

The Diamond Lemma for non-terminating rewriting systems using deterministic reduction strategies (Long Version)

Cyrille Chenavier¹ and Maxime Lucas²

¹ Inria Lille - Nord Europe, Équipe Valse
`cyrille.chenavier@inria.fr`

² Inria Rennes - Bretagne Atlantique, Équipe Gallinette
`maxime.lucas@inria.fr`

Abstract

We study the confluence property for rewriting systems whose underlying set of terms admits a vector space structure. For that, we use deterministic reduction strategies. These strategies are based on the choice of standard reductions applied to basis elements. We provide a sufficient condition of confluence in terms of the kernel of the operator which computes standard normal forms. We present a local criterion which enables us to check the confluence property in this framework. We show how this criterion is related to the Diamond Lemma for terminating rewriting systems.

plan:

- **Section I: IWC theorem**
- **Section 2: rew on rationnal Weyl algebras**
 - **definition of rew. rules and rew. steps**
 - **proposition: convergent implies general form of solution to PDE**
 - **Janet bases: Janet complete implies existence of a strategy, passivity implies h -confluence criterion, as a consequence we recover formal solutions to PDE**
 - **$y' = xy$ and Janet example**

Example $y' = xy$, main steps:

- **general solution is given by $\langle u \mid x^{2n+1} \rangle = 0$ and $\langle u \mid x^{2n} \rangle = u(0)/(2^n n!)$**
- **we recover this by rew: we need $(\partial_x)^n x = x(\partial_x)^n + n(\partial_x)^{n-1}$ (using Leibniz identity and induction) and $\langle u \mid x^n \rangle = 1/(n!)(\partial_x)^n(u)|_0$ and we prove the previous two formulas by induction (use this example as a running example?)**

.

1 Introduction

The fact that local confluence together with termination implies confluence has been known for abstract rewriting systems since Newman's work [8]. For rewriting on noncommutative polynomials, a similar result known as the Diamond lemma was introduced by Bergman [2] nearly 30 years later, in order to compute normal forms in noncommutative algebras using

rewriting theory. It asserts that for terminating rewriting systems, the local confluence property can be checked on monomials.

One difficulty of rewriting polynomials is that the naive notion of rewriting path (obtained as the closure of the generating rewriting relations under reflexivity, transitivity, sum and product by a scalar) does not terminate. Instead, one needs to first consider well-formed rewriting steps before forming the reflexive transitive closure.

Nevertheless the Diamond lemma has proved to be very useful : together with the works of Bokut [3], it has given birth the theory of noncommutative Gröbner bases [7]. The latter have provided applications to various areas of noncommutative algebra such as the study of embedding problems (which appear in the works of Bokut and Bergman), homological algebra [4, 5] or Koszul duality [1, 9].

Computation of normal forms in noncommutative algebra is also used to provide formal solutions to partial differential equations. In this framework, a confluence criterion analogous to the Diamond Lemma is given by Janet bases [10], which specify a deterministic way to reduce each polynomial into normal form using standard reductions [6]. The confluence criterion may then be asserted as follows: for each monomial m and each non-standard reduction $m \rightarrow f$, f is reducible into \hat{m} , where the latter is obtained from m using only standard reductions.

In the presented paper, we propose an extension of the Diamond Lemma which offers two improvements over the one from Bergman: first it allows the treatment of non-terminating rewriting relations, and second it does not presuppose a notion of well-formed rewriting steps. This last property seems particularly promising in order to extend the Diamond Lemma to other structures.

Instead of supposing that the rewriting relation studied is terminating, we suppose given an ordering on the monomials, independent of the rewriting relation. We then use methods based on standard reductions: for every monomial m , we select exactly one reduction with left-hand side m , which is decreasing for the ordering chosen. Such choices induce a deterministic way to reduce each polynomial, obtained by applying simultaneously standard reductions on every monomial appearing in its decomposition. When these deterministic reductions terminate, one defines an operator which maps every polynomial to its unique standard normal form.

From this operator, we define a suitable notion of confluence in our setting, and show in Proposition 2.9 that it implies the usual notion of confluence for the rewriting system studied. We then provide an effective method for checking this criterion in Theorem 2.12. This method is based on a local analysis corresponding to checking local confluence on monomials. In particular, when the rewriting system is terminating, we show (Theorem 2.14) that we recover the Diamond Lemma as a particular case of Theorem 2.12.

2 A weak version of diamond lemma

2.1 Local strategies and h -normal forms

We fix a commutative field \mathbb{K} as well as a well-founded partially ordered set $(X, <_X)$. We denote by $\mathbb{K}X$ the vector space spanned by X : an element $v \in \mathbb{K}X$ is a finite formal linear combination of elements of X with coefficients in \mathbb{K} . The sum of $u = \sum \lambda_x x$ and $v = \sum \mu_x x$ equals $\sum (\lambda_x + \mu_x) x$ and the product of $\lambda \in \mathbb{K}$ by v equals $\sum (\lambda \lambda_x) x$. For every $v \in \mathbb{K}X$, there exists a unique finite set $\text{supp}(v) \subset X$, called the *support* of v , such that

$$v = \sum_{x \in \text{supp}(v)} \lambda_x x \text{ and } x \in \text{supp}(v) \Rightarrow \lambda_x \neq 0. \quad (1)$$

We extend the order $<_X$ into the multiset order on $\mathbb{K}X$, denoted $<_{\mathbb{K}X}$: for any $u, v \in \mathbb{K}X$, $u <_{\mathbb{K}X} v$ if $\text{supp}(u) \neq \text{supp}(v)$ and for any $x \in \text{supp}(u) \setminus \text{supp}(v)$, there exists $y \in \text{supp}(v) \setminus \text{supp}(u)$ such that $y >_X x$. Note that $<_{\mathbb{K}X}$ and $<_X$ coincide when restricted to X , so we simply denote this order by $<$ in the rest of this paper.

We fix a set $R \subseteq X \times \mathbb{K}X$ which represents rewrite rules of the form $x \xrightarrow[R]{} r$. The set R induces a rewriting relation on $\mathbb{K}X$ which reduces many x 's at once and defined as follows:

$$\sum_x \lambda_x x + v \xrightarrow[R]{} \sum_x \lambda_x r_x + v, \quad (2)$$

where v is any element of $\mathbb{K}X$, and for any $x \in X$ appearing in the sum, $\lambda_x \neq 0$, $x \xrightarrow[R]{} r_x \in R$ and $x \notin \text{supp}(v)$. Finally we denote by $\xrightarrow[R]{*}$ the closure of $\xrightarrow[R]{}$ under transitivity, symmetry and sum.

Definition 2.1. A local strategy h for R is the choice, for every $x \in X$ not minimal for $<$, of a rewriting rule $h_x = x \xrightarrow[R]{} r_x$ such that $r_x < x$.

In the rest of this paper, we suppose chosen such a local strategy h (note that such an h may not exist). Any vector v can be decomposed in a unique way as $\sum \lambda_x x + v'$, where $y \in \text{supp}(v')$ implies that y is minimal for $<$, and $x \in \text{supp}(v) \setminus \text{supp}(v')$ is not. We define a rewriting relation $\xrightarrow[h]{}$ as follows:

$$h_v = \sum \lambda_x x + v' \xrightarrow[h]{} \sum \lambda_x r_x + v', \quad (3)$$

where for every x , $h_x = x \xrightarrow[R]{} r_x$. Note in particular that if x is minimal for $<$, then $h_x = x \rightarrow x$ is the identity on x .

Definition 2.2. A vector v is said to be an h -normal form if it is a normal form for $\xrightarrow[h]{}$.

Example 2.3. Let $X = \{x, y, z, t\}$, $x \xrightarrow[R]{} y$, $y \xrightarrow[R]{} z + t$, $z \xrightarrow[R]{} y - t$. Note that this is not terminating since we have the infinite loop $y \xrightarrow[R]{} z + t \xrightarrow[R]{} (y - t) + t = y$. We choose the order $x > y > z, t$, and the following distinguished rewrite rules: $h_x = x \xrightarrow[h]{} y$ and $h_y = y \xrightarrow[h]{} z + t$. Then the R -normal forms are the $\lambda_t t$, while the h -normal forms are all the expressions of the form $\lambda_t t + \lambda_z z$.

Lemma 2.4. Let v be a vector in $\mathbb{K}X$. Either v is minimal for $<$, or there exists $v' < v$ such that $v \xrightarrow[h]{} v'$. In particular, h -normal forms are precisely the minimal elements of $\mathbb{K}X$ for $<$.

For each $v \in \mathbb{K}X$ and strategy local strategy h , there exists at most one v' such that $v \xrightarrow[h]{} v'$, and $\xrightarrow[h]{}$ is compatible with the termination order $<$. As a consequence, any $v \in \mathbb{K}X$ is sent by multiple applications of $\xrightarrow[h]{}$ to a unique h -normal form that we denote by $H(v)$. This defines a map $H : \mathbb{K}X \rightarrow \mathbb{K}X$.

Proposition 2.5. The map H is a linear projector, in the sense that for all $u, v \in \mathbb{K}X$ and $\lambda \in \mathbb{K}$, $H(u + v) = H(u) + H(v)$, $H(\lambda u) = \lambda H(u)$ and $H(H(u)) = H(u)$.

Proof. The h -normal forms are closed under sums, so that $H(H(v)) = H(v)$ for every v , that is H is a projector. Moreover, if $u \xrightarrow[h]{} u'$ and $v \xrightarrow[h]{} v'$, then we have $u + v \xrightarrow[h]{} u' + v'$. Iterating $\xrightarrow[h]{}$, we get $H(u + v) = H(H(u) + H(v)) = H(u) + H(v)$. \square

2.2 A confluence criterion

In this section we investigate the confluence properties of R . The main idea behind this section is that under suitable hypothesis $\xrightarrow[h]{}$ should form a terminating, confluent subrelation of $\xrightarrow[R]{}$.

We start in Definition 2.6 and the following propositions by relating the confluence of $\xrightarrow[R]{}$ to properties on h . Then Theorem 2.12, we prove a confluence criterion to check whether R satisfies Definition 2.6.

Definition 2.6. We say that R is *h-confluent* if for every rewrite rule $x \xrightarrow[R]{} v \in R$, we have $H(x - v) = 0$.

Example 2.7. Let us take the same example as in Example 2.3. We have three equations to check:

$$H(x) = z + t = H(y), \quad H(y) = z + t = H(z + t), \quad H(z) = z = H(y - t),$$

and so R is *h-confluent*. Replacing the rule $z \xrightarrow[R]{} y - t$ by $z \xrightarrow[R]{} y$, we get $H(z) = z$ and $H(y) = z + t$, so R is not *h-confluent* anymore.

Proposition 2.8. If R is *h-confluent*, then $u \xleftarrow[R]{*} v$ if and only if $H(u - v) = 0$.

Proof. The relation $\xleftarrow[R]{*}$ is the closure of $\xrightarrow[R]{}$ under transitivity, symmetry and sum. Since the relation $H(u - v) = 0$ is closed under these operations, we get one implication.

Reciprocally, if $H(u - v) = 0$ then by definition of H we have $u \xleftarrow[h]{*} v$, and in particular $u \xleftarrow[R]{*} v$. \square

Proposition 2.9. If R is *h-confluent* then $\xrightarrow[R]{}$ is confluent.

Proof. Let $v, v_1, v_2 \in \mathbb{K}X$ be such that $v \xrightarrow[R]{*} v_i$, for $i = 1, 2$. From Proposition 2.8, $v_1 - v_2$ belongs to $\ker(H)$, that is $H(v_1) = H(v_2)$. Denoting by u the common value, we get $v_i \xrightarrow[R]{*} u$, which proves the proposition. \square

Note that the previous proposition is a sufficient but not a necessary condition: taking X to be the integers, with the relations $n \xrightarrow[R]{} n + 1$ is confluent, but there exist no local strategy h making R *h-confluent*.

We now introduce our criterion to show that R is *h-confluent*. For that, we assume that the set of relations R is equipped with a well-founded order \prec satisfying the following decreasingness property:

Definition 2.10. We say that R is *locally h-confluent* if for every $x \in X$ and $f = x \xrightarrow[R]{} v$, then letting $h_x = x \xrightarrow[h]{} r_x$, we have the confluence diagram:

$$\begin{array}{ccc} x & \xrightarrow{f} & v \\ h_x \downarrow & & \uparrow \text{ } * \\ r_x & \xleftarrow{\dots} & v' \end{array}$$

where each rewriting step occurring in the dotted arrows is strictly smaller than f with respect to \prec .

Example 2.11. Continuing with Example 2.3, let us define an order \prec on R by the following ordering: $(x \xrightarrow{R} y), (y \xrightarrow{R} z + t) \prec (z \xrightarrow{R} y - t)$. This is guided by the heuristic that rules advancing towards an h -normal form should be favored over rules that do not: here z is an h -normal form so the rule rewriting it is large for \prec . The following diagrams show that R is locally h -confluent:

$$\begin{array}{ccc} \begin{array}{ccc} x & \xrightarrow{R} & y \\ h_x \downarrow & & \parallel \\ y & \xlongequal{\quad} & y \end{array} & \begin{array}{ccc} y & \xrightarrow{R} & z + t \\ h_y \downarrow & & \parallel \\ z + t & \xlongequal{\quad} & z + t \end{array} & \begin{array}{ccc} z & \xrightarrow{R} & y - t \\ h_z \parallel & & \downarrow R \\ z & \xlongequal{\quad} & z \end{array} \end{array}$$

Our main result is the following.

Theorem 2.12. *If R is locally h -confluent, then R is h -confluent. In particular, \xrightarrow{R} is confluent.*

Proof. We reason by induction on r according to the order \prec . Looking at the square corresponding to r :

$$\begin{array}{ccc} x & \xrightarrow{r} & v \\ h_x \downarrow & & \downarrow * \\ r_x & \xrightarrow{\prec \dots \succ} & v' \end{array}$$

we have $H(x) = H(r_x)$ by definition of H , and $H(r_x) = H(v') = H(v)$ by induction hypothesis, which concludes the proof. \square

Remark 2.13. Local h -confluence implies that the pair of rewriting relations $(\xrightarrow{h}, \xrightarrow{R})$ is decreasing with respect to conversions (see [11, Definition 3]), using the order \prec on R and the discrete ordering on \xrightarrow{h} . By [11, Theorem 3], this implies that $(\xrightarrow{h}, \xrightarrow{R})$ commute. Using the fact that $\xrightarrow{h} \subseteq \xrightarrow{R}$, one can then recover that \xrightarrow{R} is confluent.

Let us show how the Diamond Lemma fits as a particular case of our setup.

Theorem 2.14 ([2]). *Assume that \xrightarrow{R} is terminating and that for every $x \in X$, $x \xrightarrow{R} r$ and $x \xrightarrow{R} r' \in R$, r and r' are joinable. Then, \xrightarrow{R} is confluent.*

Proof. We define an ordering $x > y$ on X as the transitive closure of the relation “there exists $v \in \mathbb{K}X$ such that $x \xrightarrow{R} v$ and $y \in \text{supp}(v)$ ”. This is well-founded since by hypothesis \xrightarrow{R} is terminating. By definition, if $x \in X$ is not minimal for $>$, then x is not an R -normal form. Let us fix an arbitrary rewriting step $h_x = x \xrightarrow{h} r_x$. By definition of $>$, for any $y \in \text{supp}(r_x)$ we have $y < x$ and so $r_x < x$, which shows that h is a local strategy. Ordering the rewrite rules by their left hand sides makes R locally h -confluent. Theorem 2.12 finally shows that R is confluent. \square

3 Rewriting and partial derivative equations

3.1 Rewriting systems on rational Weyl algebras

Dire qu'on commence par rappeler des notions classiques sur les algèbres rationnelles de Weyl et les ordres monomiaux.

We fix a set $\{x_1, \dots, x_n\}$ of indeterminates and we denote by $\mathbb{Q}(x_1, \dots, x_n)$ the field of fractions of the polynomial algebra $\mathbb{Q}[x_1, \dots, x_n]$ over \mathbb{Q} . Let us introduce another set of variable $\Delta := \{\partial_1, \dots, \partial_n\}$, and let us denote by Δ^c the free commutative monoid over Δ , i.e.,

$$\Delta^c = \{\partial_1^{\alpha_1} \dots \partial_n^{\alpha_n} \mid \alpha_i \in \mathbb{N}\}.$$

Given $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$, we denote by $\partial^\alpha := \partial_1^{\alpha_1} \dots \partial_n^{\alpha_n}$.

Definition 3.1. The *rational Weyl algebra* over $\mathbb{Q}(x_1, \dots, x_n)$ is the set of polynomials over the indeterminates Δ and coefficients in $\mathbb{Q}(x_1, \dots, x_n)$, subject to the following commutation rule:

$$\partial_i f = f \partial_i + \frac{d}{dx_i}(f), \quad f \in \mathbb{Q}(x_1, \dots, x_n), \quad 1 \leq i \leq n, \quad (4)$$

where $d/dx_i : \mathbb{Q}(x_1, \dots, x_n) \rightarrow \mathbb{Q}(x_1, \dots, x_n)$ is the partial derivative operator with respect to the indeterminate x_i . This algebra is denoted by $B_n(\mathbb{Q})$.

A *monomial order* \preceq on Δ^c is a well-founded total order on Δ^c that is compatible with multiplication of monomials, i.e., $\partial^\alpha \preceq \partial^\beta$ implies $\partial^{\alpha+\gamma} \preceq \partial^{\beta+\gamma}$, for every $\alpha, \beta, \gamma \in \mathbb{N}^n$.

Given a set $F := \{P_1, \dots, P_k\} \subseteq B_n(\mathbb{Q})$

3.2 Janet bases and h -confluence

In this section, we take $\mathbb{K} = \mathbb{R}(x_1, x_2, \dots, x_n)$ the field of real rational functions in n variables, and look at the \mathbb{K} -algebra $A = \mathbb{K}[\partial_1, \dots, \partial_n]$. We suppose given an ordering $\partial_n > \partial_{n-1} > \dots > \partial_1$. By monomial, we mean unitary monomial.

Example 3.2. Elements of A should be thought of as systems of linear partial derivative equations. For example, the equation $x_1 \frac{\partial u}{\partial x_1} - u = 0$ corresponds to the element $x_1 \partial_1 - 1$ in A .

Similarly, the 1-dimensional heat equation $\frac{\partial u}{\partial t} = \kappa \frac{\partial^2 u}{\partial x^2}$ corresponds (taking $x_1 = t$ and $x_2 = x$) to the element $\partial_1 - \kappa \partial_2^2$.

Definition 3.3. For any monomial m and $1 \leq k \leq n$ we denote by $\nu_k(m)$ the power of ∂_k in m . For any $\vec{j} = (j_1, \dots, j_n) \in \mathbb{N}^n$, we denote by $\vec{\partial}^{\vec{j}}$ the monomial m such that $\nu_k(m) = j_k$ for all k . For any subset $E \subset \{1, \dots, n\}$, we denote by $Mon(E)$ the set of monomials m such that $\nu_k(m) = 0$ for all $k \notin E$. In particular, $Mon(\{1, \dots, n\})$ is the set of all monomials of A which we denote simply by Mon , while $Mon(\emptyset)$ is reduced to $\{1\}$.

Definition 3.4. A *cone* is a pair (m, E) , where $m \in A$ and $E \subset \{1, \dots, n\}$. m is called the *origin of the cone*, while E is the *direction*. A cone is *monomial* if m is a monomial. We denote by $(m, E)^*$ the family of monomials of the form mp , where $p \in Mon(E)$.

If S is a family of monomials, a *cone-partition* of S is a family of monomial cones (m_i, E_i) for $i \in I$ such that for $i \neq j$, $(m_i, E_i)^* \cap (m_j, E_j)^* = \emptyset$ and $S = \coprod_{i \in I} (m_i, E_i)^*$. In other words the $(m_i, E_i)^*$ form a partition of S into monomial cones. It is a finite cone-partition if I is finite.

Definition 3.5. A family of monomial cones (m_i, E_i) with distinct origins is said to be *complete* if it induces a cone-partition of the monomial ideal generated by the m_i s.

A family of cones (p_i, E_i) is said to be *complete* if $(lm(p_i), E_i)$ is complete.

Lemma 3.6. A complete family of cones gives rise to a local strategy on A .

Sketch. We use the monomial ordering on reducible monomials, and reducible ones are bigger than irreducible ones.

Then we only need to define h on reducible ones. For $x \in \text{Red}(R)$, there exists a unique (m_i, E_i) in the cone-partition such that $x = m_i p$ with $p \in E_i$ and m_i corresponds to an element $m_i + r$ of R . Then h is defined by $h_x = x = m_i p \xrightarrow{R} -rp$. \square

In order to produce suitable cone-partitions as in the previous lemma, we introduce the notion of multiplicative variables.

Definition 3.7. Let M be a subset of Mon , and let $m \in M$. We define a subset $\mu_M(m)$ of $\{1, \dots, n\}$. Let us write $m = \partial_1^{i_1} \partial_2^{i_2} \dots \partial_n^{i_n}$, and take $k \in \{1, \dots, n\}$. Then $k \in \mu_M(m)$ if the following implication is true:

$$\forall m' \in M, \quad (\forall j < k, \nu_j(m') = \nu_j(m)) \quad \Rightarrow \quad \nu_k(m') \leq \nu_k(m).$$

We call $(m, \mu_M(m))$ the cone of m in M . If M is clear then we will just write $\mu(m)$. If $k \in \mu(m)$ we will say that ∂_k is a *multiplicative variable* of m .

Lemma 3.8. Let $M \subset \text{Mon}$ and $m, m' \in M$. If $m \neq m'$, then $(m, \mu(m))^* \cap (m', \mu(m'))^* = \emptyset$.

Proof. Since $m \neq m'$, there exists k minimal such that $\nu_k(m) \neq \nu_k(m')$. Without loss of generality, we can suppose $\nu_k(m) < \nu_k(m')$. By definition of μ , we therefore have that $k \notin \mu(m)$.

Take now $p \in (m, \mu(m))^* \cap (m', \mu(m'))^*$. Then $p = mq$, with $\nu_k(q) = 0$, and so $\nu_k(p) = \nu_k(m)$. But p is a multiple of m' and so $\nu_k(m) = \nu_k(p) \geq \nu_k(m')$, which is contradictory. \square

Example 3.9. TODO.

Definition 3.10. A set of monomials M is *Janet-complete* if the family of all $(m, \mu(m))$ is complete.

A set of polynomials R is *Janet-complete* if $\text{lm}(R)$ is Janet-complete.

Conclusion. We introduced a sufficient condition, based on deterministic reduction strategies, of confluence for rewriting systems on vector spaces. As a particular case, we recover the Diamond Lemma. This work maybe extended in particular into two main directions. The first one consists in weakening our assumption on the set \mathbb{K} of coefficients, by allowing non invertible coefficients. A second extension consists in characterising Janet bases in this framework, with the objective to develop constructive methods in the analysis and formal resolution of PDE's.

References

- [1] Roland Berger. Koszulity for nonquadratic algebras. *J. Algebra*, 239(2):705–734, 2001.
- [2] George M. Bergman. The diamond lemma for ring theory. *Adv. in Math.*, 29(2):178–218, 1978.
- [3] Leonid A. Bokut'. Imbeddings into simple associative algebras. *Algebra i Logika*, 15(2):117–142, 245, 1976.
- [4] Yuji Kobayashi. Complete rewriting systems and homology of monoid algebras. *J. Pure Appl. Algebra*, 65(3):263–275, 1990.
- [5] Yuji Kobayashi. Gröbner bases of associative algebras and the Hochschild cohomology. *Trans. Amer. Math. Soc.*, 357(3):1095–1124, 2005.
- [6] Paul-André Mellès. *Axiomatic Rewriting Theory I: A Diagrammatic Standardization Theorem*, pages 554–638. Springer Berlin Heidelberg, Berlin, Heidelberg, 2005.

- [7] Teo Mora. An introduction to commutative and noncommutative Gröbner bases. *Theoret. Comput. Sci.*, 134(1):131–173, 1994.
- [8] Maxwell H. A. Newman. On theories with a combinatorial definition of “equivalence.”. *Ann. of Math. (2)*, 43:223–243, 1942.
- [9] Stewart B. Priddy. Koszul resolutions. *Trans. Amer. Math. Soc.*, 152:39–60, 1970.
- [10] Werner M. Seiler. Spencer cohomology, differential equations, and Pommaret bases. In *Gröbner bases in symbolic analysis*, volume 2 of *Radon Ser. Comput. Appl. Math.*, pages 169–216. Walter de Gruyter, Berlin, 2007.
- [11] Vincent Van Oostrom. Confluence by decreasing diagrams. In *International Conference on Rewriting Techniques and Applications*, pages 306–320. Springer, 2008.