Small left distributive quasigroups

David Stanovský[⋆]
e-mail: stanovsk@karlin.mff.cuni.cz
Charles University, Prague, Czech Republic
Jan Vlachý
e-mail: jan.vlachy@gmail.com
Charles University, Prague, Czech Republic

We are interested in the structure of finite *left distributive quasigroups* (LDQ), i.e. quasigroups such that the left translations are automorphsims, or equivalently, satisfying the identity

$$x(yz) = (xy)(xz).$$

Our work has essentially two parts: to give an overview of Galkin's theory in a modern way, and to apply the theory to find the smallest non-medial LD quasigroup. Particularly, we find the smallest solution to the eighth problem from the famous Belousov's list: an LDQ that is not isotopic to a Bol loop.

The LD law says that the left multiplication group, $LMlt(Q)$ (generated by all left translations), is a subgroup of the group of automorphisms, $Aut(Q)$. The fundamental theorem of Galkin's theory says that each finite LDQ admits so called *Galkin representation*, that is $Q \simeq (G/T, \circ)$, where G is a group, $\varphi \in Aut(G)$, T is the subgroup of fixed points of φ, and the operation on cosets is given by

$$xT \circ yT = x\varphi(x^{-1}y)T.$$

There is a canonical way to represent an LDQ: take $G = LMlt(Q)$ and φ the inner automorphism given by L_e, the left translation by an (arbitrarily chosen) element $e \in Q$; then, $T = LMlt(Q)_e$, the stabilizer of e. There is also a minimal repres entation of a given LDQ, with respect to the size of G: one can reduce the canonical one to $G = LMlt(Q)'$, the commutator subgroup (and no smaller representation exists). One of the consequences is a weak form of Lagrange's theorem for LDQs.

The class of LD quasigroups includes *medial idempotent quasigroups* (MIQ), given by the identity

$$(xy)(uv) = (xu)(yv).$$

The subclass of MIQs plays a role similar to abelian groups in group theory (in fact, they are the abelian LDQs, in the sense of universal algebra). By Toyoda's theorem, MIQs are isotopic to abelian groups, with operation given by $x \circ y = \alpha(x) + \beta(y)$, where α, β is a pair of commuting automorphisms.

Unlike medial quasigroups, not all LDQs are isotopic to groups. Those that are, have very nice properties, such as (full) Lagrange's theorem, or a weak form of Sylow's theorems. Other ingredients for the classification of small LDQs include the classificat ion of LDQs with no non-trivial subquasigroups (all of them are medial and can be constructed from finite fields), and classification of both left and right distributive quasigroups.

The main original results of the present work are, (1) a proof that all LDQs of size < 15 are medial, (2) a proof that there are exactly two non-isomorphic

LDQs of size 15, and Galkin representation for both of them. The proof mostly involves computation in groups that are candidates for multiplication groups of LD quasigroups.

Our work has been motivated by the eighth Belousov's problem: to decide whether all LDQs are isotopic to Bol loops. The negative answer was already given in 1970s, but the counterexample was huge. Using exhaustive computer search, we found that the smalles t counterexample has 15 elements, and in fact, no smaller exists just because all smaller LDQs are medial (thus isotopic to groups). On 15 elements, there are exactly two non-isomorphic non-medial LDQs: the core of the smallest proper Bruck loop (hence, is otopic to a Bol loop), and one which fails to be isotopic to a Bol loop.

Our arguments are still partly assisted by a computer, but in a much more acceptable way: we used the GAP system just to do computations in certain specific small groups (avoiding exhaustive search). Also, the counterexample to Belousov's problem is no mor e presented as a 15 by 15 table of numbers, but the Galkin representation gives a natural description using the (only non-abelian) 75-element group over its 5-element subgroup.