Coassociativity of deconcatenation: a diagrammatic proof

RANNOU Pierre

September 30, 2009

1 Introduction

This paper is inspired by [Lod08]. In this book, Loday uses a diagramatic representation of operations and co-operations in bialgebras. We use this diagramatic syntax and rewriting techniques, especially confluence, to prove identities in algebras generated by a free semi-group or a free monoid.

2 Deconcatenation

Let A be an alphabet. The elements of A are called *letters*.

Definition 1 *: A^+ is the* free semi-group generated by A*. Its elements are nonempty lists of letters. They are called (nonempty)* words.

For instance, if our alphabet is $A = \{a,b\}$, then $aabba$ is a nonempty word in A^+.

Definition 2 *Concatenation $\cdot$ is the operation which, to each pair $(u,v) \in (A^+)^2$, associates the word formed by the letters of u followed by the letters of v.*

For instance, $abba \cdot bba = abbabba$.

Remark 1 *Concatenation is associative.*

For instance, $(ab \cdot b) \cdot a = abb \cdot a = abba = ab \cdot ba = ab \cdot (b \cdot a)$.

A $\mathbb{Z}$-*module* is an (additive) Abelian group.

Definition 3 *The free $\mathbb{Z}$-module generated by a set X is the set $\mathbb{Z}X$ whose elements are formal sums of elements of X with coefficients in $\mathbb{Z}$.*

For instance, if $X = \{x,y\}$, we have $x+y-x+y+y = y+y+y = 3y$ in $\mathbb{Z}X$.

Remark 2 *: If X is a finite set, $\mathbb{Z}X$ is isomorphic to $\mathbb{Z}^{|X|}$.*

For instance, $\mathbb{Z}X$ is isomorphic to $\mathbb{Z}^2$ in the above example.

Definition 4 *The* nonunital algebra *$\mathbb{Z}S$ generated by a semi-group S is the free $\mathbb{Z}$-module generated by S equipped with a multiplication $\cdot$ extending the multiplication of S and distributive over the sum.*

For instance, if $S = A^+$ with $A = \{a, b\}$, we have $(2abb - 3ba) \cdot aa = 2abbaa - 3baaa$ in $\mathbb{Z}S$.

Definition 5 *If P and Q are $\mathbb{Z}$-modules, the* tensor product *$P \otimes Q$ is the free $\mathbb{Z}$-module generated by elements of the form $p \otimes q$ with $p \in P$ and $q \in Q$, quotiented by the following equalities:*

- $(p + p') \otimes q = (p \otimes q) + (p' \otimes q)$;
- $p \otimes (q + q') = (p \otimes q) + (p \otimes q')$;
- $0 \otimes q = 0 = p \otimes 0$.

We write $P^{\otimes n}$ for the $\mathbb{Z}$-module $P \otimes \cdots \otimes P$ (n times).

Remark 3 $(\mathbb{Z}X)^{\otimes n} = \mathbb{Z}X^n$.

Hence, we get $p_1 \otimes \cdots \otimes p_n \in \mathbb{Z}X^n$ for any $p_1, \cdots, p_n \in \mathbb{Z}X$

We extend the multiplication of $\mathbb{Z}S$ to $\mathbb{Z}S^2$ as follows:

$$(u \otimes v) \cdot w = u \otimes (v \cdot w), \quad u \cdot (v \otimes w) = (u \cdot v) \otimes w.$$

Definition 6 *Let A be an alphabet and let $S = A^+$. Deconcatenation is the co-operation $\delta : \mathbb{Z}S \to \mathbb{Z}S^2$ defined as follows:*

$$\delta(w) = \sum_{w = u \cdot v} u \otimes v \text{ for any } w \in S.$$

For instance, $\delta(abaa) = a \otimes baa + ab \otimes aa + aba \otimes a$.

Alternatively, δ is recursively defined as follows:

- $\delta(a) = 0$ for any $a \in A$;
- $\delta(u \cdot v) = u \cdot \delta(v) + \delta(u) \cdot v + u \otimes v$ for any $u, v \in S$.

Remark 4 *$\delta(u) \cdot v$ consists of all terms of $\delta(u \cdot v)$ whose first component is a prefix of u and similarly, $u \cdot \delta(v)$ consists of all terms of $\delta(u \cdot v)$ whose second component is a postfix of v.*

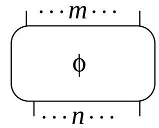
Theorem 1 *Deconcatenation is* coassociative*:*

$$\textit{If } \delta(w) = \sum_{w=u_i\cdot v_i} u_i \otimes v_i, \textit{ then}$$

$$\sum_{w=u_i\cdot v_i} \delta(u_i) \otimes v_i = \sum_{w=u_i\cdot v_i} u_i \otimes \delta(v_i).$$

3 Σ-diagrams

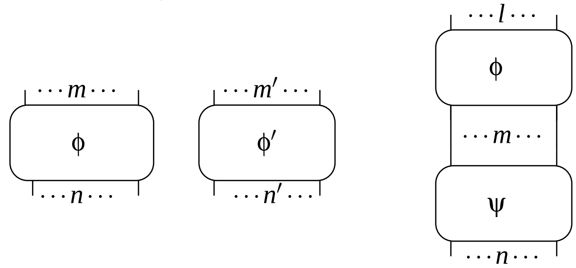
For any $m, n \in \mathbb{N}$, a diagram $\phi : m \to n$ is pictured as follows:



It is interpreted as a map $f : \mathcal{X}^m \to \mathcal{X}^n$ where $\mathcal{X}$ is some fixed set.

There are two operations on diagrams:

parallel composition sequential composition



They are interpretated as follows:

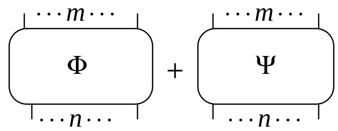
- if $f : \mathcal{X}^m \to \mathcal{X}^n$ is the interpretation of $\phi : m \to n$ and if $f' : \mathcal{X}^{m'} \to \mathcal{X}^{n'}$ is the interpretation of $\phi' : m' \to n'$, then $f \times f' : \mathcal{X}^{m+m'} \to \mathcal{X}^{n+n'}$ is the interpretation of the parallel composition of ϕ with ϕ';

- if $f : \mathcal{X}^l \to \mathcal{X}^m$ is the interpretation of $\phi : l \to m$ and if $g : \mathcal{X}^m \to \mathcal{X}^n$ is the interpretation of $\psi : m \to n$, then $g \circ f : \mathcal{X}^l \to \mathcal{X}^n$ is the interpretation of sequential composition of ϕ with ψ.

For more details on diagrams, see [Laf03].

Definition 7 *A* Σ-diagram $\Phi : m \to n$ *is a (finite) formal sum* $\Sigma k_i \phi_i$ *where the* $K_i \in \mathbb{Z}$ *and the* $\phi_i : m \to n$ *are diagrams with the same number of inputs and the same number of outputs.*

On Σ-diagrams, there is also a sum, which is pictured as follows:



Note that the Σ-diagrams Φ, Ψ have the same number of inputs and the same number of outputs. Similarly, we define the opposite $-\Phi : m \to n$ and the *null* Σ-diagram $0 : m \to n$.

A Σ-diagram $\Phi : m \to n$ is interpreted as a $\mathbb{Z}$-linear map $f : (\mathbb{Z}\mathcal{X})^{\otimes m} \to (\mathbb{Z}\mathcal{X})^{\otimes n}$. The interpretation of the operations is similar to the case of diagrams, except for parallel composition, which is interpreted by $\otimes$ instead of $\times$. The intrepretation of $+$ is straightforward.

Diagrams are built from atomic ones, called *gates*, using parallel and sequential composition. In particular, the identity diagram is picture as parallel wires. Σ-diagrams are built in the same way except that there are sums with coefficients.

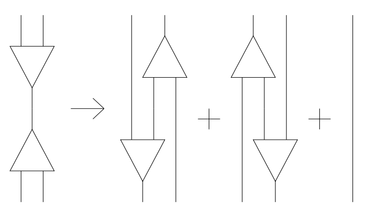
Definition 8 *A* rewrite rule *is of the form* $\phi \to \Psi$ *where* $\phi : m \to n$ *is a diagram and* $\Psi : m \to n$ *is a* Σ*-diagram.*

Now we asssume that $\mathcal{X}$ is the semi-group A^+ where A is an alphabet. The gates are:

concatenation $\cdot$ deconcatenation δ

From the recursive definition of deconcatenation, we deduce the following *interaction* rule:

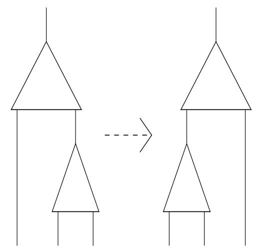
$$\delta(u \cdot v) = u \cdot \delta(v) + \delta(u) \cdot v + u \otimes v$$



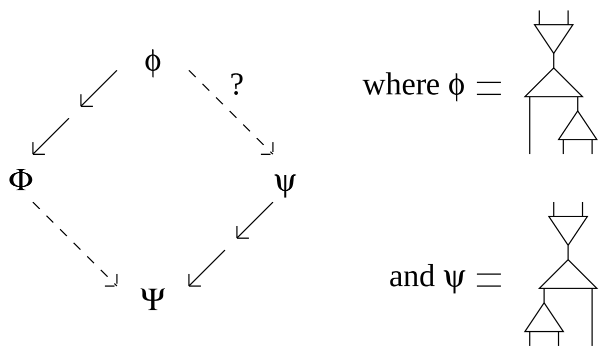
Similar kinds of rules are introduced in [Laf97] (interactions for diagrams) and [ER06] (interactions for Σ-diagrams).

4 Diagramatic proof of the theorem

We introduce the *coassociativity* rule:



The theorem is proved by induction on length of words. The structure of the proof is described by a confluence diagram:

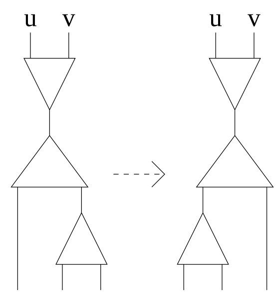


There are two kinds of arrow:

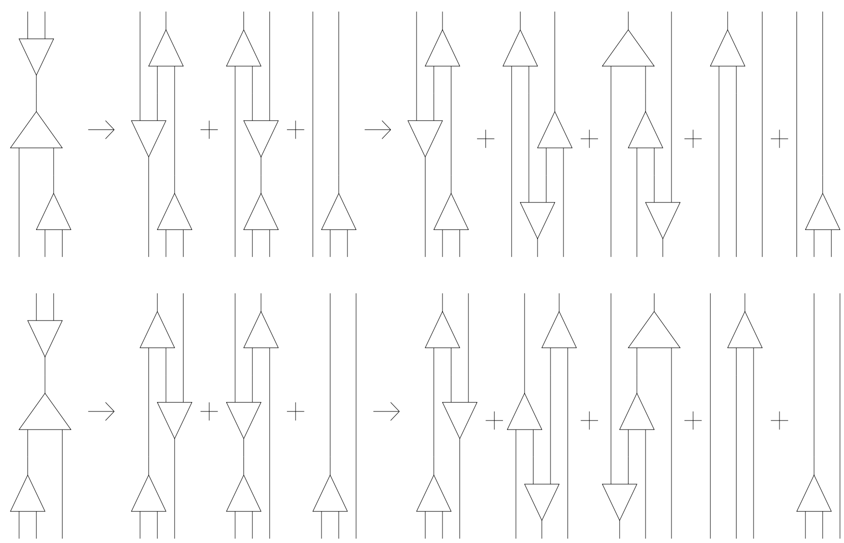
- broken arrow for coassociativity;
- solid arrow for interaction.

We want to prove that coassociativity holds for composed words. This means that the rule $\phi \to \psi$ holds. First, we apply interaction to ϕ to move deconcatenation gates above, and we get a Σ-diagram Φ. Then, by induction hypothesis, we apply coassociativity to Φ to get another Σ-diagram Ψ. Finally, we check that ψ reduces to Ψ by interaction. Consequently the four Σ-diagrams ϕ, Φ, Ψ, and ψ have the same interpretation and the rule $\phi \to \psi$ holds.

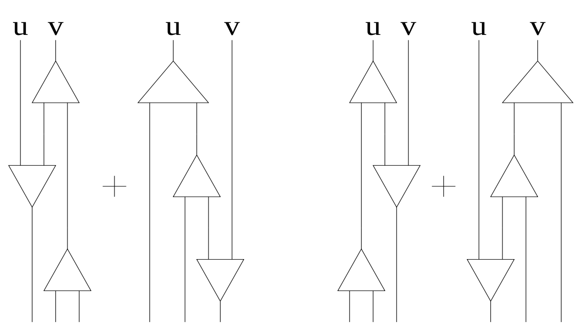
Coassociativity holds obviously for letters, since $\delta(a) = 0$ for any $a \in A$. Now, let u and v be two words in A^+ for which deconcatenation is coassociative. We want to prove that deconcatenation is coassociative for $w = u \cdot v$. In other words, the following reduction holds:



We apply interaction to the left and right members:



The two results differ only on two terms:



By induction hypothesis, we can apply coassociativity to the left Σ-diagram, and we get the right one.

5 Deconcatenation for monoids

Let A be an alphabet

Definition 9 *A^* is the* free monoid generated *by A. Its elements are those of A^+ and the* empty word ε.

Remark 5 *ε is the unit for concatenation.*

Definition 10 *The unital Z-algebra (or ring) $\mathbb{Z}M$, is the free $\mathbb{Z}$-module generated by the module M equipped with a multiplication $\cdot$ extending the multiplication of M and distributive over the sum.*

We write $M = A^*$, and $S = A^+$.

Definition 11 Full deconcatenation $\Delta : \mathbb{Z}M \to \mathbb{Z}M^2$*, is defined as follows:*

$$\Delta(w) = \sum_{w=u\cdot v} u \otimes v$$

Definition 12 Primitive deconcatenation $\delta : \mathbb{Z}M \to \mathbb{Z}M^2$ *extanding* $\delta : \mathbb{Z}S \to \mathbb{Z}S^2$*, is defined as follows:*

- $\delta(w) = \sum_{\substack{w=u\cdot v \\ u,v\neq\varepsilon}} u \otimes w$
- $\delta(\varepsilon) = -\varepsilon \otimes \varepsilon$

Remark 6 *The relation between the two deconcatenations is*

$$Delta(u) = \delta(u) + u \otimes \varepsilon + \varepsilon \otimes u.$$

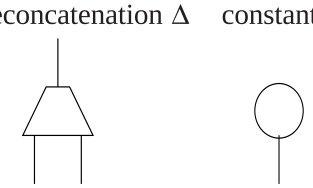
This remark explains why $\delta(\varepsilon) = -(\varepsilon \otimes \varepsilon)$:

$$\Delta(\varepsilon) = \delta(\varepsilon) + \varepsilon \otimes \varepsilon + \varepsilon \otimes \varepsilon = -\varepsilon \otimes \varepsilon + 2\varepsilon \otimes \varepsilon = \varepsilon \otimes \varepsilon$$

Theorem 2 *Full deconcatenation is coassociative.*

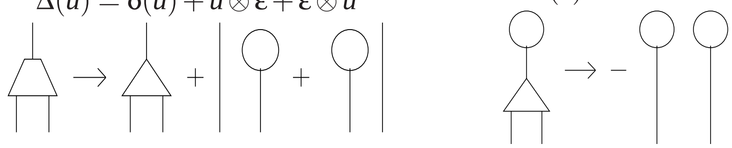
We have two new gates, one for full deconcatenation, and one for constant ε:

full deconcatenation Δ constant ε

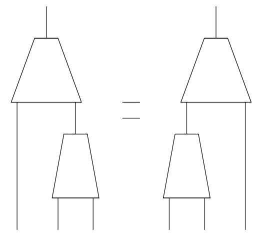


We have two new rules:

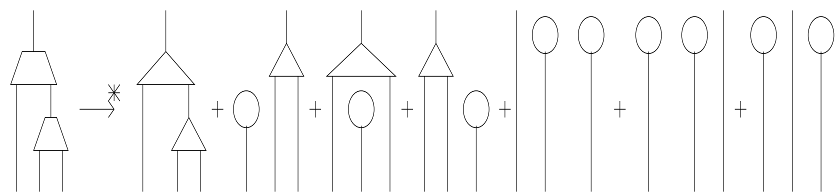
$\Delta(u) = \delta(u) + u \otimes \varepsilon + \varepsilon \otimes u$ $\qquad$ $\delta(\varepsilon) = -\varepsilon \otimes \varepsilon$

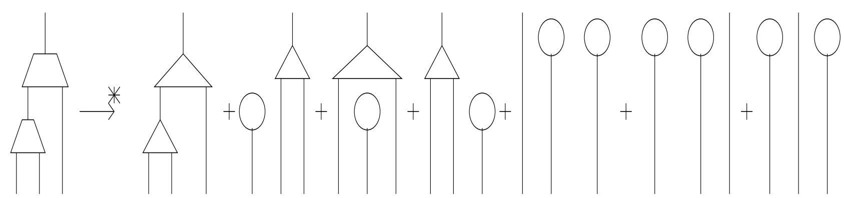


Coassociativity of full deconcatenation is pictured as follows:

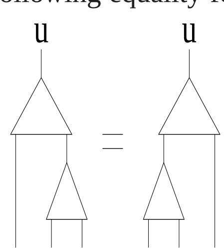


Reducing those diagrams by the new rules gives:





Hence, it remains to show the following equality for $u \in A^*$:



We have two cases:

- if $u = \varepsilon$, we get $\varepsilon \otimes \varepsilon \otimes \varepsilon$ in both cases;
- if $u \in A^+$, we apply theorem 1.

References

[ER06] T. Ehrhard and L. Regnier. Differential interaction nets. *TCS*, 364:166–195, 2006.

[Laf97] Y. Lafont. Interaction combinators. *Information and Computation*, 137:69–101, 1997.

[Laf03] Y. Lafont. Towards an algebraic theory of boolean circuits. *Pure and Applied Algebra*, 184:257–310, 2003.

[Lod08] J. L. Loday. *Generalized bialgebras and triples of operads*. Astérisque 320, 2008.