Distributive groupoids are symmetric-by-medial: An elementary proof

David Stanovský

Abstract. We present an elementary proof (purely in equational logic) that distributive groupoids are symmetric-by-medial.

Keywords: distributive groupoids, automated reasoning, Prover9

Classification: 20N02, 03B35, 68T15

1. Introduction

We prove that, in groupoids, the identities

$$x \cdot yz \approx xy \cdot xz, \tag{1}$$

$$xy \cdot z \approx xz \cdot yz \tag{2}$$

imply the identities

$$(xy \cdot zu) \cdot ((xy \cdot zu) \cdot (xz \cdot yu)) \approx xz \cdot yu, \tag{3}$$

$$((xy \cdot zu) \cdot (xz \cdot yu)) \cdot (xz \cdot yu) \approx xy \cdot zu, \tag{4}$$

$$(xy \cdot zu) \cdot (xz \cdot yu) \approx (xz \cdot yu) \cdot (xy \cdot zu). \tag{5}$$

Groupoids satisfying the identities (1), (2) are called *distributive groupoids* and those satisfying (3), (4), (5) are called *symmetric-by-medial*. (In fact, (3), (5) obviously imply (4).) For an idempotent distributive groupoid G, symmetry-by-mediality is equivalent to the fact that there exists a congruence α such that G/α is medial and all blocks of α are symmetric subgroupoids of G (Theorem IV.6.1 of [1]). We thus prove the following

Theorem 1. *Distributive groupoids are symmetric-by-medial.*

For better understanding of the problem, consider terms $A = xy \cdot zu$ and $B = xz \cdot yu$. The goal is to show that, in distributive groupoids, these terms

This work is a part of the research project MSM 0021620839 financed by MŠMT ČR. The author was partly supported by the GAČR grant #201/05/0002.

satisfy so called *symmetric laws*, i.e. $A \cdot AB \approx B$ and $BA \cdot A \approx B$, and that they *commute*, i.e. $AB \approx BA$.

Theorem 1 was shown by J. Ježek and T. Kepka in [2]. First, since every distributive groupoid is a subdirect product of an idempotent distributive groupoid and an A-semigroup (Theorem III.1.8 of [1]), and since the identities trivially hold in A-semigroups, one can focus on idempotent groupoids only. (Note that our proof does not assume idempotency.) The proof of Ježek and Kepka then makes use of structure properties of subdirectly irreducible distributive groupoids and their congruences that are maximal in various respects. Remarkably, axiom of choice is used.

Having finished the elaborate argument, Ježek and Kepka immediately asked, how difficult would be an elementary proof. For more than twenty years, nobody was able to find one, despite some effort. We present such a proof, found with a significant help of W. McCune's automated theorem prover Prover9 [3]. Our benchmark tests show that this is the only theorem prover currently able to prove Theorem 1 in its autonomous mode in reasonable time.

2. The proof

Proposition 2. *Distributive groupoids satisfy* (3) *and* (4).

Proof:

$$
\begin{aligned}
&(xy \cdot zu) \cdot ((xy \cdot zu) \cdot (xz \cdot yu)) = \\
&\overset{(2)}{\approx} (xy \cdot zu) \cdot ((x \cdot zu)(y \cdot zu) \cdot (xz \cdot yu)) \\
&\overset{(2)}{\approx} (xy \cdot zu) \cdot ((x \cdot zu)(xz \cdot yu) \cdot (y \cdot zu)(xz \cdot yu)) \\
&\overset{(1)}{\approx} (xy \cdot zu) \cdot ((xz \cdot xu)(xz \cdot yu) \cdot (z \cdot zu)(xz \cdot yu)) \\
&\overset{(1)}{\approx} (xy \cdot zu) \cdot ((xz \cdot (xu \cdot yu)) \cdot (y \cdot zu)(xz \cdot yu)) \\
&\overset{(2)}{\approx} (xy \cdot zu) \cdot ((xz \cdot (xy \cdot u)) \cdot (y \cdot zu)(xz \cdot yu)) \\
&\overset{(1)}{\approx} (xy \cdot zu) \cdot ((xz \cdot (xy \cdot u)) \cdot (yz \cdot yu)(xz \cdot yu)) \\
&\overset{(2)}{\approx} (xy \cdot zu) \cdot ((xz \cdot (xy \cdot u)) \cdot ((yz \cdot xz) \cdot yu)) \\
&\overset{(2)}{\approx} (xy \cdot zu) \cdot ((xz \cdot (xy \cdot u)) \cdot ((yx \cdot z) \cdot yu)) \\
&\overset{(2)}{\approx} (xy \cdot zu) \cdot ((xz \cdot (xy \cdot u)) \cdot (yx \cdot yu)(z \cdot yu)) \\
&\overset{(1)}{\approx} (xy \cdot zu) \cdot ((xz \cdot (xy \cdot u)) \cdot (y \cdot xu)(z \cdot yu)) \\
&\overset{(1)}{\approx} (xy \cdot z)(xy \cdot u) \cdot ((xz \cdot (xy \cdot u)) \cdot (y \cdot xu)(z \cdot yu))
\end{aligned}
$$

$$
\begin{aligned}
&\overset{(2)}{\approx} (xz\cdot yz)(xy\cdot u)\cdot((xz\cdot(xy\cdot u))\cdot(y\cdot xu)(z\cdot yu))\\
&\overset{(2)}{\approx} ((xz\cdot(xy\cdot u))\cdot(yz\cdot(xy\cdot u)))\cdot((xz\cdot(xy\cdot u))\cdot(y\cdot xu)(z\cdot yu))\\
&\overset{(1)}{\approx} (xz\cdot(xy\cdot u))\cdot((yz\cdot(xy\cdot u))\cdot(y\cdot xu)(z\cdot yu))\\
&\overset{(2)}{\approx} (xz\cdot(xy\cdot u))\cdot((yz\cdot(xu\cdot yu))\cdot(y\cdot xu)(z\cdot yu))\\
&\overset{(2)}{\approx} (xz\cdot(xy\cdot u))\cdot((y(xu\cdot yu)\cdot z(xu\cdot yu))\cdot(y\cdot xu)(z\cdot yu))\\
&\overset{(2)}{\approx} (xz\cdot(xy\cdot u))\cdot((y(xu\cdot yu)\cdot(y\cdot xu)(z\cdot yu))\cdot(z(xu\cdot yu)\cdot(y\cdot xu)(z\cdot yu)))\\
&\overset{(1)}{\approx} (xz\cdot(xy\cdot u))\cdot((y\cdot xu)(y\cdot yu)\cdot(y\cdot xu)(z\cdot yu))\cdot(z(xu\cdot yu)\cdot(y\cdot xu)(z\cdot yu))\\
&\overset{(1)}{\approx} (xz\cdot(xy\cdot u))\cdot((y\cdot xu)\cdot(y\cdot yu)(z\cdot yu))\cdot(z(xu\cdot yu)\cdot(y\cdot xu)(z\cdot yu))\\
&\overset{(2)}{\approx} (xz\cdot(xy\cdot u))\cdot((y\cdot xu)(yz\cdot yu)\cdot(z(xu\cdot yu)\cdot(y\cdot xu)(z\cdot yu)))\\
&\overset{(1)}{\approx} (xz\cdot(xy\cdot u))\cdot((y\cdot xu)(y\cdot zu)\cdot(z(xu\cdot yu)\cdot(y\cdot xu)(z\cdot yu)))\\
&\overset{(1)}{\approx} (xz\cdot(xy\cdot u))\cdot(y(xu\cdot zu)\cdot(z(xu\cdot yu)\cdot(y\cdot xu)(z\cdot yu)))\\
&\overset{(1)}{\approx} (xz\cdot(xy\cdot u))\cdot(y(xu\cdot zu)\cdot((z\cdot xu)(z\cdot yu)\cdot(y\cdot xu)(z\cdot yu)))\\
&\overset{(2)}{\approx} (xz\cdot(xy\cdot u))\cdot(y(xu\cdot zu)\cdot((z\cdot xu)(y\cdot xu)\cdot(z\cdot yu)))\\
&\overset{(2)}{\approx} (xz\cdot(xy\cdot u))\cdot(y(xu\cdot zu)\cdot((zy\cdot xu)(z\cdot yu)))\\
&\overset{(1)}{\approx} (xz\cdot(xy\cdot u))\cdot(y(xu\cdot zu)\cdot((zy\cdot xu)(zy\cdot zu)))\\
&\overset{(1)}{\approx} (xz\cdot(xy\cdot u))\cdot(y(xu\cdot zu)\cdot(zy\cdot(xu\cdot zu)))\\
&\overset{(2)}{\approx} (xz\cdot(xy\cdot u))\cdot(y\cdot zy)(xu\cdot zu)\\
&\overset{(2)}{\approx} (xz\cdot(xy\cdot u))\cdot(y\cdot zy)(xz\cdot u)\\
&\overset{(1)}{\approx} (xz\cdot xy)(xz\cdot u)\cdot(y\cdot zy)(xz\cdot u)\\
&\overset{(1)}{\approx} (x\cdot zy)(xz\cdot u)\cdot(y\cdot zy)(xz\cdot u)\\
&\overset{(2)}{\approx} (x\cdot zy)(y\cdot zy)\cdot(xz\cdot u)\\
&\overset{(2)}{\approx} (xy\cdot zy)\cdot(xz\cdot u)\\
&\overset{(2)}{\approx} (xz\cdot y)\cdot(xz\cdot u)\\
&\overset{(1)}{\approx} xz\cdot yu.
\end{aligned}
$$

The proof of the second identity is dual. □

Lemma 3. *Distributive groupoids satisfy the identity*

$$xy \cdot zz \approx xy \cdot z. \tag{6}$$

Proof: $xy \cdot zz \overset{(3)}{\approx} (xz \cdot yz) \cdot ((xz \cdot yz) \cdot (xy \cdot zz)) \overset{(2)}{\approx} (xy \cdot z) \cdot ((xz \cdot yz) \cdot (xy \cdot zz)) \overset{(2)}{\approx} (xy \cdot z) \cdot ((xy \cdot z) \cdot (xy \cdot zz)) \overset{(1)}{\approx} (xy \cdot z) \cdot (xy \cdot (z \cdot zz)) \overset{(1)}{\approx} xy \cdot (z \cdot (z \cdot zz)) \overset{(1)}{\approx} xy \cdot (zz \cdot (z \cdot zz)) \overset{(1)}{\approx} xy \cdot (zz \cdot (zz \cdot zz)) \overset{(2)}{\approx} xy \cdot (zz \cdot (zz \cdot z)) \overset{(1)}{\approx} (xy \cdot zz) \cdot (xy \cdot (zz \cdot z)) \overset{(1)}{\approx} (xy \cdot zz) \cdot ((xy \cdot zz) \cdot (xy \cdot z)) \overset{(2)}{\approx} (xy \cdot zz) \cdot ((xy \cdot zz) \cdot (xz \cdot yz)) \overset{(3)}{\approx} xz \cdot yz \overset{(2)}{\approx} xy \cdot z.$ □

Lemma 4. *Distributive groupoids satisfy the identities*

$$(xx \cdot y) \cdot z \approx xy \cdot z \qquad \text{and} \qquad x \cdot (y \cdot zz) \approx x \cdot yz. \tag{7}$$

Proof: $(xx \cdot y) \cdot z \overset{(2)}{\approx} (xy \cdot xy)z \overset{(2)}{\approx} (xy \cdot z)(xy \cdot z) \overset{(1)}{\approx} xy \cdot zz \overset{(6)}{\approx} xy \cdot z$. The proof of the other identity is dual. □

Lemma 5. *Distributive groupoids satisfy the identity*

$$xy \cdot x \approx x \cdot yx. \tag{8}$$

Proof: $xy \cdot x \overset{(2)}{\approx} xx \cdot yx \overset{(2)}{\approx} (x \cdot yx)(x \cdot yx) \overset{(1)}{\approx} x \cdot (yx \cdot yx) \overset{(1)}{\approx} x(y \cdot xx) \overset{(7)}{\approx} x \cdot yx.$ □

Lemma 6. *Distributive groupoids satisfy the identity*

$$(xy \cdot zu) \cdot (xy \cdot zu) \approx xy \cdot zu. \tag{9}$$

Proof: $(xy \cdot zu) \cdot (xy \cdot zu) \overset{(1)}{\approx} xy \cdot (zu \cdot zu) \overset{(1)}{\approx} xy \cdot (z \cdot uu) \overset{(7)}{\approx} xy \cdot zu.$ □

Lemma 7. *Distributive groupoids satisfy the identity*

$$(xy \cdot zu) \cdot ((xz \cdot yu) \cdot (xy \cdot zu)) \approx xz \cdot yu. \tag{10}$$

Proof: Denote $A = xy \cdot zu$ and $B = xz \cdot yu$. We prove that $A \cdot BA \approx B$. So, $A \cdot BA \overset{(3)}{\approx} (B \cdot BA) \cdot BA \overset{(1)}{\approx} B \cdot (BA \cdot A) \overset{(4)}{\approx} BB \overset{(9)}{\approx} B.$ □

Proposition 8. *Distributive groupoids satisfy the identity* (5).

Proof: Denote $A = xy \cdot zu$ and $B = xz \cdot yu$. We prove that $AB \approx BA$. So, $AB \overset{(10)}{\approx} A \cdot (A \cdot BA) \overset{(8)}{\approx} A \cdot (AB \cdot A) \overset{(8)}{\approx} (A \cdot AB) \cdot A \overset{(3)}{\approx} BA.$ □

The proof of Proposition 2 involves 35 equalities. The proof of Proposition 8 would involve $9 \cdot 35 + 51 = 366$ equalities, if it were proved directly from the axioms.

3. Automated reasoning techniques used

This seems to be the first automatically generated solution of a relatively old problem in the field of selfdistributive groupoids. We obtained the proof of Theorem 1 with Prover9 [3] (version Feb 2006A) in the autonomous mode shortly after its release. We tried the following computations on a 1.9 GHz personal computer.

A. (1),(2) $\vdash$ (5).
Result: 30 hours, proof of length 152, level 24, max. clause weight 45.

B. (1),(2) $\vdash$ (3).
Result: 5 minutes, proof of length 26, level 12, max. clause weight 41.

C. (1),(2),(3),(4) $\vdash$ (5).
Result: 5 seconds, proof of length 25, level 11, max. clause weight 47.

While the proof of C. nicely splits into several lemmas and gives quite understandable argument (and so is presented in the present paper), despite some effort we were unable to simplify the proof of B.; we present an almost exact translation of the computer generated proof.

Recently, we evaluated various state-of-the-art ATP systems on these problems, using the SystemOnTPTP service (maintained by G. Sutcliffe at University of Miami) at

`http://www.cs.miami.edu/ tptp/cgi-bin/SystemOnTPTP`

First, we asked to solve the task C. with 100 seconds time limit; the table shows results (only successful systems are listed):

EQP 0.9d	1.4
Gandalf c-2.6	0.1
Metis 2.0	24.8
Prover9 0607	3.2
SNARK 20061020	2.7
SOS 2.0	88.2
SPASS 3.0	0.6
Vampire 8.1	0.1
Vampire 9.0	0.1

Remarkably, Waldmeister 806, the winner of the UEQ division of the CASC competition [4], based on Knuth-Bendix algorithm, failed. (An independent computation on our computer shows that it fails in much larger time limit with both KBO and LPO settings.)

Next, we asked successful systems to solve the task B. with 999 seconds time limit, but all of them failed, including Prover9. Failure of Prover9 is caused by a slight change of default parameters in newer versions. An independent computation on our computer shows that while Prover9 (February 2006) needs only 5 minutes to solve B., Prover9 (June 2007) needs about 45 minutes, giving a similar answer.

Remark. After finishing this work we learned that the problem was approached also by Robert Veroff, Michael Kinyon, William McCune and J.D. Phillips in September 2005. They used Otter, a precursor of Prover9, and obtained proofs of comparable complexity. They used rather complicated methods to obtain a proof, since Otter fails in the autonomous mode. They never tried to translate the proof into mathematical language.

References

[1] Ježek J., Kepka T., Němec P., *Distributive groupoids*, Rozpravy ČSAV **91** (1981), no. 3.
[2] Ježek J., Kepka T., *Distributive groupoids and symmetry-by-mediality*, Algebra Universalis **19** (1984), no. 2, 208–216.
[3] McCune W.W., *Prover9*, available at `http://www.cs.unm.edu/~mccune/prover9`.
[4] Sutcliffe G., Suttner C., *The State of CASC*, AI Communications **19** (2006), no. 1, 35–48.

Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 186 75 Prague 8, Czech Republic

E-mail: stanovsk@karlin.mff.cuni.cz

(*Received* November 20, 2007)