Available online at www.sciencedirect.com
ScienceDirect
Discrete Mathematics 308 (2008) 3381–3385
DISCRETE MATHEMATICS
www.elsevier.com/locate/disc

Note

Shortest single axioms for commutative moufang loops of exponent 3

Nick C. Fiala

Department of Mathematics, St. Cloud State University, St. Cloud, MN 56301, USA

Received 30 November 2006; received in revised form 7 June 2007; accepted 21 June 2007
Available online 2 August 2007

Abstract

In this note, we attempt to find all shortest single product axioms for commutative Moufang loops of exponent 3. These investigations were aided by the automated theorem-prover Prover9 and the model-generator Mace4.

Keywords: Steiner triple system; Hall triple system; Commutative Moufang loop of exponent 3; Single product axiom; Automated reasoning

1. Introduction

A *Steiner triple system*, or STS, is a pair $(X, \mathscr{B})$ where X is a set, the elements of which are called *points*, and $\mathscr{B}$ 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 $GF(3)$ [3].

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 quasigroup Q is *commutative* if $xy = yx$ for all $x, y \in Q$. A quasigroup Q is *Moufang* if $(xy)(zx) = (x(yz))x$ for all $x, y, z \in Q$. 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 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 $(X, \mathscr{B})$, 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 $\{x, y, (xy)(xy)\}$, $y \neq e, x, xx$ [4].

E-mail address: ncfiala@stcloudstate.edu.

0012-365X/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2007.06.016

The variety of CML^3's can be axiomatized in terms of product only by the three identities below.

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

$$(xx)(xy) = y, \tag{2}$$

$$(xy)(zx) = (x(yz))x. \tag{3}$$

Indeed, a model of (1)–(3) is clearly a commutative quasigroup. The results of [7] imply that a Moufang quasigroup is, in fact, a Moufang loop. Then (1) and (2) imply that the loop has exponent 3.

Therefore, it is natural to ask if there is a single identity in product only that axiomatizes the variety of CML^3's. In other words, does there exist a single identity in product only that is valid in all CML^3's and such that all models of the identity are CML^3's? We will call such an identity a *single product axiom for* CML^3*'s*. If such an identity exists, then it is natural to ask what is the length (in terms of the number of variable occurrences) of a shortest such identity.

Short single product axioms for some other varieties of quasigroups and loops that are constructed from STS's are known. For example, short single product axioms are known for the varieties of squags and sloops [2]. Short single product axioms are also known for the smallest non-trivial subvariety of the variety of CML^3's, the groups of exponent 3. In [10], the following identities were each shown to be single product axioms for groups of exponent 3.

$$y((y(y(x(zz))))z) = x, \quad y((y((yx)z))(zz)) = x, \quad y((((yy)(xz))z)z) = x.$$

Furthermore, in [5], it was shown that these three identities comprise all of the shortest single product axioms for groups of exponent 3 (up to renaming, mirroring, and symmetry) with the possible exceptions of the identities below.

$$y(y((y(xz))(zz))) = x, \quad (yy)((y((xz)z))z) = x.$$

The status of these two identities is unknown. It is known that a finite model of either one of them must be a group of exponent 3 [5].

In this note, we attempt to find all shortest single product axioms for CML^3's. These investigations were aided by the automated theorem-prover Prover9 [9] and the model-generator Mace4 [8]. The scripting language Perl was also used to further automate our search.

2. Single axioms

In this section, we describe our search for the shortest single product axioms for CML^3's.

Any such identity must have one side consisting of a single variable (otherwise the identity would be valid in any zero semigroup), said variable must not be the left-most (right-most) variable on the other side (otherwise the identity would be valid in any left-zero (right-zero) semigroup), said variable 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 the identity 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 (such a loop of order 27 exists by the results of [1,5,6]).

We began by generating all such identities (up to renaming, mirroring, and symmetry) with three distinct variables and eight variable occurrences. A single product axiom for CML^3's of this length would clearly be as short as possible. This resulted in 3300 candidate identities.

Next, we sent the negation of each of these identities (stored in the Perl variable `$negated_identity`) to Mace4 and ran

```
assign(domain_size, 81).        % model of size 81
formulas(theory).               % formulas
x*y =y*x.                       % (1)
(x*x)*(x*y) =y.                 % (2)
(x*y)*(z*x) =(x*(y*z))*x.       % (3)
$negated_identity.              % negated candidate identity
end_of_list.                    % end of formulas
```