SELFDISTRIBUTIVE GROUPOIDS OF SMALL ORDERS

Jaroslav Ježek and Tomáš Kepka

Abstract. After enumerating isomorphism types of at most five-element left distributive groupoids, we prove that a distributive groupoid with less than 81 elements is necessarily medial.

0. Introduction

By a groupoid we mean a nonempty set together with a binary, multiplicatively denoted operation. A groupoid is called left distributive if it satisfies the identity $x(yz) = (xy)(xz)$. Right distributive groupoids are defined dually, and distributive groupoids are the groupoids that are both left and right distributive. A groupoid is called medial if it satisfies the identity $(xy)(uv) = (xu)(yv)$. Medial groupoids have been studied under various other names like entropic, abelian, Abelian, and surcommutative.

After giving (in Section 1) a table of the numbers of isomorphism types of at most five-element groupoids in the variety of left distributive groupoids (and in some important subvarieties), we proceed to our main result in Section 2, claiming that the smallest possible cardinality of a non-medial distributive groupoid is 81.

The two varieties, of distributive and of medial groupoids, are closely connected. As one can easily see, every idempotent medial groupoid is distributive. On the other hand, according to [6], every distributive groupoid is trimedial, i.e., the subgroupoid generated by any three elements of a distributive groupoid is medial.

The two-element group is an example of a non-distributive medial groupoid. On the other hand, constructions of non-medial distributive groupoids are not so immediate. The first examples can be found in [2] and [4]. Bol [2] constructs a non-associative commutative Moufang loop of order 81, and Hall [4] constructs an affine Steiner triple system of the same order; both these structures are equivalent with symmetric distributive quasigroups. It is proved in [4] in a special case and in [10] in general that every non-medial distributive quasigroup contains at least 81 elements. So, the aim of Section 2 is to generalize this result from quasigroups to groupoids.

1. Left distributive groupoids of order at most five

Let us denote by LD, ILD, MLD, SLD, ISLD, D, IM, CD and CIM the varieties of left distributive groupoids, idempotent left distributive groupoids, medial left distributive groupoids, left distributive semigroups, idempotent left distributive semigroups, distributive groupoids, idempotent medial groupoids, commutative distributive groupoids and

commutative idempotent medial groupoids, respectively. Table 1 contains the following information. The number in the row labeled i and in the column labeled V represents the number of isomorphism types of i-element groupoids in the variety V.

	LD	ILD	MLD	SLD	ISLD	D	IM	CD	CIM
2	6	3	5	4	3	4	3	2	1
3	48	17	32	16	9	19	13	7	3
4	720	141	405	93	38	120	71	24	7
5	33425	1704	25185	682	179	921	449	103	22

Table 1

Table 2 specifies the numbers of isomorphism types of left distributive groupoids according to the number of idempotent elements. The number in the row labeled i and in the column labeled j represents the number of pairwise non-isomorphic left distributive groupoids of order i with precisely j idempotents.

	0	1	2	3	4	5
2	1	2	3	0	0	0
3	2	17	12	17	0	0
4	25	233	179	142	141	0
5	704	21699	3936	3115	2267	1704

Table 2

The numbers were computed manually for two- and three-element groupoids. A primitive computer program is able to generate all four-element groupoids in a historically short period of time, check for the left distributive ones and store each, whenever it fails to be isomorphic with the previously stored ones. On the other hand, the number 5^{25} of the multiplication tables of five-element groupoids is too big; in order to obtain the required numbers, we had to classify five-element groupoids according to the isomorphism types of their unary derived operations $f(x) = xx$, and find in each case separately a suitable restrictive condition on the multiplication tables to be generated by a computer program.

Let us also mention that there are 8 isomorphism types of quasitrivial left distributive three-element groupoids; for four- and five-element groupoids the numbers are 24 and 71, respectively. A groupoid G is called quasitrivial if $xy \in \{x, y\}$ for all $x, y \in G$. Left distributive quasitrivial groupoids were completely described in [1].

2. Non-medial distributive groupoids of the least possible order

2.1. Theorem. *Let G be a non-medial distributive groupoid such that every proper subgroupoid of G is medial. Then G is a quasigroup.*

Proof. In the process of proving we shall need some results from [6], and so we assume that the reader is acquainted with that paper. The proof will be divided into eight parts.

Claim 1. *G is finitely generated.* Indeed, G is not medial and thus $(ab)(cd) \neq (ac)(bd)$ for some $a, b, c, d \in G$. But then G is generated by these four elements.

Claim 2. *G is idempotent.* This is due to Theorem III.1.8 of [6].

Claim 3. *G is ideal-free.* Suppose that this is not true, so that G contains a proper prime ideal I by Proposition V.1.11 of [6]. Then both I and $K = G - I$ are medial subgroupoids of G and consequently the factor G/I is also medial, since it is isomorphic to the groupoid K with an annihilating element added. Denote by r the congruence $(I \times I) \cup \mathrm{id}_G$, so that $G/I = G/r$. For each $a \in I$, the left and right translations L_a and R_a are homomorphisms of G into I. Moreover, we have

$$\bigcap_{a \in I} \mathrm{Ker}(L_a) \cap \bigcap_{a \in I} \mathrm{Ker}(R_a) \cap r = \mathrm{id}_G.$$

This shows that G is isomorphic to a subdirect product of some factors of G, all of which are medial. But then G is also medial, a contradiction.

Claim 4. *The factor G/p, where p is the congruence of G defined by $(x, y) \in p$ if and only if $xe = ye$ for all $e \in G$, is not medial.* Suppose, on the contrary, that $(ab \cdot cd)e = (ac \cdot bd)e$ for all $a, b, c, d, e \in G$ and denote by M the set of the ordered quadruples $(x, y, u, v) \in G^4$ such that $xy \cdot uv = xu \cdot yv$. Let $(x, y, u, v) \in M$ and $z \in G$. We have

$$\begin{aligned}
(zx \cdot y)(uv) &= (zy \cdot xy)(uv) = (zy \cdot uv)(xy \cdot uv) = (zy \cdot uv)(xu \cdot yv) = \\
&\quad (zu \cdot yv)(xu \cdot yv) = (zu \cdot xu)(yv) = (zx \cdot u)(yv), \\
(x \cdot zy)(uv) &= (xz \cdot uv)(xy \cdot uv) = (xu \cdot zv)(xu \cdot yv) = (xu)(zy \cdot v), \\
(xy)(u \cdot zv) &= (xy \cdot uz)(xy \cdot uv) = (xu \cdot yz)(xu \cdot yv) = (xy)(y \cdot zv),
\end{aligned}$$

so that $(zx, y, u, v) \in M$, $(x, zy, u, v) \in M$ and $(x, y, u, zv) \in M$. Now let $a, b, c, d \in G$. We have $(a, b, d, d) \in M$, since G is right distributive and idempotent. It follows from the above proved properties of M that $(ab \cdot a, cb, ab \cdot d, cd) \in M$. By Theorem IV.2.3 of [6] we have $(ab \cdot c)(ab) = (ab \cdot a)(cb)$ and so

$$\begin{aligned}
ab \cdot cd &= (ab \cdot c)(ab \cdot d) = ((ab \cdot c)(ab))((ab \cdot c)d) = \\
&\quad ((ab \cdot a)(cb))((ab \cdot d)(cd)) = ((ab \cdot a)(ab \cdot d))(cb \cdot cd) = \\
&\quad (ab \cdot ad)(c \cdot bd) = (a \cdot bd)(c \cdot bd) = ac \cdot bd.
\end{aligned}$$

Thus G turns out to be medial, a contradiction.

Claim 5. *No non-trivial factor of G is a semigroup of right zeros.* Suppose that r is a congruence of G such that G/r is a semigroup of right zeros, i.e., G/r satisfies $xy = y$. Denote by A_i $(i \in I)$ the blocks of r, so that the sets A_i are left ideals of G. If $r \neq G \times G$, then for any $i \in I$, A_i is a medial groupoid, so that we can consider the endomorphism groupoid E_i of A_i and E_i is again medial. We can define a homomorphism f of G into the product of the groupoids E_i $(i \in I)$ by $f(a) = L_a|A_i$. But $\mathrm{Ker}(f) = p$, as it is easy to see, and so G/p is medial; we get a contradiction with Claim 4. This proves $r = G \times G$.

Claim 6. *G is both left- and right-ideal-free.* Define a relation r on G by $(a,b) \in r$ if and only if the elements a and b generate the same left ideal of G. Obviously, $(a,b) \in r$ if and only if $b = a_1(\dots(a_n a))$ and $a = b_1(\dots(b_m b))$ for some elements $a_1, \dots, a_n, b_1, \dots, b_m$ of G and it is clear that r is a congruence of G. Moreover, $a \cdot bc = ab \cdot ac = (a \cdot ac)(b \cdot ac)$ for all $a, b, c \in G$, $(a \cdot bc, b \cdot ac) \in r$ and we see that the factor $H = G/r$ is left permutable, i.e., satisfies the identity $x \cdot yz = y \cdot xz$. Suppose that H is non-trivial. Since H is finitely generated by Claim 1, it possesses a non-trivial simple factor K. This groupoid is left permutable and also ideal-free by Claim 3. Consequently, K is not a quasigroup (because a non-trivial distributive quasigroup cannot be left permutable); also, it is not a semigroup of left zeros, and it is not a commutative semigroup. Now, all simple distributive groupoids have been found in [5]; if we take a look through the list, we can see that only one possibility remains for K: the groupoid K is a semigroup of right zeros. However, this is a contradiction with Claim 5. Thus $r = G \times G$ and G is left-ideal-free. Analogously, G is rigt-ideal-free.

Claim 7. *G is divisible.* Indeed, it follows from Claim 6 and from Theorem V.6.6 of [6] that G is regular and therefore the factor G/p is isomorphic to the subgroupoid Ga of G for every $a \in G$. With respect to Claim 4, $Ga = G$ and G is right divisible. One can show similarly that G is left divisible.

Claim 8. *G is a quasigroup.* By Claim 7 and Theorem 2.6 of [7], there exist a commutative Moufang loop $G(+)$ with the same underlying set as G and two surjective central endomorphisms f, g of $G(+)$ such that $fg = gf$ and $ab = f(a)+g(b)$ for all $a, b \in G$. Denote by R the subring generated by f and g in the ring of central endomorphisms of $G(+)$ (see [8]). Then R is a finitely generated commutative ring, and hence, as it is well known, R is noetherian. Moreover, the loop $G(+)$ can be viewed as a special R-quasimodule (see [8]). It is an easy consequence of Claim 1 that the quasimodule $G(+)$ is finitely generated, and therefore it is noetherian by Proposition 4.6 of [8]. However, the mappings f and g are also surjective endomorphisms of the notherian quasimodule $G(+)$ and consequently both f and g are injective. We have proved that f and g are automorphisms of $G(+)$, which implies that G is a quasigroup.

2.2. Corollary. *Let G be a finite non-medial distributive groupoid. Then G contains a non-medial subquasigroup.*

According to Lemma VI.6.2 of [10], every non-medial distributive quasigroup contains at least 81 elements. This, combined with 2.2, yields

2.3. Corollary. *Every non-medial distributive groupoid contains at least 81 elements.*

Moreover, if we combine these results with Theorem 12.4 of [9], we obtain

2.4. Corollary. *The number of isomorphism types of non-medial distributive groupoids of order 81 is 6.*

The number of isomorphism types of medial distributive groupoids of order 81 is much larger. For example, every semilattice is a medial distributive groupoid and one can show

easily that there exist more than 10^{80} pairwise non-isomorphic semilattices of order 81. On the other hand, proceeding similarly as in the proof of Theorem 14.7 of [9], it is not difficult to show that there exist, up to isomorphism, precisely 18 non-medial distributive groupoids of order 82. It would be interesting to find some limits or bounds for the ratio of the number of non-medial distributive groupoids to that of medial ones of the same order.

References

1. R. El. Bashir and A. Drápal, *Quasitrivial left distributive groupoids*, Commentationes Math. Univ. Carolinae **35** (1994), 597–606.
2. G. Bol, *Gewebe und Gruppen*, Math. Ann. **114** (1937), 414–431.
3. A. Drápal, T. Kepka and M. Musílek, *Group conjugation has non-trivial LD-identities*, Commentationes Math. Univ. Carolinae **35** (1994), 219–222.
4. M. Hall, Jr., *Automorphisms of Steiner triple systems*, IBM J. of Research Development **4** (1960), 460–471.
5. J. Ježek and T. Kepka, *Atoms in the lattice of varieties of distributive groupoids*, Colloquia Math. Soc. J. Bolyai **14**. Lattice Theory, Szeged, 1974, 185–194.
6. J. Ježek, T. Kepka and P. Němec, *Distributive groupoids*, Rozpravy ČSAV, Řada mat. a přír. věd **91**. Academia, Praha, 1981.
7. T. Kepka, *Distributive division groupoids*, Math. Nachr. **87** (1979), 103–107.
8. T. Kepka, *Notes on quasimodules*, Commentationes Math. Univ. Carolinae **20** (1979), 229–247.
9. T. Kepka and P. Němec, *Commutative Moufang loops and distributive groupoids of small orders*, Czech. Math. J. *31* (1981), 633–669.
10. J. P. Soublin, *Étude algébrique de la notion de moyenne*, J. Math. Pures et Appl. **50** (1971), 53–264.

MFF UK, Sokolovská 83, 18600 Praha 8