# Congruences compatible with the shuffle product*

Gérard Duchamp and Jean-Gabriel Luque **

No Institute Given

## 1 Introduction

Partially commutative structures share many nice combinatorial properties with their free counterpart [8, 19, 21]. They have also been use intensively in the computer science area [12, 13]. These structures can be rapidly describded as being presented with

$$< A;\ \{[a,b]\}_{(a,b)\in\theta} >_{\mathbf{cat}}$$

where $A$ is a set of generators (an alphabet), $\theta \in A^2$ an unoriented grah without loop, **cat** a suitable category (Monoid, Group, $K$-associative algebras, Lie algebras) and $[a,b]$ expresses the fact that $a$ and $b$ commute in the structures of **cat**.

The simplest (and already bearing all the combinatorial power [10]) of these structures is the partially commutative monoid $< A;\ \{ab = ba\}_{(a,b)\in\theta} >_{\mathbf{Mon}}$ (denoted $M(A,\theta)$) whose algebra over a semiring $K$ ($K < A,\theta > := K[M(A,\theta)]$) is called the algebra of partially commutative polynomials.
It is well known that, if a congruence $\equiv$ (i.e. an equivalence over the free monoid $A^*$) is generated by commutations (i.e. is the kernel of a natural morphism $nat : A^* \to M(A,\theta)$) then the shuffle product of two classes is a class-sum ① (This can be verified by hand in the general case and in case $K$ is a ring, is related to the fact that $K < A,\theta >$ is the envelopping algebra of the - free - Lie algebra generated by the letters [20]).

This amounts to say that, if two series $S_i = \sum_{w\in A^*}(S_i, w)w;\ i = 1,2$ are $\equiv$-satured (i.e. are constant on every class of $\equiv$) then their shuffle product $S_1 \sqcup\!\sqcup S_2$ is again saturated, which in turn reflects, by duality, the fact that there exists a coproduct $c_\equiv : K[A^*/_\equiv] \to K[A^*/_\equiv] \otimes K[A^*/_\equiv]$ such that the square

$$\begin{tikzcd} K < A > \arrow[r, "c"] \arrow[d, "nat"'] & K < A > \otimes K < A > \arrow[d, "nat \otimes nat"] \\ K[A^*/_\equiv] \arrow[r, "c_\equiv"] & K[A^*/_\equiv] \otimes K[A^*/_\equiv] \end{tikzcd} \qquad (1)$$

is commutative ($c$ being the coproduct dual to the shuffle). The converse was shown by Duchamp and Krob [7] with the restriction that $K$ be a ring of characteristic 0.

The aim of our paper is to discuss the property defined by (1) which will be called, throughout, the paper $K - \sqcup\!\sqcup$ compatibility.
Let us mention here that only the shuffle product is worth and give rise to such an

* Partially supported by the Program Support of MENRT.

** LIFAR, Faculté des Sciences et des Techniques, 76821 Mont-Saint-Aignan CEDEX, France. Emails: Gerard.Duchamp,Jean-Gabriel.Luque@univ-rouen.fr

① The structure constants are the partially commutative subword coefficients [5, 19].

interesting discussion as the compatibility with the other classical rational laws (sum, external product, star and also Cauchy, Hadamard and infiltration products [6]) over series give weaker or equivalent results (for full details see Commentary 3). The structure of the paper is the following.

First (section 2), we prove that the result of DUCHAMP and KROB holds in almost every case, the only exception being the rings of prime characteristic for which differences of words that are primitive elements can occur. The iteration of these adjunctions exhausts every finitely generated congruence. More formally, we have:

**Theorem 1** *Let $\equiv$ be a finitely generated congruence on $A^*$ which is $K-\sqcup\!\sqcup$ compatible then*

1. *If $K$ is not a ring or if the characteristic of $K$ ($ch(K)$) is not prime then $A^*/_\equiv$ is a partially commutative monoid.*
2. *If $ch(K) = p$ is prime, then it exists $R \subset A^* \times A^*$ finite with a partition $R = \bigcup_{i\in[1,n]} R_i$ such that for $i \in [1,n]$, $R_i$ consists in pairs $(u,v) \in R$ such that (the image of) $u - v$ is primitive in $K[A^*/_{\equiv_{\bigcup_{j=1}^{i-1} R_j}}]$.*

In a second part (section 3), we investigate some properties of the new family of monoids (cancellability, gradation, embeddability in a group, roots ).

**Theorem 2** *Let $\equiv$ be a finitely generated congruence on $A^*$ which is $K-\sqcup\!\sqcup$ compatible and generated by relators of the form $u \equiv v$ where $u - v$ is primitive, then we have the following altenative.*

1. *The monoid $A^*/_\equiv$ is not cancellable.*
2. *It exists a weight function $\omega : A \to \mathbb{N}^*$ for which $\equiv$ is homogeneous and $A^*/_\equiv$ embeds in a group.*

# 2 Compatibility with the shuffle product

This section is devoted to study the $K-\sqcup\!\sqcup$ compatibility of a congruence. First, we address the problem in the general case ($K$ is a semiring) and give some results common to all the semirings. We treat the case when $K$ is the boolean semiring and when it is a ring, we develop some results about the primitive polynomials which are useful to prove our theorem 1. In the last paragraph of this section, we sketch the proof.

## 2.1 General properties

In the sequel we will denote $\mathbb{N}.1_K$ the subsemiring of a semiring $K$ generated by $1_K$. We first remark that a congruence is $K-\sqcup\!\sqcup$ compatible if and only if it is $\mathbb{N}.1_K-\sqcup\!\sqcup$ compatible. The property below is straightforward from this observation.

**Lemme 3** *Let $\phi : K_1 \to K_2$ be a morphism of semirings then*

1. *If $\equiv$ is $K_1-\sqcup\!\sqcup$ compatible then it is $K_2-\sqcup\!\sqcup$ compatible.*
2. *If $\phi$ is into the converse holds.*

This shows that, in order to study the $K - ⧢$ compatibility of a congruence, it suffices to study its $\mathbb{N}.1_K - ⧢$ compatibility.

**Remark 1** *If $\equiv$ is $\mathbb{N} - ⧢$ compatible then it is $K - ⧢$ compatible for each semiring $K$.*

The properties below will be useful in the sequel, their proof are easy and we omit them.

**Lemme 4** *1. If $\equiv_1$ and $\equiv_2$ are $K - ⧢$ compatible congruences then $\equiv_1 \vee \equiv_2$ and $\equiv_1 \wedge \equiv_2$ also are (supremum and infimum are defined with respect to relation "is coarser than").*

2. *Let $R$ be a relator on $A^*$. The congruence $\equiv_R$ generated by $R$ is $K - ⧢$ compatible if and only if for each pair $(w_1, w_2) \in R$ we have $c(w_1) \equiv_R^{\otimes 2} c(w_2)$.*
3. *Let $u \in A^+$ and $n$ be the maximal integer such that $u$ can be written as $u = u_1 a^n$ with $a \in A$. Then for each $K$ we have $(c(u), u_1 \otimes a^n) = 1$.*
4. *Each congruence generated by relators of the form $a \equiv b$ (LI) or $dc \equiv cd$ (LC) with $a, b, c, d \in A$ is $K - ⧢$ compatible.*
5. *Let $B \subseteq A$ be a subalphabet of $A$. If $\equiv$ is $K - ⧢$ compatible then its restriction to $B^*$ is.*

## 2.2 The boolean case

This paragraph deals with the case when $K = \mathbb{B}$ (the boolean semiring). The $\mathbb{B} - ⧢$ compatibility is completely characterized by the following proposition.

**Proposition 5** *A congruence is $\mathbb{B} - ⧢$ compatible if and only if it is generated by relators like $a \equiv 1$ (LE), $a \equiv b$ (LI) or $ab \equiv ba$ (LC), with $a, b \in A$.*

**Sketch of the proof** The "if" part is immediate using properties (1), (2) and (4) of lemma 4.
We prove now the converse. Let $A' = \{a \in A | a \not\equiv 1\}$ and $S \subseteq A'$ be a section of $\equiv \cap (A^* \times A^*)$. Let (LE) be the set $\{(a, 1)\}_{a \in A - A'}$ and (LI$_S$) the set $\{(a, b)\}_{a \equiv b, a \in S, b \in A' - S}$, it is easily seen that $\equiv$ is generated by $\equiv_S := \equiv \cap (S^* \times S^*)$, (LE) and (LI$_S$). It suffices now to show that $\equiv_S$ is generated by (LC) relators (property (5) of lemma 4 implies that $\equiv_S$ is $\mathbb{B} - ⧢$ compatible). We proceed in two steps.

1. We prove first that $\equiv_S$ is multihomogeneous. Suppose it were not the case and consider $\equiv_m$ the multihomogeneous part of $\equiv_S$ (i.e. the meet of $\equiv_S$ and the multihomogeneity equivalence). We take a pair $(u, v)$ such that $u \equiv_S v$ and $u \not\equiv_m v$ with $u$ minimal. Setting $u = u_1 a$ with $a \in A$, the minimality of $|u|$ implies that it exists two complementary words $v_I$ and $v_J$ of $v$ such that $v_I \equiv_m u_1$ and $v_J = a$. Then, $v \equiv_m v_I v_J \equiv_m u_1 a = u$, which contradicts our hypothesis and proves the multihomogeneity of $\equiv_S$.
2. We consider $\equiv_\theta$ the congruence generated by the pairs $(ab, ba)$ with $a, b \in A$ and $ab \equiv_S ba$. We prove first that if $u \equiv_S v$ and $v \in A^* a$ then it exists $u_1 \equiv_\theta v$ such that $u_1 \in A^* a$, by induction on $|u|$.

Suppose $\equiv_S \neq \equiv_\theta$ and consider a pair $(u, v)$ of words such that $u \equiv_s v$ and $u \not\equiv_\theta v$ with $|u| + |v|$ minimal and a letter $a \in S$ such that $u \equiv_\theta u_1 a^r$ and $v \equiv_\theta v_1 a^s$ with $r, s \neq 0$ and $r + s \geq 2$ maximal. We show that $r = s$ and $u_1 \equiv_\theta v_1$ which implies $u \equiv_\theta v$, contradicts our hypothesis and shows the result.

■

### 2.3 Primitive elements

We suppose now that $K$ is a ring and we examine the link between $K - \sqcup\!\sqcup$ compatibilty and primitivity of polynomials.

**Definition 6** *Let $K$ be a ring and $\equiv$ be a $K - \sqcup\!\sqcup$ compatible congruence. A polynomial $P \in K[A^*/_\equiv]$ is called primitive if and only if $c_\equiv(P) = P \otimes 1 + 1 \otimes P$.*

As usual we have the following property.

**Proposition 7** *The submodule $Prim(K[A^*/_\equiv])$ of primitive polynomials endowed with the Lie bracket $[\quad , \quad]$ is a Lie algebra.*

We suppose now that $\equiv = \equiv_\theta$ is a relation generated by commutations. Recall first that the free partially commutative monoid is

$$\mathbb{M}(A, \theta) = < A | \{ab = ba\}_{(a,b) \in \theta} > .$$

The monoid $\mathbb{M}(A, \theta)$ can be totally ordered by a relation $<_{std}$ in the following way :

$$t <_{std} t' \Leftrightarrow std(t) <_{lex} std(t')$$

where $std(t)$ denotes the maximal word for the lexicographical order in the commutation class $t$. Using this order Lalonde [16, 15] has generalized the notion of Lyndon word : the set of Lyndon traces is defined as the set of connected and primitive② traces minimal in their conjugate classes and denoted $Ly(A, \theta)$. In his thesis Lalonde has shown the following theorem.

**Theorem** *(Lalonde) Let $\Lambda : Ly(A, \theta) \Rightarrow L_K(A, \theta)$ (the - free - Lie algebra generated by the letters in $K < A, \theta >$) be the mapping defined by*

$$\begin{cases} \Lambda(a) = a & \text{if } a \in A \\ \Lambda(l) = [\Lambda(l_1), \Lambda(l_2)] & \text{if } l = l_1 l_2,\ l_1, l_2 \in Ly(A, \theta) \text{ and} \end{cases}$$

*then $(\Lambda(l))_{l \in Ly(A,\theta)}$ is a basis of $L_K(A, \theta)$ as a $K$ module and for each Lyndon trace $l \in Ly(A, \theta)$ one has*

$$\Lambda(l) = l + \sum_{t >_{std} l} \beta_t t$$

We have the following proposition.

② In the sense of traces (i.e. a trace is primitive if it can not be written as the power of an other trace)

**Proposition 8** *Let $p$ be a prime integer and $u-v$ be a primitive polynomial of $\mathbb{Z}/p\mathbb{Z} < A, \theta >$ such that $u, v \in \mathbb{M}(A, \theta)$. Then $u = a^{p^\alpha}$ and $v = b^{p^\beta}$ or $u = a^{p^\alpha} b^{p^\beta}$ and $v = b^{p^\beta} a^{p^\alpha}$.*

**Sketch of the proof** We denote $L^{(p)}_{\mathbb{Z}/p\mathbb{Z}}(A, \theta)$ the Lie algebra of the primitive polynomials.

a) We first prove that the only monomials $u$ which are primitive are of the form $u = a^{p^\alpha}$.
b) We show that if $a_1 \cdots a_n - b_1 \cdots b_m$ is a primitive polynomial then we have $a_1 \cdots a_n = a_n \cdots a_1$ and $b_1 \cdots b_m = b_m \cdots b_1$ or $n = m$ and $a_1 \cdots a_n = b_n \cdots b_1$[3].
c) Using Lalonde's theorem we prove that the set $\{(\varLambda(l))^{p^e}\}$ generates $L^{(p)}_{\mathbb{Z}/p\mathbb{Z}}(A, \theta)$ as a $K$-module and we write $u - v$ in the form

$$u - v = l^{p^e} + \sum_{t > l^{p^e}} \gamma_t t.$$

Without restriction we can consider that $u <_{std} v$ and then $u = l^{p^e}$. According to (b) we consider two cases
  i) If $u = \overline{u}$ and $v = \overline{v}$, we prove that $u$ and $v$ are primitive and by (a) we get the claim.
  ii) Suppose that $u = \overline{v}$. Remarking that, if a power $l^e$ $(e > 0)$ is not of the form $a^\alpha$ or $a^\alpha b^\beta$, one has $l^e = awb^\alpha c^\beta$ with $a, b, c \in A$, $w \in \mathbb{M}(A, \theta)$, $\alpha, \beta > 0$ with $\alpha + \beta$ maximal, $c \neq b$ and $a \neq c$. In this case $(c(l^e), awc^\beta \otimes b^\alpha) = 1$ (by property (3) of lemma 4) and $(c(\overline{l^e}), awc^\beta \otimes b^\alpha) = 0$, which proves that if $u \neq a^\alpha b^\beta$ and $u \neq a^\alpha$, $u-v$ is not primitive. Solving the equations $c(a^\alpha - b^\beta) = (a^\alpha - b^\beta) \otimes 1 + (a^\alpha - b^\beta) \otimes 1$ and $c(a^\alpha b^\beta - b^\beta a^\alpha) = (a^\alpha b^\beta - b^\beta a^\alpha) \otimes 1 + 1 \otimes (a^\alpha b^\beta - b^\beta a^\alpha)$, $\alpha$ and $\beta$ are necessarily two powers of $p$.

■

### 2.4 Structure of compatible congruences

This paragraph is devoted to sketch the proof of theorem 1. We recall it here.

**Theorem 1** *Let $\equiv$ be a $K - \sqcup\!\sqcup$ compatible and finitely generated congruence on $A^*$. Then*

1. *If $K$ is not a ring or if the characteristic of $K$ ($ch(K)$) is not prime then $A^*/_\equiv$ is a partially commutative monoid.*
2. *If $ch(K) = p$ is prime, then it exists $R \subset A^* \times A^*$ finite with a partition $R = \bigcup_{i \in [1,n]} R_i$ such that for $i \in [1, n]$, $R_i$ consists in pairs $(u, v)$ such that (the image of) $u - v$ is primitive in $K[A^*/_{\equiv_{\bigcup_{j=1}^{i-1} R_j}}]$.*

[3] In the sequel, the mirror image of a trace $u$ will be denoted by $\overline{u}$.

**Sketch of the proof** We prove first (2). Suppose that $A$ is finite (one can restrict ourselves to the letters of the words of the relators), let $K$ be a ring and $\equiv$ be a finitely generated congruence on $A^*$ which is $K - ⊔⊔$ compatible. It is always possible to derive a finite set of relators $R \subset A^* \times A^*$ closed in the following sense

$$u \equiv v \text{ and } \max\{u, v\} < max\{\max\{u', v'\} | (u', v') \in R\} \Longrightarrow (u, v) \in R.$$

We construct $(R_i)_{i\in[0,n]}$ in the following way.

1. We set $S_0 = R_0 = \emptyset$.
2. For each $i > 0$, $R_i$ is the set of the pairs $(u, v) \in R - \bigcup_{j\leq i-1} S_j$ such that $u - v$ is primitive in $K[A^*/_{\equiv_{\bigcup_{j\leq i-1} R_j}}]$.
3. The relator $S_i$ is the set of the pairs $(u, v) \in R - \bigcup_{j\leq i-1} R_j$ such that $u \equiv_{R_i} v$.

One can prove that this process ends, remarking that for each $i$ if $\equiv_{\bigcup_{j\leq i-1} R_j} \neq \equiv_R$ we have $R_i \neq \emptyset$. Now let us prove (1). We may consider two cases.

1. If $K$ is not a ring or a ring of characteristic 0. If $1_K + 1_K = 1_K$, as one has $\mathbb{B} \hookrightarrow K$ lemma 3 and propositon 5 prove that it is generated by (LE), (LI) or (LC) relators (see lemma 5). If $1_K + 1_K \neq 1_K$, Lemma 3 implies that $\equiv$ is generated by (LE), (LI) or (LC) relators , examining all these cases, we find that only (LE) is impossible. In the two cases $A^*/_\equiv$ is a free partially commutative monoid.
2. If $K$ is ring of characteristic $n \neq 0$ not prime. We consider two cases.
   (a) If $n \neq p^\alpha$ with $p$ prime and $\alpha > 1$. Then, it exists at least two prime factors $p_1$ and $p_2$ of $n$. By lemma 3 $\equiv$ is $\mathbb{Z}/p_1\mathbb{Z} - ⊔⊔$ compatible and $\mathbb{Z}/p_2\mathbb{Z} - ⊔⊔$ compatible. Proposition 8 and assertion (2) imply that $\equiv$ is generated only by (LI) or (LC) relators.
   (b) If $n = p^m$, then by lemma 3 $\equiv$ is $\mathbb{Z}/p^2\mathbb{Z} - ⊔⊔$ compatible. Again by lemma 3 it is $\mathbb{Z}/p\mathbb{Z}$-compatible which implies, using proposition 8, that the only primitive polynomials $u - v$ are of the form $a^{p^\alpha} - b^{p^\beta}$ or $a^{p^\alpha} b^{p^\beta} - b^{p^\beta} a^{p^\alpha}$. Remarking that $\binom{p^\alpha}{p^{\alpha-1}} \neq 0\ [p^2]$, we find that these relators occur only when $\alpha = \beta = 0$. Using assertion (2), again proposition 8 gives the result.

■

Such a familly $(R_i)_{i\in[1,n]}$ will be called a `primitive partition` of $\equiv$. The minimal length of the primitive partitions will be called the `depth` of $\equiv$.

**Example 2** *1. All the congruences generated by relators of the form $a^{p^\alpha} = b^{p^\beta}$ or $a^{p^\alpha} b^{p^\beta} = b^{p^\beta} a^{p^\alpha}$ are $\mathbb{Z}/p\mathbb{Z} - ⊔⊔$ compatible with depth 1.*

*2. The congruence generated by*

$$\begin{cases} a^{2^\alpha} b^{2^\beta} a^{2^\alpha} b^{2^\beta} = b^{2^\beta} a^{2^\alpha} b^{2^\beta} a^{2^\alpha} \\ a^{2^{\alpha+1}} b^{2^\beta} = b^{2^\beta} a^{2^{\alpha+1}} \\ b^{2^{\beta+1}} a^{2^\alpha} = a^{2^\alpha} b^{2^{\beta+1}} \end{cases}$$

*with $\alpha, \beta \in \mathbb{N} - \{0\}$ are $\mathbb{Z}/2\mathbb{Z} - ⊔⊔$ compatible with depth*[4] 2.

[4] We only known congruences with depth 2.

## 3 Group properties

### 3.1 Compatibility with Magnus transformation

In this paragraph we show that, when $\equiv$ is a $K - ⧢$ compatible congruence ($K$ semiring), one can define a Magnus transformation on $K[A^*/_{\equiv}]$ . Recall that the Magnus transformation is the unique endomorphism of $K < A >$ such that $\mu(a) = 1 + a$ for each letter $a$. One has here

**Lemme 9** *Let $K$ be a semiring and $\equiv$ be a congruence $K - ⧢$ compatible. Then it exists an unique morphism $\mu_{\equiv}$ such that the square*

$$\begin{tikzcd} K < A > \arrow[r, "\mu"] \arrow[d, "nat"'] & K < A > \arrow[d, "nat"] \\ K[A^*/_{\equiv}] \arrow[r, "\mu_{\equiv}"] & K[A^*/_{\equiv}] \end{tikzcd} \tag{2}$$

*is commutative.*

**Proof** It suffices to remark that $\mu = (Id \otimes ev) \circ c$ where $ev$ is the linear mapping from $K < A >$ on $K$ sending each word $w \in A^*$ on 1. This application is constant over $A^*$, then it is compatible with the congruence $\equiv$ (i.e. it exists an application $ev_{\equiv}$ sending each class of word to 1). Furthermore, as $\equiv$ is $K - ⧢$ compatible, $c_{\equiv}$ exists and, therefore our morphism is $\mu_{\equiv} = (Id \otimes ev_{\equiv}) \circ c_{\equiv}$. ■

**Commentary 3** *Before closing the general case, let us mention that the problem of compatibility can also be addressed for other rational laws. This laws are "." (concatenation or Cauchy product), $*$ (star operation, partially defined),$\times$ (external product) and $+$ (union or sum) for the first kind (which is the realm of Kleene-Schützenberger theorem [14]) and for the second kind $\odot$ (Hadamard product), $⧢$ (shuffle product), $\uparrow$ (infiltration product [18]) and $\uparrow_q$ (q-infiltration product⑤, the dual of the coproduct $c_q = (a \otimes 1 + 1 \otimes a) + qa \otimes a)$). The results can be summarized as follows*

| *Kind* | Laws | *Compatible with commutation* | *Other* |
|---|---|---|---|
| *First* | $\times$ | *Yes* | *All* |
| | $+$ | *Yes* | *All* |
| | . | *No* | *?* |
| | $*$ | *No* | *?* |
| *Second* | $\odot$ | *Yes* | *All* |
| | $⧢$ | *Yes* | *depends of $K$* |
| | $\uparrow$ | *Yes* | *as $⧢$* |
| | $\uparrow_q$ | *Yes* | *as $⧢$* |

⑤ It can be shown that $q$-infiltration is the only dual law satisfying alphabetical and algebraic constraints [6]

### 3.2 Homogeneous congruences compatible with the shuffle

In this paragraph, we examine the congruences which are homogeneous for some weight function $\omega : A \to \mathbb{N}^+$. The function $\omega$ is extended to $A^*$ by $\omega(w) = \sum_{a\in \mathrm{Alph}(w)} |w|_a \omega(a)$, where $|w|_a$ is the partial degree of $w$ with respect to the letter $a$. Remarking that $\omega$ is a morphism the following result is straigthforward.

**Lemme 10** *Let $R \subset A^* \times A^*$. The following assertions are equivalent.*

1. *For each $(u, v) \in R$, $\omega(u) = \omega(v)$.*
2. *For each $u, v \in A^*$, $u \equiv_R v \Rightarrow \omega(u) = \omega(v)$.*

**Definition 11** *We will say that $\equiv$ is homogeneous (for $\omega$) if and only if it satisfies the assertions of lemma 10.*

**Theorem 2** *Let $\equiv$ be a finitely generated congruence on $A^*$ which is $K - \sqcup\!\sqcup$ compatible and generated by relators of the form $u \equiv v$ where $u - v$ is primitive, then we have the following altenative.*

1. *The monoid $A^*/_\equiv$ is not cancellable.*
2. *It exists a weight function $\omega : A \to \mathbb{N}^*$ for which $\equiv$ is homogeneous and $A^*/_\equiv$ embeds in a group.*

**Sketch of the proof** Suppose that $A^*/_\equiv$ is cancellable. If $ch(K)$ is not prime then $A^*/_\equiv$ is a free partially commutative monoid, and the result is straightforward from [9]. If $ch(K)$ is prime, $\equiv$ is generated by relators of type $a^{p^\alpha} b^{p^\beta} = b^{p^\beta} a^{p^\alpha}$ (pLC) and $a^{p^\alpha} = b^{p^\beta}$ (pLI). As all the (pLC) relators are multihomogeneous it suffices to prove the existence of a weight function for which (pLI) is homogeneous. We prove that, if we have two relators $a^{p^{\alpha_i}} \equiv b^{p^{\beta_i}}$ $(i = 1, 2)$ one has $\alpha_1 - \beta_1 = \alpha_2 - \beta_2$. Denoting $d_{a,b}$ this difference, the result is a consequence of the following lemma whose proof is easy and left to the reader.

**Lemme 12** *Let $G$ be the graph of an equivalence relation on $A$. Let $d : G \to \mathbb{Z}$ be a function such that*

$$(a, b),(a, c) \in G \Rightarrow d(a, b) + d(b, c) + d(c, a) = 0.$$

*Then,*

1. *It exists a (potential) function $h : A \to \mathbb{Z}$ such that $d(a, b) = h(b) - h(a)$.*
2. *If $A$ is finite, we can choose $h$ positive.*

**End of the proof** We remark that $d_{a,b} + d_{b,c} + d_{c,a} = 0$, according to lemma 12 we can construct a function $h : A \to \mathbb{N}^+$ such that $d_{a,b} = h(b) - h(a)$. With the weight function $\omega := p^h$, the congruence $\equiv$ is homogeneous. On the other hand we have $\mu_\equiv(A^*) \subset 1 + \mathcal{M}_K(A^*/_\equiv)$ where $\mathcal{M}_K(A^*/_\equiv)$ is the ideal of series $S$ such that $(S, 1) = 0$. But, as $\equiv$ is homogeneous, $1 + \mathcal{M}_K(A^*/_\equiv)$ is a group. Furthermore $\mu_\equiv(w) = w + \sum_{\omega(u)<\omega(w)} n_u u$, which implies that $\mu_\equiv : A^*/_\equiv \hookrightarrow 1 + \mathcal{M}_K(A^*/_\equiv)$ is into. This proves the result. ∎

We now give quickly some properties of the Magnus group $1+\mathcal{M}_K(A^*/_\equiv)$. It has been shown in [9] that, if $ch(K)=0$, the function $S \to S^n;\ n>0$ is one to one within the Magnus group (the monoid then is partially commutative). We cannot expect such a property in characteristic $p$ as the congruence $a^p \equiv b^p$ can occur with $a \not\equiv b$. However, we have

**Proposition 13** *Let $K$ be a ring of prime characteristic $p$ and $\equiv$ a $K-\sqcup\!\sqcup$ compatible and cancellable congruence. Then:*
*i) If $q \not\equiv 0\ [p]$ the function $S \to S^q$ is one to one within the Magnus group $1+\mathcal{M}_K(A^*/_\equiv)$.*
*ii) If $q_i \not\equiv 0\ [p];\ i=1,2$ then $S^{q_1}T^{q_2}=T^{q_2}S^{q_1}$ implies $ST=TS$*

**Proof** Solving degree by degree

$$(1+\sum_{i=1}^{\infty} X_i)^q = (1+\sum_{i=1}^{\infty} Y_i) \tag{3}$$

(with two auxilliary alphabets such that $deg(X_i)=deg(Y_i)$), it can easily be seen that the series $\sum_{k=0}^{\infty} \binom{\frac{1}{q}}{k} X^k$ has its coefficients in $\mathbb{Z}[1/q]$. This proves (i).
Now (ii) is a consequence of (i) as the hypothesis can be reformulated $T^{-q_2}S^{q_1}T^{q_2}=S^{q_1}$.
■

## 4 Conclusion

We have seen that in "almost every case", the congruences compatible with the shuffle product give partially commutative quotients. The only degenerate case occurs when the characteristic of the ground ring is prime. Only then, does a bunch of new phenomena arise. A process (primitive partitions) to analyse these new congruences has been described. Moreover, for congruences of depth one, we have a complete description of the relators. This allows to prove, thanks to a "Magnus-type" transformation, that the quotients are either "not cancellable" or "embeddable in a group". This transformation gives us the opportunity to use some analytic tools as the series of the $q-root$ for $q$ prime to the characteristic. An infinite family of congruences of depth two has been provided. The problem of describing higher depth remains however open.

## References


1. J. Berstel and C. Reutenauer, *Rational Series and Their Languages,* (EATCS Monographs on Theoretical Computer Science, Springler-Verlagm Berlin, 1988).
2. N.Bourbaki, *Éléments de mathématiques, Groupes et algèbres de Lie, Chap. 2 et 3* (Hermann, Paris, 1972).
3. P.Cartier, D.Foata, *Problèmes combinatoires de commutation et réarrangement*, Lect. Not. In Math., n 85, 1969.
4. K.T.Chen, R.H.Fox, R.C.Lyndon, *Free differential calculus IV- The quotient groups of the lower central series,* Ann. Of Math, 1958.
5. V. Diekert and G. Rozenberg, *The book of traces* (World Scientific, Singapour, 1995).

6. G. Duchamp, M. Flouret, É. Laugerotte, *Operations over Automata with Multiplicities,* in Automato implementation procedeeding WIA, J.M. Champarnaud, D.Maurel and D. Ziadi eds,**1660**, 183-191,1999.
7. G. Duchamp , D. Krob, *Factorisations dans le monoïde partiellement commutatif libre*, C.R. Acad. Sci. Paris, t. **312**, série I (1991), 189-192.
8. G.Duchamp, D.Krob, *Free partially commutative structures J. Algebra* **156**-2 (1993) 318–361.
9. G.Duchamp, D.Krob, *Partially commutative Magnus transformation* Int. J. of Alg. And comp., 3-1, 1993,15-41.
10. G.Duchamp, J.G.Luque, *Transitive Factorizations*, Colloque FPSAC'99 Barcelone,1999.
11. M.Flouret, *Contribution à l'algorithmique non commutative*, Thèse de doctorat, Univerité de Rouen, 1999.
12. P. Gastin, *Decidability of the Star problem in* $A^* \times \{b\}^*$, Information Processing Letters, 44,65-71,1992.
13. S. Gaubert, J.Mairesse, *Medeling and analysis of timed Petri nets using heap of pieces*, IEEE,Trans. Autom. Control, Vol 44, n4,683-697,1999.
14. S.C. Kleene, *Representation of events in nerve nets and finite automata*, Automata Studies, Princeton Univ. Press (1956), 3-42.
15. D. Krob and P.Lalonde, *Partially commutative Lyndon words Lect. Notes in Comput. Sci.* **665** (1993) 237–246.
16. P.Lalonde, *Contribution à l'étude des empilements* (Thèse de doctorat, LACIM, 1991).
17. M.Lothaire, *Combinatorics on words*, Addison Wesley, 1983.
18. P. Ochsenschläger, Binomialkoeffitzenten und Shuffle-Zahlen, Technischer Bericht, Fachbereich Informatik, T. H. Darmstadt,1981.
19. W.Schmitt, *Hopf algebras and identities in free partially commutative monoids*, T.C.S. North Holland, 1990.
20. J.Y. Thibon, *Intégrité des algèbres de séries formelles sur un alphabet partiellement commutatif*,T.C.S (1985), North-Holland.
21. X.G.Viennot, *Heaps of pieces I: Basic definitions and combinatorial lemmas* In G. Labelle et al., editors, Proceeding Combinatoire énumeratice, Montréal Quebec 1985, nymber 1234 in Lectures notes in Mathematics, 321-350, Berlin-Heidelberg-New York, 1986, Springer.