ELSEVIER

Journal of Pure and Applied Algebra 111 (1996) 59–82

JOURNAL OF PURE AND APPLIED ALGEBRA

The structure group for the associativity identity

Patrick Dehornoy *

Mathématiques, Université Caen, 14 032 Caen, France

Communicated by J.D. Stasheff; received 22 June 1993; revised 25 June 1995

Abstract

A group of elementary associativity operators is introduced so that the bracketing graphs which are the skeletons of Stasheff's associahedra become orbits and can be constructed as subgraphs of the Cayley graph of this group. A very simple proof of Mac Lane's coherence theorem is given, as well as an oriented version of this result. We also sketch a more general theory and compare the cases of associativity and left self-distributivity.

0. Introduction

The general purpose of this paper can be summarized as the introduction of some algebraic structure on the faces of Stasheff's associahedra which are CW-complexes whose faces correspond to the complete bracketings of a given string (see [12]). We introduce a "structure group of associativity" $\widetilde{\mathcal{G}}_{\mathcal{A}}$ so that the (skeletons of the) associahedra become orbits for some natural action of $\widetilde{\mathcal{G}}_{\mathcal{A}}$ – exactly like the usual regular polyhedra are orbits for the action of (the finite subgroups of) the orthogonal groups $O(n)$. The main point is that the group $\widetilde{\mathcal{G}}_{\mathcal{A}}$ shares many algebraic properties with Artin's braid groups B_n, a similarity which actually extends in part to the general case where associativity is replaced by any another algebraic identity.

In former papers ([2, 4, 5]) we have developed an analysis of the left distributivity identity in terms of a structure group that captures the geometry of this particular identity. This analysis was used to prove the decidability of the corresponding word problem and to describe the free objects of the variety. Our aim is to show that a similar approach is relevant in the case of other algebraic identities. In the present paper we shall concentrate on the case of associativity, which is both very natural and well known

* E-mail: dehornoy@geocub.greco-prog.fr

0022-4049/96/$15.00 © 1996 Elsevier Science B.V. All rights reserved
SSDI 0022-4049(95)00119-0

but also significantly different and technically easier than left distributivity. Again a "structure group" $\widetilde{\mathcal{G}}_{\mathcal{A}}$ will be involved, and we shall show that the algebraic properties of this group reflect and somehow explain the geometric properties of the associativity identity. In this framework, which can be seen as a variant of the categorical approach of [11], Mac Lane's coherence theorem for associativity can be reformulated as the fact that the relation arising from the pentagonal identity constitutes, together with other "universal" relations, an exact presentation for the group $\widetilde{\mathcal{G}}_{\mathcal{A}}$.

We obtain a direct and very simple proof for the pentagon theorem which relies on the possibility of generating by associativity any given term from a sufficiently large string of characters (the characteristic sequences of a term). With more work one also obtains an *oriented* version of this theorem where the rewrite rule $x(yz) \to (xy)z$ replaces the symmetric relation $x(yz) = (xy)z$. This improved result claims that the pentagon relation is still sufficient to generate all relations in the oriented case. We also show that the structure monoid $\mathcal{M}_{\mathcal{A}}$ corresponding to oriented associativity embeds in the group $\widetilde{\mathcal{G}}_{\mathcal{A}}$. It follows that the (skeletons of the) associahedra are faithful orbits under the natural action of $\mathcal{M}_{\mathcal{A}}$. This provides a description of these graphs as the closure of a finite set of initial edges under some simple algebraic operation (reduction with respect to a right complement), which easily implies that this graph is topologically a sphere.

These properties are established using the particular form of the relations defining the group $\widetilde{\mathcal{G}}_{\mathcal{A}}$, specially the fact that these relations admit a right complement (see [6]) and that this complement satisfies some coherence condition which reflects a deep technical similarity between the group $\widetilde{\mathcal{G}}_{\mathcal{A}}$ and Artin's braid groups B_n. It is remarkable that the coherence of the complement, which is fundamental in the present case of associativity, is equally crucial in the case of left distributivity. It has seemed useful to establish a parallel between these cases. This should in particular make the latter one more accessible.

The paper is organized as follows. The first section introduces the structure group of associativity. Section 2 gives the proof of the pentagon theorem and its oriented version. Section 3 compares the cases of associativity and left distributivity and emphasizes the common features. In Section 4 finally we sketch a more general theory, and show that a significant part of the crucial coherence property used in Sections 2 and 3 can be obtained by a uniform geometrical argument. This considerably lowers the length of a proof which a priori is very long.

1. The elementary associativity operators

In the sequel Σ is an infinite set whose elements are called variables and are typically denoted by X, Y, Z. The set of all terms constructed using the variables in Σ and a binary operator $*$, i.e., the free binary algebra generated by Σ, is denoted by $\mathcal{T}(\Sigma)$. We use P, Q, R, ... for the elements of $\mathcal{T}(\Sigma)$. Then the associativity identity is expressed

by the equality

$$X * (Y * Z) = (X * Y) * Z \qquad (\mathscr{A})$$

Definition. The relation $=_{\mathscr{A}}$ is the least congruence on $\mathscr{T}(\Sigma)$ that contains all pairs

$$(Q * (R * S),\ (Q * R) * S).$$

In other words, the quotient $\mathscr{T}(\Sigma)/=_{\mathscr{A}}$ is the free semigroup generated by Σ. Our task is to describe the congruence $=_{\mathscr{A}}$. To this end we introduce a partial operator $\Omega_{\mathscr{A}}$ on $\mathscr{T}(\Sigma)$ as follows: the term P belongs to the domain of $\Omega_{\mathscr{A}}$ if and only if P can be expressed as $Q * (R * S)$, and, in this case, $\Omega_{\mathscr{A}}$ maps P to the corresponding term $Q * (R * S)$. It is clear that $\Omega_{\mathscr{A}}$ maps every term to an $=_{\mathscr{A}}$-equivalent term, and that, more generally, two terms P, P' are $=_{\mathscr{A}}$-equivalent if and only if there exists a finite sequence of terms from P to P' such that every term is obtained from the previous one by applying either $\Omega_{\mathscr{A}}$ or $\Omega_{\mathscr{A}}^{-1}$ to some subterm.

Precisely we wish to keep track of the subterms the operators $\Omega_{\mathscr{A}}$ or $\Omega_{\mathscr{A}}^{-1}$ are applied to. It is convenient to consider the terms of $\mathscr{T}(\Sigma)$ as *rooted binary trees* the leaves of which are variables. We address a point in such a tree by a finite sequence of 0's and 1's that describes the path from the root of the tree to the considered point: 0 means going to the left, 1 means going to the right. We denote by $\mathbb{S}$ the set of all addresses (i.e., the free monoid generated by 0 and 1), and by Λ the empty address. Elements of $\mathbb{S}$ are denoted x, y, ...

Example. In the term $(X*Y)*Z$, the address of the variable X is 00, while the address of Y is 01.

With these notations it should be clear that a term P belongs to the domain of the operator $\Omega_{\mathscr{A}}$ if and only if the point 11 is either the address of a variable of P, or is a strict prefix of such an address.

Definition. For x in $\mathbb{S}$, $\Omega_{\mathscr{A}}(x)$ is the partial operator on $\mathscr{T}(\Sigma)$ corresponding to applying $\Omega_{\mathscr{A}}$ to the subterm whose root has address x.

Example. Let P be the term $X * (X * (X * X))$. Then $\Omega_{\mathscr{A}}$, which is also $\Omega_{\mathscr{A}}(\Lambda)$ by construction, maps the term P to the term $(X*X)*(X*X)$, while $\Omega_{\mathscr{A}}(1)$ maps P to the term $X * ((X*X)*X)$.

Similarly we introduce for every point x in $\mathbb{S}$ a disjoint copy denoted x^{-1}, and define $\Omega_{\mathscr{A}}(x^{-1})$ to be the converse operator $\Omega_{\mathscr{A}}(x)^{-1}$. Now let us extend the notation $\Omega_{\mathscr{A}}$ to finite sequences of points and inverses of points, so that $\Omega_{\mathscr{A}}(\alpha \cdot \beta)$ is the reverse composition of $\Omega_{\mathscr{A}}(\alpha)$ and $\Omega_{\mathscr{A}}(\beta)$ (apply $\Omega_{\mathscr{A}}(\alpha)$ first and then $\Omega_{\mathscr{A}}(\beta)$). For instance $\Omega_{\mathscr{A}}(00^{-1} \cdot 1)$ is the reverse composition of $\Omega_{\mathscr{A}}(00)^{-1}$ and $\Omega_{\mathscr{A}}(1)$.

Definition. The monoid $\mathscr{M}_{\mathscr{A}}$ (resp. $\mathscr{G}_{\mathscr{A}}$) is the monoid generated by all operators $\Omega_{\mathscr{A}}(x)$ with x in $\mathbb{S}$ (resp. in $\mathbb{S} \cup \mathbb{S}^{-1}$).

With our notations the elements of $\mathcal{M}_{\mathcal{A}}$ are exactly the operators $\Omega_{\mathcal{A}}(u)$ with u a finite sequence of elements of $\mathbb{S}$, i.e. an element of the free monoid $\mathbb{S}^*$ generated by $\mathbb{S}$, and the elements of $\mathcal{G}_{\mathcal{A}}$ are the operators $\Omega_{\mathcal{A}}(\alpha)$ with α a finite sequence of elements of $\mathbb{S} \cup \mathbb{S}^{-1}$, i.e., an element of the free monoid $(\mathbb{S} \cup \mathbb{S}^{-1})^*$ generated by $\mathbb{S} \cup \mathbb{S}^{-1}$. Practically we shall use $\cdot$ for denoting the monoid product (concatenation) of $\mathbb{S}^*$ and $(\mathbb{S} \cup \mathbb{S}^{-1})^*$, and ε to denote their unit (i.e. the empty sequence), not to be confused with the length 1 sequence Λ that consists of the empty address. It should be clear that the following holds:

Lemma 1.1. *Two terms P, P' in $\mathcal{T}(\Sigma)$ are $=_{\mathcal{A}}$-equivalent if and only if there exists a sequence α in $(\mathbb{S} \cup \mathbb{S}^{-1})^*$ such that the operator $\Omega_{\mathcal{A}}(\alpha)$ maps P to P'.*

Remark When the partial function $\Omega_{\mathcal{A}}(\alpha)$ is viewed as a set of pairs of terms (the set of all pairs $(P, \Omega_{\mathcal{A}}(\alpha)(P))$), it becomes exactly the set of all instances of some pair (K_α^+, K_α^-), defined as the pairs obtained from (K_α^+, K_α^-) by applying a substitution, i.e., by replacing each variable by a given term (depending on that variable). Clearly each pair (K_α^+, K_α^-) is a consequence of the associativity identity $(\mathcal{A})$, and actually the monoid $\mathcal{G}_{\mathcal{A}}$ can be seen as a monoid structure defined on the set of all consequences of $(\mathcal{A})$ (see [3] for some additional details).

Our purpose is to study the monoids $\mathcal{M}_{\mathcal{A}}$ and $\mathcal{G}_{\mathcal{A}}$. Observe that $\mathcal{G}_{\mathcal{A}}$ is "nearly" a group: the operator $\Omega_{\mathcal{A}}(x)^{-1}$ is a near-inverse of $\Omega_{\mathcal{A}}(x)$ in as far as the product $\Omega_{\mathcal{A}}(x \cdot x^{-1})$ is the identity of the domain of $\Omega_{\mathcal{A}}(x)$. Of course it could be claimed that the "real" nature of $\mathcal{G}_{\mathcal{A}}$ is a groupoid structure in the language of categories. However, it will be convenient to keep on using here a purely algebraic language which is more appropriate to describe the subsequent constructions.

Definition. Assume that f and g are partial mappings whose domains intersect; f and g are *compatible*, denoted $f \sim g$, (resp. *strongly compatible*) if there exists at least one element x in the intersection of the domains of f and g such that f and g agree on x (resp. if f and g agree on every element in the intersection of their domains).

For instance the above remark about $\Omega_{\mathcal{A}}^{-1}(\xi)$ being a near-inverse of $\Omega_{\mathcal{A}}(x)$ means that the operators $\Omega_{\mathcal{A}}(x \cdot x^{-1})$ and $\Omega_{\mathcal{A}}(\varepsilon)$ (i.e., the identity of $\mathcal{T}(\Sigma)$) are strongly compatible. Actually in the present special case of associativity, the facts that the same variables appear on each side of the identity $(\mathcal{A})$ and that each one appears only once imply (see [3]) that the compatibility relation coincides with the strong compatibility relation, and that these relations are congruences on $\mathcal{G}_{\mathcal{A}}$. Then the quotient monoid $\mathcal{G}_{\mathcal{A}}/\sim$ is a group.

1.1. The relations in $\mathcal{M}_{\mathcal{A}}$ and $\mathcal{G}_{\mathcal{A}}$

Owing to Lemma 1.1, we can consider that a complete description of the monoid $\mathcal{G}_{\mathcal{A}}$ constitutes a convenient achievement for the initial task of studying the equivalence $=_{\mathcal{A}}$,

and therefore of describing in some sense the geometry of associativity. So the point is to establish a presentation of the monoids $\mathcal{M}_{\mathcal{A}}$ and $\mathcal{G}_{\mathcal{A}}$ in terms of their generators $\Omega_{\mathcal{A}}(x)$ and $\Omega_{\mathcal{A}}(x^{-1})$, that is to provide an exhaustive list of the relations that connect the operators $\Omega_{\mathcal{A}}(x)$ one to each other.

The case of the near-inverses $\Omega_{\mathcal{A}}(x^{-1})$ is rather trivial and we concentrate on the positive relations that involve only the operators $\Omega_{\mathcal{A}}(x)$ with x in $\mathbb{S}$. There are two kinds of relations. The first ones are "general" relations which have little to do really with the specific case of associativity. A first family appears when operators associated with nonoverlapping subterms are involved. The basic case is the one of $\Omega_{\mathcal{A}}(0)$ and $\Omega_{\mathcal{A}}(1)$: clearly the result of applying to a term $\Omega_{\mathcal{A}}(0)$ first and then $\Omega_{\mathcal{A}}(1)$, or the converse, leads to the same resulting term. More generally, if we say that two addresses x, y are *orthogonal* if neither x is a prefix of y nor y is a prefix of x, the relation

$$\Omega_{\mathcal{A}}(x \cdot y) = \Omega_{\mathcal{A}}(y \cdot x) \tag{$\perp$}$$

holds for every pair x, y of orthogonal addresses.

The second type of general relations appears when operators associated with "completely nested" subterms are involved. For instance $\Omega_{\mathcal{A}}(\Lambda)$ maps $Q*(R*S)$ to $(Q*R)*S$. Now if some operator $\Omega_{\mathcal{A}}(\alpha)$ maps Q to Q', $\Omega_{\mathcal{A}}(0\alpha)$ maps $Q*(R*S)$ to $Q'*(R*S)$ – we denote by 0α the sequence obtained from α by adding an initial 0 to each factor of α –, while $\Omega_{\mathcal{A}}(00\alpha)$ maps $(Q*R)*S$ to $(Q'*R)*S$. So we certainly have

$$\Omega_{\mathcal{A}}(0\alpha \cdot \Lambda) = \Omega_{\mathcal{A}}(\Lambda \cdot 00\alpha),$$

a relation that just expresses that the subterm which had address 0 before $\Omega_{\mathcal{A}}(\Lambda)$ was applied has address 00 after $\Omega_{\mathcal{A}}(\Lambda)$ has been applied. Similar relations appear when an arbitrary point z replaces Λ. So, the relation

$$\Omega_{\mathcal{A}}(z0x \cdot z) = \Omega_{\mathcal{A}}(z \cdot z00x) \tag{1}$$

holds for every z and x in $\mathbb{S}$. The same argument works for the subterm at 10, which is moved to 01 by $\Omega_{\mathcal{A}}(\Lambda)$, and for the subterm at 11, which is moved to 1, leading to parallel relations

$$\Omega_{\mathcal{A}}(z10x \cdot z) = \Omega_{\mathcal{A}}(z \cdot z01x) \tag{2}$$

$$\Omega_{\mathcal{A}}(z11x \cdot z) = \Omega_{\mathcal{A}}(z \cdot z1x) \tag{3}$$

When we consider the above relations, we see that, for every pair (x, y) in $\mathbb{S} \times \mathbb{S}$, there exists exactly one relation of the form

$$\Omega_{\mathcal{A}}(x \cdot \ldots) = \Omega_{\mathcal{A}}(y \cdot \ldots)$$

except in the case of the pairs $(z, z1)$ that corresponds neither to nonoverlapping subterms nor to completely nested subterms. The algebraic treatment of the monoid $\mathcal{M}_{\mathcal{A}}$ that will be subsequently applied suggests (or, at least, a posteriori legitimates) to

completing our list with relations of the same type for the pairs $(z,z1)$. This, however, is easy, and a direct verification gives, for every z in $\mathbb{S}$, the relation

$$\Omega_{\mathscr{A}}(z1\cdot z\cdot z0)=\Omega_{\mathscr{A}}(z\cdot z) \tag{4}$$

i.e., precisely the pentagon relation. In contradistinction with the other relations that automatically arise from our way to introduce the generators $\Omega_{\mathscr{A}}(x)$, the equalities (4) are specific relations that we can only record and not explain by general reasons. Very informally we could think of the other equalities as the "free" part of the construction while the equalities (4) represent the only really "nonfree" part.

The nontrivial question is whether the above list of relations generate all relations of $\mathscr{M}_{\mathscr{A}}$. It will be convenient to introduce the monoid admitting these relations as a presentation (and therefore of which $\mathscr{M}_{\mathscr{A}}$ is a quotient by construction).

Definition The relation $\equiv^{+}_{\mathscr{A}}$ is the congruence on $\mathbb{S}^*$ generated by all pairs of the following five types:

$$(z0x\cdot z1y,\ z1y\cdot z0x)$$
$$(z0x\cdot z,\ z\cdot z00x)$$
$$(z10x\cdot z,\ z\cdot z01x)$$
$$(z11x\cdot z,\ z\cdot z1x)$$
$$(z1\cdot z\cdot z0,\ z\cdot z)$$

and $\equiv_{\mathscr{A}}$ is the congruence on $(\mathbb{S}\cup\mathbb{S}^{-1})^*$ generated by $\equiv^{+}_{\mathscr{A}}$ together with all pairs $(z\cdot z^{-1},\varepsilon)$ and $(z^{-1}\cdot z,\varepsilon)$ for z in $\mathbb{S}$. Finally $\widetilde{\mathscr{M}}_{\mathscr{A}}$ is the monoid $\mathbb{S}^*/\!\equiv^{+}_{\mathscr{A}}$, and $\widetilde{\mathscr{G}}_{\mathscr{A}}$ is the group $(\mathbb{S}\cup\mathbb{S}^{-1})^*/\!\equiv_{\mathscr{A}}$.

By construction, we have:

Lemma 1.2. (i) *For any positive sequences u, v in $\mathbb{S}^*$, $u\equiv^{+}_{\mathscr{A}} v$ implies $\Omega_{\mathscr{A}}(u)=\Omega_{\mathscr{A}}(v)$;*

(ii) *for any sequences α, β in $(\mathbb{S}\cup\mathbb{S}^{-1})^*$, $\alpha\equiv_{\mathscr{A}}\beta$ implies that $\Omega_{\mathscr{A}}(\alpha)$ and $\Omega_{\mathscr{A}}(\beta)$ are strongly compatible operators.*

We shall now turn to the converse implications. The first one constitutes a form of Mac Lane's theorem in [11]. Actually these converse implications will show that the monoids $\mathscr{M}_{\mathscr{A}}$ and $\widetilde{\mathscr{M}}_{\mathscr{A}}$ are isomorphic, as well as the groups $\mathscr{G}_{\mathscr{A}}/\!\sim$ and $\widetilde{\mathscr{G}}_{\mathscr{A}}$.

2. The characteristic sequences of a term

In order to prove that the relation $\Omega_{\mathscr{A}}(\alpha)=\Omega_{\mathscr{A}}(\beta)$ implies $\alpha\equiv_{\mathscr{A}}\beta$, we need some method for converting the hypothesis, which is a "semantic" statement involving the action of the operators $\Omega_{\mathscr{A}}(x)$ on the terms into a purely "syntactic" statement. The

trick we use is to construct in the syntactic world of $\mathbb{S}^*$ a copy of the terms so that the action of the operators $\Omega_{\mathscr{A}}(x)$ has the wished syntactic counterpart.

This, however, is very easy in the case of associativity. We restrict to terms involving only the variable X, the set of which is denoted by $\mathscr{T}(X)$. We denote by $X^{(n)}$ the term $X*(X*(\cdots(X*X)\cdots))$, n times X, and, for P in $\mathscr{T}(X)$, we write $|P|$ for the number of occurrences of X in P. We start from the following trivial statement:

Lemma 2.1. *For any term P in $\mathscr{T}(X)$, the equivalence $X^{(|P|)} =_{\mathscr{A}} P$ holds, as well as the equivalence $X^{(|P|+n)} =_{\mathscr{A}} P*X^{(n)}$ for any $n \geq 1$.*

By Lemma 1.1 there must exist sequences of addresses that describe the above equivalences. The idea is to introduce for every term P such a "characteristic sequence" $\chi_{\mathscr{A}}(P)$ with the property that the operator $\Omega_{\mathscr{A}}(\chi_{\mathscr{A}}(P))$ constructs the term P from the basic term $X^{(|P|)}$, and then to use the sequence $\chi_{\mathscr{A}}(P)$ as a syntactic version of P. It is uneasy to obtain, toward an inductive construction, a definition of a sequence $\chi_{\mathscr{A}}(Q*R)$ in terms of the sequences $\chi_{\mathscr{A}}(Q)$ and $\chi_{\mathscr{A}}(R)$ only. But everything becomes easy when using a second type of characteristic sequence associated with the second equivalence in the above lemma.

Lemma 2.2. *Let $\chi_{\mathscr{A}}$ and $\chi'_{\mathscr{A}}$ be the mappings of $\mathscr{T}(X)$ into $\mathbb{S}^*$ inductively defined by the formulas $\chi_{\mathscr{A}}(X) = \chi'_{\mathscr{A}}(X) = \varepsilon$ and*

$$\chi_{\mathscr{A}}(Q*R) = \chi'_{\mathscr{A}}(Q)\cdot 1\chi_{\mathscr{A}}(R),$$
$$\chi'_{\mathscr{A}}(Q*R) = \chi'_{\mathscr{A}}(Q)\cdot 1\chi'_{\mathscr{A}}(R)\cdot \Lambda.$$

Then, for every term P and every positive integer n, the operator $\Omega_{\mathscr{A}}(\chi_{\mathscr{A}}(P))$ maps $X^{(|P|)}$ to P, and the operator $\Omega_{\mathscr{A}}(\chi'_{\mathscr{A}}(P))$ maps $X^{(|P|+n)}$ to $P*X^{(n)}$.

The proof is an obvious induction. Now assume that the operator $\Omega_{\mathscr{A}}(u)$ maps the term P to the term P'. Then both the operators $\Omega_{\mathscr{A}}(\chi_{\mathscr{A}}(P'))$ and $\Omega_{\mathscr{A}}(\chi_{\mathscr{A}}(P)\cdot u)$ map the term $X^{(|P|)}$ to P'. So if the converse of Lemma 1.2 is true, we can expect that the sequences $\chi_{\mathscr{A}}(P')$ and $\chi_{\mathscr{A}}(P)\cdot u$ be $\equiv^+_{\mathscr{A}}$-equivalent. Similarly both $\Omega_{\mathscr{A}}(\chi'_{\mathscr{A}}(P'))$ and $\Omega_{\mathscr{A}}(\chi'_{\mathscr{A}}(P)\cdot 0u)$ map the term $X^{(|P|+1)}$ to $P'*X$, and we can expect a parallel $\equiv^+_{\mathscr{A}}$-equivalence. Now this is just a matter of verification involving the defining relations of $\equiv^+_{\mathscr{A}}$.

Lemma 2.3. (i) *If u belongs to $\mathbb{S}^*$ and $\Omega_{\mathscr{A}}(u)$ maps P to P', the equivalences*

$$\chi_{\mathscr{A}}(P') \equiv^+_{\mathscr{A}} \chi_{\mathscr{A}}(P)\cdot u \quad \text{and} \quad \chi'_{\mathscr{A}}(P') \equiv^+_{\mathscr{A}} \chi'_{\mathscr{A}}(P)\cdot 0u$$

hold in $\mathbb{S}^*$.

(ii) *Similarly if α belongs to $(\mathbb{S}\cup\mathbb{S}^{-1})^*$ and $\Omega_{\mathscr{A}}(\alpha)$ maps P to P', the equivalences*

$$\chi_{\mathscr{A}}(P') \equiv_{\mathscr{A}} \chi_{\mathscr{A}}(P)\cdot \alpha \quad \text{and} \quad \chi'_{\mathscr{A}}(P') \equiv_{\mathscr{A}} \chi'_{\mathscr{A}}(P)\cdot 0\alpha$$

hold in $(\mathbb{S}\cup\mathbb{S}^{-1})^*$.

Proof. (i) Using induction on the length of the sequence u, we may assume that u reduces to a single point, say, x. We prove the formulas inductively on the length of x (as a sequence of 0's and 1's). We begin with the case $x = \Lambda$. Assume that P is $Q * (R * S)$. Then P' is $(P * Q) * S$, and the definitions together with relation (3) yield

$$\begin{aligned}\chi_{\mathscr{A}}(P') &= \chi'_{\mathscr{A}}(Q) \cdot 1\chi'_{\mathscr{A}}(R) \cdot \Lambda \cdot 1\chi_{\mathscr{A}}(S)\\ &\equiv^{+}_{\mathscr{A}} \chi'_{\mathscr{A}}(Q) \cdot 1\chi'_{\mathscr{A}}(R) \cdot 11\chi_{\mathscr{A}}(S) \cdot \Lambda = \chi_{\mathscr{A}}(P) \cdot \Lambda\end{aligned}$$

Similarly, using relation (1) we have

$$\begin{aligned}\chi_{\mathscr{A}}(P') &= \chi'_{\mathscr{A}}(Q) \cdot 1\chi'_{\mathscr{A}}(R) \cdot \Lambda \cdot 1\chi'_{\mathscr{A}}(S) \cdot \Lambda\\ &\equiv^{+}_{\mathscr{A}} \chi'_{\mathscr{A}}(Q) \cdot 1\chi'_{\mathscr{A}}(R) \cdot 11\chi'_{\mathscr{A}}(S) \cdot \Lambda \cdot \Lambda\\ &\equiv^{+}_{\mathscr{A}} \chi'_{\mathscr{A}}(Q) \cdot 1\chi'_{\mathscr{A}}(R) \cdot 11\chi'_{\mathscr{A}}(S) \cdot 1 \cdot \Lambda \cdot 0\\ &= \chi'_{\mathscr{A}}(P) \cdot 0\end{aligned}$$

Now assume that P is $Q * R$ and x is $0y$. Then P' is $Q' * R$, where $\Omega_{\mathscr{A}}(y)$ maps Q to Q'. By induction hypothesis, we assume $\chi_{\mathscr{A}}(Q') \equiv^{+}_{\mathscr{A}} \chi_{\mathscr{A}}(Q) \cdot y$ and $\chi'_{\mathscr{A}}(Q') \equiv^{+}_{\mathscr{A}} \chi'_{\mathscr{A}}(Q) \cdot 0y$. Then we have

$$\begin{aligned}\chi_{\mathscr{A}}(P') &= \chi_{\mathscr{A}}(Q' * R) = \chi'_{\mathscr{A}}(Q') \cdot 1\chi_{\mathscr{A}}(R)\\ &\equiv^{+}_{\mathscr{A}} \chi'_{\mathscr{A}}(Q) \cdot 0y \cdot 1\chi_{\mathscr{A}}(R)\\ &\equiv^{+}_{\mathscr{A}} \chi'_{\mathscr{A}}(Q) \cdot 1\chi_{\mathscr{A}}(R) \cdot 0y = \chi_{\mathscr{A}}(P) \cdot x\end{aligned}$$

by relation ($\perp$), and similarly

$$\begin{aligned}\chi'_{\mathscr{A}}(P') &= \chi_{\mathscr{A}}(Q' * R) = \chi'_{\mathscr{A}}(Q') \cdot 1\chi'_{\mathscr{A}}(R) \cdot \Lambda\\ &\equiv^{+}_{\mathscr{A}} \chi'_{\mathscr{A}}(Q) \cdot 0y \cdot 1\chi'_{\mathscr{A}}(R) \cdot \Lambda\\ &\equiv^{+}_{\mathscr{A}} \chi'_{\mathscr{A}}(Q) \cdot 1\chi'_{\mathscr{A}}(R) \cdot 0y \cdot \Lambda\\ &\equiv^{+}_{\mathscr{A}} \chi'_{\mathscr{A}}(Q) \cdot 1\chi'_{\mathscr{A}}(R) \cdot \Lambda \cdot 00y = \chi'_{\mathscr{A}}(P) \cdot 0x\end{aligned}$$

by relation (1). This gives the desired formulas, and the argument is parallel is the case $x = 1z$ using relations (2) and (3).

(ii) If $\Omega_{\mathscr{A}}(x)$ maps the term P to the term P', then the operator $\Omega_{\mathscr{A}}(x^{-1})$ maps P' to P. So point (i) immediately gives the formulas of (ii) in the case where α reduces to a unique factor x^{-1}. Then the induction is straightforward. □

The previous computation is sufficient to complete the analysis in the unoriented case, i.e., to describe the relation between $\mathscr{G}_{\mathscr{A}}$ and $\widetilde{\mathscr{G}}_{\mathscr{A}}$. Because the domain of the operator $\Omega_{\mathscr{A}}(\alpha)$ is always nonempty, we may state the following

Proposition 2.4. *For any sequences α, β in $(\mathbb{S} \cup \mathbb{S}^{-1})^*$, the operators $\Omega_{\mathscr{A}}(\alpha)$ and $\Omega_{\mathscr{A}}(\beta)$ are compatible if and only if they are strongly compatible if and only if the equivalence $\alpha \equiv_{\mathscr{A}} \beta$ holds.*

Proof. Assume that $\Omega_{\mathscr{A}}(\alpha)$ and $\Omega_{\mathscr{A}}(\beta)$ both map the term P to the term P'. By Lemma 2.3(ii) both sequences α and β are $\equiv_{\mathscr{A}}$-equivalent to $\chi_{\mathscr{A}}(P') \cdot \chi_{\mathscr{A}}(P)^{-1}$. □

The oriented case, i.e., the case of $\mathscr{M}_{\mathscr{A}}$ and $\widetilde{\mathscr{M}}_{\mathscr{A}}$ where we restrict to only one direction of associativity rewriting, is more interesting. At the present point, the formulas of Lemma 2.3(i) only yield a partial result.

Lemma 2.5. *If u, v are positive sequences in $\mathbb{S}^*$, and the operators $\Omega_{\mathscr{A}}(u)$ and $\Omega_{\mathscr{A}}(v)$ are compatible, then there exists a positive sequence w satisfying $w \cdot u \equiv^+_{\mathscr{A}} w \cdot v$.*

So we are left with the question as to whether left cancellation is allowed in the monoid $\widetilde{\mathscr{M}}_{\mathscr{A}}$. This question will be solved using the special form of its defining relations. As we have pointed out, these relations have the property that, for any pair of distinct generators (x, y), there exists exactly one relation that is a pair whose left member begins with x and right member begins with y. More precisely, let $C_{\mathscr{A}}$ be the mapping of $\mathbb{S}^2$ into $\mathbb{S}^*$ defined by

$$C_{\mathscr{A}}(x,y) = \begin{cases} \varepsilon & \text{if } x \text{ and } y \text{ are equal,} \\ x & \text{if } x \text{ and } y \text{ are prefix-incompatible, or } x \text{ is } y1, \\ & \text{or } x0 \text{ is a prefix of } y, \text{ or } x1 \text{ is a strict prefix of } y, \\ x \cdot x0 & \text{if } y \text{ is } x1, \\ y00z & \text{if } x \text{ is } y0z, \\ y10z & \text{if } x \text{ is } y01z, \\ y1z & \text{if } x \text{ is } y11z. \end{cases}$$

Then the congruence $\equiv^+_{\mathscr{A}}$ is exactly the congruence on $\mathbb{S}^*$ generated by all pairs

$$(x \cdot C_{\mathscr{A}}(y,x),\ y \cdot C_{\mathscr{A}}(x,y)),$$

which we shall express by saying that $C_{\mathscr{A}}$ is a *right complement* for $\equiv^+_{\mathscr{A}}$. A typical example of a congruence associated with a right complement is braid equivalence used to define Artin's braid groups B_n. It is shown in [6] that Garside's treatment of the groups B_n can be extended to arbitrary groups admitting a right complemented presentation, provided that the complement satisfies some combinatorial properties. We shall presently prove that the complement $C_{\mathscr{A}}$ above satisfies these requirements.

Associated with the complement $C_{\mathscr{A}}$ is a notion of *word reduction* in $(\mathbb{S} \cup \mathbb{S}^{-1})^*$. Since the equivalence $x \cdot C_{\mathscr{A}}(y,x) \equiv^+_{\mathscr{A}} y \cdot C_{\mathscr{A}}(y,x)$ holds for every x, y in $\mathbb{S}$, so does the equivalence

$$y^{-1} \cdot x \equiv_{\mathscr{A}} C_{\mathscr{A}}(x,y) \cdot C_{\mathscr{A}}(y,x)^{-1}.$$

We say that the sequence α *reduces* to the sequence β if β can be obtained from α by iteratively replacing patterns of the form $y^{-1} \cdot x$ by the corresponding patterns $C_{\mathscr{A}}(x,y) \cdot C_{\mathscr{A}}(y,x)^{-1}$. It is clear that the irreducible sequences are the sequences of

the form $u \cdot v^{-1}$ with u, v positive sequences, i.e., sequences in $\mathbb{S}^*$. It not obvious that any sequence should reduce in a finite number of steps to an irreducible sequence, but it is not hard to see that reduction, when it terminates, leads to a unique irreducible sequence. We define the (a priori partial) mapping $C^*_{\mathscr{A}}$ of $\mathbb{S}^* \times \mathbb{S}^*$ into $\mathbb{S}^*$ by the condition that, for u, v in $\mathbb{S}^*$, $C^*_{\mathscr{A}}(u,v) \cdot C^*_{\mathscr{A}}(v,u)^{-1}$ is the irreducible sequence to which the sequence $v^{-1} \cdot u$ reduces. By construction the mapping $C^*_{\mathscr{A}}$ extends the mapping $C_{\mathscr{A}}$, and constitutes the appropriate extension of $C_{\mathscr{A}}$ to finite sequences as in particular the equality

$$u \cdot C^*_{\mathscr{A}}(v,u) \equiv_{\mathscr{A}} v \cdot C^*_{\mathscr{A}}(u,v)$$

holds for every finite sequence u, v, provided that the complements are defined.

Definition. The right complement $C_{\mathscr{A}}$ is *coherent* if the equivalence

$$C^*_{\mathscr{A}}(C_{\mathscr{A}}(x,y), C_{\mathscr{A}}(z,y)) \equiv^+_{\mathscr{A}} C^*_{\mathscr{A}}(C_{\mathscr{A}}(x,z), C_{\mathscr{A}}(y,z)) \quad \mathscr{R}(x,y,z)$$

holds for every x, y, z in $\mathbb{S}$.

The coherence is exactly what is needed to guarantee that the closure under complement of the initial arrays x, y, z in the Cayley graph of $\widetilde{\mathscr{M}}_{\mathscr{A}}$ leads to a well-defined unique terminal point, which will be the least common multiple of x, y and z. The analysis of [6] yields

Lemma 2.6. *Assume that the equivalence relation $\equiv^+_{\mathscr{A}}$ has the property that, for any u in $\mathbb{S}^*$, the lengths of the sequences u' satisfying $u' \equiv^+_{\mathscr{A}} u$ have a finite supremum, and moreover that the complement $C_{\mathscr{A}}$ is coherent. Then the monoid $\widetilde{\mathscr{M}}_{\mathscr{A}}$ admits left cancellation.*

The finiteness condition above is easy, for $u' \equiv^+_{\mathscr{A}} u$ implies $\Omega_{\mathscr{A}}(u') = \Omega_{\mathscr{A}}(u)$. Define the weight of a term P (viewed as a word) as the sum of the ranks of the opening brackets in P, where the rank of a character is just the number of characters before it. Every operator $\Omega_{\mathscr{A}}(x)$ strictly lowers the weight of any term it is applied to, and therefore if $\Omega_{\mathscr{A}}(u)$ maps P to P', the length of u, as well as the length of any sequence u' verifying $\Omega_{\mathscr{A}}(u') = \Omega_{\mathscr{A}}(u)$, is bounded by the weight of the term P.

We are left with the verification of the coherence condition for $C_{\mathscr{A}}$. This is a priori a brute force argument consisting in an exhaustive examination of the various cases arising from all possible mutual positions of the points x, y, z. Actually the construction of the complement $C_{\mathscr{A}}$ implies that a great many cases are automatically settled. This will be exposed in Section 4 below. In the present case, this implies that it suffices to verify the equivalences $\mathscr{R}(1,y,\Lambda)$, $\mathscr{R}(y,\Lambda,1)$ and $\mathscr{R}(\Lambda,1,y)$ when 0 is a prefix of y or 1 is a strict prefix of y. Observe that simultaneously verifying the three above equivalences only require three $C_{\mathscr{A}}$-reductions (and not six). It is enough to distinguish five cases.

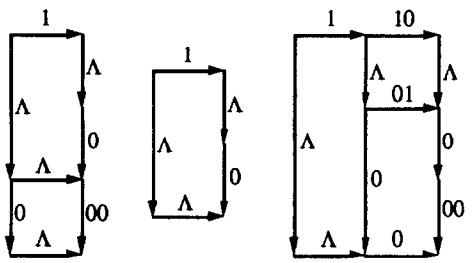

Fig. 1. Coherence of the complement $C_{\mathscr{A}}$, case of $\{\Lambda, 1, 11\}$.

First assume that y has the form $0y'$. The formulas are

$$C^*_{\mathscr{A}}(C_{\mathscr{A}}(0y', 1), C_{\mathscr{A}}(\Lambda, 1)) = 000y' = C^*_{\mathscr{A}}(C_{\mathscr{A}}(0y', \Lambda), C_{\mathscr{A}}(1, \Lambda)),$$

$$C^*_{\mathscr{A}}(C_{\mathscr{A}}(1, \Lambda), C_{\mathscr{A}}(0y', \Lambda)) = \Lambda = C^*_{\mathscr{A}}(C_{\mathscr{A}}(1, 0y'), C_{\mathscr{A}}(\Lambda, 0y')),$$

$$C^*_{\mathscr{A}}(C_{\mathscr{A}}(\Lambda, 0y'), C_{\mathscr{A}}(1, 0y')) = \Lambda \cdot 0 = C^*_{\mathscr{A}}(C_{\mathscr{A}}(\Lambda, 1), C_{\mathscr{A}}(0y', 1)).$$

If y has the form $10y'$, one obtains similar equalities where only the first value is modified and is now $001y'$. The result is the same if y has the form $110y'$ (the first value becomes $01y'$), or the form $111y'$ (the first value is $1y'$). The last case is for $y = 11$. Again similar equalities are obtained, with value $\Lambda \cdot 0 \cdot 00$ for the first two complements. The latter case is the only really critical one (although very simple indeed). The associated reductions are illustrated in the Cayley graph of Fig. 1 whose meaning should be clear: reduction consists in "closing" the open patterns made of two arrows with the same origin by appending the new arrows prescribed by the complement $C_{\mathscr{A}}$. Observe that in the case of this simple complement, the desired equivalences happen to be merely equalities. Nevertheless, they are *not* trivial, and they definitely express some intrinsic property of associativity.

Owing to Lemmas 2.4 and 2.5 we have obtained

Proposition 2.7. *If u, v are positive sequences in $\mathbb{S}^*$, and the operators $\Omega_{\mathscr{A}}(u)$ and $\Omega_{\mathscr{A}}(v)$ are compatible, then $u \equiv^+_{\mathscr{A}} v$ holds.*

In other words, the monoids $\mathscr{M}_{\mathscr{A}}$ and $\widetilde{\mathscr{M}}_{\mathscr{A}}$ are isomorphic, i.e., the relations listed in Section 1 do form a presentation of the monoid $\mathscr{M}_{\mathscr{A}}$.

Additional results about the congruence $\equiv^+_{\mathscr{A}}$ and the monoid $\mathscr{M}_{\mathscr{A}}$ can easily be obtained. For instance, reductions associated with the complement $C_{\mathscr{A}}$ always have to terminate. Let α be any sequence in $(\mathbb{S} \cup \mathbb{S}^{-1})^*$, and P be any term in the domain of the operator $\Omega_{\mathscr{A}}(P)$, which we know cannot be empty. Let $u_1, u_2, \ldots$ be an enumeration of the distinct positive sequences u that have the property that α reduces to some sequence admitting u as an initial segment. By construction, reduction does not modify the domain of the corresponding operators, so the term P belongs to the domain of each operator $\Omega_{\mathscr{A}}(u_i)$. It follows that the lengths of the sequences u_i are bounded above by the weight of the term P, and therefore that there are only finitely many of them.

This in turn means that the reduction of α has to terminate. By [6], this implies that the monoid $\mathcal{M}_{\mathcal{A}}$ is right regular.

Next the operator $\Omega_{\mathcal{A}}^{-1}$ is a symmetric copy of the operator $\Omega_{\mathcal{A}}$. It follows that the monoid similar to $\mathcal{M}_{\mathcal{A}}$ constructed from $\Omega_{\mathcal{A}}^{-1}$ is exactly the opposite monoid of $\mathcal{M}_{\mathcal{A}}$, and that this monoid is still associated with a coherent right complement obtained from $C_{\mathcal{A}}$ by exchanging the roles of 0 and 1. In the terms of [6] this means that the congruence $\equiv_{\mathcal{A}}^{+}$ is also associated with a coherent *left* complement, and this implies that the monoid $\widetilde{\mathcal{M}}_{\mathcal{A}}$ admits right cancellation. Thus the situation of the monoid $\widetilde{\mathcal{M}}_{\mathcal{A}}$ and of the group $\widetilde{\mathcal{G}}_{\mathcal{A}}$ is exactly the one of the braid monoids P_n and the braid groups B_n with respect to the complements. In particular, we have

Proposition 2.8. *The congruence $\equiv_{\mathcal{A}}^{+}$ is exactly the restriction of the congruence $\equiv_{\mathcal{A}}$ to positive sequences. The monoid $\mathcal{M}_{\mathcal{A}}$ embeds in the group $\widetilde{\mathcal{G}}_{\mathcal{A}}$, and every element of $\widetilde{\mathcal{G}}_{\mathcal{A}}$ can be expressed as the (right, or left) quotient of two elements of $\mathcal{M}_{\mathcal{A}}$.*

According to the double reduction procedure of [6], the word problem for the congruence $\equiv_{\mathcal{A}}^{+}$ is decidable, and actually has a polynomial complexity with respect to the lengths of the considered sequences. Incidentally, a unique normal form for the elements of $\widetilde{\mathcal{G}}_{\mathcal{A}}$ is described in [3] using another approach.

The associahedra

There is a close connection between the Cayley graphs of the group $\widetilde{\mathcal{G}}_{\mathcal{A}}$ and the associahedra. In Stasheff's original paper [12] where they were used to emphasize the obstruction to the existence of an associative law in certain spaces, the associahedra are constructed as CW-complexes whose faces correspond to bracketings of a fixed string. Like in [8] we shall consider here the skeletons of these CW-complexes, i.e., the graphs whose vertices correspond to the faces of the CW-complex, and the edges connect faces that have a common boundary.

Definition. For any term P, the graph K_P (resp. the oriented graph K_P^+) is constructed as follows: the vertices are the images of P under some operator in $\mathcal{G}_{\mathcal{A}}$ (resp. in $\mathcal{M}_{\mathcal{A}}$) and an (oriented) edge connects Q to R if some transformation $\Omega_{\mathcal{A}}(x)$ with x in $\mathbb{S}\cup\mathbb{S}^{-1}$ (resp. in $\mathbb{S}$) maps Q to R.

Fig. 2 shows two such (oriented) graphs. Observe that each graph K_P contains exactly one vertex, say Q, of the form $X_1*(X_2*(\cdots(X_{n-1}\cdots X_n)\ldots))$, and that for such a term the graph K_Q, which is also K_P, is nothing but the unoriented version of the oriented graph K_Q^+. By construction, the graph K_P is the 2-skeleton of the associahedron of the term P as defined in [12], and considering the oriented version K_P^+ amounts to introducing some orientation on this associahedron.

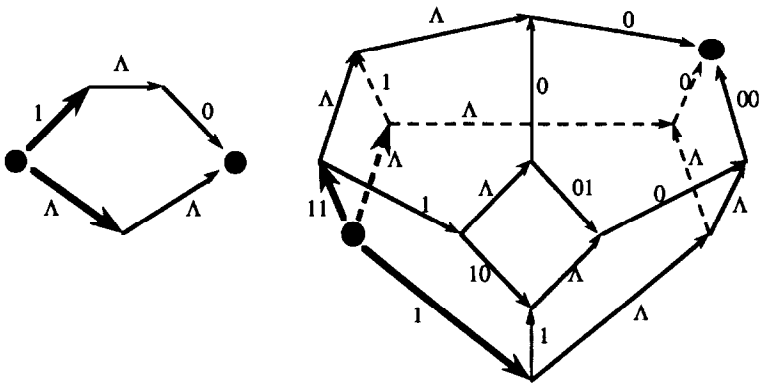

Fig. 2. The oriented graphs $K^+_{X^{(4)}}$ and $K^+_{X^{(5)}}$.

By construction, the group $\widetilde{\mathcal{G}}_{\mathcal{A}}$ and the monoid $\widetilde{\mathcal{M}}_{\mathcal{A}}$ operate (a partial operation) on the graphs K_P via $\Omega_{\mathcal{A}}$. This gives a projection of the Cayley graph of $\widetilde{\mathcal{G}}_{\mathcal{A}}$ and $\widetilde{\mathcal{M}}_{\mathcal{A}}$ onto these graphs. The nontrivial result is that this projection is injective. This is exactly what Propositions 2.4 and 2.7 tell.

Proposition 2.9. *Let P be any term in $\mathcal{T}(\Sigma)$.*

(i) *The partial action of the group $\widetilde{\mathcal{G}}_{\mathcal{A}}$ induced by $\Omega_{\mathcal{A}}$ is transitive and faithful on the graph K_P.*

(ii) *The partial action of the monoid $\mathcal{M}_{\mathcal{A}}$ induced by $\Omega_{\mathcal{A}}$ is faithful on the oriented graph K^+_P. Actually the latter one is exactly the Cayley graph of the subset of $\mathcal{M}_{\mathcal{A}}$ made by (the classes of) the sequences u such that the term P belongs to the domain of $\Omega_{\mathcal{A}}(u)$.*

Proof. By definition, the graph K_P is the orbit of P under $\mathcal{G}_{\mathcal{A}}$. Since two operators $\Omega_{\mathcal{A}}(\alpha)$, $\Omega_{\mathcal{A}}(\alpha')$ agree on some particular term if and only if they agree everywhere if and only if $\alpha \equiv_{\mathcal{A}} \alpha'$ holds, the action becomes faithful when one collapses $\mathcal{G}_{\mathcal{A}}$ to $\widetilde{\mathcal{G}}_{\mathcal{A}}$. The argument is similar for $\mathcal{M}_{\mathcal{A}}$. □

We deduce a purely abstract (or syntactic) construction of the (oriented) graphs K_P.

Corollary 2.10. *Assume that $x_1, \ldots, x_n$ are the addresses such that the term P lies in the domain of the operator $\Omega_{\mathcal{A}}(x_i)$. Then the oriented graph K^+_P is the closure under $C_{\mathcal{A}}$-right reduction of n initial arrows labelled $x_1, \ldots, x_n$.*

Proof. Let K'_P be the above subgraph of the Cayley graph of $\mathcal{M}_{\mathcal{A}}$. By faithfulness of the action of $\mathcal{M}_{\mathcal{A}}$, we may identify K'_P with its projection on K^+_P, and the point is to show that K'_P covers all of K^+_P. We claim that, for every vertex Q of K'_P, all successors of Q in K^+_P belong to K'_P. By definition, the property is true for the initial vertex P, and it suffices to show that the property holds for the immediate successors of Q when it holds for Q. Assume that R is the image of Q under $\Omega_{\mathcal{A}}(y)$, and that

$y_1, \ldots, y_q$ are the points in $\mathbb{S}$ such that the term Q belongs to the domain of $\Omega_{\mathscr{A}}(y_j)$. A direct verification shows that the points z such that the term R belongs to the domain of $\Omega_{\mathscr{A}}(z)$ are exactly the first factors of the complements $C_{\mathscr{A}}(y_1, y), \ldots, C_{\mathscr{A}}(y_q, y)$ which are nonempty, and this is exactly the needed fact. □

For instance, the graphs of Fig. 2 show the construction in the cases of the terms $X^{(4)}$ and $X^{(5)}$ as the closure, respectively, of the initial edges $\{\Lambda, 1\}$ and $\{\Lambda, 1, 11\}$ (printed in bold) under $C_{\mathscr{A}}$-reduction. Observe that this construction shows that the latter graphs when viewed as simplicial complexes are, respectively, a 1-sphere and a 2-sphere. More generally, the coherence of $C_{\mathscr{A}}$ implies that the closure of n initial edges is topologically an $(n-1)$-sphere.

Remark We have seen that the coherence of the complement $C_{\mathscr{A}}$ implies that the graphs K_P are subgraphs of the Cayley graph of $\mathscr{M}_{\mathscr{A}}$. Conversely, the faces of these graphs are commutative by construction, so that the property for the Cayley graph of being a union of such graphs essentially implies the coherence of the complement. Hence the existence of embeddings of the graphs K_P into the Cayley graph of $\mathscr{M}_{\mathscr{A}}$ and the coherence of the complement $C_{\mathscr{A}}$ are essentially equivalent properties.

3. Self-distributivity versus associativity

We now sketch a comparison between the previous case of associativity and the case of the left selfdistributivity identity

$$X * (Y * Z) = (X * Y) * (X * Z). \tag{$\mathscr{D}$}$$

We shall use in the sequel the same notations as previously, just replacing the subscripts "$\mathscr{A}$" by "$\mathscr{D}$". The study of that case was motivated by the fact that results like the decidability of the word problem or the concrete description of the free structures were missing until recently, or, strangely enough, were available only using some very strong logical assumptions (c.f. [10]). Answering such questions is of course straightforward in the case of associativity. A complete analysis of distributivity appears in [4], and we just wish to emphasize here the common features and the discrepancies between both cases.

So $=_{\mathscr{D}}$ will be the congruence on $\mathscr{T}(\Sigma)$ generated by all pairs

$$(\, Q * (R * S)\,,\ (Q * R) * (Q * S)),$$

and $\Omega_{\mathscr{D}}$ will be the partial operator on $\mathscr{T}(\Sigma)$ which maps every term of the form $Q * (R * S)$ to the corresponding term $(Q * R) * (Q * S)$. The analog of Lemma 1.1 clearly holds, and we have to find the relations between the operators $\Omega_{\mathscr{D}}(x)$. Again we find some general relations, namely

$$\Omega_{\mathscr{D}}(z0x \cdot z1y) = \Omega_{\mathscr{D}}(z1y \cdot z0x) \tag{$\perp$}$$

("nonoverlapping" case) and

$$\Omega_{\mathscr{D}}(z0x \cdot z) = \Omega_{\mathscr{D}}(z \cdot z00x \cdot z10x)$$

$$\Omega_{\mathscr{D}}(z10x \cdot z) = \Omega_{\mathscr{D}}(z \cdot z01x)$$

$$\Omega_{\mathscr{D}}(z11x \cdot z) = \Omega_{\mathscr{D}}(z \cdot z11x)$$

("strictly nested" case). The remaining case is the one of z and $z1$, and we find

$$\Omega_{\mathscr{D}}(z1 \cdot z \cdot z1 \cdot z0) = \Omega_{\mathscr{D}}(z \cdot z1 \cdot z)$$

a specific relation of distributivity where a heptagon replaces Mac Lane–Stasheff's pentagon.

As in Section 1, we introduce the congruence $\equiv^+_{\mathscr{D}}$ on $\mathbb{S}^*$ generated by the pairs of positive sequences appearing in the above relation, and its completion $\equiv_{\mathscr{D}}$ for arbitrary sequences, and let $\widetilde{\mathscr{M}}_{\mathscr{D}}$ and $\widetilde{\mathscr{G}}_{\mathscr{D}}$ be the associated monoid and group. The analog of Lemma 1.2 holds, and we turn to the converse question of whether the compatibility of $\Omega_{\mathscr{D}}(\alpha)$ and $\Omega_{\mathscr{D}}(\beta)$ implies the $\equiv^+_{\mathscr{D}}$-equivalence of α and β.

The problem again is to define inside $(\mathbb{S} \cup \mathbb{S}^{-1})^*$ a syntactic copy of the terms of $\mathscr{T}(X)$. The quotient $\mathscr{T}(X)/=_{\mathscr{D}}$, i.e., the free left distributive structure with one generator, is a much more complicated structure than $\mathscr{T}(X)/=_{\mathscr{A}}$, which is the free semigroup with one generator, and therefore we cannot expect a simple result like the one of Lemma 2.1. Nevertheless, it happens that there still exists a way of generating every term in $\mathscr{T}(X)$ from some canonical simple terms, actually again the right powers $X^{(n)}$.

Lemma 3.1. *For any term P in $\mathscr{T}(X)$, the equivalence $X^{(n)} =_{\mathscr{D}} P * X^{(n-1)}$ holds for n large enough.*

This result is effective, and its proof can be converted into the following analog of Lemma 2.2.

Lemma 3.2. *Let $\chi_{\mathscr{D}}$ be the mapping of $\mathscr{T}(X)$ into $(\mathbb{S} \cup \mathbb{S}^{-1})^*$ inductively defined by the formulas $\chi_{\mathscr{D}}(X) = \varepsilon$ and*

$$\chi_{\mathscr{D}}(Q * R) = \chi_{\mathscr{D}}(Q) \cdot 1\chi_{\mathscr{D}}(R) \cdot \Lambda \cdot 1\chi_{\mathscr{D}}(Q)^{-1}.$$

Then for every term P and every integer n which is large enough, the operator $\Omega_{\mathscr{D}}(\chi_{\mathscr{D}}(P))$ maps the term $X^{(n)}$ to $P * X^{(n-1)}$.

A technically important fact is that the characteristic sequences $\chi_{\mathscr{D}}(P)$ entail in general negative factors. This will forbid to directly use them to study the positive congruence $\equiv^+_{\mathscr{D}}$. Now the main argument remains the same one: if the operator $\Omega_{\mathscr{D}}(\alpha)$ maps the term P to the term P', both $\Omega_{\mathscr{D}}(\chi_{\mathscr{D}}(P'))$ and $\Omega_{\mathscr{D}}(\chi_{\mathscr{D}}(P) \cdot 0\alpha)$ map (for n large enough) the term $X^{(n)}$ to $P' * X^{(n-1)}$, and therefore the corresponding sequences

are conjectured to be $\equiv_{\mathscr{D}}$-equivalent. This is actually true, which again constitutes a nontrivial intrinsic property of the considered identity, here left distributivity.

Lemma 3.3. *If* α *belongs to* $(\mathbb{S} \cup \mathbb{S}^{-1})^*$ *and* $\Omega_{\mathscr{D}}(\alpha)$ *maps* P *to* P', *the equivalence*

$$\chi_{\mathscr{D}}(P') \equiv^+_{\mathscr{D}} \chi_{\mathscr{D}}(P \cdot 0\alpha)$$

holds in $(\mathbb{S} \cup \mathbb{S}^{-1})^*$.

Now the only conclusion we extract is that, if both $\Omega_{\mathscr{D}}(\alpha)$ and $\Omega_{\mathscr{D}}(\beta)$ map P to P', then both sequences 0α and 0β are $\equiv_{\mathscr{D}}$-equivalent to $\chi_{\mathscr{D}}(P') \cdot \chi_{\mathscr{D}}(P)^{-1}$, which is still far for proving $\alpha \equiv_{\mathscr{D}} \beta$. (Observe that exclusively using the sequences $\chi'_{\mathscr{A}}(P)$ in Section 2 would lead to a similar problem.)

Actually the missing property, namely the fact that $0\alpha \equiv_{\mathscr{D}} 0\beta$ implies $\alpha \equiv_{\mathscr{D}} \beta$, will follow from the study of the congruence $\equiv^+_{\mathscr{D}}$ along the lines we sketched in Section 2 for $\equiv^+_{\mathscr{A}}$. Indeed, it is really easy to show that the corresponding implication holds in the case of *positive* sequences, i.e., that for u, v in $\mathbb{S}^*$ the equivalence $0u \equiv^+_{\mathscr{D}} 0v$ implies $u \equiv^+_{\mathscr{D}} v$. The problem is then to obtain for every sequence α in $(\mathbb{S} \cup \mathbb{S}^{-1})^*$ a convenient decomposition of the form $\alpha \equiv_{\mathscr{D}} u \cdot v^{-1}$ where u and v are positive sequences. This is exactly what the reduction associated with a right complement does. Now by very construction the congruence $\equiv^+_{\mathscr{D}}$ is associated with a right complement $C_{\mathscr{D}}$, and the point is to study the coherence of this complement and the termination of the corresponding reductions.

For the coherence property, we invoke again the subsequent results of Section 4 to reduce to the triples $(1, y, \Lambda)$. One still has to separate five cases corresponding to y being of the form $0y'$, $10y'$, $110y'$, $111y'$ or 111. The latter case is the most intricate, and the explicit formulas are

$$\begin{aligned}
&C_{\mathscr{D}^*}(C_{\mathscr{D}}(\Lambda,1), C_{\mathscr{D}}(11,1)) = \Lambda \cdot 1 \cdot 0 \cdot 11 \cdot 01 \cdot 10 \cdot 00 \\
&\quad \equiv^+_{\mathscr{D}} \Lambda \cdot 1 \cdot 11 \cdot 10 \cdot 0 \cdot 01 \cdot 00 = C_{\mathscr{D}^*}(C_{\mathscr{D}}(\Lambda,11), C_{\mathscr{D}}(1,11)), \\
&C_{\mathscr{D}^*}(C_{\mathscr{D}}(1,11), C_{\mathscr{D}}(\Lambda,11)) = 1 \cdot \Lambda \cdot 11 \cdot 1 \cdot 01 \cdot 0 \\
&\quad \equiv^+_{\mathscr{D}} 1 \cdot 11 \cdot 10 \cdot \Lambda \cdot 1 \cdot 0 = C_{\mathscr{D}^*}(C_{\mathscr{D}}(1,\Lambda), C_{\mathscr{D}}(11,\Lambda)), \\
&C_{\mathscr{D}^*}(C_{\mathscr{D}}(11,\Lambda), C_{\mathscr{D}}(1,\Lambda)) = 11 \cdot 1 \cdot \Lambda = C_{\mathscr{D}^*}(C_{\mathscr{D}}(11,1), C_{\mathscr{D}}(\Lambda,1)).
\end{aligned}$$

Fig. 3 illustrates the three involved reductions, and is to be compared with Fig. 1 that corresponds in the case of associativity. We conclude that the complement $C_{\mathscr{D}}$ is coherent. The lengths of the sequences u' satisfying $u' \equiv^+_{\mathscr{D}} u$ are bounded because every operator $\Omega_{\mathscr{D}}(x)$ strictly increases the size of any term it is applied to (and no operator $\Omega_{\mathscr{D}}(u)$ associated with a positive sequence u may have an empty domain). So by Lemma 2.6 we know that the monoid $\widetilde{\mathscr{M}}_{\mathscr{D}}$ admits left cancellation.

New ingredients are needed to guarantee that $C_{\mathscr{D}}$-reduction have to terminate, for the number of distinct terms that can be deduced using distributivity from a given term may clearly be infinite, so that the simple argument of Section 2 does not apply any more. On the other hand, the length of the complements $C_{\mathscr{D}}(x, y)$ may be 2 or 3,

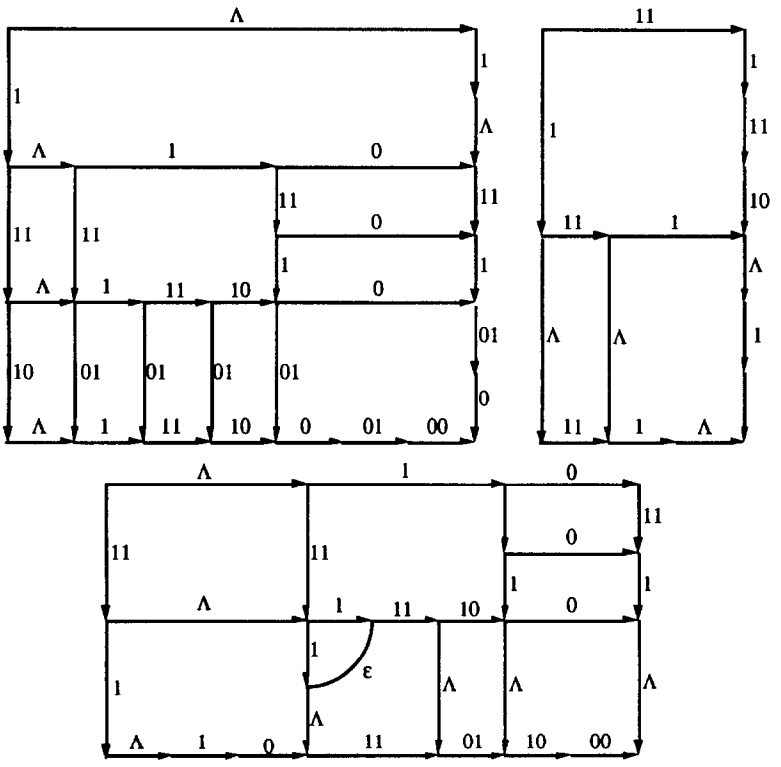

Fig. 3. Coherence of the complement $C_{\mathscr{D}}$, case of $\{\Lambda, 1, 11\}$.

and therefore there is no direct evidence for the termination. The strategy used in [4] consists in guessing the explicit form of the sequences in the closure of the set $\mathbb{S}$ under iterated application of $C_{\mathscr{D}}$. Call such sequences *simple* sequences. The complement of two such simple sequences is proved by a direct computation to be a simple sequence, and this proves that $C_{\mathscr{D}}$-reduction always terminates because it preserves the *degree* of the sequences defined as the minimal number of simple sequences or inverses of simple sequences the given sequence can be expressed as a product of. The definition of simple sequences originates in the existence of a *lower common extension* for any term P with respect to left distributivity: there exists a (least) positive sequence $\Delta_{\mathscr{D}}(P)$ that is, up to $\equiv^+_{\mathscr{D}}$-equivalence, a right multiple of every x in $\mathbb{S}$ such that the term P belongs to the domain of the operator $\Omega_{\mathscr{D}}(x)$. Simple sequences are the divisors of some sequence $\Delta_{\mathscr{D}}(P)$.

Once the termination of $C_{\mathscr{D}}$-reduction is known (which means that the monoid $\tilde{\mathscr{M}}_{\mathscr{D}}$ is right regular), some care is still needed to conclude that $0\alpha \equiv_{\mathscr{D}} 0\beta$ implies $\alpha \equiv_{\mathscr{D}} \beta$. Under the hypothesis $0\alpha \equiv_{\mathscr{D}} 0\beta$ there exist positive sequences u, u', v, v' satisfying

$$0\alpha \equiv_{\mathscr{D}} 0u \cdot 0v^{-1} \quad \text{and} \quad 0\beta \equiv_{\mathscr{D}} 0u' \cdot 0v' - 1,$$

and it is known that $0u \equiv^+_{\mathscr{D}} 0u'$ implies $u \equiv^+_{\mathscr{D}} u'$. But the hypothesis $u \cdot v^{-1} \equiv_{\mathscr{D}} u' \cdot v'^{-1}$ does not imply $u \equiv^+_{\mathscr{D}} u'$ and $v \equiv^+_{\mathscr{D}} v'$ in general. At this point the crucial property is given

by the coherence of the complement:

Lemma 3.4 (Dehornoy [6]). *Under the hypotheses of Lemma 2.6, the equivalence* $u \cdot v^{-1} \equiv_{\mathscr{D}} u' \cdot v'^{-1}$ *implies the existence of positive sequences* w, w' *satisfying*

$$u \cdot w \equiv^{+}_{\mathscr{D}} u' \cdot w' \quad \text{and} \quad v \cdot w \equiv^{+}_{\mathscr{D}} v' \cdot w'.$$

Then from $0u \cdot 0v^{-1} \equiv_{\mathscr{D}} 0u' \cdot 0v'^{-1}$ we deduce $0u \cdot w \equiv^{+}_{\mathscr{D}} 0u' \cdot w'$ and $0v \cdot w \equiv^{+}_{\mathscr{D}} 0v' \cdot w'$ for some w, w', which easily leads to $u \cdot w_1 \equiv^{+}_{\mathscr{D}} u' \cdot w'_1$ and $v \cdot w_1 \equiv^{+}_{\mathscr{D}} v' \cdot w'_1$ for some w_1, w'_1, and therefore to $u \cdot v^{-1} \equiv_{\mathscr{D}} u' \cdot v'^{-1}$, yielding the desired result:

Proposition 3.5. *For any sequences* α, β *in* $(\mathbb{S} \cup \mathbb{S}^{-1})^*$, *the operators* $\Omega_{\mathscr{D}}(\alpha)$ *and* $\Omega_{\mathscr{D}}(\beta)$ *are compatible if and only if their domains are nonempty and the equivalence* $\alpha \equiv_{\mathscr{D}} \beta$ *holds.*

It follows that the monoid $\mathscr{G}_{\mathscr{D}}$ quotiented by compatibility identifies with a subset of the group $\widetilde{\mathscr{G}}_{\mathscr{D}}$. This subset is a strict subset because the domain of the operator $\Omega_{\mathscr{D}}(\alpha)$ may be empty, what we mention never happens with the operators $\Omega_{\mathscr{A}}(\alpha)$.

This result settles the problem of describing $\mathscr{G}_{\mathscr{D}}$ in a satisfactory way, i.e., shows that the relations listed above, and specially the heptagonal one, generate all relations between the operators $\Omega_{\mathscr{A}}(x)$. Due to the fact that the characteristic sequences we used in the case of distributivity involve negative factors, we cannot directly obtain a corresponding result for the case of positive sequences. We conjecture that the monoids $\mathscr{M}_{\mathscr{D}}$ and $\widetilde{\mathscr{M}}_{\mathscr{D}}$ are isomorphic, i.e., that for positive sequences u, v the compatibility of the operators $\Omega_{\mathscr{D}}(u)$ and $\Omega_{\mathscr{D}}(v)$ (which is known to be merely equivalent to their equality) is equivalent to $u \equiv^{+}_{\mathscr{D}} v$.

By the results of [6] it is known that a sufficient condition for the above conjecture be true is that the monoid $\widetilde{\mathscr{M}}_{\mathscr{D}}$ admits right cancellation. Now, like for the case of associativity, we observe that the opposite monoid of $\mathscr{M}_{\mathscr{D}}$ is the monoid associated with the operators $\Omega^{-1}_{\mathscr{D}}(x)$, and therefore appears in connection with "reversed" left distributivity identity

$$(X * Y) * (X * Z) = X * (Y * Z). \qquad (\mathscr{D}^o)$$

Up to reversing the order of all factors, the relations given above in the case of the identity $(\mathscr{D})$ hold for $(\mathscr{D}^o)$. In particular, it is easily verified that the congruence $\equiv^{+}_{\mathscr{D}^o}$ is associated with a right complement $C_{\mathscr{D}^o}$. So by Lemma 2.6 the coherence of the complement $C_{\mathscr{D}^o}$ would be a sufficient condition for the monoid $\widetilde{\mathscr{M}}_{\mathscr{D}^o}$ to be left cancellative, i.e., for the monoid $\widetilde{\mathscr{M}}_{\mathscr{D}}$ to be right cancellative. Unfortunately, this condition does not hold, as the following counterexample shows:

$$C^*_{\mathscr{D}^o}(C_{\mathscr{D}^o}(\Lambda, 11), C_{\mathscr{D}^o}(1, 11)) = C^*_{\mathscr{D}^o}(\Lambda, 10 \cdot 1 \cdot 11) = 00 \cdot 0 \cdot \Lambda \cdot 10 \cdot 1 \cdot 11,$$
$$C^*_{\mathscr{D}^o}(C_{\mathscr{D}^o}(\Lambda, 1), C_{\mathscr{D}^o}(11, 1)) = C^*_{\mathscr{D}^o}(0 \cdot \Lambda \cdot 1, 11 \cdot 1)$$

and the $C_{\mathscr{D}^o}$-reduction of the sequence $1^{-1} \cdot \Lambda^{-1} \cdot 0^{-1} \cdot 11 \cdot 1$ does not terminate, so that the latter complement does not exist.

This does not prove that the monoid $\widetilde{\mathcal{M}}_{\mathcal{D}}$ is not right cancellative, but it shows that some new argument is needed. To sum up we have

Lemma 3.6. *The following are equivalent:*

(i) *The monoids $\mathcal{M}_{\mathcal{D}}$ and $\widetilde{\mathcal{M}}_{\mathcal{D}}$ are isomorphic.*

(ii) *The monoid $\widetilde{\mathcal{M}}_{\mathcal{D}}$ admits right cancellation.*

(iii) *The congruence $\equiv^{+}_{\mathcal{D}}$ is the restriction of the congruence $\equiv_{\mathcal{D}}$ to positive sequences.*

(iv) *The monoid $\widetilde{\mathcal{M}}_{\mathcal{D}}$ embeds in the group $\widetilde{\mathcal{G}}_{\mathcal{D}}$.*

About point (iii) above Lemma 3.4 implies that, for positive sequences u, v, the equivalence $u \equiv_{\mathcal{D}} v$ holds if and only if the equivalence $u \cdot w \equiv^{+}_{\mathcal{D}} v \cdot w$ holds for some (positive) sequence w.

We leave the previous lemma pending. This means that the question of describing the "distribuhedra", defined in the obvious way, in terms of the Cayley graph of the monoid $\widetilde{\mathcal{M}}_{\mathcal{D}}$ remains open. By Proposition 3.5 we know that the group $\widetilde{\mathcal{G}}_{\mathcal{D}}$ operates transitively and faithfully on the distribuhedra, but the oriented version of this result relies on a proof of the properties of Lemma 3.6. So presently we cannot guarantee that no collapse occurs in the passage from the Cayley graph of $\widetilde{\mathcal{M}}_{\mathcal{D}}$ to the distribuhedra. Observe that, excepted in some trivial cases where it reduces to a single point, the distribuhedra are always infinite graphs. The approach of [2] introduces a stratification in these graphs so that each level is finite. The first level is essentially described ("simple extensions" of [4]), but the general case will certainly require new developments.

So the examples of associativity and distributivity prove to be rather similar although distributivity requires much more sophisticated algebraic treatment because it does not preserve the size of the terms. Moreover, the fact that the associativity identity is syntactically symmetric enables to automatically convert one-sided results into two-sided ones, what obviously fails in the case of distributivity. But in both cases the crucial point for proving that some given relations constitute an exhaustive list of generators for all relations between the involved operators is the possibility of associating to every term a canonical sequence such that the associated operator constructs this term from some uniform starting term. More precisely, we use the existence, for each pair of terms (P, P') in $\mathcal{T}(X)$, of a canonical sequence such that the associated operator maps some term where P occurs into the term obtained by replacing P by P'.

As a final remark, let us observe that the (true) fact that $0\alpha \equiv_{\mathcal{A}} 0\beta$ implies $\alpha \equiv_{\mathcal{A}} \beta$ could be established following the scheme sketched here for distributivity. Therefore, the result of Proposition 2.4 could also be obtained by only using the sequences $\chi'_{\mathcal{A}}(P)$ and then applying the above implication.

4. The coherence of the complement in the general case

The previous approach applies of course to the case of any identity, or even of any set of identities. In the latter case, one just has to introduce as many elementary operators

as different involved identities. Similarly, if several operators are used one can still use the same analysis, but it will be necessary to take into account not only the position where an identity is applied to a term but also the name of the operators occurring at each node of the tree between the root and the considered position. Practically, this entails such a combinatorial complexity for the corresponding geometric relations that the algebraic study of the associated monoid might turn to be intractable in most cases (but computers could be used to systematically verify conditions like complement coherence).

We shall just consider here the case of one identity involving one binary operation, a direct generalization of the cases of associativity and left distributivity. Such an identity has the generic form

$$F(X,Y,\ldots) = G(X,Y,\ldots), \tag{$\mathscr{I}$}$$

where F and G are fixed terms in $\mathscr{T}(\Sigma)$. Like previously, we introduce the operator $\Omega_{\mathscr{I}}$ that maps every term with the form $F(P,Q,\ldots)$ to the corresponding term $G(P,Q,\ldots)$. To guarantee that $\Omega_{\mathscr{I}}$ as well as its inverse are functional, we have to assume that the same variables occur in F and G. This hypothesis, however, can be dropped when $\Omega_{\mathscr{I}}$ is introduced directly on the identities using unification like in [3].

We look for the relations satisfied by the operators $\Omega_{\mathscr{I}}(x)$ for x in $\mathbb{S}$. Of course, we cannot assume anything for the specific relations, but we still have the two types of general relations met previously. The relations for nonoverlapping subterms are always

$$\Omega_{\mathscr{I}}(z0x \cdot z1y) = \Omega_{\mathscr{I}}(z1y \cdot z0x). \tag{$\perp$}$$

The relations for strictly nested subterms take the form

$$\Omega_{\mathscr{I}}(zsx \cdot zs_1x \cdot \cdots \cdot zs_px \cdot z) = \Omega_{\mathscr{I}}(z \cdot zt_1x \cdot \cdots \cdot zt_qx), \tag{$\mathscr{S}$}$$

where s is any point in the support of the term F, $s_1, \ldots, s_p$ are the other points in the support of F where the variable Z occurring at s again occurs (if any), and $t_1, \ldots, t_q$ are the points in the support of G where Z occurs. We assume that some ordering on the set $\mathbb{S}$ has been fixed. The choice of this ordering is not essential since distinct points in the support of a term F are orthogonal, and therefore the various relations (s) we could write are equivalent owing to relations $(\perp)$. In the above situation we say that the points $s_1, \ldots, s_p$ are the *companions* of s with respect to $\mathscr{I}$, and that the points $t_1, \ldots, t_q$ are the *cocompanions* of s. For instance, in the case of left distributivity, the point 0 has no companion, but it admits 00 and 10 as cocompanions.

By construction, the above relations are associated with the partial complement $C_{\mathscr{I}}$ defined by

$$C_{\mathscr{I}}(x,y) = \begin{cases} \varepsilon & \text{if } x \text{ and } y \text{ are equal,} \\ x & \text{if } x \text{ and } y \text{ are orthogonal,} \\ xs_1z \cdot \cdots \cdot xs_pz \cdot x & \text{if } y \text{ is } xsz \text{ for some } s \text{ in the support of } F \text{ and } s_1, \ldots, s_p \text{ are the companions of } s \text{ with respect to } \mathscr{I}, \\ yt_1z \cdot \cdots \cdot yt_qz & \text{if } x \text{ is } ysz \text{ for some } s \text{ in the support of } F \text{ and } t_1, \ldots, t_q \text{ are the cocompanions of } s \text{ with respect to } \mathscr{I}. \end{cases}$$

Definition The point s is *critical* for the identity $F = G$ if s is nonvoid and is a strict prefix of some point in the support of the term F.

The missing relations in the list above, and therefore the missing cases in the above complement, correspond to pairs (x, xs) where s is critical for $\mathscr{I}$. In the cases of associativity and left distributivity, the term F is $X*(Y*Z)$, and 1 is the only critical point.

In the previous cases, the existence of the right complement and the coherence pro perty of this complement turned out to be crucial. We wish here to point out that a large part of this coherence property follows from its very definition. This results in a more simple criterion for proving full coherence by means of a reduced number of verifications. We say that a mapping f of $\mathbb{S}^2$ into $\mathbb{S}^*$ is *prefix-compatible* if $f(zx, zy)$ is always equal to $zf(x,y)$. The mapping $C_{\mathscr{I}}$ is obviously prefix-compatible, as well as the complements $C_{\mathscr{A}}$, $C_{\mathscr{D}}$ or $C_{\mathscr{D}^o}$ previously considered. Actually, every complement extending $C_{\mathscr{I}}$ arising from the choice of an additional relation for each critical point will be prefix-compatible.

Proposition 4.1. *Assume that C is a prefix-compatible complement extending the mapping $C_{\mathscr{I}}$. Let $\equiv^+$ be the congruence on $\mathbb{S}^*$ associated with C, and $\mathscr{R}(x,y,z)$ stand for*

$$C^*(C(x,y), C(z,x)) \equiv^+ C^*(C(x,z), C(y,z)).$$

Then C is coherent if and only if the relations $\mathscr{R}(x,y,\Lambda)$, $\mathscr{R}(y,\Lambda,x)$ and $\mathscr{R}(\Lambda,x,y)$ hold when x is critical for $\mathscr{I}$ and either x is orthogonal to y or x is a strict prefix of y.

Proof. We shall prove the conjunction of $\mathscr{R}(x,y,z)$, $\mathscr{R}(y,z,x)$ and $\mathscr{R}(z,x,y)$ for every triple (x,y,z) in $\mathbb{S}^3$, using an exhaustive review of all possible cases. By prefix-compatibility we may assume that the greatest common prefix of x, y and z is Λ, and by symmetry we may choose the ordering of x, y, z as we wish. Also observe that when two points, say, for instance x and y, play symmetric roles it is sufficient to

establish the relations $\mathscr{R}(x,y,z)$ and $\mathscr{R}(z,x,y)$ since the last relation $\mathscr{R}(y,z,x)$ is an instance of the first one.

Case 1. Two points are equal. We may assume $x = y$, and we obtain

$$\begin{aligned} C^*(C(x,y),C(z,y)) &= C^*(\varepsilon, C(z,x)) = \varepsilon \\ &= C^*(C(x,z),C(x,z)) = C^*(C(x,z),C(y,z)), \\ C^*(C(z,x),C(y,x)) &= C^*(C(z,x),\varepsilon) = C(z,x) = C(z,y) \\ &= C^*(C(z,y),\varepsilon) = C^*(C(z,y),C(x,y)), \end{aligned}$$

which is enough by the last remark above.

Case 2. One point is orthogonal to the greatest common prefix of the other ones. We may assume that z is orthogonal to the common prefix z' of x and y. The hypothesis that C is prefix-compatible implies that each factor in $C(x,y)$ and $C(y,x)$ begins with z' and therefore that z is orthogonal to each such factor. One obtains

$$\begin{aligned} C^*(C(x,y),C(z,y)) &= C^*(C(x,y),z) = C(x,y) \\ &= C^*(x,y) = C^*(C(x,z),C(y,z)), \\ C^*(C(z,x),C(y,x)), &= C^*(z,C(y,x)) = z \\ &= C^*(z,C(x,y)) = C^*(C(z,y),C(x,y)). \end{aligned}$$

Case 3. One point is a prefix of the other ones. We may assume that z is a prefix of the greatest common prefix z' of x and y. By prefix-compatibility we may assume $z = \Lambda$.

Case 3.1. The points x and y are not critical for $\mathscr{S}$. There exists unique points s and t in the support of F such that x is sx' and y is ty'. Let $s_1, \ldots, s_p$ (resp. $t_1, \ldots, t_q$) be the companions of s (resp. of t), and $s'_1, \ldots, s'_{p'}$ (resp. $t'_1, \ldots, t'_{q'}$) be the cocompanions of s (resp. of t).

Case 3.1.1. The points s and t coincide. For $\mathscr{R}(x,y,z)$ we have (because s is orthogonal to each s_i)

$$\begin{aligned} C^*(C(x,y),C(z,x)) &= C^*(sC(x',y'),C(\Lambda,sx')) \\ &= C^*(sC(x',y'),s_1x' \cdot \cdots \cdot s_px' \cdot \Lambda) \\ &= C^*(sC(x',y'),\Lambda) \\ &= s'_1C(x',y') \cdot \cdots \cdot s'_{p'}C'(x',y') \\ &= C^*(s'_1x' \cdot \cdots \cdot s'_{p'}x', s'_1y' \cdot \cdots \cdot s'_{p'}y') \\ &= C^*(C(sx',\Lambda),C(sy',\Lambda)) = C^*(C(x,z),C(y,z)), \end{aligned}$$

while for $\mathscr{R}(z,x,y)$ we find

$$\begin{aligned}
C^*(C(z,x),C(y,x)) &= C^*(C(\Lambda,sx'),C(sy',sx'))\\
&= C^*(s_1x'\cdot\cdots\cdot s_px'\cdot\Lambda,sC(y',x'))\\
&= s_1x'\cdot\cdots\cdot s_px'\cdot C^*(\Lambda,sC(y',x'))\\
&= s_1x'\cdot\cdots\cdot s_px'\cdot s_1C(y',x')\cdot\cdots\cdot s_pC(y',x')\cdot\Lambda\\
&\equiv s_1x'\cdot s_1C(y',x')\cdot\cdots\cdot s_px'\cdot s_pC(y',x')\cdot\Lambda.
\end{aligned}$$

Then $C^*(C(z,y),C(x,y))$ leads to a similar formula where $s_iy'\cdot s_iC(x',y')$ replaces $s_ix'\cdot s_iC(y',x')$, and because these sequences are pairwise $\equiv^+$-equivalent $\mathscr{R}(z,x,y)$ follows.

Case 3.1.2. The point s is a companion of the point t. Assume that s is t_j.

$$\begin{aligned}
C^*(C(x,y),C(z,y)) &= C^*(x,C(\Lambda,y)) = C(sx',t_1y'\cdot\cdots t_qy'\cdot\Lambda)\\
&= C^*(sC(x',y'),\Lambda)\\
&= s_1'C(x',y')\cdot\cdots\cdot s_{p'}'C(x',y')\\
&= C^*(s_1'x'\cdot\cdots\cdot s_{p'}'x',t_1'y'\cdot\cdots\cdot t_{q'}')\\
&= C^*(C(x,\Lambda),C(y,\Lambda)) = C^*(C(x,z),C(y,z))\\
C^*(C(z,x),C(y,x)) &= C^*(C(\Lambda,t_jx'),C(ty',t_jx')) = C^*(C(\Lambda,t_jx'),ty),\\
&\equiv t_1x'\cdot\cdots\cdot\widehat{t_jx'}\cdot\cdots\cdot t_qx'\cdot\Lambda\\
&\equiv C^*(C(\Lambda,ty),t_jx') = C^*(C(\Lambda,ty'),C(t_jx',ty'))\\
&= C^*(C(z,y),C(x,y)).
\end{aligned}$$

Case 3.1.3 The point s is distinct from t and its companions. Because the point s is orthogonal to each of $t_1,\ldots,t_q$, and the points s_i' and t_j' are pairwise orthogonal, one has

$$\begin{aligned}
C^*(C(x,y),C(z,y)) &= C^*(x,C(\Lambda,y)) = C(sx',t_1y'\cdot\cdots t_qy'\cdot\Lambda)\\
&= C(sx',\Lambda) = s_1'x'\cdot\cdots\cdot s_{p'}'x'\\
&= C^*(s_1'x'\cdot\cdots\cdot s_{p'}'x',t_1'y'\cdot\cdots\cdot t_{q'}')\\
&= C^*(C(x,\Lambda),C(y,\Lambda)) = C^*(C(x,z),C(y,z)),\\
C^*(C(z,x),C(y,x) &= C^*(C(\Lambda,sx'),C(ty',sx'))\\
&= C^*(s_1x'\cdot\cdots\cdot s_px'\cdot\Lambda,ty')\\
&= s_1x'\cdot\cdots\cdot s_px'\cdot t_1y'\cdot\cdots\cdot t_qy'\cdot\Lambda,
\end{aligned}$$

and because the points s_i and t_j are pairwise distinct and therefore orthogonal the factors s_ix' and t_jy' above can be permuted, so that the above expression for $C^*(C(z,x),C(y,x))$ is $\equiv$-equivalent to the similar one obtained from $C^*(C(z,y),C(x,y))$. This finishes Case 3.1.

Case 3.2 At least one of x, y is critical for $\mathscr{I}$. We assume that the point x is critical. Then no general argument works and a specific verification is needed for the remaining choices of y. We may assume that y is not a prefix of x, for, in the latter case, y has to be critical as well and we can exchange x and y. So it remains to consider the case of y being orthogonal to x, and the case of x being a strict prefix of y. □

The examples of associativity and left distributivity suggest that further reductions in the number of cases could appear. In particular, for every critical point x as above there must exist a *finite* set of points A_x such that the desired equivalences hold for any y whenever they hold for y in A_x. The reason is that, for y large enough, the equalities

$$C(x, yz) = C(x, y) \quad \text{and} \quad C(yz, x) = C(y, x)z$$

hold for every z. For instance, in the cases of associativity and distributivity one can take for A_1 the set $\{0, 10, 11, 110, 111\}$. We leave the question of giving a uniform definition of such sets A_x open in the general case.

References

[1] P. Cartier, Développements récents sur les groupes de tresses, applications à la topologie et à l'algèbre, Séminaire Bourbaki, exposé 716 (1989).
[2] P. Dehornoy, Free distributive groupoids, J. Pure Appl. Algebra 61 (1989) 123–146.
[3] P. Dehornoy, Structural monoids associated to equational varieties, Proc. Amer. Math. Soc. 117 (1993) 293–304.
[4] P. Dehornoy, Braid groups and left distributive operations, Trans. Amer. Math. Soc., 345 (1994) 115–151.
[5] P. Dehornoy, From large cardinals to braids via distributive algebra, J. Knot Theory and Ramifications 4 (1995) 33–79.
[6] P. Dehornoy, Groups with a complemented presentation, J. Pure Appl. Algebra, to appear.
[7] D.B. Epstein et al., Word Processing in Groups (Jones and Barlett, 1992).
[8] M.M. Kapranov, The permutoassociahedron, Mac Lane's coherence theorem and asymptotic zones for the KZ equation, J. Pure Appl. Algebra 85 (1993) 119–142.
[9] A. Lascoux and M.P. Schützenberger, Symmetry and flag manifolds, Lecture Notes in Mathematics, Vol. 996(Springer, Berlin, 1983) 118–144.
[10] R. Laver, The left distributive law and the freeness of an algebra of elementary embeddings, Adv. Math. 91 (1992) 209–231.
[11] S. Mac Lane, Natural associativity and commutativity, Rice Univ. Studies 49 (1963) 28–46.
[12] J.D. Stasheff, Homotopy associativity of H-spaces I, Trans. Amer. Math. Soc. 108 (1963) 275–292.