AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **40** (2008), Pages 167–171

A shortest single axiom with neutral element for commutative Moufang loops of exponent 3

Nick C. Fiala

Department of Mathematics
St. Cloud State University
St. Cloud, MN 56301
U.S.A.
ncfiala@stcloudstate.edu

Abstract

In this brief note, we exhibit a shortest single product and neutral element axiom for commutative Moufang loops of exponent 3 that was found with the aid of the automated theorem-prover Prover9.

1 Introduction

A *Steiner triple system*, or STS, is a pair $(X, \mathcal{B})$ where X is a set, the elements of which are called *points*, and $\mathcal{B}$ is a set of 3-subsets of X, the elements of which are called *blocks*, such that every 2-subset of points is contained in exactly one block. A *Hall triple system*, or HTS, is an STS such that any three non-collinear points lie in a subsystem isomorphic to the affine plane $AG(2,3)$ over $GF(3)$ [4].

A *quasigroup* consists of a non-empty set Q equipped with a binary operation, which we simply denote by juxtaposition, such that for all $a, b \in Q$, there exist unique $x, y \in Q$ such that $ax = b$ and $ya = b$. Alternatively, a quasigroup is an algebra $(Q; \cdot, \backslash, /)$ of type $(2,2,2)$ such that $x\backslash(x \cdot y) = y$, $(x \cdot y)/y = x$, $x \cdot (x\backslash y) = y$, and $(x/y) \cdot y = x$. A *loop* is a quasigroup L possessing a *neutral element* $e \in L$ such that $ex = xe = x$ for all $x \in L$. A loop L is *commutative* if $xy = yx$ for all $x, y \in L$. A loop L is *Moufang* if $(xy)(zx) = (x(yz))x$ for all $x, y, z \in L$. A loop L with neutral element e is of *exponent* 3 if $(xx)x = x(xx) = e$ for all $x \in L$.

Quasigroups and loops are of interest not only in algebra but in combinatorics as well. In fact, given an HTS $(X, \mathcal{B})$, we can construct a commutative Moufang loop of exponent 3, or CML^3, whose elements are the elements of X as follows: fix a point $e \in X$ and define $ex = xe = x$ for all $x \in X$, define xx to be the third point in the unique block containing $\{e, x\}$ for all $x \in X$, $x \neq e$, and define xy to be the third point in the unique block containing $\{xx, yy\}$ for all $x, y \in X$, $x, y \neq e, x \neq y$.

This construction turns X into a CML^3 with neutral element e and, conversely, each CML^3 L with neutral element e gives rise to an HTS whose points are the elements of L and whose blocks are the 3-subsets of L of the form $\{x, y, (xy)(xy)\}$, $y \neq e, x, x^2$ [5].

It is not difficult to see that the variety of CML^3's can be axiomatized in terms of product by the identities $xy = yx$, $(xx)(xy) = y$, and $(xy)(zx) = (x(yz))x$ or in terms of product and e by the identities below.

$$xy = yx \tag{1}$$

$$ex = x \tag{2}$$

$$(xx)(xy) = y \tag{3}$$

$$(xy)(zx) = (x(yz))x \tag{4}$$

Therefore, it is natural to ask if there is a single identity in product or in product and e that axiomatizes the variety of CML^3's. In other words, does there exist a single identity in product (and e) that is valid in all CML^3's (with neutral element e) and such that all models of the identity are CML^3's (with neutral element e)? We will call such an identity a *single product* (*and neutral element*) *axiom for* CML^3*'s*. If such an identity exists, then it is natural to ask what is the length of a shortest such identity (in terms of the number of variable and constant occurrences). Single product axioms for some other varieties of quasigroups and loops that are constructed from STS's and other types of combinatorial designs are known. For example, single product axioms are known for the varieties of squags and sloops [3]. Also, in [7], single product axioms were found for some varieties of groupoids associated with strongly 2-perfect m-cycle systems.

We view single product and neutral element axioms as more natural and appealing since varieties of loops are usually axiomatized with specific reference to the neutral element as a constant, or nullary operation, in said structure. However, it is not always possible to axiomatize a variety by a single identity in all of the operations of the variety. For instance, the variety of groups can be axiomatized by a single identity in product and inverse [9], [13] and the variety of Boolean groups can be axiomatized by single identities in product [12] and in product and neutral element [11], but no variety of groups can be axiomatized by a single identity in product, inverse, and neutral element [13], [14].

In this brief note, we exhibit a shortest single product and neutral element axiom for CML^3's that was found with the aid of the automated theorem-prover Prover9 [10], a resolution theorem-prover for first-order logic with equality. The scripting language Perl was also used to further automated our search.

2 A single axiom for CML^3's

In this section, we describe our search for a shortest single product and neutral element axiom for CML^3's.

Any such identity must have one side consisting of a single variable (otherwise it would be valid in any zero semigroup), say z, z must not be the left-most (right-most) variable on the other side (otherwise it would be valid in any left-zero (right-zero) semigroup), z must occur a multiple of three plus one times on the other side, and every other variable must occur a multiple of three times (otherwise it would not be valid in $\mathbb{Z}_3$). Any such identity must also have at least three distinct variables since any identity with less than three distinct variables that satisfies the conditions above is valid in a commutative, diassociative, non-Moufang loop of exponent 3 with neutral element e (such a loop of order 27 exists by the results of [2], [6], and [8]).

We began by generating a large number of such identities in three distinct variables x, y, and z with x and y occurring three times each, z occurring once on each side, and e occurring once. A single product and neutral element axiom for CML^3's of this kind would clearly be as short as possible. However, a single product and neutral element axiom for CML^3's of this sort need not exist at all.

We then used Prover9 to extract some of these identities that are valid in the variety of CML^3's with neutral element e by sending each of them to Prover9 and searching for a proof that it is implied by (1), (2), (3), and (4). For example, the identity $e(x((x((x(yy))z))y)) = z$ is easily seen to be valid in all CML^3's with neutral element e.

Next, we sent each of these identities to Prover9 to search for a proof that it implies (1), (2), (3), and (4), and is therefore a single product and neutral element axiom for CML^3's, until one was found. For example, running Prover9 on the input

```
set(auto).  % autonomous mode
op(500, infix, *).  % binary operation
clauses(sos).  % set of support clauses
e * (x * ((x * ((x * (y * y)) * z)) * y)) = z.  % candidate identity
a * b != b * a | e * a != a | (a * a) * (a * b) != b |
 (a * b) * (c * a) != (a * (b * c)) * a.  % not CML^3 with
                                          % neutral element e
end_of_list.  % end of set of support clauses
```

produces a proof that the identity from above is a single product and neutral element axiom for CML^3's. We suppress the proof because of its length (78 lines, most of which correspond to several non-trivial steps) and because it can be easily verified with another Prover9 run on the above input (the proof is also available from the author upon request).

Theorem 2.1. *The identity*

$$e(x((x((x(yy))z))y)) = z$$

is a shortest single product and neutral element axiom for CML^3*'s.*

Interestingly, the identity $x((x((x(yy))z))y) = z$ is not a single product axiom for CML^3's since it is valid in the structure $(\{0, 1, 2\}; \cdot)$ where $\cdot$ is defined by $x \cdot y = 2x + 2y \pmod 3$ (it is easily verified that this is a quasigroup but not a loop).

We end with two problems.

Problem 2.2. Find all shortest single product and neutral element axioms for CML^3's.

Problem 2.3. A loop L with neutral element e has the *weak inverse property*, or is a WIP-*loop*, if $(e/(xy))x = e/y$ (equivalently, $x((yx)\backslash e) = y\backslash e$) for all $x, y \in L$. In [1], the correspondence between HTS's and CML^3's is generalized to a correspondence between STS's and commutative WIP-loops of exponent 3. It is not difficult to see that the variety of commutative WIP-loops of exponent 3 can be axiomatized in terms of product by the identities $xy = yx$, $((xx)x)y = y$, and $x((xy)(xy)) = yy$ or in terms of product and e by the identities $xy = yx$, $ex = x$, and $x((xy)(xy)) = yy$. Find a (all) shortest single product and neutral element axiom(s) for commutative WIP-loops of exponent 3 or show that none exist.

References

[1] M. H. Armanious, Commutative loops of exponent 3 with $x \cdot (x \cdot y)^2 = y^2$ *Demonstratio Math.* **35** (2002), 469–475.

[2] O. Chein, Moufang loops of small order. I, *Trans. Amer. Math. Soc.* **188** (1974), 31–51.

[3] D. Donovan and Sheila Oates-Williams, Single laws for sloops and squags, *Discrete Math.* **92** (1991), 79–83.

[4] M. Hall Jr., Automorphisms of Steiner triple systems, *IBM J. Res. Develop.* **4** (1960), 460–472.

[5] M. Hall Jr., Group theory and block designs, *Proc. Internat. Conf. Theory of Groups*, Gordon and Breach, New York, 1967, 115–144.

[6] J. Hart and K. Kunen, Single axioms for odd exponent groups, *J. Automat. Reason.* **14** (1995), 383–412.

[7] A. Khodkar and S. Zahrai, On single laws for varieties of groupoids associated with strongly 2-perfect m-cycle systems, *Algebra Universalis* **46** (2001), 499–513.

[8] M. K. Kinyon, K. Kunen and J. D. Phillips, A generalization of Moufang and Steiner loops, *Algebra Universalis* **48** (2002), 81–101.

[9] K. Kunen, Single axioms for groups, *J. Automat. Reason.* **9** (1992), 291–308.

[10] W. McCune, Prover9 (`http://www.cs.unm.edu/∼mccune/prover9/`).

[11] W. McCune and L. Wos, Applications of automated deduction to the search for single axioms for exponent groups, in: *Logic Programming and Automated Reasoning*, Springer-Verlag, Berlin, 1992, 131–136.

[12] C. A. Merdith and A. N. Prior, Equational logic, *Notre Dame J. Formal Logic* **9** (1968), 212–226.

[13] B. H. Neumann, Another single law for groups, *Bull. Austral. Math. Soc.* **23** (1981), 81–102.

[14] A. Tarski, Equational logic and equational theories of algebras, in: *Contributions to Math. Logic*, North-Holland, Amsterdam, 275–288.

(Received 23 Jan 2007)