):I_C^\infty$ is proven in [1, théorème 4.1.4]). The proof is incremental i.e. the result is proven indeterminate per indeterminate, according to the ordering. We believe that Aubry's proof can easily be generalized to handle the ideal $(C):S_C^\infty$ together with the ideal $(C):I_C^\infty$. It then would provide an incremental proof of Lazard's lemma.

1.2 The Lazard's lemma

Theorem 1 permits us now to prove Lazard's lemma using the scheme of Lazard's original idea (notice that the original Lazard's lemma involves theorem 1).

Theorem 2 *The ideal $\mathfrak{U} = (C):S_C^\infty$ is radical.*

Proof The ideal $\mathfrak{U}$ is radical if and only if $R/\mathfrak{U}$ does not contain any nilpotent element.

Let M be a multiplicative family of a ring R which only contains non zero divisors. Then, an element $a \in R$ is a zero divisor if and only if a is a zero divisor in $M^{-1}R$.

Thus by theorem 1, the ideal $(C):S_C^\infty$ is radical if and only if $R' = k(t_1, \ldots, t_m)[x_1, \ldots, x_n]/\mathfrak{U}$ does not contain any nilpotent element.

Denote $p_1, \ldots, p_n$ the elements of C and $s_1, \ldots, s_n$ their separants. The ring R' is isomorphic to the ring R_n defined by

$$R_0 = k(t_1, \ldots, t_m), \quad R_i = R_{i-1}[x_i]/(p_i):s_i^\infty.$$

Assume R_{i-1} is a direct product of fields $k_1 \times \cdots \times k_r$. Then R_i is isomorphic to the product $(1 \le j \le r)$ of rings $k_j[x_i]/(p_i):s_i^\infty$. The key point is that the image of s_i in $k_j[x_i]$ is the separant of the image of p_i. Thus in

$k_j[x_i]$, the ideal $(p_i) : s_i^\infty$ is generated by the product of the irreducible simple factors of p_i. It is thus the intersection of the maximal ideals $\mathfrak{m}_\ell$ generated by these factors. By the chinese remainders theorem [5, Exercise 2.6, page 79], the ring $k_j[x_i]/(p_i) : s_i^\infty$ is isomorphic to the direct product of the fields $k_j[x_i]/\mathfrak{m}_\ell$. By the axioms of products (a direct product of direct product of fields is itself a direct product of fields) the ring R_i is a direct product of fields.

Thus, since R_0 is a product of fields, so is R'.

A direct product of fields contains no nilpotent element. □

2 Regular chains

2.1 Two equivalent definitions

Denote $p_1, \ldots, p_n$ the elements of the triangular system C and $i_1, \ldots, i_n$ their initials. For every $1 \leq \ell \leq m$, denote $\mathfrak{U}_\ell = (p_1, \ldots, p_\ell) : (i_1 \cdots i_\ell)^\infty$.

Definition 1 *A triangular system $C = \{p_1, \ldots, p_n\}$ is a* regular chain *in the sense of [2] (see also [6]) if, for every $2 \leq \ell \leq n$, the initial of p_ℓ is regular (i.e. a nonzero divisor) in the ring*

$$Y_{\ell-1} = k[t_1, \ldots, t_{m_{\ell-1}}, x_1, \ldots, x_{\ell-1}]/\mathfrak{U}_{\ell-1}$$

where $t_{m_{\ell-1}}$ is the highest t indeterminate less than $x_{\ell-1}$ w.r.t. the chosen ordering on the set of indeterminates.

Lemma 2 *A triangular system C is a regular chain in the sense of [2] if and only if, for every $2 \leq \ell \leq n$, the initial of p_ℓ is regular in the ring*

$$X_{\ell-1} = k[t_1, \ldots, t_m, x_1, \ldots, x_{\ell-1}]/\mathfrak{U}_{\ell-1}.$$

Proof For, if R is a ring, x is an indeterminate over R and $a \in R$ then a is regular if and only if a is regular in $R[x]$. □

Definition 2 *A triangular system C is a* regular chain *in the sense of [4] if, for every $2 \leq \ell \leq n$, the initial of p_ℓ is invertible in the ring*

$$Z_{\ell-1} = k(t_1, \ldots, t_m)[x_1, \ldots, x_{\ell-1}]/\mathfrak{U}_{\ell-1}.$$

Lemma 3 *Every regular element of Z_ℓ is invertible* $(1 \leq \ell \leq n)$.

Proof Theorem 1 implies that in $k(t_1, \ldots, t_m)[x_1, \ldots, x_\ell]$, the ideal $\mathfrak{U}_\ell$ has dimension zero. The algebraic variety V_ℓ of $\mathfrak{U}_\ell$ is thus a finite set of points. Therefore, a regular element of Z_ℓ, which is an element f which lies in none of the associated primes of $\mathfrak{U}_\ell$, does not vanish on any point of V_ℓ. Thus $(\mathfrak{U}_\ell, f) = (1)$ by Hilbert's theorem of zeros [5, Corollary 1.7, page 34] hence f is invertible in Z_ℓ. $\square$

Theorem 3 *Both definitions of regular chains are equivalent.*

Proof Let M be a multiplicative family of a ring R which only contains non zero divisors. Then, an element $a \in R$ is a zero divisor if and only if a is a zero divisor in $M^{-1}R$.

Assume C is a regular chain in the sense of [2]. Fix some index $2 \leq \ell \leq n$. The initial of p_ℓ is a non zero divisor in $Y_{\ell-1}$. Thus it is a non zero divisor in $X_{\ell-1}$ by lemma 2. Thus it is a non zero divisor in $Z_{\ell-1}$ by the remark above. Thus it is invertible in $Z_{\ell-1}$ by lemma 3. Therefore C is a regular chain in the sense of [4].

Assume C is a regular chain in the sense of [4]. Fix some index $2 \leq \ell \leq n$. The initial i_ℓ of p_ℓ is invertible in $Z_{\ell-1}$. Thus there exists some polynomial $b \in k[t_1, \ldots, t_m, x_1, \ldots, x_{\ell-1}]$ such that $b\, i_\ell = a \in k[t_1, \ldots, t_m]$ in $X_{\ell-1}$. If i_ℓ is a zero divisor in $X_{\ell-1}$ then so is a: a contradiction to theorem 1. Thus i_ℓ is a non zero divisor in $X_{\ell-1}$. Thus, by lemma 2, the set C is a regular chain in the sense of [2]. $\square$

2.2 Squarefree regular chains

Assume $C = \{p_1, \ldots, p_n\}$ is a regular chain. Denote $H_C = I_C \cup S_C$ the set of the initials and the separants of C.

Definition 3 *The regular chain C is said to be* squarefree *if the separant s_ℓ of p_ℓ is invertible in Z_ℓ* $(1 \leq \ell \leq n)$.

Theorem 4 *If C is a squarefree regular chain then $(C) : I_C^\infty = (C) : H_C^\infty$ is radical.*

Proof If h is invertible modulo an ideal $\mathfrak{A}$ then $\mathfrak{A} : h^\infty = \mathfrak{A}$ thus we have $(C) : I_C^\infty = (C) : H_C^\infty$.

If $\mathfrak{A}$ is radical, whatever h, the ideal $\mathfrak{A} : h^\infty$ is radical (for, on one hand $\mathfrak{A} : h^\infty$ is the intersection of the prime ideals minimal over $\mathfrak{A}$ which do not contain h and, on the other hand an intersection of prime ideals is radical).

The ideal $(C) : H_C^\infty = \mathfrak{A} : h^\infty$ where $\mathfrak{A} = (C) : S_C^\infty$ is radical (by Lazard's lemma) and h is the product of the initials of the elements of C. $\square$

Theorem 5 *Let C be a squarefree regular chain. Let g be a polynomial in $k(t_1, \ldots, t_m)[x_1, \ldots, x_\ell]$ (for some $1 \le \ell \le n$). Assume that $0 < \deg(g, x_\ell) < \deg(p_\ell, x_\ell)$, that the initial of g is invertible in $Z_{\ell-1}$ and that $p_\ell = g\,h$ in $Z_{\ell-1}[x_\ell]$ (for some h). Then the two triangular sets C_g and C_h obtained from C by replacing p_ℓ by g or by h form squarefree regular chains and*

$$(C) : I_C^\infty = (C_g) : I_{C_g}^\infty \cap (C_h) : I_{C_h}^\infty.$$

Proof We work in the polynomial ring $k(t_1, \ldots, t_m)[x_1, \ldots, x_n]$. Denote i_k, i_g, i_h, s_k, s_g, s_h the initials and separants of p_k ($1 \le k \le n$), g and h. Recall $\mathfrak{U}_k = (p_1, \ldots, p_k) : (i_1 \cdots i_k)^\infty$. Denote $\mathfrak{G}_k$ (resp. $\mathfrak{H}_k$) the ideal obtained by replacing p_ℓ and i_ℓ by g and i_g (resp. h and i_h) in the formula.

The initial $i_\ell = i_g\, i_h$ is invertible modulo $\mathfrak{U}_{\ell-1} = \mathfrak{G}_{\ell-1}$. Thus so are i_g and i_h. Therefore

$$\mathfrak{U}_k \quad \subset \quad \mathfrak{G}_k,\, \mathfrak{H}_k \quad (1 \le k \le n) \tag{1}$$

Thus the initial of p_k, which is invertible modulo $\mathfrak{U}_{k-1}$, is invertible modulo $\mathfrak{G}_{k-1}$ and $\mathfrak{H}_{k-1}$ ($1 \le k \le n$) and C_g and C_k are regular chains.

For the same reason, the separant s_ℓ, which is invertible modulo $\mathfrak{U}_\ell$, is invertible modulo $\mathfrak{G}_\ell$ and $\mathfrak{H}_\ell$. Moreover, $s_\ell = s_g\, h + s_h\, g$ modulo $\mathfrak{U}_{\ell-1}$. Since $g \in \mathfrak{G}_\ell$ we have $s_\ell = s_g\, h$ modulo $\mathfrak{G}_\ell$ thus s_g is invertible modulo $\mathfrak{G}_\ell$. A similar argument shows that s_h is invertible modulo $\mathfrak{H}_\ell$. Using (1) again we conclude that C_g and C_h are squarefree regular chains.

Consider the ideal $(C) : I_C^\infty$. By Lazard's lemma, it is radical and has dimension zero. Therefore, it has finitely many zeros (taken in a universal field extension of the base field) which are pairwise distinct. Denote V its set of zeros. Since the initials of the elements of C do not vanish on V the number of zeros $|V| = \prod_{i=1}^n \deg(p_i, x_i)$. Similar statements hold for $(C_g) : I_{C_g}^\infty$ and for $(C_h) : I_{C_h}^\infty$. Denote V_g and V_h the sets of zeros of these two last ideals. Relation (1) implies that $(C) : I_C^\infty \subset (C_g) : I_{C_g}^\infty \cap (C_h) : I_{C_h}^\infty$ i.e. that

$V \supset V_g \cup V_h$. We have $\deg(p_\ell, x_\ell) = \deg(g, x_\ell) + \deg(h, x_\ell)$ which implies that $|V| = |V_g| + |V_h|$. Moreover, $V_g \cap V_h$ is empty (for a common zero of g and h would annihilate $s_\ell = s_g\, h + s_h\, g$). Thus $V = V_g \cup V_h$. A polynomial belongs to a radical ideal if and only if it vanishes on every of its zeros (Hilbert's theorem of zeros). Thus $(C) : I_C^\infty = (C_g) : I_{C_g}^\infty \cap (C_h) : I_{C_h}^\infty$. $\Box$

References

[1] Philippe Aubry. *Ensembles triangulaires de polynômes et résolution de systèmes algébriques. Implantation en Axiom.* PhD thesis, Université Paris VI, 1999.

[2] Philippe Aubry, Daniel Lazard, and Marc Moreno Maza. On the theories of triangular sets. *Journal of Symbolic Computation*, 28:105–124, 1999.

[3] François Boulier, Daniel Lazard, François Ollivier, and Michel Petitot. Representation for the radical of a finitely generated differential ideal. In *proceedings of ISSAC'95*, pages 158–166, Montréal, Canada, 1995.

[4] François Boulier, François Lemaire, and Marc Moreno Maza. PARDI ! Technical report, Université Lille I, LIFL, 59655, Villeneuve d'Ascq, France, 2001. in preparation, to be submitted to the JSC.

[5] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer Verlag, 1995.

[6] Mickael Kalkbrener. A Generalized Euclidean Algorithm for Computing Triangular Representations of Algebraic Varieties. *Journal of Symbolic Computation*, 15:143–167, 1993.

[7] Marie-Paule Malliavin. *Algèbre commutative. Applications en gémoétrie et en théorie des nombres.* maîtrise de mathématiques pures. Masson, Paris, 1985.

[8] Sally Morrison. Yet another proof of Lazard's lemma. private communication, december 1995.

[9] Sally Morrison. The Differential Ideal $[P] : M^\infty$. *Journal of Symbolic Computation*, 28:631–656, 1999.

[10] Oscar Zariski and Pierre Samuel. *Commutative Algebra.* Van Nostrand, New York, 1958.