Available online at www.sciencedirect.com
SCIENCE DIRECT®

ELSEVIER

Journal of Symbolic Computation 40 (2005) 1106–1125

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Linear groupoids and the associated wreath products

J.D. Phillips[a,*], Petr Vojtěchovský[b]

[a] *Department of Mathematics & Computer Science, Wabash College, Crawfordsville, IN 47933, USA*
[b] *Department of Mathematics, University of Denver, 2360 S Gaylord Street, Denver, CO 80208, USA*

Received 7 June 2004; accepted 15 February 2005
Available online 7 July 2005

Abstract

A groupoid identity is said to be linear of length $2k$ if the same k variables appear on both sides of the identity exactly once. We classify and count all varieties of groupoids defined by a single linear identity. For $k = 3$, there are 14 nontrivial varieties and they are in the most general position with respect to inclusion. Hentzel et al. [Hentzel, I.R., Jacobs, D.P., Muddana, S.V., 1993. Experimenting with the identity $(xy)z = y(zx)$. J. Symbolic Comput. 16, 289–293] showed that the linear identity $(xy)z = y(zx)$ implies commutativity and associativity in all products of at least five factors. We complete their project by showing that no other linear identity of any length behaves this way, and by showing how the identity $(xy)z = y(zx)$ affects products of fewer than five factors; we include distinguishing examples produced by the finite model builder Mace4. The corresponding combinatorial results for labelled binary trees are given. We associate a certain wreath product with any linear identity. Questions about linear groupoids can therefore be transferred to groups and attacked by group-theoretical computational tools, e.g., GAP. Systematic notation and diagrams for linear identities are devised. A short equational basis for Boolean algebras involving the identity $(xy)z = y(zx)$ is presented, together with a proof produced by the automated theorem prover OTTER.

MSC: primary 20N0; secondary 18B40, 20B40, 20N05

Keywords: Linear groupoid; Linear identity; Balanced identity; Strictly balanced identity; The identity $(xy)z = y(zx)$; Binary tree; Wreath product; Robbins axiom; Boolean algebra; Identity-hedron

* Corresponding author. Tel.: +1 765 361 6431; fax: +1 765 361 6340.
E-mail addresses: phillipj@wabash.edu (J.D. Phillips), petr@math.du.edu (P. Vojtěchovský).
URL: http://www.math.du.edu/~petr (P. Vojtěchovský).

0747-7171/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2005.02.003

1. Motivation

It is customary to call an identity *balanced* if the same variables occur on both sides of the identity the same number of times. When each of the k variables of a balanced identity ι appears on each side of ι exactly once, ι is called *strictly balanced* or *linear of length* $2k$. We use the name *linear* in this paper.

Thus, the *associative law* $x(yz) = (xy)z$ is a linear identity of length 6, and the *medial law* $(xy)(uv) = (xu)(yv)$ is a linear identity of length 8.

There does not seem to be any systematic account of groupoids (i.e., sets with one binary operation) satisfying a linear identity, although several specific identities have been studied in considerable detail. For instance, Ježek and Kepka wrote a series of papers on linear identities with identical bracketings on both sides, e.g., the *medial groupoids* defined by the above medial law (Ježek and Kepka, 1983), the *left* (resp. *right*) *permutable groupoids* defined by $x(yz) = x(zy)$ (resp. $(xy)z = (xz)y$) (Ježek and Kepka, 1984a), and the *left* (resp. *right*) *modular groupoids* defined by $x(yz) = z(yx)$ (resp. $(xy)z = (zy)x$) (Ježek and Kepka, 1984b). These papers deal mostly with a representation of linear groupoids by means of commutative semigroups, with the description of all (finite) simple linear groupoids in a given variety, and with universal algebraic properties of the varieties of linear groupoids.

We were drawn to the subject by the fascinating identity

$$(xy)z = y(zx), \tag{1}$$

which, as far as we know, has not been named yet. Hentzel et al. (1993) showed that for any groupoid G satisfying (1) and for any product of $m \geq 5$ elements of G, the m factors commute and associate, i.e., the result of the product is independent of parentheses and of the order in which the elements are multiplied. This sounds paradoxical, since it is certainly not true for $m = 3$, and one would intuitively expect the situation to become more complex with increasing m.

No explanation (beside a proof!) for this phenomenon is offered in Hentzel et al. (1993). A superficial explanation could go as follows: the longer the products become, the more ways there are in which the substitution rule (1) can be applied to them. Unfortunately, it is not clear at all why this should overpower the growing number of possible products, or why it only works for (1) and not for other linear identities.

1.1. Contents

We introduce a systematic notation for linear identities, and capture the behavior of linear identities as substitutions in diagrams called identity-hedrons. Given two linear identities, we decide when one implies the other. Consequently, we can count how many distinct varieties of groupoids defined by a single linear identity of given length there are. The answer depends on the number of cyclic subgroups of symmetric groups. We show that the only linear identity that implies associativity and commutativity in sufficiently long products is (1). This result can be restated in terms of transformations of labelled binary trees. We introduce a canonical way of constructing a certain subgroup of a wreath product from any linear identity. This construction seems to be of interest on its own, since