A localized version of the basic triangle theorem

G. Duchamp, Nihar Gargava

A localized version of the basic triangle theorem

G.H.E. Duchamp

University Paris 13, Sorbonne Paris City, 93430 Villetaneuse, France,

Nihar Gargava

École Polytechnique Fédérale de Lausanne, CH-1015, Lausanne, Switzerland

August 7, 2019 07-08-2019 17:06

Abstract

In this short note, we give a localized version of the basic triangle theorem, first published in 2011 (see [4]) in order to prove the independence of hyperlogarithms over various function fields. This version provides direct access to rings of scalars and avoids the recourse to fraction fields as that of meromorphic functions for instance.

1 Original theorem

Non commutative differential equations with left multiplier can be expressed in the context of general differential algebras. Notations about alphabets and (noncommutative) series are standard and can be found in [1].

Theorem 1.1 (Th 1 in [4]) *Let $(\mathscr{A},d)$ be a k-commutative associative differential algebra with unit ($ker(d)=k$, a field) and $\mathscr{C}$ be a differential subfield of $\mathscr{A}$ (i.e. $d(\mathscr{C})\subset\mathscr{C}$ and $k\subset\mathscr{C}$). Let X be some alphabet (i.e. some set) and we define $\mathbf{d}:\mathscr{A}\langle\langle X\rangle\rangle\to\mathscr{A}\langle\langle X\rangle\rangle$ to be the map given by $\langle\mathbf{d}(S)\mid w\rangle=d(\langle S\mid w\rangle)$. We suppose that $S\in\mathscr{A}\langle\langle X\rangle\rangle$ is a solution of the differential equation*

$$\mathbf{d}(S)=MS\ ;\ \langle S\mid 1_{X^*}\rangle=1_{\mathscr{A}} \tag{1}$$

where the multiplier M is a homogeneous series (a polynomial in the case of finite

X) of degree 1*, i.e.*

$$M = \sum_{x \in X} u_x x \in \mathscr{C}\langle\langle X \rangle\rangle \ . \qquad (2)$$

The following conditions are equivalent :

i) The family $(\langle S \mid w \rangle)_{w \in X^*}$ *of coefficients of* S *is free over* $\mathscr{C}$*.*

ii) The family of coefficients $(\langle S \mid y \rangle)_{y \in X \cup \{1_{X^*}\}}$ *is free over* $\mathscr{C}$*.*

iii) The family $(u_x)_{x \in X}$ *is such that, for* $f \in \mathscr{C}$ *and* $\alpha \in k^{(X)}$ *(i.e. supp*(α) *is finite)*

$$d(f) = \sum_{x \in X} \alpha_x u_x \Longrightarrow (\forall x \in X)(\alpha_x = 0) \ . \qquad (3)$$

iv) The family $(u_x)_{x \in X}$ *is free over k and*

$$d(\mathscr{C}) \cap \mathrm{span}_k \Big((u_x)_{x \in X} \Big) = \{0\} \ . \qquad (4)$$

Proof. For convenience of the reader, we enclose here the demonstration given in Th 1 [4].
(i)$\Longrightarrow$(ii) Obvious.
(ii)$\Longrightarrow$(iii)
Suppose that the family $(\langle S \mid y \rangle)_{y \in X \cup \{1_{X^*}\}}$ (coefficients taken at letters and the empty word) of coefficients of S were free over $\mathscr{C}$ and let us consider the relation as in (3)

$$d(f) = \sum_{x \in X} \alpha_x u_x \ . \qquad (5)$$

We form the polynomial $P = -f 1_{X^*} + \sum_{x \in X} \alpha_x x$. One has $\mathbf{d}(P) = -d(f) 1_{X^*}$ and

$$d(\langle S \mid P \rangle) = \langle \mathbf{d}(S) \mid P \rangle + \langle S \mid \mathbf{d}(P) \rangle = \langle MS \mid P \rangle - d(f) \langle S \mid 1_{X^*} \rangle = (\sum_{x \in X} \alpha_x u_x) - d(f) = 0 \qquad (6)$$

whence $\langle S \mid P \rangle$ must be a constant, say $\lambda \in k$. For $Q = P - \lambda.1_{X^*}$, we have

$$\mathrm{supp}(Q) \subset X \cup \{1_{X^*}\} \text{ and } \langle S \mid Q \rangle = \langle S \mid P \rangle - \lambda \langle S \mid 1_{X^*} \rangle = \langle S \mid P \rangle - \lambda = 0 \ .$$

This, in view of (ii), implies that $Q = 0$ and, as $Q = -(f + \lambda) 1_{X^*} + \sum_{x \in X} \alpha_x x$, one has, in particular, $supp(\alpha) = \emptyset$ (and, as a byproduct, $f = -\lambda$ which is indeed the only possibility for the L.H.S. of (3) to occur).
(iii)$\Longleftrightarrow$(iv)
Obvious, (iv) being a geometric reformulation of (iii).
(iii)$\Longrightarrow$(i)

Let $\mathscr{K}$ be the kernel of $P \mapsto \langle S \mid P\rangle$ (linear $\mathscr{C}\langle X\rangle \to \mathscr{A}$) i.e.

$$\mathscr{K} = \{P \in \mathscr{C}\langle X\rangle | \langle S \mid P\rangle = 0\} . \tag{7}$$

If $\mathscr{K} = \{0\}$, we are done. Otherwise, let us adopt the following strategy.
First, we order X by some well-ordering $<$ ([2] III.2.1) and X^* by the graded lexicographic ordering $\prec$ defined as follows

$$u \prec v \Longleftrightarrow |u| < |v| \text{ or } (u = pxs_1 \text{ , } v = pys_2 \text{ and } x < y). \tag{8}$$

It is easy to check that X^* is also a well-ordered by $\prec$. For each nonzero polynomial P, we denote by $lead(P)$ its leading monomial; i.e. the greatest element of its support $\mathrm{supp}(P)$ (for $\prec$).
Now, as $\mathscr{R} = \mathscr{K} \setminus \{0\}$ is not empty, let w_0 be the minimal element of $lead(\mathscr{R})$ and choose a $P \in \mathscr{R}$ such that $lead(P) = w_0$. We write

$$P = fw_0 + \sum_{u \prec w_0} \langle P \mid u\rangle u \text{ ; } f \in \mathscr{C} \setminus \{0\} . \tag{9}$$

The polynomial $Q = \frac{1}{f}P$ is also in $\mathscr{R}$ with the same leading monomial, but the leading coefficient is now 1; and so Q is given by

$$Q = w_0 + \sum_{u \prec w_0} \langle Q \mid u\rangle u . \tag{10}$$

Differentiating $\langle S \mid Q\rangle = 0$, one gets

$$\begin{aligned} 0 &= \langle \mathbf{d}(S) \mid Q\rangle + \langle S \mid \mathbf{d}(Q)\rangle = \langle MS \mid Q\rangle + \langle S \mid \mathbf{d}(Q)\rangle = \\ &\langle S \mid M^\dagger Q\rangle + \langle S \mid \mathbf{d}(Q)\rangle = \langle S \mid M^\dagger Q + \mathbf{d}(Q)\rangle \end{aligned} \tag{11}$$

with

$$M^\dagger Q + \mathbf{d}(Q) = \sum_{x\in X} u_x(x^\dagger Q) + \sum_{u \prec w_0} d(\langle Q \mid u\rangle) u \in \mathscr{C}\langle X\rangle . \tag{12}$$

It is impossible that $M^\dagger Q + \mathbf{d}(Q) \in \mathscr{R}$ because it would be of leading monomial strictly less than w_0, hence $M^\dagger Q + \mathbf{d}(Q) = 0$. This is equivalent to the recursion

$$d(\langle Q \mid u\rangle) = -\sum_{x\in X} u_x \langle Q \mid xu\rangle \text{ ; for } x \in X \text{ , } v \in X^*. \tag{13}$$

From this last relation, we deduce that $\langle Q \mid w\rangle \in k$ for every w of length $deg(Q)$ and, because $\langle S \mid 1_{X^*}\rangle = 1_{\mathscr{A}}$, one must have $deg(Q) > 0$. Then, we write $w_0 = x_0 v$ and compute the coefficient at v

$$d(\langle Q \mid v\rangle) = -\sum_{x\in X} u_x \langle Q \mid xv\rangle = \sum_{x\in X} \alpha_x u_x \tag{14}$$

with coefficients $\alpha_x = -\langle Q \mid xv\rangle \in k$ as $|xv| = \deg(Q)$ for all $x \in X$. Condition (3) implies that all coefficients $\langle Q \mid xv\rangle$ are zero; in particular, as $\langle Q \mid x_0 v\rangle = 1$, we get a contradiction. This proves that $\mathscr{K} = \{0\}$.
□

2 Localization

We will now establish the following extension of Theorem 1 in [4]. Let $(\mathscr{A}, d)$ be a k-commutative associative differential algebra with unit ($ker(d) = k$, a field). We consider a solution of the differential equation

$$\mathbf{d}(S) = MS \; ; \; \langle S \mid 1_{X^*}\rangle = 1_{\mathscr{A}} \tag{15}$$

where the multiplier M is a homogeneous series (a polynomial in the case of finite X) of degree 1, i.e.

$$M = \sum_{x\in X} u_x x \in \mathscr{A}\langle\langle X\rangle\rangle \; . \tag{16}$$

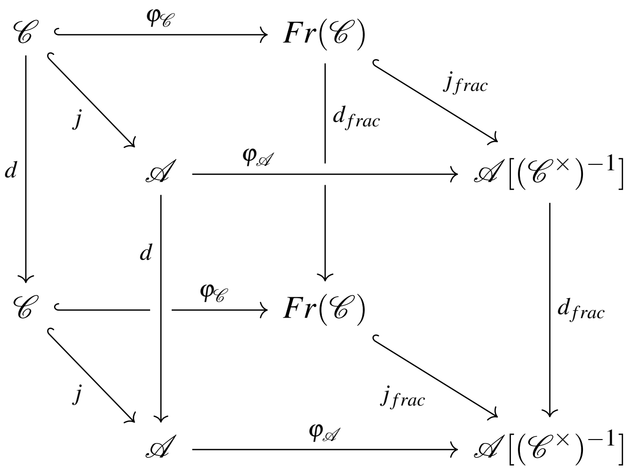
Proposition 2.1 (Thm1 in [4], Localized form) *Let $(\mathscr{A}, d)$ be a commutative associative differential ring ($\ker(d) = k$ being a field) and $\mathscr{C}$ be a differential subring (i.e. $d(\mathscr{C}) \subset \mathscr{C}$) of $\mathscr{A}$ which is an integral domain containing the field of constants. We suppose that, for all $x \in X$, $u_x \in \mathscr{C}$ and that $S \in \mathscr{A}\langle\langle X\rangle\rangle$ is a solution of the differential equation (15) and that $(u_x)_{x\in X} \in \mathscr{C}^X$.*
The following conditions are equivalent :

- *i) The family $(\langle S \mid w\rangle)_{w\in X^*}$ of coefficients of S is free over $\mathscr{C}$.*
- *ii) The family of coefficients $(\langle S \mid y\rangle)_{y\in X\cup\{1_{X^*}\}}$ is free over $\mathscr{C}$.*
- *iii') For all $f_1, f_2 \in \mathscr{C}$, $f_2 \neq 0$ and $\alpha \in k^{(X)}$, we have the property*

$$W(f_1, f_2) = f_2^2\Big(\sum_{x\in X} \alpha_x u_x\Big) \Longrightarrow (\forall x \in X)(\alpha_x = 0) \; . \tag{17}$$

where $W(f_1, f_2)$, the wronskian, stands for $d(f_1)f_2 - f_1 d(f_2)$.

Proof. (i.$\Longrightarrow$ ii.) being trivial, remains to prove (ii.$\Longrightarrow$ iii'.) and (iii'.$\Longrightarrow$ i.). To this end, we localize the situation w.r.t. the multiplicative subset $\mathscr{C}^\times := \mathscr{C} \setminus \{0\}$ as can be seen in the following commutative cube



(18)

We give here a detailed demonstration of the commutation which provides, in passing, the labelling of the arrows.

Left face. — Comes from the fact that $d(\mathscr{C}) \subset \mathscr{C}$, j being the canonical embedding.

Upper and lower faces. — We first construct the localization $\varphi_{\mathscr{A}} : \mathscr{A} \longrightarrow \mathscr{A}[(\mathscr{C}^{\times})^{-1}]$ w.r.t. the multiplicative subset $\mathscr{C}^{\times} \subset \mathscr{A} \setminus \{0\}$ (recall that $\mathscr{C}$ has no zero divisor). Now, from standard theorems (see [3], ch2 §2 remark 3 after Def. 2, for instance), we have

$$\ker(\varphi_{\mathscr{A}}) = \{u \in \mathscr{A} | (\exists v \in \mathscr{C}^{\times})(uv = 0)\} \tag{19}$$

For every intermediate ring $\mathscr{C} \subset \mathscr{B} \subset \mathscr{A}$, we remark that the composittion

$$\mathscr{B} \hookrightarrow \mathscr{A} \xrightarrow{\varphi_{\mathscr{A}}} \mathscr{A}[(\mathscr{C}^{\times})^{-1}]$$

realises the ring of fractions $\mathscr{B}[(\mathscr{C}^{\times})^{-1}]$ which can be identified with the subalgebra generated by $\varphi_{\mathscr{A}}(\mathscr{B})$ and the set of inverses $\varphi_{\mathscr{A}}(\mathscr{C}^{\times})^{-1}$. Applying this to $\mathscr{C}$, and remarking that $\mathscr{C}[(\mathscr{C}^{\times})^{-1}] \simeq Fr(\mathscr{C})$, we get the embedding j_{frac} and the commutation of upper and lower faces.

Front and rear faces. — From standard constructions (see e.g. the book [5]), there exists a unique $d_{frac} \in \mathfrak{Der}(\mathscr{A}[\mathscr{C}^{\times})^{-1}])$ such that these faces commute.

Right face. — Commutation comes from the fact that $d_{frac}j_{frac}$ and $j_{frac}d_{frac}$ coincide on $\varphi_{\mathscr{C}}(\mathscr{C})$ hence on $\varphi_{\mathscr{C}}(\mathscr{C}^{\times})$ and on their inverses. Therefore on all $Fr(\mathscr{C})$. From the constructions it follows that the arrows (derivations, morphisms) are arrows of k-algebras.

Now, we set

(i) $\bar{S} = \sum_{w\in X^*} \varphi_{\mathscr{A}}(\langle S \mid w\rangle) w \in \mathscr{A}[\mathscr{C}^{\times})^{-1}]\langle\langle X\rangle\rangle$

(ii) $\bar{M} = \sum_{x\in X} \varphi_{\mathscr{C}}(u_x) x \in \mathscr{A}[\mathscr{C}^{\times})^{-1}]\langle\langle X\rangle\rangle$

it is clear, from the commutations, that $(\mathscr{A}[\mathscr{C}^{\times})^{-1}]\langle\langle X\rangle\rangle, \mathbf{d}_{frac})$ where $\mathbf{d}_{frac}$ is the extension of d_{frac} to the series, is a differential algebra and that

$$\mathbf{d}_{frac}(\bar{S}) = \bar{M}\bar{S}\ ;\ \langle \bar{S} \mid 1\rangle = 1 \tag{20}$$

we are now in the position to resume the proofs of (ii.$\Longrightarrow$ iii'.) and (iii'.$\Longrightarrow$ i.).
ii.$\Longrightarrow$ iii'.) Supposing (ii), we remark that the family of coefficients

$$(\langle \bar{S} \mid y\rangle)_{y\in X\cup\{1_{X^*}\}}$$

is free over $\mathscr{C}$ [1] . Indeed, let us suppose a relation

$$\sum_{y\in X\cup\{1_{X^*}\}} g_y \langle \bar{S} \mid y\rangle = 0 \text{ with } (g_y)_{y\in X\cup\{1_{X^*}\}} \in \mathscr{C}^{(X\cup\{1_{X^*}\})} \tag{21}$$

this relation is equivalent to

$$\varphi_{\mathscr{A}}(\sum_{y\in X\cup\{1_{X^*}\}} g_y \langle S \mid y\rangle) = 0 \tag{22}$$

which, in view of (19), amounts to the existence of $v \in \mathscr{C}^{\times}$ such that

$$0 = v(\sum_{y\in X\cup\{1_{X^*}\}} g_y \langle S \mid y\rangle) = \sum_{y\in X\cup\{1_{X^*}\}} v g_y \langle S \mid y\rangle \tag{23}$$

which implies $(\forall y \in X\cup\{1_{X^*}\})(v g_y = 0)$ but, $\mathscr{C}$ being without zero divisor, one gets

$$(\forall y \in X\cup\{1_{X^*}\})(g_y = 0) \tag{24}$$

which proves the claim. This implies in particular, by chasing denominators, that the family of coefficients

$$(\langle \bar{S} \mid y\rangle)_{y\in X\cup\{1_{X^*}\}}$$

is free over $Fr(\mathscr{C})$. This also implies [2] that $\varphi_{\mathscr{A}}$ is injective on

$$span_{\mathscr{C}}(\langle S \mid y\rangle)_{y\in X\cup\{1_{X^*}\}} \tag{25}$$

[1] As $\varphi_{\mathscr{C}}$ is injective on $\mathscr{C}$ we identify $\varphi_{\mathscr{C}}(\mathscr{C})$ and $\mathscr{C}$, this can be unfolded on request, of course.

[2] And indeed is equivalent under the assumption of (ii).

To finish the proof that (ii.$\Longrightarrow$ iii'.), let us choose $f_1, f_2 \in \mathscr{C}$ with $f_2 \neq 0$ and set some relation which reads

$$W(f_1, f_2) = f_2^2(\sum_{x\in X} \alpha_x u_x) \tag{26}$$

with $\alpha \in k^{(X)}$, then

$$(\sum_{x\in X} \alpha_x u_x) = \frac{W(f_1, f_2)}{f_2^2} = d_{frac}(\frac{f_1}{f_2}) \tag{27}$$

but, in view of Th1 in [4] applied to the differential field $Fr(\mathscr{C})$, we get $\alpha \equiv 0$.
(iii'.$\Longrightarrow$ i.) The series $\bar{S}$ satisfies

$$\mathbf{d}(\bar{S}) = \bar{M}\bar{S} \; ; \; \langle \bar{S} \mid 1_{X^*} \rangle = 1_{\mathscr{A}[\mathscr{C}^\times)^{-1}]} = 1_{Fr(\mathscr{C})} \tag{28}$$

and remarking that

(i) all f in the differential field $Fr(\mathscr{C})$ can be expressed as $f = \frac{f_1}{f_2}$

(ii) condition (iii') for $(S, \mathscr{A}, \mathscr{C}, d, X)$ implies condition (iii) for $(\bar{S}, \mathscr{A}[\mathscr{C}^\times)^{-1}], Fr(\mathscr{C}), d_{frac}, X)$ [3] which, in turn, implies the $Fr(\mathscr{C})$-freeness of $(\langle \bar{S} \mid w \rangle)_{w\in X^*}$ hence its $\mathscr{C}$-freeness and, by inverse image [4] the $\mathscr{C}$-freeness of $(\langle S \mid w \rangle)_{w\in X^*}$.

□

Remark 2.2 It seems reasonable to think that the whole commutation of the cube could be understood by natural transformations within an appropriate category. If yes, this will be inserted in a forthcoming version.

References

[1] .– *J. Berstel, C. Reutenauer.– Rational series and their languages*, Springer Verlag, 1988.

[2] N. Bourbaki.– *Theory of Sets*, Springer-Verlag Berlin and Heidelberg GmbH & Co. K; (2nd printing 2004)

[3] N. Bourbaki.– *Commutative Algebra: Chapters 1-7*, Springer (1998)

[3] Once again we identify, with no loss, $k \subset \mathscr{C}$, the latter being idetified with its image through $\varphi_{\mathscr{A}[\mathscr{C}^\times)^{-1}]}$.
[4] If the image (through a A-linear arrow) of a family is A-free then the family itself is A-free.

[4] .– *M. Deneufchâtel, G.H.E. Duchamp, Hoang Ngoc Minh, A.I. Solomon*.– *Independence of hyperlogarithms over function fields via algebraic combinatorics*, in Lecture Notes in Computer Science (2011), Volume 6742/2011, 127-139.

[5] .– *M. van der Put, M. F. Singer*.– *Galois Theory of Linear Differential Equations*, Springer (2003)