International Journal of Algebra, Vol. 3, 2009, no. 5, 199 - 210

On Commutativity and Groupoid Identities between Products with 3 Factors

Tjark Weber

Institut für Informatik, Technische Universität München
Boltzmannstr. 3, 85748 Garching, Germany
webertj@in.tum.de

Abstract

A groupoid consists of a set G equipped with a binary operation. This article examines the relationship between commutativity and various (less common) groupoid identities between products with 3 factors, e.g., $(xy)z = (yz)x$. We systematically study all 12 identities of this form to identify additional conditions (e.g., unitality) that are sufficient for commutativity. Automated deduction techniques were used in several parts of the work.

Mathematics Subject Classification: 20N02

Keywords: commutativity, groupoid identities

1 Introduction

A *groupoid* (also called a *magma*) consist of a set G equipped with a binary operation $\cdot\colon G \times G \to G$. Despite the lack of further axioms, interesting results about groupoids exist [1]. Application of the binary operation is commonly denoted by juxtaposition: xy is short for $x \cdot y$, the product of x and y.

There are two ways to form a product of two groupoid elements x, y: xy and yx. If the groupoid operation satisfies

$$xy = yx \tag{0}$$

for all $x, y \in G$, it is said to be *commutative*.

Likewise, there are 12 ways to form a product of three groupoid elements x, y, z. They give rise to the following 12 equations (where we implicitly assume

x, y, z to be universally quantified over G):

$$
\begin{aligned}
(xy)z &= (xy)z && (1)\\
(xy)z &= (xz)y && (2)\\
(xy)z &= (yx)z && (3)\\
(xy)z &= (yz)x && (4)\\
(xy)z &= (zx)y && (5)\\
(xy)z &= (zy)x && (6)\\
(xy)z &= x(yz) && (7)\\
(xy)z &= x(zy) && (8)\\
(xy)z &= y(xz) && (9)\\
(xy)z &= y(zx) && (10)\\
(xy)z &= z(xy) && (11)\\
(xy)z &= z(yx) && (12)
\end{aligned}
$$

Note that all other equations between products with three (possibly distinct) factors are either symmetric to or equivalent permutations of one of the above. For instance, $x(yz) = z(yx)$, studied by Kleinfeld [6] in 1978, is symmetric to (6), and $x(yz) = (yx)z$, studied by Thedy [8] in 1967, is a permutation of (9).

Certainly the most well-known of these properties is (7), *associativity*. Any groupoid that is both commutative and associative is readily shown to satisfy (1)–(12). In Section 2, we study these equations to identify additional conditions that are sufficient for commutativity. Some of our results are immediate (which is readily explained by the simplicity of the properties that we investigate), others, however, are more interesting. We conclude with a discussion of the automated deduction techniques that were used in this work, and with some final remarks in Section 3.

2 Ensuring Commutativity

None of the above Equations (1)–(12) alone is sufficient for commutatitivity. In fact, even their conjunction does not imply commutativity. Figure 1 shows a finite, non-commutative groupoid that satisfies (1)–(12). We now study these properties separately to identify additional conditions that ensure commutativity.

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	a	a	a
c	a	a	b	b
d	a	a	a	b

Figure 1: A non-commutative groupoid satisfying (1)–(12)

2.1 $(xy)z = (xy)z$

This property is trivially satisfied by any groupoid, simply because equality is reflexive.

2.2 $(xy)z = (xz)y$

Equation (2) is known as *right-commutativity*. It implies commutativity if the groupoid contains a left identity, i.e., an element e such that $ex = x$ for all $x \in G$.

Lemma 1. *Any groupoid satisfying (2) that has a left identity is commutative.*

Proof. Let x, $y \in G$, and let e be a left identity. Then, using (2), $xy = (ex)y = (ey)x = yx$. □

The slightly weaker condition of containing a left-cancellative element (i.e., an element l such that $lx = ly$ implies $x = y$ for all x, $y \in G$) is not sufficient for commutativity in the presence of (2). Likewise, the symmetric condition of having a right identity (i.e., an element e such that $xe = x$ for all $x \in G$) is not sufficient either. It is easy to give a non-commutative (but right-commutative) groupoid with just two elements that serves as a counterexample to both conjectures.

2.3 $(xy)z = (yx)z$

This property obviously holds in any commutative groupoid. It implies commutativity if the groupoid contains no right-equivalent elements.

Definition 1 (Right-Equivalent). Two elements x, y of G are called *right-equivalent* if $xz = yz$ for all $z \in G$.

A groupoid is said to have *no right-equivalent elements* if, for all x and y in G, x and y are right-equivalent only if $x = y$.

Perhaps more descriptively, having no right-equivalent elements means that no two rows of the groupoid operation's matrix are equal. (For instance, the

groupoid given in Figure 1 has two right-equivalent elements: a and b.) It is easy to show that right-equivalence is in fact an equivalence relation on G. We also note that every groupoid which contains a right-cancellative element (i.e., an element r such that $xr = yr$ implies $x = y$ for all x, $y \in G$) has no right-equivalent elements. The converse, however, is not true in general.

Lemma 2. *Any groupoid satisfying (3) that has no right-equivalent elements is commutative.*

Proof. Let x, $y \in G$. Then (3) implies that xy and yx are right-equivalent. Hence $xy = yx$. □

The symmetric condition of having no left-equivalent elements is not sufficient for commutativity. A non-commutative groupoid with just two elements that satisfies (3) and even has a left identity is readily constructed.

2.4 $(xy)z = (yz)x$

It is easy to see that any groupoid satisfying Equation (4) and having a right identity is commutative. We present two non-trivial results that allow us to strengthen this observation. First, elements commute under sufficiently many multiplications from the right. (The following lemma shows that five multiplications are sufficient. Using an exhaustive computer search, we have verified that $((((ab)c)d)e)f \neq ((((ba)c)d)e)f$ in the groupoid freely generated by a, b, c, d, e, f, modulo the equivalence relation that is induced by (4). Hence four multiplications are not sufficient in general.)

Lemma 3. *For all a, b, c, d, e, f, $g \in G$, (4) implies $(((((ab)c)d)e)f)g = (((((ba)c)d)e)f)g$.*

Proof. Let a, b, c, d, e, f, $g \in G$. Then, using (4), $(((((ab)c)d)e)f)g = (((((bc)a)d)e)f)g = ((((ad)(bc))e)f)g = ((((bc)e)(ad))f)g = (((e(ad))(bc))f)g = (((bc)f)(e(ad)))g = ((e(ad))g)((bc)f) = (((ad)g)e)((bc)f) = ((ge)(ad))((bc)f) = ((ad)((bc)f))(ge) = ((d((bc)f))a)(ge) = ((((bc)f)a)d)(ge) = ((((cf)b)a)d)(ge) = (((ba)(cf))d)(ge) = (((cf)d)(ba))(ge) = ((d(ba))(cf))(ge) = ((cf)(ge))(d(ba)) = ((ge)(d(ba)))(cf) = ((e(d(ba)))g)(cf) = (g(cf))(e(d(ba))) = ((cf)(e(d(ba))))g = ((f(e(d(ba))))c)g = (((e(d(ba)))c)f)g = ((((d(ba))c)e)f)g = (((((ba)c)d)e)f)g.$ □

Although the conclusion of Lemma 3 is weaker than (3), the lemma allows to derive a corollary that is directly analog to Lemma 2.

Corollary 4. *Any groupoid satisfying (4) that has no right-equivalent elements is commutative.*

Proof. Let x, $y \in G$. Then, for arbitrary a, b, c, $d \in G$, Lemma 3 implies that $((((xy)a)b)c)d$ and $((((yx)a)b)c)d$ are right-equivalent, hence equal.

Repeating this argument four more times, we can conclude that xy and yx must be equal. □

The symmetric condition of having no left-equivalent elements is once again not sufficient for commutativity. It is easy to construct a non-commutative groupoid with four elements that satisfies (4) and has no left-equivalent elements. Also existence of a left-cancellative element is not sufficient. For a counterexample, consider the free groupoid on a single generator a, modulo the equivalence relation that is induced by (4). Obviously a is left-cancellative, but $(aa)a \neq a(aa)$.

We note that this counterexample is infinite. In fact, there is no finite counterexample: for finite groupoids, the existence of a left-cancellative element implies surjectivity of the binary operation (by the pigeonhole principle). This is sufficient to derive commutativity, as we will show now.

Equation (4) implies that elements that can be written as a product of products commute with products.

Lemma 5. *For all a, b, c, d, e, $f \in G$, (4) implies $((ab)(cd))(ef) = (ef)((ab)(cd))$.*

Proof. Let a, b, c, d, e, $f \in G$. Then, using (4), $((ab)(cd))(ef) = ((cd)(ef))(ab) = ((d(ef))c)(ab) = (((ef)c)d)(ab) = (((fc)e)d)(ab) = (((ce)f)d)(ab) = ((fd)(ce))(ab) = ((ce)(ab))(fd) = ((ab)(fd))(ce) = ((b(fd))a)(ce) = (((fd)a)b)(ce) = (((da)f)b)(ce) = ((fb)(da))(ce) = ((b(da))f)(ce) = (f(ce))(b(da)) = ((ce)(b(da)))f = ((e(b(da)))c)f = (((b(da))c)e)f = (ef)((b(da))c) = (ef)(((da)c)b) = (ef)(((ac)d)b) = (ef)(((cd)a)b) = (ef)((ab)(cd))$. □

Corollary 6. *Any groupoid satisfying (4) that has a surjective groupoid operation is commutative.*

Proof. Let x, $y \in G$. Using surjectivity of the binary operation four times, we obtain a, b, c, d, e, $f \in G$ with $x = (ab)(cd)$ and $y = ef$. Now $xy = ((ab)(cd))(ef) = (ef)((ab)(cd)) = yx$ by Lemma 5. □

Surjectivity of the binary operation is clearly not necessary for commutativity. However, we note that a weaker condition—namely that all groupoid elements that cannot be written as a product (i.e., all elements not in the range of the binary operation) commute with each other—is not sufficient. It is easy to give a non-commutative groupoid with just three elements that satisfies this condition, and Equation (4).

2.5 $(xy)z = (zx)y$

This property is equivalent to the previous one, $(xy)z = (yz)x$.

Lemma 7. *Any groupoid satisfies (5) if and only if it satisfies (4).*

Proof. Let x, y, $z \in G$. Suppose (4) holds. Then $(xy)z = (yz)x = (zx)y$. Conversely, if (5) holds, $(xy)z = (zx)y = (yz)x$. □

2.6 $(xy)z = (zy)x$

Rings satisfying this property were studied by Kleinfeld [6] in 1978. Equation (6) implies commutativity if the groupoid contains a right identity.

Lemma 8. *Any groupoid satisfying (6) that has a right identity is commutative.*

Proof. Let x, $y \in G$, and let e be a right identity. Then, using (6), $xy = (xe)y = (ye)x = yx$. □

Merely containing a right-cancellative element is not sufficient for commutativity. A counterexample with just three elements—even containing a left identity as well—is easily constructed.

2.7 $(xy)z = x(yz)$

This property simply states that the groupoid is associative, i.e., a *semigroup*. It is well-known that semigroups need not be commutative. The smallest non-commutative semigroup has just two elements, and there seems to be no obvious condition (aside from commutativity itself) that ensures commutativity in the presence of (7).

2.8 $(xy)z = x(zy)$

Property (8) is symmetric to (9), in the sense that the groupoid given by $(G, \circ)$, with $x \circ y$ defined as $y \cdot x$, satisfies (9) if and only if $(G, \cdot)$ satisfies (8). Clearly $\circ$ is commutative if and only if $\cdot$ is. Therefore the next subsection applies (modulo symmetry).

We remark that the same symmetry principle, when applied to (7), (10), (11), or (12), merely yields an equivalent permutation of the respective equation.

2.9 $(xy)z = y(xz)$

Rings satisfying this property were studied by Thedy [8] in 1967. Property (9) clearly implies commutativity if the groupoid contains a right identity, but also—and perhaps less obvious—if it merely contains no right-equivalent elements. Assuming (9), we establish a property that is weaker than (3), but stronger than the conclusion of Lemma 3 (and structurally similar to both): elements commute under two multiplications from the right.

Lemma 9. *For all a, b, c, $d \in G$, (9) implies $((ab)c)d = ((ba)c)d$.*

Proof. Let a, b, c, $d \in G$. Then, using (9), $((ab)c)d = (b(ac))d = (ac)(bd) = c(a(bd)) = c((ba)d) = ((ba)c)d$. □

Corollary 10. *Any groupoid satisfying (9) that has no right-equivalent elements is commutative.*

Proof. Similar to the proof of Corollary 4, but using Lemma 9. □

Surjectivity and having no left-equivalent elements, however, are not sufficient to ensure commutativity in the presence of (9). It is easy to give a non-commutative groupoid with two elements that satisfies (9) and even has a left identity.

2.10 $(xy)z = y(zx)$

Hentzel et al. [4, Theorem 1] have proven the remarkable result that groupoids satisfying (10) are *5-nice*, meaning that any product of 5 elements is the same, regardless of their association or order. This immediately implies commutativity under relatively weak additional assumptions. For instance, any groupoid satisfying (10) that has no equivalent elements must be commutative.

Definition 2 (Equivalent Elements). Two elements x, y of G are called *equivalent* if they are both left- and right-equivalent, i.e., if $zx = zy$ and $xz = yz$ for all $z \in G$.

A groupoid is said to have *no equivalent elements* if, for all x and y in G, x and y are equivalent only if $x = y$.

More descriptively, this condition means that no two distinct groupoid elements behave exactly the same under multiplication.

Corollary 11. *Any groupoid satisfying (10) that has no equivalent elements is commutative.*

Proof. Similar to the proof of Corollary 4, but using 5-niceness (instead of Lemma 3) to establish both left- and right-equivalence. □

Moreover, we show that (10) implies commutativity if all elements that cannot be written as a product (i.e., all elements not in the range of the binary operation) commute with each other. Note that this condition is also necessary, and hence equivalent to commutativity in the presence of (10). It is trivially satisfied in any groupoid whose binary operation is surjective.

Lemma 12. *Any groupoid satisfying (10) is commutative if and only if $xy = yx$ for all x, y in G that are not in the range of the binary operation.*

Proof. Let x, $y \in G$, and assume that non-products commute with each other. We proceed by case distinction.

Case 1: both x and y are not in the range of the binary operation. Then $xy = yx$ by assumption.

Case 2: exactly one of x and y is in the range of the binary operation. Without loss of generality, assume $x = ab$ for some a, $b \in G$. Three subcases follow.

Case 2.1: both a and b are not in the range of the binary operation. Then, using (10), $xy = (ab)y = b(ya) = b(ay) = (yb)a = (by)a = y(ab) = yx$.

Case 2.2: $a = uv$ for some u, $v \in G$. Without loss of generality, we may assume that u, v, b are not in the range of the binary operation (otherwise $xy = yx$ follows from 5-niceness). Then $(uv)y = y(uv)$ by Case 2.1. Hence $xy = yx$, using the same transformations as in Case 2.1.

Case 2.3: $b = uv$ for some u, $v \in G$. Similar to Case 2.2. This concludes the proof of Case 2.

Case 3: both x and y are in the range of the binary operation, i.e., $x = ab$, $y = cd$ for some a, b, c, $d \in G$. Without loss of generality, we may assume that a, b, c, d are not in the range of the binary operation (otherwise $xy = yx$ follows from 5-niceness). Then, using (10), $xy = (ab)(cd) = (ba)(dc) = (c(ba))d = ((ac)b)d = ((ca)b)d = (a(bc))d = (bc)(da) = c((da)b) = c(a(bd)) = c(a(db)) = c((ba)d) = (dc)(ba) = (cd)(ab) = yx$.

The above shows commutativity. The "only if" part of the statement is trivial. □

2.11 $(xy)z = z(xy)$

This property, which states that products commute, obviously holds in any commutative groupoid. Similar to (10), it implies commutativity if all elements that cannot be written as a product commute with each other.

Lemma 13. *Any groupoid satisfying (11) is commutative if and only if $xy = yx$ for all x, y in G that are not in the range of the binary operation.*

Proof. Let x, $y \in G$. and assume that non-products commute with each other. If both x and y are not in the range of the binary operation, then $xy = yx$ by

assumption. Otherwise, at least one of x and y can be written as a product. Without loss of generality, assume $x = ab$ for some $a, b \in G$. Then (11) implies $xy = (ab)y = y(ab) = yx$. The "only if" part of the statement is trivial. □

2.12 $(xy)z = z(yx)$

This property also holds in any commutative groupoid. It clearly implies commutativity if the groupoid contains an identity, i.e., an element that is both a left identity and a right identity. More interestingly, however, commutativity is already implied if the groupoid contains a one-sided identity.

Lemma 14. *Any groupoid satisfying (12) that has a left identity is commutative.*

Proof. Let x, $y \in G$, and let e be a left identity. Then, using (12), $xy = x((ee)y) = x(y(ee)) = x(ye) = (ey)x = yx$. □

Corollary 15. *Any groupoid satisfying (12) that has a one-sided (i.e., left or right) identity is commutative.*

Proof. The statement follows from Lemma 14 by the symmetry principle described in Section 2.8. □

Existence of a cancellative element, however, is not sufficient to ensure commutativity. For a counterexample, consider the free groupoid on two generators a, b, modulo the equivalence relation that is induced by (12). One can show that a is (both left- and right-) cancellative, but $ab \neq ba$.

We note that this counterexample is infinite. In fact, there is no finite counterexample: for finite groupoids, the existence of a left-cancellative element implies surjectivity of the binary operation (by the pigeonhole principle; we used the same argument before in Section 2.4). This is sufficient for commutativity, as demonstrated by the following lemma.

Lemma 16. *Any groupoid satisfying (12) with a left-cancellative element that can be written as a product is commutative.*

Proof. Let $l = ab$ (with a, $b \in G$) be left-cancellative. We first show that l commutes with every groupoid element. Using (12), $ll = (ab)l = l(ba)$. Hence $l = ba$ because l is left-cancellative. Now, for arbitrary $z \in G$, $lz = (ab)z = z(ba) = zl$.

Therefore, for arbitrary x, $y \in G$, $l(xy) = (xy)l = l(yx)$. Hence $xy = xy$ because l is left-cancellative. □

Note that Lemma 16 is a strictly stronger result than Lemma 14. By symmetry, the left-cancellative element can be replaced by a right-cancellative one.

$\cdot$	a	b	c	d	e	f	g
a	f	d	a	b	g	f	f
b	b	f	c	f	e	f	d
c	g	e	f	c	f	f	a
d	d	f	e	f	c	f	b
e	a	c	f	e	f	f	g
f	f	f	f	f	f	f	f
g	f	b	g	d	a	f	f

Figure 2: A non-commutative groupoid satisfying (12) with a surjective binary operation

Corollary 17. *Any groupoid satisfying (12) with a left- or right-cancellative element that can be written as a product is commutative.*

Proof. The statement follows from Lemma 16 by the symmetry principle described in Section 2.8. □

Even if we make the stronger assumption that *every* groupoid element can be written as a product, the left- or right-cancellative element is needed. Figure 2 shows a groupoid satisfying (12) that has a surjective binary operation, but is non-commutative (and hence has no left- or right-cancellative element). Moreover, the groupoid shown has no left-equivalent or right-equivalent elements.

3 Conclusions

In this article, we have systematically studied all groupoid identities between products with 3 (possibly distinct) factors, and identified conditions under which these identities imply commutativity: e.g., existence of a (left or right) identity, having no (right-)equivalent elements, surjectivity of the groupoid operation, commutativity of non-products. Our results are surveyed in Table 1. While some of them are immediate, others—in particular for $(xy)z = (yz)x$ (Section 2.4), for $(xy)z = y(zx)$ (Section 2.10), and for $(xy)z = z(yx)$ (Section 2.12)—were not as obvious. We have also provided or hinted at a number of counterexamples, showing that certain weaker conditions do not suffice to ensure commutativity in the presence of (one of) Equations (1)–(12).

Because of the simplicity of the axioms considered in this article, our results are easy to verify. However, proofs and counterexamples for non-commutative, non-associative operations are not always easy to find. We successfully used Waldmeister [5], a theorem prover for equational logic, and the Isabelle/HOL [7] system. Waldmeister was able to find proofs for (equational

Identity	Condition
$(xy)z = (xy)z$	commutativity
$(xy)z = (xz)y$	existence of a left identity
$(xy)z = (yx)z$	no right-equivalent elements
$(xy)z = (yz)x$	no right-equivalent elements; surjectivity
$(xy)z = (zx)y$	no right-equivalent elements; surjectivity
$(xy)z = (zy)x$	existence of a right identity
$(xy)z = x(yz)$	commutativity; non-associativity
$(xy)z = x(zy)$	no left-equivalent elements
$(xy)z = y(xz)$	no right-equivalent elements
$(xy)z = y(zx)$	no equivalent elements; non-products commute with each other
$(xy)z = z(xy)$	non-products commute with each other
$(xy)z = z(yx)$	existence of a left- or right-cancellative product

Table 1: Sufficient conditions for commutativity

logic encodings of) many lemmas in this article automatically. In particular, proofs for Lemma 3 and Lemma 5 were first found by Waldmeister. Since Waldmeister proofs may be unnecessarily long, we then implemented a small (about 300 lines of code) C program, which searched for a proof using a simple (exhaustive) breadth-first rewriting algorithm. The proofs of Lemmas 3 and 5 that are shown in this article were found by our C program, and they are the shortest proofs possible that use (4) as an oriented (i.e., from left to right) rewrite rule.

Subsequently, to increase the confidence in these computer-proven results, we interactively developed machine-readable proofs for most of them in Isabelle/HOL. Moreover, Isabelle/HOL has a built-in model generator [9], which was able to find the finite counterexamples described in this article automatically. At the same time, the model generator's failure to find smaller counterexamples implies that the ones given here are the smallest ones possible, in terms of the size of G. We also employed Equinox [2] and Paradox [3] (a theorem prover and a model generator, respectively, for first-order logic) to investigate various conjectures.

This article was mainly concerned with commutativity in the presence of Equations (1)–(12). Future work could focus on the relationship between these equations and other groupoid properties, e.g., associativity or k-niceness, on applications of our results to non-associative rings, and also on identities between products with more than 3 factors.

Acknowledgments. The author's interest in these topics was sparked by a thread in the Usenet newsgroup `de.sci.mathematik` several years ago.

Koen Classen answered my questions about Paradox, and Thomas Hillenbrand kindly provided a recent version of Waldmeister.

References

[1] R. H. Bruck. *A survey of binary systems*, volume 20 of *Ergebnisse der Mathematik und ihrer Grenzgebiete*. Springer, 1958.

[2] Koen Claessen. Equinox, a new theorem prover for full first-order logic with equality. Presentation at Dagstuhl Seminar 05431 on Deduction and Applications, October 2005.

[3] Koen Claessen and Niklas Sörensson. New techniques that improve MACE-style finite model finding. In *CADE-19, Workshop W4, Model Computation – Principles, Algorithms, Applications*, 2003.

[4] Irvin Roy Hentzel, D. P. Jacobs, and Sekhar V. Muddana. Experimenting with the identity (xy)z = y(zx). *Journal of Symbolic Computation*, 16(3):289–293, September 1993.

[5] Th. Hillenbrand. Citius altius fortius: Lessons learned from the theorem prover Waldmeister (invited paper). In I. Dahn and L. Vigneron, editors, *Proceedings of the 4th International Workshop on First-Order Theorem Proving*, volume 86(1) of *Electronic Notes in Theoretical Computer Science*. Elsevier, 2003.

[6] M. H. Kleinfeld. Rings with x(yz) = z(yx). *Communications in Algebra*, 6:1369–1373, 1978.

[7] Tobias Nipkow, Lawrence C. Paulson, and Markus Wenzel. *Isabelle/HOL – A Proof Assistant for Higher-Order Logic*, volume 2283 of *Lecture Notes in Computer Science*. Springer, 2002.

[8] A. Thedy. Ringe mit x(yz) = (yx)z. *Mathematische Zeitschriften*, 99:400–404, 1967.

[9] Tjark Weber. *SAT-based Finite Model Generation for Higher-Order Logic*. PhD thesis, Institut für Informatik, Technische Universität München, Germany, April 2008.

Received: October, 2008