LINEAR GROUPOIDS AND THE ASSOCIATED WREATH PRODUCTS

J. D. PHILLIPS AND PETR VOJTĚCHOVSKÝ

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. [3] showed that the linear identity $(xy)z = y(zx)$ implies commutativity and associativity in all products of at least 5 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 5 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.

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 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 [7], the *left* (resp. *right*) *permutable groupoids* defined by $x(yz) = x(zy)$ (resp. $(xy)z = (xz)y$) [8], and the *left* (resp. *right*) *modular groupoids* defined by $x(yz) = z(yx)$ (resp. $(xy)z = (zy)x$) [9]. 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.

1991 *Mathematics Subject Classification.* Primary: 20N0., Secondary: 18B40, 20B40, 20N05.

Key words and phrases. 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.

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, Jacobs and Muddana [3] 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 [3]. 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 identityhedrons. 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 it allows us to work with identities in a finite group instead of an (infinite) free groupoid. Finally, we present the shortest known equational basis for Boolean algebras, based on (1).

1.2. **Related work.** The identity (1) was studied by Thedy [22] for rings. It appears as identity (10) in [10]. Hosszú [4] showed that a quasigroup satisfying (1) is an abelian group.

Kleinfeld [14] investigated the left modular identity for rings. Belousov [1] and Ježek and Kepka [10, 12] worked with linear identities in the variety of quasigroups. Equational theories of some linear identities are studied in [11]. There is an extensive bibliography of early papers on balanced identities (especially medial groupoids) in the monograph [7].

2. Systematic Names for Linear Identities

Although most proofs in this paper are easy to understand intuitively, a systematic notation helps to write them down formally.

2.1. **Labelling bracketings.** Products of n factors can be represented as labelled binary trees, or as groupoid terms of length n. Unlabelled binary trees correspond to bracketings of factors in a product. The *length* of a bracketing is the number of leaves in the corresponding tree.

Products of n factors can be bracketed in C_n ways, where C_n is the *nth Catalan number* defined by the recurrence relation

$$C_1 = 1, \quad C_2 = 1, \quad C_n = C_1C_{n-1} + C_2C_{n-2} + \cdots + C_{n-2}C_2 + C_{n-1}C_1, \tag{2}$$

which is equivalent to the explicit formula

$$C_{n+1} = \frac{1}{n+1}\binom{2n}{n}. \tag{3}$$

See [23] for more on Catalan numbers and Table 1 for the first few values C_n.

Given a bracketing t of length n it is therefore possible to assign a unique name $b(t)$ to t so that $0 \leq b(t) < C_n$. One way of doing this is to (a) represent each bracketing by a sequence of symbols '(' (left parenthesis), ')' (right parenthesis) and '$\circ$' (placeholder), (b) introduce a total order on the three symbols, (c) extend this total order lexicographically to a total order on all bracketings of given length.

In this paper, we will label bracketings as follows:

When t is a bracketing of length 1, let $b(t) = 0$. When $t = t_\lambda t_\rho$ is a bracketing of length $n > 1$ that is a product of a bracketing t_λ of length $n - m$ and a bracketing t_ρ of length m, let

$$b(t) = \left(\sum_{i=1}^{m-1} C_i C_{n-i}\right) + b(t_\rho)C_{n-m} + b(t_\lambda). \tag{4}$$

Thus, the function b first counts all bracketings whose top two products are of length $n-1$ and 1, respectively, then moves on to all bracketings whose top two products are of length $n-2$ and 2, respectively, and so on. To see that b is a bijection, we prove that the bracketing t can be reconstructed from $b(t)$.

When $n = 1$, t is determined by $b(t) = 0$. Assume that $b(s)$ determines s uniquely for all bracketings s of length less than n. Let m be the biggest integer such that $\sum_{i=1}^{m-1} C_i C_{n-i} \leq b(t)$. Then m is the length of t_ρ, and $d = b(t_\rho)C_{n-m} + b(t_\lambda)$ is therefore known. Since $b(t_\lambda) < C_{n-m}$ by the induction hypothesis, we have $b(t_\rho) = \lfloor d/C_{n-m} \rfloor$, $b(t_\lambda) = d - b(t_\rho)C_{n-m}$, thus reconstructing t_λ and t_ρ from $b(t)$.

Example 2.1. Here are the first 8 of the $C_5 = 14$ bracketings of length 5:

$$(((\circ\circ)\circ)\circ)\circ = 0, \quad ((\circ(\circ\circ))\circ)\circ = 1, \quad ((\circ\circ)(\circ\circ))\circ = 2, \quad (\circ((\circ\circ)\circ))\circ = 3,$$
$$(\circ(\circ(\circ\circ)))\circ = 4, \quad ((\circ\circ)\circ)(\circ\circ) = 5, \quad (\circ(\circ\circ))(\circ\circ) = 6, \quad (\circ\circ)((\circ\circ)\circ) = 7.$$

Note that the labelling does not agree with the lexicographic order.

2.2. **Naming linear groupoid identities.** Let $u = v$ be a linear groupoid identity of length $2n$. Let $b(u)$ be the label of the bracketing of u, $b(v)$ the label of the bracketing of v, and $f \in S_n$ the permutation that must be applied to the variables of u so that they become ordered as in v. Since every variable occurs exactly once on both sides, the permutation f is uniquely determined. We can hence identify the identity $u = v$ with the quadruple $(n, b(u), b(v), f)$, which we call the *name* of $u = v$. In order to save space, we write $n_{b(u)}f_{b(v)}$ instead of $(n, b(u), b(v), f)$, or even ${}_{b(u)}f_{b(v)}$, when n is clear from the context. The variety of groupoids defined by a single linear identity ${}_if_j$ will also be denoted by ${}_if_j$.

Example 2.2. The identity $((xy)u)v = (xu)(vy)$ has name $4_0(2,4,3)_2$.

Remark 2.3. The notation can be extended to arbitrary balanced groupoid identities. However, the permutation f is then not necessarily uniquely determined. It can be assigned canonically by imposing a total order on permutations.

2.3. **Counting linear identities.** Upon interchanging the left hand side and the right hand side of a linear identity ${}_nf_j$, we obtain the identity ${}_nf^{-1}{}_i$. Naturally, we consider these two identities to be the same.

We call a linear identity *trivial* if it is of the form ${}_i()_i$, where () is the identity permutation.

For $n, m > 0$, let $s_{n,m}$ denote the number of elements of order m in the symmetric group S_n.

Lemma 2.4. *There are*

$$\frac{C_n}{2}\left(C_n n! + 1 + s_{n,2}\right) \tag{5}$$

linear identities of length $2n$. *There are*

$$\frac{C_n}{2}\left(C_n n! - 1 + s_{n,2}\right) \tag{6}$$

nontrivial linear identities of length $2n$.

Proof. In order to construct a linear identity ${}_if_j$ of length $2n$, we can choose each of the bracketings i, j in C_n ways, and the permutation f in $n!$ ways. We do not distinguish between ${}_if_j$ and ${}_jf^{-1}{}_i$; hence the factor $1/2$. However, before we divide by $1/2$, we must add all identities ${}_if_j$ for which ${}_if_j$ and ${}_jf^{-1}{}_i$ are the same. This happens if and only if $i = j$ and $f^2 = 1$. Since there are $1 + s_{n,2}$ permutations f of S_n with $f^2 = 1$, we have proved (5). Equation (6) follows from (5) upon subtracting the C_n trivial identities ${}_i()_i$. □

For the sake of completeness, we give the formula for $s_{n,2}$, which is certainly well known.

Lemma 2.5. *There are*

$$s_{n,2} = \sum_{1 \le 2m \le n} \binom{n}{2m} \cdot 1 \cdot 3 \cdot 5 \cdots (2m-1)$$

involutions in S_n.

Proof. All involutions of S_n can be obtained as follows: Select an even number $0 < 2m \le n$ of elements. Split the $2m$ elements into m pairs, each corresponding to some transposition (a, b). An easy induction shows that the number of ways in which $2m$ elements can be split into pairs (equivalently, the number of 1-factorizations of the complete graph on $2m$ vertices) is $1 \cdot 3 \cdot 5 \cdots (2m-1)$. □

3. Identity-hedrons and implications among linear identities

3.1. **Free groupoids.** The *absolutely free groupoid* A_n on generators $x_1, \ldots, x_n$ consists of all groupoid terms formed from $x_1, \ldots, x_n$, i.e., of all words $u = x_{i_1} x_{i_2} \cdots x_{i_m}$ bracketed in some way, where $m \ge 0$, $i_j \in \{1, \ldots, n\}$ for $1 \le j \le m$. The product of two terms $u, v \in A_n$ is the term uv.

Let φ be a groupoid identity. Define a binary relation $\sim$ on A_n by $u \sim v$ if and only if v is obtained from u by a single application of the identity φ. Let $\equiv$ be the reflexive and transitive closure of $\sim$ on A_n. Then $\equiv$ is a congruence of A_n, and $F = A_n/\equiv$ (also denoted by A_n/φ) is the *free groupoid* with n generators satisfying φ. Elements of F (equivalence classes of A_n) will be denoted by $[u]$, where $u \in A_n$.

Let φ, ψ be two linear groupoid identities. We say that φ *implies* ψ if every groupoid satisfying φ also satisfies ψ.

Theorem 3.1. *Let φ, ψ be two linear groupoid identities. Assume that ψ is the identity $u = v$ and that it is of length $2n$. Then φ implies ψ if and only if $[u] = [v]$ in A_n/φ.*

Proof. If $[u] = [v]$ in A_n/φ then ψ is obtained by a repeated application of φ, and hence every groupoid satisfying φ also satisfies ψ.

Assume that $[u] \neq [v]$ in A_n/φ. Then A_n/φ is a groupoid satisfying φ but not ψ, and hence φ does not imply ψ. □

3.2. **Identity-hedrons.** When viewed as a transformation of terms in an absolutely free groupoid, the primary effect of a linear identity is to change the bracketing of a given product and, at the same time, to permute the factors. This leads us to the notion of an *identity-hedron*, that we introduce by means of an example.

Consider the linear identity (1). Let X be the set of all bracketings of length 4. As in Section 2, we can identify X with the set $\{0, \dots, 4\}$, since $C_4 = 5$.

Let $u = u_1u_2u_3u_4$ be a word bracketed in some way. Then the rule (1) can be applied to it in several ways to yield another term. For instance, when $u = ((u_1u_2)u_3)u_4$, we can apply (1) in two ways to obtain the terms $(u_2(u_3u_1))u_4$ and $u_3(u_4(u_1u_2))$, respectively. Thus every application of (1) to a term u is fully described by the change in bracketing of u and by the permutation of the letters u_1, …, u_4. We can represent any such application of (1) by a labelled arrow. Upon collecting all such arrows, we obtain an *identity-hedron*, as in Figure 1. (Here, our terminology is analogous to *associahedrons*. See [20].)

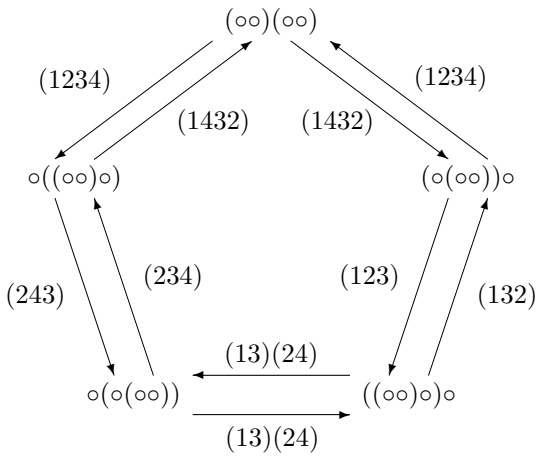

FIGURE 1. The identity $(xy)z = y(zx)$ and terms of length 4

Note that the information in an identity-hedron is redundant, since the two arrows pointing in opposite directions are labelled by permutations that are inverse to each other. We will exploit this redundancy later.

Naturally, the identity (1) can be applied more than once. This corresponds to a journey through Figure 1 along a path of arrows. Upon completing the journey,

we are left with a permutation (obtained by composing the permutations along the arrows), and hence with some linear identity determined by the starting bracketing of the path, the terminating bracketing of the path, and by the above permutation.

For instance, starting at bracketing $0 = ((\circ\circ)\circ)\circ$ and travelling counterclockwise, we see that $((ab)c)d) = (b(ca))d = (db)(ca) = a((db)c) = a(b(cd)) = ((cd)a)b$. We have returned to the same bracketing but the order of the factors is different. We could have calculated the order of the factors directly by rearranging *abcd* according to the permutation $(13)(24)(243)(1234)(1234)(132) = (13)(24)$. The linear identity corresponding to this journey is thus ${}_4(13)(24)_0$.

It should now be clear how to construct an identity-hedron for any balanced identity φ and any length of terms m. We will denote the corresponding identity-hedron by $H(\varphi, m)$.

We now make the anticipated connection between implications and journeys through identity-hedrons.

Theorem 3.2. *Let φ, ψ be linear identities. Then φ implies ψ if and only if ψ corresponds to a journey through the identity-hedron $H(\varphi, m)$, where $2m$ is the length of ψ.*

Proof. Let u, v be two terms in the absolutely free groupoid A_m such that $u = v$ is ψ. Then $[u] = [v]$ holds in A_m/φ if and only if there is a journey through $H(\varphi, m)$ that yields ψ. The rest follows from Theorem 3.1. □

4. Inclusions between Varieties of Groupoids Defined by a Linear Identity

Theorem 4.1. *Let $n \geq 3$ be an integer and let ${}_if_j$, ${}_rg_s$ be two distinct, nontrivial linear identities of length $2n$. Then ${}_if_j$ implies ${}_rg_s$ if and only if $i = j = r = s$ and $g = f^k$ for some $k \neq 0$.*

Proof. By Theorem 3.2, ${}_if_j$ implies ${}_rg_s$ if and only if ${}_rg_s$ is the result of a journey in $H = H({}_if_j, n)$. Without loss of generality, let $i \leq j$, $r \leq s$.

Since the two identities in question are of the same length, the identity-hedron H is easy to describe: it consists of several isolated bracketings and one pair of mutually inverse arrows connecting bracketings i and j (when $i = j$, the arrows are loops).

When $i \neq j$, any journey through H is of the form: (a) ${}_if_j$, (b) ${}_jf^{-1}{}_i$, (c) ${}_i()_i$, or ${}_j()_j$. None of these identities is ${}_rg_s$ since: (a) ${}_if_j \neq {}_rg_s$, (b) $i < j$, $r \leq s$, (c) g is nontrivial.

When $i = j$ then any journey through H is of the form ${}_if^k{}_i$, and we are done. □

Example 4.2. By Theorem 4.1, the identity

$$4_3(1,2,3,4)_3 \;=\; \text{“}x((yz)u) = u((xy)z)\text{”}$$

implies the identity

$$4_3(1,3)(2,4)_3 \;=\; \text{“}x((yz)u) = z((ux)y)\text{”},$$

TABLE 1. The number $\mathcal{L}(n)$ of varieties of groupoids defined by a single linear identity of length $2 \leq n \leq 6$, together with all constants needed to evaluate $\mathcal{L}(n)$, based on Proposition 4.3.

$s_{n,m}$	2	3	4	5	6
2	1				
3	3	2			
4	9	8	6		
5	25	20	30	24	20
6	75	80	180	144	240

n	2	3	4	5	6
$\varphi(n)$	1	2	2	4	2
C_n	1	2	5	14	42
$\mathcal{L}(n)$	2	15	321	11,845	635,083

but the two identities are not equivalent. This is also witnessed by the groupoid with the following multiplication table:

	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

We can now easily count the varieties of groupoids defined by a single linear identity of length $2n$. Recall that $s_{n,m}$ denotes the number of elements of order m in the group S_n. Let φ be the *Euler function*, i.e., $\varphi(m)$ is the number of positive integers less than m that are relatively prime to m.

Proposition 4.3. *There are*

$$\mathcal{L}(n) = 1 + \binom{C_n}{2} n! + C_n \sum_{m \geq 2} \frac{s_{n,m}}{\varphi(m)} \tag{7}$$

varieties of groupoids defined by a single linear identity of length $2n$.

Proof. There is 1 trivial variety (all groupoids). The second summand of (7) accounts for all linear identities ${}_if_j$ with $i < j$. It remains to count the varieties defined by some nontrivial ${}_if_i$. We know from Theorem 4.1 that ${}_if_i = {}_jg_j$ (as varieties) if and only if $i = j$, $f = g^k$ and $g = f^l$ for some $k \neq 0 \neq l$. There are C_n bracketings i of length n. If $f \in S_n$ is a permutation of order m, it gives rise to a cyclic subgroup $G \leq S_n$ of order m. The permutations g satisfying $g = f^k$, $f = g^l$ for some $k \neq 0 \neq l$ are then precisely the generators of G. It is well known that a cyclic group of order m has $\varphi(m)$ generators. □

Remark 4.4. The summand $s_{n,m}/\varphi(m)$ counts the number of cyclic subgroups of order m in S_n, and, therefore, the sum $\sum_{m \geq 2} \frac{s_{n,m}}{\varphi(m)}$ in (7) is the number of nontrivial cyclic subgroups of S_n.

Table 1 gives the values of $\mathcal{L}(n)$, for $2 \leq n \leq 6$.

Theorem 4.5. *Assume that $f \in S_n$, $g \in S_m$ are nonidentity permutations, $n \neq m$. Then the varieties ${}_nf_j$, ${}_mg_s$ are not the same.*

Proof. Without loss of generality, let $n < m$. Then the identity-hedron $H({}_mg_s, n)$ contains no arrows, and hence ${}_mg_s$ does not imply ${}_nf_j$, by Theorem 3.2. □

TABLE 2. The 14 nontrivial varieties of groupoids defined by a single linear identity of length 6. We omit "3" from their systematic names.

identity	systematic name	is equivalent to	remark
$(xy)z = (yx)z$	${}_0(1,2)_0$		
$(xy)z = (zy)x$	${}_0(1,3)_0$		right modular groupoids
$(xy)z = (xz)y$	${}_0(2,3)_0$		right permutable groupoids
$(xy)z = (zx)y$	${}_0(1,2,3)_0$	${}_0(1,3,2)_0$	
$(xy)z = x(yz)$	${}_0()_1$	${}_1()_0$	semigroups
$(xy)z = y(xz)$	${}_0(1,2)_1$	${}_1(1,2)_0$	
$(xy)z = z(yx)$	${}_0(1,3)_1$	${}_1(1,3)_0$	
$(xy)z = x(zy)$	${}_0(2,3)_1$	${}_1(2,3)_0$	
$(xy)z = z(xy)$	${}_0(1,2,3)_1$	${}_1(1,3,2)_0$	
$(xy)z = y(zx)$	${}_0(1,3,2)_1$	${}_1(1,2,3)_0$	Eq. (1)
$x(yz) = y(xz)$	${}_1(1,2)_1$		
$x(yz) = z(yx)$	${}_1(1,3)_1$		left modular groupoids
$x(yz) = x(zy)$	${}_1(2,3)_1$		left permutable groupoids
$x(yz) = z(xy)$	${}_1(1,2,3)_1$	${}_1(1,3,2)_1$	

4.1. **The fourteen varieties of length** 6**.** Note that 14 is both the number of nontrivial varieties defined by a single linear identity of length 6 (Table 1), and the number of nontrivial linear identities of length 6 (Lemma 2.4). For the convenience of the reader, these 14 identities can be found in Table 2.

For each identity ${}_if_j$ of Table 2 we now construct a finite groupoid satisfying ${}_if_j$ but not any other of the remaining 13 identities. The multiplication tables of these groupoids are gathered in Figure 2. The multiplication table of a groupoid satisfying ${}_if_j$ is labelled by ${}_if_j$. All $m \times m$ multiplication tables of Figure 2 have rows and columns labelled by $0, \ldots, m-1$, in this order.

All examples in Figure 2 are as small as possible. They were found by Mace 4 [17]. The groupoid ${}_0(1,2,3)_0$ was hardest to find; it took Mace 4 about 5 hours on a Pentium 3 machine with 765 megabytes of RAM.

Corollary 4.6. *The* 14 *nontrivial varieties defined by a single linear identity of length* 6 *are in a general position with respect to inclusion, i.e., none of these varieties is contained in the union of the remaining* 13 *varieties.*

Remark 4.7. Ježek and Kepka determined that there are 11 varieties of quasigroups defined by a single linear identity of length ≤ 6, and found all inclusions among them [10, Theorem 1.8]. Kirnasovsky [13] studied the same problem for length ≤ 8.

4.2. **Linear identities of length** 8 **implied by** (1)**.** Let us answer a question posed in [3].

Proposition 4.8. *Exactly* 45 *out of the* 320 *nontrivial linear identities of length* 8 *are implied by* (1)*. These identities can be found with the aid of Figure* 1*.*

Proof. Recall that upon completing one counterclockwise round in Figure 1 starting at bracketing 0, the 4 symbols are permuted according to (13)(24). We claim that

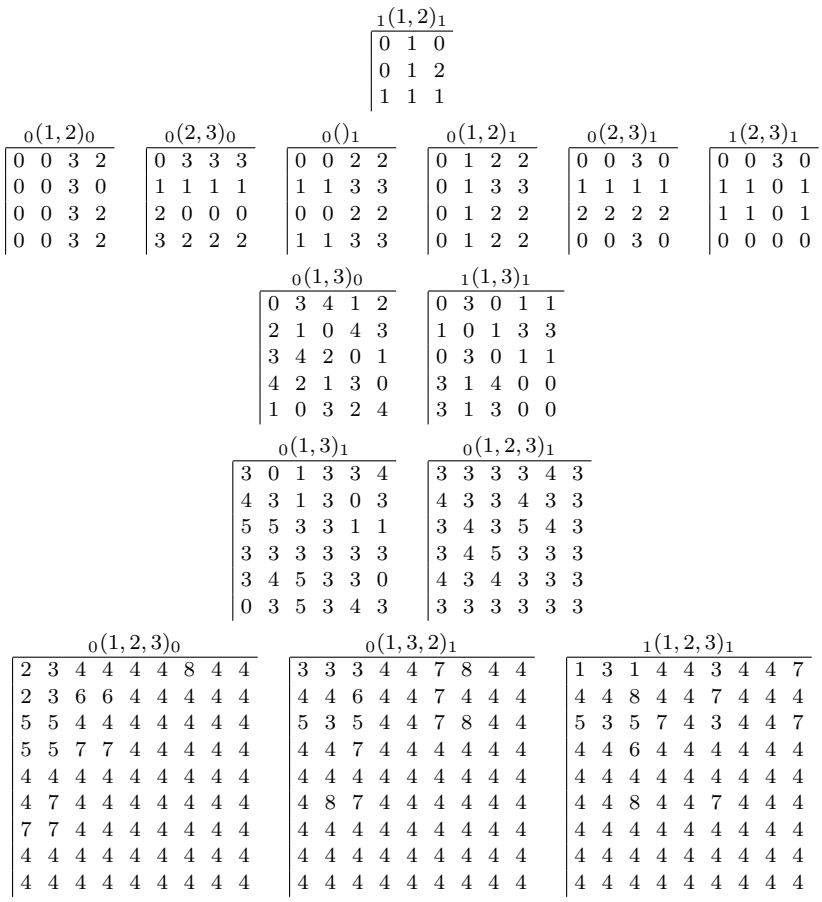

FIGURE 2. The groupoid man. Smallest distinguishing examples for the 14 nontrivial varieties of groupoids defined by a single linear identity of length 6.

all permutations g corresponding to one counterclockwise round in Figure 1 are involutions. This is easy to see, since the permutation obtained by starting at bracketing i is a conjugate of the permutation obtained by starting at bracketing $i-1$ (cf., for $i=1$, we get $(132)(13)(24)(132)^{-1}$).

We can now describe all journeys through Figure 1: Select two bracketings i, j out of the 5 possible bracketings, allowing $i=j$. The shortest nonempty counterclockwise path from i to j yields some identity ${}_if_j$. Upon extending this path by another complete counterclockwise round, we obtain identity ${}_igf_j$ that is different from ${}_if_j$ (since g is an involution). The two bracketings i, j can be chosen in $5\cdot 5=25$ ways. Hence we obtain 50 identities following the above procedure. Five of these identities are trivial (those corresponding to two full rounds).

We are done by Theorem 3.2. □

We verified by the finite model builder Mace 4 [17] that the groupoid $A \times B$ defined by

A	0	1	2	3	4	5	6	7	8
0	2	3	5	7	5	6	8	8	8
1	4	3	6	6	6	6	8	8	8
2	5	5	6	8	8	8	8	8	8
3	6	6	6	8	8	8	8	8	8
4	7	7	6	8	8	8	8	8	8
5	6	8	8	8	8	8	8	8	8
6	8	8	8	8	8	8	8	8	8
7	6	8	8	8	8	8	8	8	8
8	8	8	8	8	8	8	8	8	8

B	0	1	2	3	4	5	6	7
0	2	3	2	7	2	6	2	2
1	4	2	2	2	5	2	2	6
2	2	2	2	2	2	2	2	2
3	2	5	2	2	6	2	2	2
4	7	2	2	6	2	2	2	2
5	6	2	2	2	2	2	2	2
6	2	2	2	2	2	2	2	2
7	2	6	2	2	2	2	2	2

satisfies (1) but none of the remaining $320 - 45$ linear identities of length 8 not implied by (1).

5. Ultimately AC-nice groupoids and labelled binary trees

As in [21] and [16], two groupoid terms are said to be *AC-identical* if one is obtained from the other by a repeated application of associativity and commutativity.

For an integer $m > 1$, we then say that a groupoid G is *mAC-nice* if any two products of the same m elements of G yield the same element of G. mAC-nice groupoids are called *m-nice* in [3].

By [3, Lemma 2.2], every groupoid satisfying (1) is 5AC-nice. By [3, Lemma 2.3], an mAC-nice groupoid is $(m+1)$AC-nice, provided $m \geq 3$. Note that 2AC-nice groupoids are precisely commutative groupoids, and 3AC-nice groupoids are groupoids that are commutative and associative. 3AC-niceness therefore does not follow from 2AC-niceness.

It thus makes sense to say:

Definition 5.1. A groupoid G is *ultimately AC-nice* if it is mAC-nice for some $m \geq 3$. A linear identity ${}_if_j$ is *ultimately AC-nice* if every groupoid satisfying ${}_if_j$ is ultimately AC-nice.

In the last paragraph of [3], the authors of [3] claim, without proof, that there is a groupoid that satisfies $x(yz) = z(yx)$ but that is not 5AC-nice. We prove a general result (Theorem 5.6) along similar lines: *the only ultimately AC-nice linear identity is* (1).

This result can be visualized in terms of transformations of labelled binary trees as follows:

First notice that a linear identity ${}_if_j$ is ultimately AC-nice if and only if all free groupoids satisfying ${}_if_j$ are ultimately AC-nice. One application of a linear identity to a word in the absolutely free groupoid can be depicted by two labelled binary trees. Figure 3 shows this for the associative law and for the commutative law. Since two groupoid products with the same factors coincide in the presence of associativity and commutativity, we see that given two labelled binary trees T_1, T_2 with the same n leaves, it is possible to obtain T_2 from T_1 by finitely many applications of the two laws. Can the same feat be achieved by a single linear identity φ, at least for sufficiently large trees? This is precisely the question whether φ is ultimately AC-nice, and we answer it in Theorem 5.6. The proof of Theorem 5.6 is split into several steps:

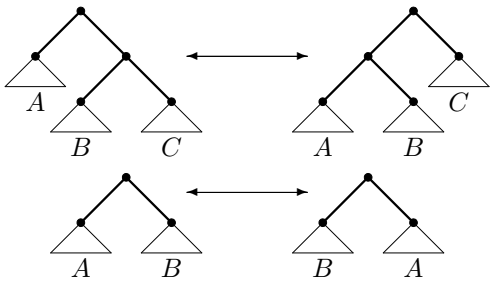

FIGURE 3. Associativity and commutativity as transformations of labelled binary trees

Lemma 5.2. *Let $n_i f_j$ be a linear identity such that $f \in S_n$ satisfies $f(1) = 1$ or $f(n) = n$. Then the free groupoid on two generators satisfying $n_i f_j$ is not ultimately AC-nice.*

Proof. Let A be the absolutely free groupoid on generators x, y. For $m \geq 3$, consider the words $u = u_1 \dots u_m$, $v = v_1 \dots v_m \in A$ such that $u_1 = v_m = x$, $v_1 = u_m = y$, $u_k = v_k = x$ for $1 < k < m$. Assume that $f(1) = 1$. No matter what the bracketing of u is, we see that no application of the identity ${}_i f_j$ can move u_1 from the left-most position. Since $u_1 \neq v_1$, the products u, v do not coincide in $A/{}_i f_j$. Similarly when $f(n) = n$. □

Lemma 5.3. *The free commutative groupoid on one generator is not ultimately AC-nice.*

Proof. Let F be the free commutative groupoid with generator x. Define powers x^n by $x^1 = x$, $x^n = xx^{n-1}$. Then for any even $m \geq 4$ we have $x^m \neq (xx)^{m/2}$, since commutativity is not strong enough to split any of the factors xx. □

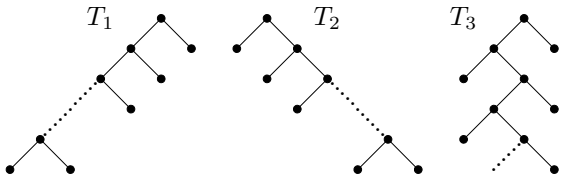

FIGURE 4. The proof of Theorem 5.6

Proposition 5.4. *Let $n_i f_j$ be an ultimately AC-nice linear identity with $i \leq j$. Then $i = 0$, $j = C_n - 1$.*

Proof. Let F be the free groupoid on 1 generator satisfying $n_i f_j$. Since $n_i f_j$ is ultimately AC-nice, it must be possible to transform the tree T_1 of Figure 4 into

the tree T_2 of the same Figure by a repeated application of ${}_nf_j$, provided the two trees have the same number of leaves and are sufficiently large. Note that ${}_if_j$ is applicable to T_1 if and only if the bracketing i is of the form $(\cdots((\circ\circ)\circ)\cdots)\circ$, i.e., if and only if $i = 0$. Similarly, ${}_if_j$ is applicable to T_2 if and only if $j = C_n - 1$. □

Proposition 5.5. *The only ultimately AC-nice linear identity of length* 6 *is* (1).

Proof. Proposition 5.4 eliminates 8 identities of the form ${}_if_i$ from Table 2. The identities ${}_0()_1$, ${}_0(1,2)_1$, ${}_0(2,3)_1$ fix either 1 or 3, and are therefore eliminated by Lemma 5.2. Finally, the two identities ${}_0(1,3)_1$, ${}_0(1,2,3)_1$ are consequences of the commutative law, and hence are eliminated by Lemma 5.3. □

Theorem 5.6. *The only ultimately AC-nice linear identity is* (1).

Proof. The only nontrivial linear identity of length ≤ 4 is the commutative law $xy = yx$, which is not ultimately AC-nice by Lemma 5.3. Thanks to Proposition 5.5, it suffices to consider ultimately AC-nice linear identities of length ≥ 8. Let ${}_nf_j$ be such an identity, $i \leq j$, $n \geq 4$. By Proposition 5.4, we have $i = 0$, $j = C_n - 1$. Consider the tree T_3 of Figure 4. We claim that ${}_nf_j$ is not applicable to T_3, no matter how large T_3 is. This is because it is impossible to make at least $n - 1$ consecutive moves to the left (or to the right) along the branches of T_3. □

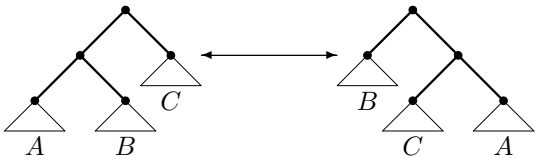

FIGURE 5. The identity (1) as a transformation of labelled binary trees

The only ultimately AC-nice linear identity (1) is visualized in Figure 5.

Note that our proofs depend essentially on infinite (free) groupoids. Is this dependence necessary?

Conjecture 5.7. *Let ${}_nf_j$ be a linear identity such that every* finite *groupoid satisfying ${}_nf_j$ is ultimately AC-nice. Then ${}_nf_j$ is the identity* (1).

6. Wreath Products Associated with Linear Identities

Let φ be a linear identity, and $m > 0$ an integer. By composing arrows in the identity-hedron $H(\varphi, m)$, we can determine all linear identities of length $2m$ implied by φ. Although it may seem that it only makes sense to compose consecutive arrows of an identity-hedron, we show below that it is possible to compose arbitrary arrows.

In this section, maps are applied to the right of their arguments, and therefore composed from left to right.

6.1. **The associated wreath products.** Let us first recall some group-theoretical definitions:

Let B be a group acting on another group A via $a \mapsto a^b$, where $a \in A$, $b \in B$. Then the *semidirect product* $A \ltimes B$ is the group defined on $A \times B$ by $(a_1, b_1)(a_2, b_2) = (a_1 a_2^{(b_1^{-1})}, b_1 b_2)$. We use $a_2^{(b_1^{-1})}$ rather than $a_2^{b_1}$ in the definition of a semidirect product because we compose maps from left to right.

Let B be a group acting on a set X, and let A be another group. Then B also acts on the set A^X of all maps from X to A via $xf^b = x^{b^{-1}} f$, $f \in A^X$, $b \in B$, $x \in X$. The *wreath product* $A \operatorname{wr}_X B$ of A and B is the semidirect product $A^X \ltimes B$ under this action.

When X is a finite set $\{1, \cdots, n\}$, the maps A^X can be identified with the direct product A^n, and the elements of $A \operatorname{wr}_X B$ can be represented as $((p_1, \ldots, p_n), p) = ((p_i), p)$, where $p_i \in A$, $p \in B$. When B is a subgroup of S_n acting naturally on X, the multiplication in $A \operatorname{wr}_X B$ is described by the explicit formula

$$((a_i), a) \cdot ((b_i), b) = ((a_i)(b_i)^{(a^{-1})}, ab) = ((a_i b_{ia}), ab), \tag{8}$$

where, in accordance with our conventions, ia is the image of i under a.

Let us return to linear identities.

Fix a linear identity φ. Let m be a positive integer and let X be the set of all bracketings of length m, $X = \{0, \ldots, C_m - 1\}$. Let $B = S_X$, $A = S_m$, and $W = A \operatorname{wr}_X B$.

Consider the arrow leading from bracketing $i \in X$ to bracketing $j \in X$ labelled by $\pi \in A$ in the identity-hedron $H(\varphi, m)$. We will represent this arrow and its inverse (exploiting the redundancy) by a single element $((a_0, \ldots, a_{C_m - 1}), a) = ((a_i), a)$ of W by letting a be the transposition (i, j), and by setting $a_i = \pi$, $a_j = \pi^{-1}$, $a_r = id_{\{1,\ldots,m\}}$ for $r \notin \{i, j\}$.

We claim that the multiplication formula (8) then generalizes composition of consecutive arrows (transformations). To see this, consider the word u bracketed according to i. Let v be the word obtained from u when $((a_j), a)$ is applied to u. Since u is bracketed according to i, the permutations a_j, $j \neq i$ are irrelevant. Hence v will be bracketed according to ia and the letters of u will be reordered in v according to a_i. Let w be the word obtained from v after $((b_j), b)$ is applied to v. Then w is bracketed according to iab and the letters of u will be reordered in w according to $a_i b_{ia}$. This agrees with (8).

Definition 6.1. Given a linear identity φ and a positive integer m, let $W(\varphi, m)$ be the subgroup of W generated by the elements $((a_i), a) \in W$ corresponding to all arrows (and their inverses) in the identity-hedron $H(\varphi, m)$, as described above.

6.2. **Wreath products and AC-niceness.** We have managed to associate a certain subgroup $W(\varphi, m)$ of a wreath product with a linear identity φ and a positive integer m. We now show how these wreath products can be used to express mAC-niceness for (1). Conceivably, $W(\varphi, m)$ will be useful in other settings, too.

Let G be a subgroup of $A \operatorname{wr}_X B$. Then G acts on X via the original action of B, i.e., $x^{((p_i),p)} = xp$, where $x \in X$, $p_i \in A$, $p \in B$. For $x \in X = \{0, \ldots, C_m - 1\}$, let $G_x \leq G$ be the stabilizer of x and $O_x \subseteq X$ the orbit of x under this action of G. Denote by P_x the projection of G_x onto the xth component of $A \operatorname{wr}_X B$, i.e., $P_x = \{p_x;\ ((p_i), p) \in G_x\} \leq A$.

Proposition 6.2. *Let φ be a linear identity and m a positive integer. Then all groupoids satisfying φ are mAC-nice if and only if there is a bracketing $x \in X$ such that $G = W(\varphi, m)$ satisfies $P_x = S_m$, $O_x = X$.*

Proof. Let $x \in X$ be such that $P_x = A = S_m$ and $O_x = X$. Let H be a groupoid satisfying φ, and let u, v be two products with the same m factors. Since $O_x = X$, the bracketings of u, v can be changed to x. Let u', v' be the corresponding products bracketed according to x. Since $P_x = A$, the factors of u', v' can be reordered freely without changing the value of u', v'. Hence $u = u' = v' = v$ and H is mAC-nice.

For the converse, assume that every groupoid satisfying φ is mAC-nice. Let $F = A_m/\varphi$ be the free groupoid on m generators satisfying φ. By our assumption, F is mAC-nice. Fix a bracketing x. Consider any two words u, $v \in A_m$ bracketed according to x. Since F is mAC-nice, $[u] = [v]$ in F. In other words, v can be obtained from u by a repeated application of φ. This shows $P_x = S_m$. We can show similarly that $O_x = X$. □

Example 6.3. Consider again Figure 1. Let x be any of the 5 bracketings. Clearly, $O_x = X$. Thanks to the shape of the transformation diagram (a cycle), it is also easy to see that the only way to return to x is to complete several clockwise or counterclockwise cycles around the diagram. Let π be the permutation of the four symbols obtained after one counterclockwise round starting at x. Then π^{-1} corresponds to one clockwise round. Hence $P_x = \langle \pi \rangle$. Since S_4 is not cyclic, we have $P_x \neq S_4$. Since x was arbitrary, we have proved that (1) is not 4AC-nice, by Proposition 6.2.

6.3. **Computing the associated wreath products in GAP.** Are calculations in $W(\varphi, m)$ more convenient than those in the free groupoid on m generators satisfying φ? It depends.

The advantage of $W(\varphi, m)$ is that it is a finite group, and hence all tools of computational group theory apply to it. Importantly, up to C_m applications of φ are encoded in a single element of $W(\varphi, m)$. Also note that the elements of $W(\varphi, m)$ capture the essence of φ; namely all possible applications of φ to words of length m, not the words themselves.

On the other hand, $W(\varphi, m)$ is huge. There are $m^m \cdot C_m$ terms of length m in the free groupoid on m generators. In comparison, the size of W (of which $W(\varphi, m)$ is a subgroup) is $(m!)^{C_m} \cdot C_m!$, eventually a much bigger number.

By Proposition 6.2, mAC-niceness of a linear identity φ can be determined by the study of the (projections of) stabilizers and the orbits of the action of $W(\varphi, m)$ on all bracketings of length m.

Since stabilizers and orbits of permutation groups are implemented efficiently in GAP [2], we wrote a short library of functions that verifies mAC-niceness for a given linear identity φ. The library is available electronically [19]. We describe the main functions here.

Given a positive integer m and a linear identity φ, the function

`GeneratorsByIdentity(`m, φ`)`

returns the generators of $W(\varphi, m)$ as elements of $S_m \operatorname{wr}_X S_{C_m}$. Once the generators of $W(\varphi, m) = G$ are determined, the orbit O_0 and the stabilizer P_0 of the bracketing labelled 0 are returned by

`BlockStabilizerAction(`G, `[1..m])`.

The batch function

`IsNice`$(m,\ \varphi)$

first calculates O_0, P_0 and then returns true if and only if $O_0 = S_{C_m}$, $P_0 = S_m$, i.e., if and only if the identity φ is mAC-nice.

Example 6.4. Here is a transcript of the GAP calculations. The results were obtained almost instantaneously. (This will not be true for larger values of m.)

```
gap> G := Group( GeneratorsByIdentity( 5, "(xy)z=y(zx)") );
<permutation group with 42 generators>
gap> Size(G);
559649088897488712105984000000000000000
gap> IsNice( 5, "(xy)z=y(zx)");
true
```

It is worth noting that G is not all of the wreath product $S_5 \text{ wr}_X S_{C_5}$; it is a subgroup of index 2.

7. A Short Equational Basis for Boolean Algebras

Several authors have observed that a quasigroup satisfying (1) is an abelian group. (The earliest reference appears to be [4].) We give a direct and more general proof of this fact based on ultimate AC-niceness of (1).

We say that a groupoid has *one-sided cancellation* if either (i) $xy = xz$ implies $y = z$ for every x, y, z, or (ii) $yx = zx$ implies $y = z$ for every x, y, z.

Lemma 7.1. *Let G be a groupoid satisfying* (1)*. If G has a neutral element or if G has one-sided cancellation then it is commutative and associative.*

Proof. Consider a product u consisting of $m < 5$ elements of G. When G has a neutral element 1, we can extend u to a product of 5 elements by letting $v = ((u \cdot 1) \cdot 1) \cdots 1$. When G has one-sided cancellation, say cancellation on the right, we can pick an element $g \in G$ and extend u into a product of 5 elements by letting $w = ((u \cdot g) \cdot g) \cdots g$.

When $u = xy$, let $u' = yx$. When $u = x(yz)$, let $u' = (xy)z$. (We only discuss these two cases since we are only interested in commutativity and associativity.) Let v' (resp. w') be the product v (resp. w) in which u is replaced by u'. Since every groupoid satisfying (1) is 5AC-nice [3], we conclude that $v = v'$, $w = w'$. But $((u \cdot 1) \cdot 1) \cdots 1 = v = v' = ((u' \cdot 1) \cdot 1) \cdots 1$ yields $u = u'$ because 1 is a neutral element, and, similarly, $w = w'$ yields $u = u'$ because g can be cancelled on the right. □

We conclude this paper with an application of (1) to Boolean algebras.

Finding short equational bases for varieties of algebras is an important project in algebra. The variety of Boolean algebras has traditionally occupied a privileged position in this regard. As early as 1933, Huntington [5, 6] showed that the following three equations form an appealing short basis for the variety of Boolean algebras:

$$x + y = y + x, \tag{9}$$

$$(x + y) + z = x + (y + z), \tag{10}$$

$$n(n(x) + y) + n(n(x) + n(y)) = x. \tag{11}$$

Shortly thereafter, Robbins conjectured that (11) could be replaced with the following shorter equation, which has since come to be known as the *Robbins equation*:

$$n(n(x+y)+n(x+n(y)))=x. \tag{12}$$

That is, he conjectured that (9) and (10), together with the Robbins equation form an even shorter basis for the variety of Boolean algebras. But a proof remained elusive for nearly 70 years. The *Robbins Problem*, as it came to be known, was one of the celebrated open problems in algebra for most of the 20th century. It was one of Tarski's favorite problems [16].

Finally, in 1997, Bill McCune solved the problem using his automated theorem prover, OTTER [17]. The buzz generated by McCune's accomplishment was loud enough to warrant coverage in the New York Times [15]! We use equation (1) to offer an even shorter basis for Boolean algebras (Theorem 7.2).

Theorem 7.2. *The following two equations form a basis for the variety of Boolean algebras:*

(additive version of (1)) $(x+y)+z=y+(z+x)$,

(Robbins equation) $n(n(x+y)+n(x+n(y)))=x$.

Proof. We offer a computer generated proof, found by OTTER [17], that the two identities imply $x+y=y+x$. Associativity of $+$ then follows. For a primer on OTTER proofs see [17] or [18].

```
2 [] (x*y)*z=y* (z*x).
3 [] n(n(x*y)*n(x*n(y)))=x.
5 [] A*B!=B*A.
6 [copy,5,flip.1] B*A!=A*B.
7 [copy,2,flip.1] x* (y*z)= (z*x)*y.
8 [para_into,2.1.1.1,2.1.1] (x* (y*z))*u=y* (u* (z*x)).
9 [copy,8,flip.1] x* (y* (z*u))= (u* (x*z))*y.
10 [para_into,7.1.1.2,7.1.1] x* ((y*z)*u)= ((u*y)*x)*z.
11 [para_into,7.1.1.2,2.1.1] x* (y* (z*u))= (z*x)* (u*y).
12 [para_into,7.1.1,2.1.1] x* ((y*z)*u)= (z* (u*x))*y.
18 [para_into,3.1.1.1.1.1,7.1.1] n(n((x*y)*z)*n(y*n(z*x)))=y.
20 [para_into,3.1.1.1.1.1,2.1.1] n(n(x* (y*z))*n((z*x)*n(y)))=z*x.
22 [para_into,3.1.1.1.1,3.1.1] n(x*n(n(x*y)*n(n(x*n(y)))))=n(x*y).
26 [para_into,3.1.1.1.2.1,2.1.1] n(n((x*y)*z)*n(y* (n(z)*x)))=x*y.
36 [para_into,8.1.1,2.1.1] (x*y)* (z*u)=x* (z* (y*u)).
43 [copy,36,flip.1] x* (y* (z*u))= (x*z)* (y*u).
57 [para_into,9.1.1.2,7.1.1] x* ((y*z)*u)= (y* (x*u))*z.
67 [copy,57,flip.1] (x* (y*z))*u=y* ((x*u)*z).
85 [para_into,10.1.1.2.1,7.1.1] x* (((y*z)*u)*v)= ((v*z)*x)* (u*y).
93,92 [para_into,10.1.1,7.1.1,flip.1] ((x*y)*z)*u= (x*z)* (y*u).
109 [back_demod,85,demod,93,93] x* ((y*z)* (u*v))= (v*x)* (u* (z*y)).
146 [para_from,11.1.1,9.1.1.2,demod,93]
    x* ((y*z)* (u*v))=(y* (x*v))* (u*z).
153 [copy,146,flip.1] (x* (y*z))* (u*v)=y* ((x*v)* (u*z)).
169,168 [para_into,12.1.1.2,2.1.1,flip.1] (x* (y*z))*u=z* (x* (y*u)).
187 [back_demod,153,demod,169] x* (y* (z* (u*v)))=z* ((y*v)* (u*x)).
238 [back_demod,67,demod,169] x* (y* (z*u))=z* ((y*u)*x).
320 [para_into,43.1.1.2,7.1.1] x* ((y*z)*u)= (x*u)* (z*y).
362 [para_into,18.1.1.1.1.1.1,11.1.1,demod,169,169]
```

```
    n(n(x* ((y*z)* (u*v)))*n(u* (x*(y*n(v*z))))=x* (y*u).
397,396 [para_from,18.1.1,3.1.1.1.1]
    n(x*n(n((y*x)*z)*n(n(x*n(z*y)))))=n((y*x)*z).
426 [para_from,92.1.1,18.1.1.1.2.1,demod,169]
    n(n(x* (y* ((z*u)*v)))*n((z*x)*(u*n(v*y))))= (z*u)*x.
529,528 [para_from,168.1.1,3.1.1.1.2.1,demod,169]
    n(n(x*(y* (z*u)))*n(x* (y* (z*n(u)))))=y* (z*x).
562 [para_into,20.1.1.1.1.1.1,92.1.1,demod,169]
    n(n((x*y)* (z* (u*v)))*n(y* (v*((x*z)*n(u))))=v* ((x*z)*y).
580 [para_into,20.1.1.1.2.1.1,11.1.1,demod,169,169]
    n(n(x* (y* (z* (u*v))))*n(y*((z*v)* (x*n(u)))))=v* (y* (z*x)).
592 [para_into,20.1.1.1.2.1,2.1.1] n(n(x*(y*z))*n(x* (n(y)*z)))=z*x.
621 [para_into,238.1.1.2,7.1.1] x* ((y*z)*u)=u*((z*y)*x).
663 [para_from,238.1.1,20.1.1.1.1.1.1.2,demod,169,169,169]
    n(n(x* (y*((z*u)*v)))*n((y*x)* (u* (z*n(v))))=u* (z* (y*x)).
854 [para_into,22.1.1.1.2.1.1.1,7.1.1,demod,397]
    n((x*y)*z)=n(y* (z*x)).
913 [para_into,854.1.1.1,168.1.1] n(x* (y* (z*u)))=n((z*x)* (u*y)).
1552 [para_into,26.1.1.1.2.1.2,238.1.1,demod,169,169,169]
    n(n((x*y)* (z*(u*v)))*n(y* (x* ((u*z)*n(v))))=z* (u* (x*y)).
1677 [para_from,621.1.1,7.1.1.2,demod,93,169]
    x* (y* ((z*u)*v))=x* ((u*y)* (z*v)).
1713 [copy,1677,flip.1] x* ((y*z)* (u*v))=x* (z* ((u*y)*v)).
4027,4026 [para_into,109.1.1,320.1.1,demod,169,flip.1]
    (x*y)* (z* (u*v))=x* (y* (z*(u*v))).
5558 [back_demod,1552,demod,4027]
    n(n(x* (y* (z* (u*v))))*n(y* (x*((u*z)*n(v))))=z* (u* (x*y)).
5895 [back_demod,663,demod,4027]
    n(n(x* (y*((z*u)*v)))*n(y* (x* (u* (z*n(v))))))=u* (z* (y*x)).
5929 [back_demod,562,demod,4027]
    n(n(x* (y* (z* (u*v))))*n(y* (v* ((x*z)*n(u))))=v*((x*z)*y).
8313,8312 [para_into,187.1.1,238.1.1,demod,169,flip.1]
    x* ((y*z)*(u*v))=x* (z* (y* (u*v))).
10221,10220 [back_demod,1713,demod,8313,flip.1]
    x*(y* ((z*u)*v))=x* (y* (u* (z*v))).
10325,10324 [back_demod,580,demod,8313]
    n(n(x* (y* (z* (u*v))))*n(y* (v* (z* (x*n(u))))))=v* (y* (z*x)).
10345,10344 [back_demod,362,demod,8313]
    n(n(x* (y* (z* (u*v))))*n(u* (x* (z*n(v*y))))=x*(z*u).
11602 [back_demod,5929,demod,10221,10325]
    x* (y* (z*u))=x* ((u*z)*y).
11604,11603 [back_demod,5895,demod,10221]
    n(n(x* (y* (z* (u*v))))*n(y* (x* (z*(u*n(v))))))=z* (u* (y*x)).
11622 [back_demod,5558,demod,10221,11604]
    x* (y*(z*u))=x* (y* (u*z)).
11820 [back_demod,426,demod,10221]
    n(n(x* (y* (z*(u*v))))*n((u*x)* (z*n(v*y))))= (u*z)*x.
11855 [para_from,11602.1.1,913.1.1.1]
    n(x* ((y*z)*u))=n((z*x)* (y*u)).
11865 [para_from,11602.1.1,20.1.1.1.1.1,demod,93]
    n(n(x* ((y*z)*u))*n((z*x)*(y*n(u))))= (z*y)*x.
11883 [copy,11855,flip.1] n((x*y)* (z*u))=n(y* ((z*x)*u)).
12163,12162 [para_into,11622.1.1.2,7.1.1]
```

```
    x* ((y*z)*u)=x* (z* (y*u)).
12176,12175 [back_demod,11883,demod,12163]
    n((x*y)* (z*u))=n(y* (x* (z*u))).
12190,12189 [back_demod,11865,demod,12163,12176,529,flip.1]
    (x*y)*z=x* (y*z).
12505 [back_demod,11820,demod,12190,10345,12190]
    x* (y*z)=z* (y*x).
14989,14988 [para_into,592.1.1.1.1.1,12505.1.1]
    n(n(x* (y*z))*n(z* (n(y)*x)))=x*z.
14996 [para_into,592.1.1.1.2.1,12505.1.1,demod,14989] x*y=y*x.
14997 [binary,14996.1,6.1] $F.
```

□

Remark 7.3. It is tempting to try to apply Lemma 7.1 in order to prove Theorem 7.2. Unfortunately, this is only possible if one shows that there is a neutral element 0 with respect to addition, necessarily equal to $n(x + n(x))$ for any x. (The addition $+$ is not cancellative.) We were unable to prove the existence of 0 without first establishing commutativity of addition.

8. Acknowledgement

We thank Alexander Hulpke of Colorado State University for his help with implementation of wreath products arising from linear identities in GAP. We also thank Jaroslav Ježek of Charles University for bringing several papers on linear groupoids to our attention.

References

[1] V. D. Belousov, *Balanced identities in algebras of quasigroups*, Aequationes Math. **8** (1972), 1–73.
[2] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.3; Aachen, St Andrews (1999). (Visit http://www-gap.dcs.st-and.ac.uk/˜gap).
[3] Irvin Roy Hentzel, David P. Jacobs and Sekhar V. Muddana, *Experimenting with the Identity* $(xy)z = y(zx)$, J. Symbolic Computation **16** (1993), 289–293.
[4] M. Hosszú, *Some functional equations related with the associative law*, Publ. Math. Debrecen **3** (1954), 205-214.
[5] E .V. Huntington, *Boolean algebra. A correction,*, Trans. Amer. Math. Soc. **35** (1933), 557–558.
[6] E. V. Huntington, *New sets of independent postulates for the algebra of logic, with special reference to Whitehead and Russell's Principia Mathematica*, Trans. Amer. Math. Soc. **35** (1933), 274–304.
[7] Jaroslav Ježek and Tomáš Kepka, *Medial groupoids*, Rozpravy Československé Akad. Věd Řada Mat. Přírod. Věd **93** (1983), no. **2**, 93 pp.
[8] Jarosla Ježek and Tomáš Kepka, *Permutable groupoids*, Czechoslovak Math. J. **34** (**109**) (1984), no. **3**, 396–410.
[9] Jaroslav Ježek and Tomáš Kepka, *Modular groupoids*, Czechoslovak Math. J. **34**(**109**) (1984), no. **3**, 477–487.
[10] Jaroslav Ježek and Tomáš Kepka, *Varieties of groupoids determined by short linear identities*, Czechoslovak Math. J. **39**(**114**) (1989), no. **4**, 644–658.
[11] Jaroslav Ježek and Tomáš Kepka, *Linear equational theories and semimodule representations*, Internat. J. Algebra Comput. **8** (1998), no. **5**, 599–615.
[12] Jaroslav Ježek and Tomáš Kepka, *The equational theory of paramedial cancellation groupoids*, Czechoslovak Math. J. **50** (**125**) (2000), no. **1**, 25–34.

[13] Oleg U. Kirnasovsky, *Some results on the up to fourth length balanced identities*, Quasigroups and Related Systems **5** (1998), 13–34.
[14] M. H. Kleinfeld, *Rings with* $x(yz) = z(yx)$, Communications in Algebra **6** (1978), 1369–1373.
[15] Gina Kolata, *Computer Math Proof Shows Reasoning Power*, The New York Times, December 10, 1996. Available electronically at http://www.nytimes.com/library/cyber/week/1210math.html
[16] W. W. McCune, *Solution of the Robbins Problem*, JAR **19**, no. **3** (1997), 263–276.
[17] W. W. McCune, `Mace4` and `OTTER`, Argonne National Laboratory, 2003. Available at http://www-unix.mcs.anl.gov/AR.
[18] J. D. Phillips, *See Otter digging for algebraic pearls*, Quasigroups and Related Systems **10** (2003), 95–114.
[19] J. D. Phillips and Petr Vojtěchovský, GAP library for wreath products associatied with linear identities. (Available electronically at http://www.math.du.edu/~petr in section research | computing.)
[20] Jim Stasheff, *What is ... an Operad?*, Notices of the Amer. Math. Soc. **51**, no. **6**, 630–631.
[21] M. Stickel, *A unification algorithm for assocaitive-commutative functions*, J. ACM **28**(1981), no. **3**, 423–434.
[22] A. Thedy, *Ringe mit* $x(yz) = (yx)z$, Math. Zeitschr. **99** (1967), 400–404.
[23] J. H. van Lint and R. M. Wilson, A Course in Combinatorics, Cambridge University Press 1992.

Department of Mathematics & Computer Science, Wabash College, Crawfordsville, Indiana 47933, U.S.A.
E-mail address: `phillipj@wabash.edu`

Department of Mathematics, University of Denver, 2360 S Gaylord St, Denver, CO, 80208, U.S.A.
E-mail address: `petr@math.du.edu`