The Diamond Lemma for non-terminating rewriting systems using deterministic reduction strategies

Cyrille Chenavier[1] and Maxime Lucas[2]

[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 over vector spaces using deterministic reduction strategies. These strategies are based on the choice of standard reductions applied to basis elements. We show that the confluence property is interpreted 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.

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 $m \to f$, f is reducible into $\widehat{m}$, 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 of 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 notions of both confluence in our setting, and show in Proposition 3.4 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 3.7. 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 3.8) that we recover the Diamond Lemma as a particular case of Theorem 3.7.

2   Local strategies and h-normal forms

We fix a commutative field $\mathbb{K}$ as well as a well-founded ordered set $(X, <)$. 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 $\mathbb{K}$. In particular, for every $v \in \mathbb{K}X$, there exists a unique finite set $\mathrm{supp}(v) \subset X$, called the *support* of v, such that

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

We denote by $\mathrm{supp}(v)^c = X \setminus \mathrm{supp}(v)$. 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 $\sum(\lambda\lambda_x)x$. We extend the order $<$ into the multiset order, still written $<$, on $\mathbb{K}X$: we have $u < v$ if for every $x \in \mathrm{supp}(u) \cap \mathrm{supp}(v)^c$, there exists $y \in \mathrm{supp}(v) \cap \mathrm{supp}(u)^c$ such that $y > x$.

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 the rewriting relation on $\mathbb{K}X$, still written $\xrightarrow{R}$, defined as follows:

$$\sum \lambda_x x + v \xrightarrow{R} \sum \lambda_x r_x + v, \tag{2}$$

whenever $\lambda_x \neq 0$, $x \xrightarrow{R} r_x \in R$ and $x \notin \mathrm{supp}(v)$.

Definition 2.1. A *local strategy* 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 $r_x < x$.

Suppose chosen such a local strategy h. Any vector v can be decomposed in a unique way as $\sum \lambda_x x + v'$, where $y \in \mathrm{supp}(v')$ implies that y is minimal for $<$, and $x \in \mathrm{supp}(v) \cap \mathrm{supp}(v')^c$ is not. We define a rewriting relation $\xrightarrow{h}$ as follows:

$$\sum \lambda_x x + v' \xrightarrow{h} \sum \lambda_x r_x + v', \tag{3}$$

where for every x, $h_x = x \xrightarrow{R} r_x$.

Definition 2.2. A vector v is said to be a *h-normal form* if it is a normal form for $\underset{h}{\longrightarrow}$.

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

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

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

Proposition 2.5. *The map H is a linear projector.*

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 $u \underset{h}{\longrightarrow} u'$ and $v \underset{h}{\longrightarrow} v'$, then we have $u + v \underset{h}{\longrightarrow} u' + v'$. Iterating $\underset{h}{\longrightarrow}$, we get $H(u + v) = H(H(u) + H(v)) = H(u) + H(v)$. $\qquad\square$

3 A confluence criterion

Definition 3.1. We say that R is *h-confluent* if for every rewrite rule $x \underset{R}{\longrightarrow} v \in R$, we have $x - v \in \ker(H)$.

Example 3.2. Let us take the same example as in 2.3. Then $H(x) = H(y) = z + t$, with $H(z) = z = H(y - t)$, and so R is h-confluent. Replacing the rule $z \underset{R}{\longrightarrow} y - t$ by $z \underset{R}{\longrightarrow} y$, we get $H(z) = z$ and $H(y) = z + t$, so R is not h-confluent anymore.

Proposition 3.3. *If R is h-confluent, then $u \underset{R}{\overset{*}{\longleftrightarrow}} v$ if and only if $u - v \in \ker(H)$.*

Proof. The relation $\underset{R}{\overset{*}{\longleftrightarrow}}$ is the closure of $\underset{R}{\longrightarrow}$ under transitivity, symmetry and sum. Since the relation $u - v \in \ker(H)$ is closed under these operations, we get one implication.

Reciprocally, if $u - v \in \ker(H)$ then by definition of H we have $u \underset{h}{\overset{*}{\longleftrightarrow}} v$, and in particular $u \underset{R}{\overset{*}{\longleftrightarrow}} v$. $\qquad\square$

Proposition 3.4. *If R is h-confluent, then $\underset{R}{\longrightarrow}$ is confluent.*

Proof. Let v, v_1, $v_2 \in \mathbb{K}X$ be such that $v \underset{R}{\overset{*}{\longrightarrow}} v_i$, for $i = 1$, 2. From Proposition 3.3, $v_1 - v_2$ belongs to $\ker(H)$, that is $H(v_1) = H(v_2)$. Denoting by u the common value, we get

$$
\begin{array}{ccc}
v & \overset{*}{\longrightarrow} & v_1 \\
{\scriptstyle *}\downarrow & & \downarrow{\scriptstyle *} \\
v_2 & \underset{*}{\longrightarrow} & u.
\end{array}
$$

$\qquad\square$

In Theorem 3.7, we introduce a confluence criterion when R satisfies 3.1. For that, we assume that R is equipped with a well-founded order $\prec$ satisfying the following decreasingness property:

Definition 3.5. We say that R is *locally h-confluent* if for every non minimal $x \in X$ and $r = x \xrightarrow{R} v$, then letting $h_x = x \xrightarrow{h} r_x$, we have the confluence diagram:

$$
\begin{array}{ccc}
x & \xrightarrow{\ r\ } & v \\
{\scriptstyle h_x}\downarrow & & \vdots {\scriptstyle *} \\
r_x & \cdots\!\xrightarrow{*}\!\cdots & v',
\end{array}
$$

where each rewriting step occurring in the dotted arrows are strictly smaller than r for $\prec$.

Example 3.6. Continuing with Example 2.3, let us define an order $\prec$ on R as follows:

$$(x \xrightarrow{R} y), (y \xrightarrow{R} z + t) \prec (z \xrightarrow{R} y - t).$$

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:

$$
\begin{array}{ccc}
x & \xrightarrow{R} & y \\
{\scriptstyle h_x}\downarrow & & \| \\
y & =\!\!= & y
\end{array}
\qquad
\begin{array}{ccc}
y & \xrightarrow{R} & z+t \\
{\scriptstyle h_y}\downarrow & & \| \\
z+t & =\!\!= & z+t
\end{array}
\qquad
\begin{array}{ccc}
z & \xrightarrow{R} & y-t \\
{\scriptstyle h_z}\| & & \downarrow {\scriptstyle R} \\
z & =\!\!= & z
\end{array}
$$

Our main result is the following.

Theorem 3.7. *If R is locally h-confluent, then R is h-confluent. In particular, $\xrightarrow{R}$ is confluent.*

Proof. We reason by induction on r. Looking at the square corresponding to r:

$$
\begin{array}{ccc}
x & \xrightarrow{\ r\ } & v \\
{\scriptstyle h_x}\downarrow & & \vdots {\scriptstyle *} \\
r_x & \cdots\!\xrightarrow{*}\!\cdots & v',
\end{array}
$$

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. $\qquad\square$

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

Theorem 3.8 ([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 the relation $x > y$ on X whenever $x \xrightarrow{R} v$ exists such that $y \in \mathrm{supp}(v)$. The induced order relation is well-founded. 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 $>$, $r_x < x$ so that h is a local strategy. Ordering the rewrite rules by their left hand sides makes R locally h-confluent. Theorem 3.7 finally shows that R is confluent. $\qquad\square$

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 Melliès. *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.