Commentationes Mathematicae Universitatis Carolinae

Patrick Dehornoy

An associative operation on monogenic left distributive systems

Commentationes Mathematicae Universitatis Carolinae, Vol. 36 (1995), No. 1, 1--6

Persistent URL: http://dml.cz/dmlcz/118724

Terms of use:

© Charles University in Prague, Faculty of Mathematics and Physics, 1995

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* http://project.dml.cz

An associative operation on monogenic left distributive systems

Patrick Dehornoy

Abstract. Term substitution induces an associative operation on the free objects of any equational variety. In the case of left distributivity, the construction can be extended to any monogenic structure.

Keywords: non-associative binary systems
Classification: 20N02

The binary systems made of a set endowed with a product that satisfies the left distributivity identity

(LD) $$x \cdot (y \cdot z) = (x \cdot y) \cdot (x \cdot z)$$

have been studied in [9] and have received recently special attention because of their connection with set theory and braid theory (see for instance [4]). Although the name *LD-groupoid* has been widely used in literature for such systems, we shall use here the name *LD-system*, which avoids any confusion with another possible meaning of the word groupoid. In some of the main presently known LD-systems, like the finite tables A_n investigated by R. Laver ([10]) and A. Drápal ([5] and subsequent papers), a second operation $\circ$ exists so that $\circ$ is associative, $\cdot$ is left distributive with respect to $\circ$ and the following mixed identities are obeyed

(LA_1) $$(x \circ y) \cdot z = x \cdot (y \cdot z)$$

(LA_2) $$x \circ y = (x \cdot y) \circ x.$$

In this case the complete structure has been called an *LD-algebra.* In [2] (building on earlier work in [1] and an observation of J. Zapletal) we have discussed the question of defining an associative operation on an arbitrary LD-system in order to obtain an LD-algebra, and given a partial solution (such an associative operation cannot exist in all cases: for instance a free LD-system cannot be turned into an LD-algebra). Other results about the construction of an associative operation on an LD-system can also be found in [6], while [7] and [8] describe particular examples of LD-algebras. The purpose of this note is to observe that there exists a uniform way to define an associative operation on any monogenic LD-system. The present construction generalizes the former one in the sense that, when an

LD-algebra structure exists, its $\circ$ operation is connected with the new product in a simple way. In the particular case of the structures A_n our construction turns to coincide with the operation $\bullet$ considered in [6].

Assume first that S is any signature, i.e. any sequence of operators with prescribed arities, and X is a fixed letter. Denote by $\mathcal{T}_S[X]$ the set of all well-formed terms constructed using the operators of S and a fixed variable X.

Definition. For P, Q in $\mathcal{T}_S[X]$, the term $P{\times}Q$ is the term obtained from Q by substituting P to every occurrence of X in Q.

It is clear that the operation $\times$ is associative on $\mathcal{T}_S[X]$. Now assume that $\mathcal{I}$ is a set of S-identities, and let $\equiv_{\mathcal{I}}$ be the least congruence on $\mathcal{T}_S[X]$ that contains all instances of the elements of $\mathcal{I}$. Then $\mathcal{T}_S[X]/\equiv_{\mathcal{I}}$ is the monogenic free object in the equational variety associated with $\mathcal{I}$. We observe that the operation $\times$ on $\mathcal{T}_S[X]$ is certainly compatible with the congruence $\equiv_{\mathcal{I}}$: the fact that $P \equiv_{\mathcal{I}} P'$ implies $P{\times}Q \equiv_{\mathcal{I}} P'{\times}Q$ for every term Q is true for any congruence, and the fact that $Q \equiv_{\mathcal{I}} Q'$ implies $P{\times}Q \equiv_{\mathcal{I}} P{\times}Q'$ for every term P is true whenever the congruence is closed under substitution, which is clearly the case here. It follows that the operation $\times$ induces a well-defined associative operation on $\mathcal{T}_S[X]/{\equiv_{\mathcal{I}}}$. Moreover the class of the variable X is in any case a unit of $\times$, so that finally the monogenic free structure $\mathcal{T}_S[X]/{\equiv_{\mathcal{I}}}$ receives this way a monoid structure.

We consider now the particular case of binary systems, i.e. the case when the signature contains a single binary operator. In the case of semigroups, i.e. when the set $\mathcal{I}$ reduces to the associativity identity, the free monogenic structure is simply the set of positive integers equipped with addition, and it is immediate to verify that the associated operation $\times$ is the usual multiplication.

We turn to the case of LD-systems, i.e. the case when the set $\mathcal{I}$ reduces to the left distributivity identity (LD). In the subsequent formulas, missing brackets are always supposed to be added in the rightmost possible position: $x_1 \cdot x_2 \cdot x_3$ stand for $x_1 \cdot (x_2 \cdot x_3)$. We denote by $(\mathfrak{f}, \cdot)$ the free LD-system with one generator, and we use 1 to denote this generator (which is unique). It is known (see [4]) that $\mathfrak{f}$ is endowed with a (unique) linear ordering $<$ such that

$$\sup(x, y) < x \cdot y < x \cdot y'$$

holds for every x, y, y' satisfying $y < y'$. Then the above general construction applies to $(\mathfrak{f}, \cdot)$ and one obtains

Proposition 1. (i) *There exists a unique operation* $\times$ *on* $\mathfrak{f}$ *that is left distributive with respect to* $\cdot$ *and admits* 1 *as a right unit.*

(ii) *The structure* $(\mathfrak{f}, \times, 1)$ *is a monoid and the following identities are satisfied in* $(\mathfrak{f}, \cdot, \times)$

$$(\mathrm{I}_1) \qquad (x \cdot y){\times}z = x \cdot (y{\times}z)$$

$$(\mathrm{I}_2) \qquad (x_1 \cdot \ldots \cdot x_p \cdot 1){\times}z = x_1 \cdot \ldots \cdot x_p \cdot z.$$

(iii) *The monoid* $(\mathfrak{f}, \times, 1)$ *is left cancellative, but not right cancellative, and the inequality* $\sup(x, y) \leq x{\times}y$ *always holds.*

Proof: (i) It is clear by construction that the operation $\times$ induced by term substitution satisfies the equalities $x{\times}1 = x$ and $x{\times}(y \cdot z) = (x{\times}y) \cdot (x{\times}z)$. Conversely these equalities completely determine $\times$ using induction on the size of the terms that represent the elements of $\mathfrak{f}$.

(ii) That $(\mathfrak{f}, \times, 1)$ is a monoid is then a general result. Now (I_1) is a consequence of left distributivity. Clearly the formula is true for $z = 1$. Assume it proved both for z' and z''. We have

$$\begin{aligned}(x \cdot y){\times}(z' \cdot z'') &= ((x \cdot y){\times}z') \cdot ((x \cdot y){\times}z'')\\ &= (x \cdot (y{\times}z')) \cdot (x \cdot (y{\times}z''))\\ &= x \cdot ((y{\times}z') \cdot (y{\times}z''))\\ &= x \cdot (y{\times}(z' \cdot z''))\end{aligned}$$

so that the formula still holds for $z' \cdot z''$. Thus (I_1) is always true, and an immediate induction gives (I_2), using the fact that $1{\times}y$ is simply y.

(iii) Assume that $y < y'$ holds in $\mathfrak{f}$. Then there exists a positive integer k and elements $z_1, \ldots, z_k$ of $\mathfrak{f}$ such that y' is $(..(y \cdot z_1) \cdot z_2..) \cdot z_k$. It follows that $x{\times}y'$ is equal to

$$(..((x{\times}y) \cdot (x{\times}z_1)) \cdot (x{\times}z_2)..) \cdot (x{\times}z_k),$$

and therefore $x{\times}y < x{\times}y'$ is true. This shows that the left translations of $\times$ are strictly increasing, and therefore injective. Thus the monoid $(\mathfrak{f}, \times, 1)$ admits left cancellation. On the other hand the following counterexample shows that the right translations of $\times$ need not be increasing, and that right cancellation is not allowed in $(\mathfrak{f}, \times, 1)$. Write 2 for $1 \cdot 1$, and 3 for $2 \cdot 1$. We have

$$2{\times}2 = (1 \cdot 1){\times}2 = 1 \cdot (1{\times}2) = 1 \cdot 2 = 1 \cdot (1 \cdot 1) = (1 \cdot 1) \cdot (1 \cdot 1) = 2 \cdot 2,$$
$$3{\times}2 = (2 \cdot 1){\times}2 = 2 \cdot (1{\times}2) = 2 \cdot 2.$$

Finally let x be any element of $\mathfrak{f}$. If x is 1, then $x{\times}y$ is y for every y, and clearly $\sup(x, y) \leq x{\times}y$ always holds. Otherwise there exists $p \geq 1$ and $x_1, \ldots, x_p$ such that x is $x_1 \cdot \ldots \cdot x_p \cdot 1$. Then for every y the inequality $1 \leq y$ holds, and, because all left translations of $\cdot$ are strictly increasing, this implies

$$x_1 \cdot \ldots \cdot x_p \cdot 1 \leq x_1 \cdot \ldots \cdot x_p \cdot y,$$

i.e. $x \leq x{\times}y$. Moreover one has

$$y < x_p \cdot y < \ldots < x_1 \cdot \ldots \cdot x_p \cdot y,$$

which gives $y < x{\times}y$ whenever x is not 1. □

The question of left division in $(\mathfrak{f}, \times, 1)$ remains open: for x in $\mathfrak{f}$, we have no characterization of those elements that are $x{\times}y$ for some y. The only remark we have is that, if z is $x{\times}y$ for some y, then the next element of $\mathfrak{f}$ (with respect to $<$) that is $x{\times}y'$ for some y' is $z \cdot x$, corresponding to $y' = y \cdot 1$.

Remark. Formulas (I_1) and (I_2) can be used to practically compute normal forms for the elements of $\mathfrak{f}$ according to the method of [3]. Starting from the normal form of x, it is easy to determine the normal form of $x \cdot 1$. Then one uses the formula

$$x \cdot y = (x \cdot 1) \times y,$$

which is a particular case of (I_1), to inductively compute the normal form of $x \cdot y$ from the normal form of $x \cdot 1$ by substitution in a normal term representing y. The advantage is that one reduces in this way to compute normal forms of the form $x' \cdot y'$ with $x' \geq y'$, which is the only case where an algorithmic method is known.

We now quit the framework of free structures. If we consider congruences on terms that are not associated with identities, i.e. that are not closed under substitution, there is no reason why the operation $\times$ should still be compatible with the congruence. But we observe that, in the specific case of left distributivity, the compatibility is forced by (I_2) above.

Proposition 2. *Assume that* $(\mathfrak{g}, \cdot)$ *is any monogenic LD-system, and that* g *is a generator of* $(\mathfrak{g}, \cdot)$.

(i) *There exists a unique operation* $\times$ *on* $\mathfrak{g}$ *that is left distributive with respect to* $\cdot$ *and admits* g *as a right unit.*

(ii) *The structure* $(\mathfrak{g}, \times, g)$ *is a monoid and the above identities* (I_1) *and* (I_2) (*with* g *replacing* 1) *are satisfied in* $(\mathfrak{g}, \cdot, \times)$.

Proof: Let π denote the canonical projection of $\mathfrak{f}$ onto $\mathfrak{g}$ that sends 1 to g. We claim that the operation $\times$ of $\mathfrak{f}$ is compatible with π. We already observed that $\pi(x) = \pi(x')$ always implies $\pi(x \times y) = \pi(x' \times y)$ by very construction. Now assume $\pi(y) = \pi(y')$. If x is 1, then $\pi(1 \times y)$, which is $\pi(y)$, is equal to $\pi(1 \times y')$, which is $\pi(y')$. Now assume that x is $x_1 \cdot \ldots \cdot x_p \cdot 1$. By ($\mathrm{I}_2$), we have

$$\begin{aligned} \pi(x \times y) &= \pi(x_1 \cdot \ldots \cdot x_p \cdot y) \\ &= \pi(x_1) \cdot \ldots \cdot \pi(x_p) \cdot \pi(y) \\ &= \pi(x_1) \cdot \ldots \cdot \pi(x_p) \cdot \pi(y') \\ &= \pi(x_1 \cdot \ldots \cdot x_p \cdot y') = \pi(x \times y'). \end{aligned}$$

Hence the operation $\times$ of $\mathfrak{f}$ induces a well-defined operation on $\mathfrak{g}$. The uniqueness is obvious since the requirements force the operation $\times$ of $\mathfrak{g}$ to be the π-projection of the operation $\times$ on $\mathfrak{f}$. Then (ii) follows immediately. $\square$

Point (i) above shows that the operation $\times$ on $\mathfrak{g}$ is defined inductively 'on the right' by the rules

$$\begin{aligned} x \times g &= x, \\ x \times (y \cdot z) &= (x \times y) \cdot (x \times z), \end{aligned}$$

and, then, the symmetric ‘left’ rules

$$g \times z = z,$$
$$(x \cdot y) \times z = x \cdot (y \times z)$$

follow as a consequence. Now the latter left rules define $\times$ as well, and then the right rules follow.

It remains to compare the present construction with the one described in [2] (or, in a particular framework, in [1]). So assume that $(\mathfrak{g}, \cdot)$ is a monogenic LD-system, and that g is a generator of $(\mathfrak{g}, \cdot)$. With the above notations, we have, for every x and y in $\mathfrak{g}$,

$$(x \cdot g) \times (y \cdot g) = x \cdot (g \times (y \cdot g)) = x \cdot y \cdot g.$$

Now assume that $\circ$ is another binary operation on $\mathfrak{g}$ so that $\circ$ and $\cdot$ satisfy Axiom (LA_1): then $x \cdot y \cdot g$ is $(x \circ y) \cdot g$. So, if the mapping $x \mapsto x \cdot g$ happens to be injective, the operation $\circ$ is immediately defined from $\times$ by the equality

$$(x \circ y) \cdot g = (x \cdot g) \times (y \cdot g).$$

These conditions are met in particular in the case of the finite LD-systems A_n (in this case the mapping $x \mapsto x \cdot g$ is even a bijection), and we recover in this way the standard LD-algebra structure associated with A_n. More precisely our present operation $\times$ coincides with the one denoted $\bullet$ in [6], as the above right rules show. As a conclusion we could revert our viewpoint and say that the above construction is the generalization to the case of any monogenic LD-system (including the free one) of the standard construction developed for A_n. Observe that the results of [7] which show that a lot of, and perhaps even all, monogenic LD-systems can be constructed in some sense from the A_n's, make the existence of this generalization rather natural.

Remark. The present construction can be extended very easily to non-monogenic free structures by introducing the initial clause $x \times g = x$ for every generator g. One still obtains an associative operation, but it has no unit in general, and, in the case of left distributivity, Identity (I_1) need not hold any longer, so that the extension to non-free systems is problematic.

References

[1] Dehornoy P., *Infinite products in monoids*, Semigroup Forum **34** (1986), 21–68.

[2] ———, *The adjoint representation of a left distributive magma*, Comm. in Algebra **20**-4 (1992), 1201–1215.

[3] ———, *A Normal Form for the Free Left Distributive Law*, Int. J. for Algebra & Computation, to appear.

[4] ———, *From Large Cardinals to Braids via Distributive Algebra*, preprint, 1994.

[5] Drápal A., *Homomorphisms of primitive left distributive groupoids*, Comm. in Algebra **22**-7 (1994), 2579–2592.

[6] ———, *On the semigroup structure of cyclic left distributive algebras*, preprint, 1993, to appear in Semigroup Forum.
[7] ———, *Finite Left Distributive Algebras with One Generator*, preprint, 1994.
[8] El Bashir R., Drápal A., *Quasitrivial left distributive groupoids*, preprint, 1993.
[9] Kepka T, *Notes on left distributive groupoids*, Acta Univ. Carolinae **22**-2 (1981), 21–37.
[10] Laver R., *On the algebra of elementary embeddings of a rank into itself*, Advances in Math., to appear.

Mathématiques, Université, 14 032 Caen, France
E-mail: dehornoy@geocub.greco-prog.fr

(*Received* June 28, 1994)