The diamond lemma for free modules

Cyrille Chenavier

Université Paris-Est Marne-la-Vallée

Abstract

We study rewriting systems over free modules, that is linear combinations of free generators with noninvertible coefficients. We provide a sufficient condition in terms of local confluence restricted to generators for the global rewrite relation to be confluent: this condition is formulated in terms of syzygies. When the coefficients belong to a domain, we equip the set of syzygies with a module structure, which provides a finer criterion: the local confluence has to be checked over a subset of syzygies, namely a generating set for the module structure.

1 Introduction

The diamond lemma for noncommutative polynomials was introduced by Bergman [4] for computing normal forms in noncommutative algebras using rewriting theory. The diamond lemma together with the works of Bokut [5] gave birth the theory of noncommutative Gröbner bases [7]. The latter provides applications in various areas of noncommutative algebra: study of embedding problems, this was the motivation of Bokut and Bergman, homological algebra [1, 6] or Koszul duality [2, 3], for instance.

The diamond lemma is based on the observation that the set of noncommutative polynomials admitting a unique normal form is a vector space. Hence, the set of noncommutative monomials being a linear basis of noncommutative polynomials, it is sufficient to check the local confluence property over these monomials. The diamond lemma asserts that when the so called overlapping/inclusion ambiguities (which correspond to critical pairs for term rewriting) are joinable, then every monomial admits a unique normal form, so that the global rewrite relation is confluent.

In this work, we are interested in the study of linear combinations of monomials where the coefficients in these combinations do not form a field. In this framework, elements with a unique normal form do not form a subspace anymore: consider for instance a rewrite rule $2y \longrightarrow x$, where the coefficients belong to the ring of integers $\mathbb{Z}$. Since 2 is not inverible in $\mathbb{Z}$, the monomial y is a normal form but $y + y = 2y$ is not a normal form! This observation has the following consequence: a rewrite relation such that every monomial admits a unique normal form has no reason to be confluent. For instance, consider the two rewrite rules $2y \longrightarrow -x$ and $2x \longrightarrow -y$. Then, one can show that for every $n \in \mathbb{Z}$, nx and ny admit a unique normal form, but $2x + 2y$ rewrites both in x and y which are not joinable!

In Theorem 4.5, we present an analogous version of the diamond lemma for rewriting systems over linear combinations with noninveritble coefficients. This work does not concern noncommutative polynomials but the more general case of *free left module* (formal definitions are given at the beginning of the next section): we do not take into account the structure of monomials. The adaptation of the criterion of Theorem 4.5 to noncommutative polynomials with noninvertible coefficients is a further work. Two other further works should be mentionned there: when the coefficients are $\mathbb{Z}$, the underlying module structure is the one of abelian groups, so that we wish to develop rewriting theory in this context. Another perspective is the study of the case where monomials are terms of the λ-calculus, which is the framework of *algebraic λ-calculus* [8].

2 Rewrite systems over free left modules

Throughout the paper, we fix a not necessarily commutative ring $\mathbf{R}$ and a set X. We denote by $\mathbf{R}X$ the free left module over X, that is the set of finite formal linear combinations of elements of X with coefficients in $\mathbf{R}$. Given such two elements $f = \sum r_x x$ and $g = \sum s_x x$, the sum $f+g$ is equal to $\sum (r_x + s_x)\, x$ and the left product of $r \in \mathbf{R}$ with f is equal to $\sum (r r_x)\, x$, where $r r_x$ is the product of r and r_x in $\mathbf{R}$.

A set $\mathscr{R}$ of rewrite rules over $\mathbf{R}X$ is said to be *left-monomial* if its elements are of the form $rx \longrightarrow f$, where r, x and f belong to $\mathbf{R}$, X and $\mathbf{R}X$, respectively. Our first objective is to extend $\mathscr{R}$ into a rewrite relation on $\mathbf{R}X$, still written $\longrightarrow$, in such a way that the congruence relation induced by $\longrightarrow$ is the left ideal generated by $\mathscr{R}$. In other words, we want to have the following equivalence:

$$f \overset{*}{\longleftrightarrow} g \iff f - g = \sum s\,(rx - f)\,, \tag{1}$$

with the sum over a finite set of indexes $(s,\ rx \longrightarrow f) \in \mathbf{R} \times \mathscr{R}$. For that, we choose representatives for every left class modulo r, so that every element $s \in \mathbf{R}$ admits a decomposition $r_1 r + r_2$ where r_2 is the chosen representative of the left class of s. The rewrite relation induced by $\mathscr{R}$ is defined by

$$(r_1 r + r_2)\, x + g \longrightarrow r_1 f + r_2 x + g, \tag{2}$$

where x belongs with a zero coefficient in the decomposition of g. The rewrite relation (2) satisfies the equivalence (1).

Example 2.1. When the ring $\mathbf{R}$ is left euclidean, we choose the representatives of left classes as the set of remainders for the euclidean division. Here, we present the explicit description of the rewrite relation for two examples of euclidean rings: the ring of integers $\mathbb{Z}$ and a commutative field $\mathbb{K}$. Consider a rewrite rule $nx \longrightarrow f$ over $\mathbb{Z}X$ and an integer m. By euclidean division, m is equal to $qn + r$. Then, $mx + g$ rewrites into $qf + rx + g$. A commutative field $\mathbb{K}$ is an euclidean ring where the euclidean division of μ by λ is $\mu = (\mu/\lambda)\,\lambda$. Then, the rewrite rule $\lambda x \longrightarrow f$ induces the rewrite step $\mu x + g \longrightarrow (\mu/\lambda)\, f + g$.

3 Compatible termination order

In the next section, we formulate the diamond lemma for rewrite relations over $\mathbf{R}X$ induced by a left-monomial set of rewrite rules $\mathscr{R}$. For that, we assume that the rewrite relation induced by $\mathscr{R}$ satisfies the following hypothesis:

$$\forall\ (rx \longrightarrow f,\ h) \in \mathscr{R} \times \mathbf{R}X,\ rx + h \downarrow f + h, \tag{3}$$

where $f \downarrow g$ means that f and g are joinable. Moreover, we also need that the rewrite relation is equipped with a *compatible termination order* defined in Definition 3.1. In this definition we use the following notation: given $f \in \mathbf{R}X$, we denote by $\mathrm{supp}\,(f)$ the set of elements of X which belong to the decomposition of f with nonzero coefficient.

Definition 3.1. A *termination order compatible* with $\mathscr{R}$ is a is a well-founded order $\preceq$ over $\mathbf{R}X$ such that for every $f,\ g,\ h \in \mathbf{R}X$ and every $a,\ b \in \mathbf{R}$ the following conditions are satisfied:

i. if $f \longrightarrow g$, then $g \preceq f$,

ii. if $g \preceq f$ and $\mathrm{supp}(h) \cap \mathrm{supp}(f) = \emptyset$, then $g + h \preceq f + h$,

iii. if $f \preceq ax$, $g \preceq by$ and $ax + by \neq 0$, then $f + g \preceq ax + by$,

iv. if $f \preceq ax$ and $ab \neq 0$, then $bf \preceq (ba)x$.

Example 3.2. Assume that that for every $rx \longrightarrow f \in \mathscr{R}$, x does not belong to $\mathrm{supp}(f)$. Then, one can show that $\mathscr{R}$ satisfies (3). Moreover, assume that X is equipped with a well-founded order $\preceq$. Then, we define the order on $\mathbf{R}X$, still written $\preceq$, as the restriction of the multi-set order to finite subsets of X: we have $g \prec h$ if $\mathrm{supp}(g) \cap \mathrm{supp}(h) \neq \emptyset$ and for every $x \in \mathrm{supp}(g)$ such that $x \notin \mathrm{supp}(h)$, there exists $y \in \mathrm{supp}(h)$ such that $y \notin \mathrm{supp}(g)$ and $x \prec y$. Then, we can show that $\preceq$ is compatible with $\mathscr{R}$.

The diamond lemma presented in the next section concerns rewrite systems satisfying the hypothesis (3) and equipped with a compatible termination order. In the sketch of proof of the diamond lemma, we we use Lemma 3.3. We need the following definition: given $f \in \mathbf{R}X$, we say that the rewrite relation $\longrightarrow$ is *locally confluent at* f if for every g, h, $k \in \mathbf{R}X$ such that $g \prec f$, $h \prec f$, $k \prec f$, $g \longrightarrow h$ and $g \longrightarrow k$, we have $h \downarrow k$.

Lemma 3.3. *Assume that $\mathscr{R}$ is equipped with a compatible termination order and satisfies the hypothesis (3) and that $\longrightarrow$ is locally confluent at f. For every f_1, f_2, g_1, $g_2 \preceq f$ such that $f_1 \downarrow g_1$ and $f_2 \downarrow g_2$, and for every $r \in \mathbf{R}$, we have $f_1 + f_2 \downarrow g_1 + g_2$ and $rf_1 \downarrow rg_1$.*

4 The diamond lemma

The diamond lemma [4] gives a criterion for testing local confluence over so called *critical pairs*. In Corollary 4.5, we formulate the diamond lemma for rewriting systems over free modules, which consists in testing local confluence for generating sets of *syzygies*. These generating sets are analogous to critical pairs in our framework.

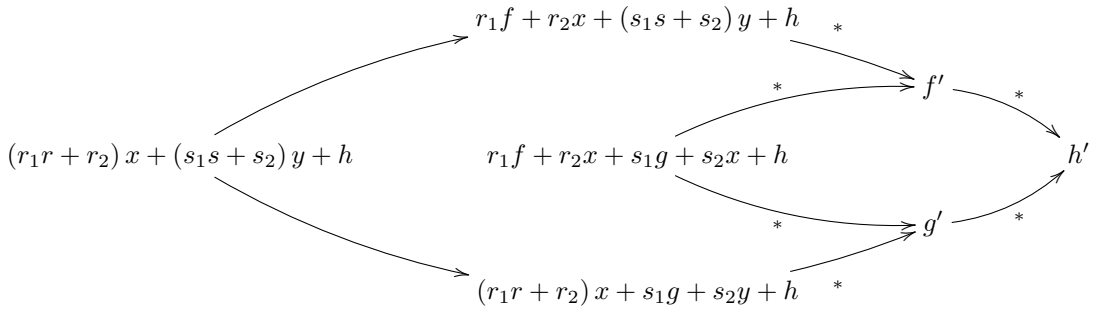
Definition 4.1. Let $p = (rx \longrightarrow f, sx \longrightarrow g)$ be a pair rewrite rules whose left-hand side are multiple of a common element x. A *syzygy* of p is a tuple (r_1, r_2, s_1, s_2) of elements of $\mathbf{R}$ such that r_2 and s_2 are the chosen representatives of their left classes modulo r ans s, respectively, and $r_1 r + r_2 = s_1 s + s_2$. The set of syzygies of p is written $\mathbf{syz}(p)$. Moreover, a syzygy (r_1, r_2, s_1, s_2) is said to be *confluent* if we have $r_1 f + r_2 x \downarrow s_1 g + s_2 x$.

Theorem 4.2. *Let $\mathscr{R}$ be a left-monomial set of rewrite rules satisfying hypothesis (3) and let $\preceq$ be a termination order compatible with $\longrightarrow$. The rewrite relation $\longrightarrow$ is confluent if and only if for every pair of rewrite rules $p = (rx \longrightarrow f, sx \longrightarrow g)$, every syzygy of p is confluent.*

Sketch of proof. Let $(r_1, r_2, s_1, s_2) \in \mathbf{syz}(p)$. Letting $h = (r_1 r + r_2)x = (s_1 s + s_2)x$, we observe that h rewrites into $r_1 f + r_2 x$ and $s_1 g + s_2 x$, which shows the direct implication.

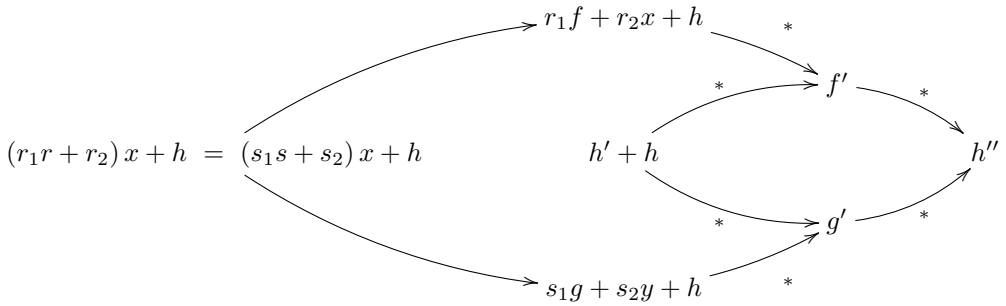
Assume that for every $p = (rx \longrightarrow f, sx \longrightarrow g)$ and for every $(r_1, r_2, s_1, s_2) \in \mathbf{syz}(p)$, we have $r_1 f + r_2 x \downarrow s_1 g + s_2 x$ and let us show that $\longrightarrow$ is confluent. The rewrite relation $\longrightarrow$ is terminating by definition of compatibility with a termination order, so that it is sufficient to show that it is locally confluent, or equivalently that is locally confluent at u for every u. We show the latter by induction on u: assume that $\longrightarrow$ is confluent at every $v \preceq u$ and that two rewrite rules $rx \longrightarrow f$ and $sy \longrightarrow g$ apply to u. Two cases have to be investigated according to $x \neq y$ or $x = y$ for proving that these two rewrite rules provide joinable terms.

First, if $x \neq y$, we let $u = (r_1 r + r_2)\, x + (s_1 s + s_2)\, y + h$ and we have the following confluence diagram:



The term f' (respectively g') and the two arrows coming to f' (respectively g') exist by hypothesis (3). By definition of a compatible rewrite order, we have $r_1 f + r_2 x + s_1 g + s_2 x + h \preceq (r_1 r + r_2)\, x + (s_1 s + s_2)\, y + h$, so that $\longrightarrow$ is confluent at $r_1 f + r_2 x + s_1 g + s_2 x + h$ by induction hypothesis, which gives h' and the two arrows coming to h'.

If $x = y$, we let $u = (r_1 r + r_2)\, x + h = (s_1 s + s_2)\, x + h$ and we have the following confluence diagram:



The tuple $(r_1,\ r_2,\ s_1,\ s_2)$ is a syzygy, so that there exists h' such that $r_1 f + r_2 x \xrightarrow{*} h' \xleftarrow{*} s_1 g + s_2 x$. By definition of a compatible termination order, $h' + h'$, $r_1 f + r_2 x$ and $s_1 g + s_2 x$ are smaller than u. The existence of f' and g' together with their coming arrows are consequences of Lemma 3.3. The existence of h'' and its coming arrows are due to the induction hypothesis. □

Our diamond lemma asserts that the confluence property has to be checked over subsets of syzygies instead of all the syzygies in the case where the ring $\mathbf{R}$ is a domain, that is $rs = 0$ if and only if $r = 0$ or $s = 0$. These subsets are generating set for an $\mathbf{R}$-module structure over syzygies given by the following operations:

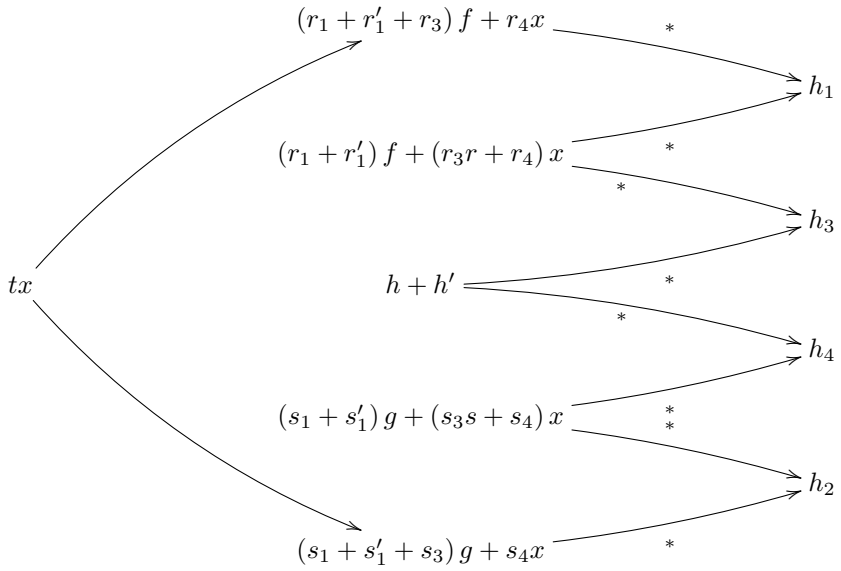
- **i.** let $\mathbf{syz}_1 = (r_1,\ r_2,\ s_1,\ s_2)$ and $\mathbf{syz}_2 = (r'_1,\ r'_2,\ s'_1,\ s'_2)$ be two syzygies of p. We write $r_2 + r'_2 = r_3 r + r_4$ and $s_2 + s'_2 = s_3 s + s_4$. Then, we get a new syzygy $\mathbf{syz}_1 + \mathbf{syz}_2 = (r_1 + r'_1 + r_3,\ r_4,\ s_1 + s'_1 + s_3,\ s_4)$ since we have $(r_1 + r'_1 + r_3)\, r + r_4 = (r_1 + r'_1)\, r + (r_2 + r'_2) = (s_1 + s'_1)\, s + (s_2 + s'_2) = (s_1 + s'_1 + s_3)\, s + s_4$.

- **ii.** Let $\mathbf{syz} = (r_1,\ r_2,\ s_1,\ s_2)$ be a syzygy of p and let $t \in \mathbf{R}$. We write $t r_2 = r_3 r + r_4$ and $t s_2 = s_3 s + s_4$. Then, we get a new syzygy $t\mathbf{syz} = (t r_1 + r_3,\ r_4,\ t s_1 + s_3,\ s_4)$ since we have $(t r_1 + r_3)\, r + r_4 = t\,(r_1 r + r_2) = t\,(s_1 s + s_2) = (t s_1 + s_3)\, s + s_4$.

Remark 4.3. If $\mathbf{R}$ is not a domain, then the element r_3 in **i.** and **ii.** is not unique, so that the sum of two syzygies and the product of a syzygy by an element of $\mathbf{R}$ is not well-defined.

Lemma 4.4. *Assume that* $\mathbf{R}$ *is a domain. Let* $p = (rx \longrightarrow f,\ sx \longrightarrow g)$, *let* $\mathbf{syz}_1 = (r_1,\ r_2,\ s_1,\ s_2)$ *and* $\mathbf{syz}_2 = (r'_1,\ r'_2,\ s'_1,\ s'_2)$ *be two confluent syzygies of* p *and let* $t \in \mathbf{R}$. *If* $\longrightarrow$ *is confluent at* $(r_1 + r'_1 + r_3)\, r + r_4 = (s_1 + s'_1 + s_3)\, s + s_4$ *(respectively* $(tr_1 + r_3)\, r + r_4 = (ts_1 + s_3)\, s + s_4$*), then* $\mathbf{syz}_1 + \mathbf{syz}_2$ *(respectively* $t\mathbf{syz}_1$*) is confluent.*

Sketch of proof. We only show that the sum of two confluent syzygies $\mathbf{syz}_1 + \mathbf{syz}_2$ is confluent. Let $h,\ h' \in \mathbf{R}X$ such that $r_1 f + r_2 x \xrightarrow{*} h \xleftarrow{*} s_1 g + s_2 x$ and $r'_1 f + r'_2 x \xrightarrow{*} h' \xleftarrow{*} s'_1 g + s'_2 x$. Letting $t = (r_1 + r'_1 + r_3)\, r + r_4 = (s_1 + s'_1 + s_3)\, s + s_4$, we have the following diagram:



The elements h_1, h_2 and their coming arrows are constructed using hypothesis (3). The elements h_3 and h_4 and their coming arrows are constructed using that $\longrightarrow$ is confluent at tx and Lemma 3.3. Finally, using again an inductive argument of confluence, we close the diagram and deduce that $\mathbf{syz}_1 + \mathbf{syz}_2$ is confluent.

Using similar arguments, we show that $t\mathbf{syz}_1$ is confluent, which concludes the proof. □

An adaptation of the proof of Theorem 4.2 using Lemma 4.4 provides our diamond lemma, formulated as follows:

Theorem 4.5. *Assume that* $\mathbf{R}$ *is a domain and that for every* $p = (rx \longrightarrow f,\ sx \longrightarrow g)$, *every element of a generating set of* $\mathbf{syz}(p)$ *is confluent. The rewrite relation* $\longrightarrow$ *is confluent.*

Example 4.6. Assume that $\mathbf{R}$ is a commutative field $\mathbb{K}$. For every $p = (\lambda x \longrightarrow f,\ \mu x \longrightarrow g)$, $\mathbf{syz}\,(p)$ is the vector space spanned by $(1/\lambda,\ 0,\ 1/\mu,\ 0)$. From Corollary 4.5, $\longrightarrow$ is confluent if and only if for every pair of rewrite rules $(\lambda x \longrightarrow f,\ \mu x \longrightarrow g)$, we have $f/\lambda \downarrow g/\mu$, which is equivalent to each $x \in X$ admits a unique normal form.

References

[1] David J. Anick. On the homology of associative algebras. *Trans. Amer. Math. Soc.*, 296(2):641–659, 1986.

[2] Roland Berger. Confluence and Koszulity. *J. Algebra*, 201(1):243–283, 1998.

[3] Roland Berger. Koszulity for nonquadratic algebras. *J. Algebra*, 239(2):705–734, 2001.

[4] George M. Bergman. The diamond lemma for ring theory. *Adv. in Math.*, 29(2):178–218, 1978.

[5] Leonid A. Bokut′. Imbeddings into simple associative algebras. *Algebra i Logika*, 15(2):117–142, 245, 1976.

[6] Yuji Kobayashi. Gröbner bases of associative algebras and the Hochschild cohomology. *Trans. Amer. Math. Soc.*, 357(3):1095–1124 (electronic), 2005.

[7] Teo Mora. An introduction to commutative and noncommutative Gröbner bases. *Theoret. Comput. Sci.*, 134(1):131–173, 1994. Second International Colloquium on Words, Languages and Combinatorics (Kyoto, 1992).

[8] Lionel Vaux. The algebraic lambda calculus. *Math. Structures Comput. Sci.*, 19(5):1029–1059, 2009.