First Results of Studying Quasigroup Identities by Rewriting Techniques

Mark E. Stickel*
Artificial Intelligence Center
SRI International
Menlo Park, California 94025
stickel@ai.sri.com

Hantao Zhang†
Computer Science Department
The University of Iowa
Iowa City, IA 52242
hzhang@cs.uiowa.edu

November 18, 1994

Abstract

Finite quasigroups in the form of Latin squares have been extensively studied in design theory. Some quasigroups satisfy constraints in the form of equations, called *quasigroup identities*. Numerous open problems of the existence of quasigroups of particular size that satisfy particular identities have been solved by automated theorem-proving methods (such as the Davis-Putnam procedure) that are complete over a finite domain. In this note, we illustrate how other kinds of questions concerning quasigroup identities can sometimes be answered by the alternative equality-based automated theorem-proving method of term rewriting and completion.

1 Introduction

This note discusses problems in quasigroups, whose multiplication tables are Latin squares. The information on Latin squares provided here is mainly drawn from a survey paper by Bennett and Zhu [2]; the interested reader may refer to that work for more information on Latin squares, their importance in design theory, and some other related applications.

Recently, automated model-generation programs have been used to solve the existence problem of quasigroups with specified size and properties. Several dozen open cases were first solved by these programs [12, 4, 6, 10, 5, 9, 8]. The finite enumeration methods used did not employ equality reasoning and were limited to finding quasigroups of specific (small) size. This note presents a complementary line of research: using rewriting techniques to prove general properties of quasigroups. For example, we might wish to show that if a quasigroup satisfies an equation, one of its conjugates will satisfy a second equation, regardless of size. This may help mathematicians to gain insights in attacking open problems in quasigroups.

In [11], we listed some problem areas for possible investigation of quasigroups using equational reasoning. This paper presents the first results of applying rewriting techniques to quasigroups, and the results are already promising. We were able to verify the theorem that all short conjugate-orthogonal identities are conjugate-equivalent to one of a list of seven identities. We conducted

*Partially supported by the National Science Foundation under Grant CCR-8922330.
†Partially supported by the National Science Foundation under Grants CCR-9202838 and CCR-9357851.

the first thorough investigation of which conjugates are orthogonal for each of these identities and found a previously unknown orthogonal pair.

2 Quasigroups and Conjugates

A quasigroup is simply a cancellative groupoid. That is, a quasigroup is an ordered pair $\langle S, * \rangle$ where S is a finite set and $*$ is a binary operation on S such that

$$\begin{aligned} a_1 * b = a_2 * b &\Rightarrow a_1 = a_2 \\ a * b_1 = a * b_2 &\Rightarrow b_1 = b_2 \end{aligned}$$

The cardinality of S, $|S|$, is called the *order* of the quasigroup. The "multiplication table" for the operation $*$ forms a Latin square, of which each row and each column is a permutation of S. Many classes of quasigroups are of interest, partly because they are very natural objects in their own right, and partly because of their relationship to design theory.

People are interested in Latin squares that satisfy a set of constraints. These constraints are often expressed in terms of the quasigroup operator $*$ plus some universally quantified variables. For example, idempotent Latin squares are those that satisfy $x * x = x$. The constraints we consider here involve the notion of "conjugate-orthogonal Latin squares".

Evidently, whenever $\langle S, * \rangle$ is any quasigroup, given values of any two variables in $x * y = z$, we can uniquely determine the value of the third variable. For example, we may therefore associate with $\langle S, * \rangle$ a function $\star$ such that $x \star z = y$ iff $x * y = z$. It is easy to see that $\langle S, \star \rangle$ is also a quasigroup. $\langle S, \star \rangle$ is one of the six *conjugates* of $\langle S, * \rangle$. These are defined via the six operations $*_{ijk}$ where i, j, and k are distinct members of $\{1, 2, 3\}$:

$$(x_i *_{ijk} x_j = x_k) \Longleftrightarrow (x_1 * x_2 = x_3)$$

We shall refer to $\langle S, *_{ijk} \rangle$ as the (i, j, k)-conjugate of $\langle S, * \rangle$. Where S is understood to be common, we will simply refer to $*_{ijk}$ as the (i, j, k)-conjugate of $*$. Needless to say, the $(1, 2, 3)$-conjugate is the same as the original quasigroup.

Example 1 Here are the six conjugates of a small Latin square:

(a)	(b)	(c)	(d)	(e)	(f)
1 4 2 3	1 2 4 3	1 3 2 4	1 2 4 3	1 3 4 2	1 3 2 4
2 3 1 4	4 3 1 2	2 4 1 3	3 4 2 1	3 1 2 4	3 1 4 2
4 1 3 2	2 1 3 4	4 2 3 1	2 1 3 4	2 4 3 1	4 2 3 1
3 2 4 1	3 4 2 1	3 1 4 2	4 3 1 2	4 2 1 3	2 4 1 3

(a) a Latin square; (b) its $(2, 1, 3)$-conjugate; (c) its $(3, 2, 1)$-conjugate; (d) its $(2, 3, 1)$-conjugate; (e) its $(1, 3, 2)$-conjugate; (f) its $(3, 1, 2)$-conjugate. □

We say that constraint C' is a *conjugate-implicant* of constraint C if whenever a quasigroup satisfies C, one of its conjugates satisfies C'. We say two constraints are *conjugate-equivalent* if they are conjugate-implicants of each other. For example, the identity $x * (x * y) = y * x$ is conjugate-equivalent to $(y * x) * x = x * y$, since the latter can be obtained by taking $*_{213}$ for $*$ in the former. A constraint is said to be *conjugate-invariant* if whenever a quasigroup satisfies the constraint, every conjugate satisfies the constraint. For example, the idempotency law, $x * x = x$, is conjugate-invariant.

	$*_{321}$	$*_{132}$	$*_{213}$	$*$	$*_{231}$	$*_{312}$
$*_{312}$	$QG1''$	$QG0''$	$QG1'$	$QG2$	$QG2''$	—
$*_{231}$	$QG0'$	$QG1''$	$QG1$	$QG2'$	—	$QG2''$
$*$	$QG1$	$QG1'$	$QG0$	—	$QG2'$	$QG2$
$*_{213}$	$QG2'$	$QG2$	—	$QG0$	$QG1$	$QG1'$
$*_{132}$	$QG2''$	—	$QG2$	$QG1'$	$QG1''$	$QG0''$
$*_{321}$	—	$QG2''$	$QG2'$	$QG1$	$QG0'$	$QG1''$

Table 1: Conjugate-Orthogonality Constraints

3 Conjugate Orthogonality

Two quasigroups $\langle S, * \rangle$ and $\langle S, \star \rangle$ over the same set S are said to be *orthogonal* iff for any two elements u, v of S, the set $\{\langle x, y \rangle \mid x * y = u, x \star y = v\}$ is singleton, or equivalently, for all elements x, y, z, w of S

$$((x * y = z * w) \wedge (x \star y = z \star w)) \Rightarrow (x = z \wedge y = w).$$

It sometimes happens that one conjugate of a quasigroup is orthogonal to one of its other conjugates. Following convention [2], we refer to a Latin square (quasigroup) of order v that is orthogonal to its (i, j, k)-conjugate as an (i, j, k)-COLS(v) (one that is also idempotent is referred to as an (i, j, k)-COILS(v)). For example, the Latin square (a) in Example 1 is both a $(1, 3, 2)$-COLS(4) and a $(3, 1, 2)$-COLS(4) since it is orthogonal to (e) and (f), its $(1, 3, 2)$- and $(3, 1, 2)$-conjugates.

Thus, $(2, 1, 3)$-COLS, $(3, 2, 1)$-COLS, and $(3, 1, 2)$-COLS are those quasigroups that satisfy $QG0$, $QG1$, and $QG2$, respectively.

$$\begin{array}{ll} QG0: & (x * y = z * w \wedge x *_{213} y = z *_{213} w) \Rightarrow (x = z \wedge y = w) \\ QG1: & (x * y = z * w \wedge x *_{321} y = z *_{321} w) \Rightarrow (x = z \wedge y = w) \\ QG2: & (x * y = z * w \wedge x *_{312} y = z *_{312} w) \Rightarrow (x = z \wedge y = w) \end{array}$$

These constraints can be rephrased uniformly in $*$ as:

$$\begin{array}{ll} QG0: & (x * y = z * w \wedge y * x = w * z) \Rightarrow (x = z \wedge y = w) \\ QG1: & (x * y = z * w \wedge v * y = x \wedge v * w = z) \Rightarrow (x = z \wedge y = w) \\ QG2: & (x * y = z * w \wedge y * v = x \wedge w * v = z) \Rightarrow (x = z \wedge y = w) \end{array}$$

The orthogonality of a pair of conjugates can be logically equivalent to, or conjugate-equivalent to, orthogonality of other pairs of conjugates. For example, $QG1$ and $QG2$ are conjugate-equivalent to the definitions of $(1, 3, 2)$-COLS and $(2, 3, 1)$-COLS, respectively. These relationships are summarized in Table 1.

Each table entry is a code name for a constraint that is defined to be logically equivalent to the orthogonality of its row and column labels. For example, $QG1$ is defined by orthogonality of $*$ and $*_{321}$, but could have been defined equivalently by orthogonality of $*_{213}$ and $*_{231}$. The constraints $QG0$, $QG0'$, and $QG0''$ are conjugate-equivalent; so are $QG1$, $QG1'$, and $QG1''$; and so are $QG2$, $QG2'$, and $QG2''$.

4 Formulation of Quasigroups for the Knuth-Bendix Procedure

Quasigroups can be characterized by six mutually defined functions $*$, $*_{132}$, $*_{213}$, $*_{231}$, $*_{312}$, and $*_{321}$ in the following way. For each equation $x *_{ijk} y = z$, solve for y in terms of x and z and solve for x in terms of y and z to produce the following twelve equations:

1:	$x * (x *_{132} z) = z$	7:	$x *_{213} (x *_{231} z) = z$
2:	$(y *_{231} z) * y = z$	8:	$(y *_{132} z) *_{213} y = z$
3:	$x *_{132} (x * z) = z$	9:	$x *_{312} (z *_{231} x) = z$
4:	$(z *_{231} y) *_{132} y = z$	10:	$(y * z) *_{312} y = z$
5:	$x *_{231} (z * x) = z$	11:	$x *_{321} (z *_{132} x) = z$
6:	$(z *_{132} y) *_{231} y = z$	12:	$(z * y) *_{321} y = z$

Applying the Knuth-Bendix completion procedure to this set of equations results in the deletion of 7–12 above and the addition of 7–9 below:

1:	$x * (x *_{132} z) = z$	7:	$x *_{213} y = y * x$
2:	$(y *_{231} z) * y = z$	8:	$x *_{312} y = y *_{132} x$
3:	$x *_{132} (x * z) = z$	9:	$x *_{321} y = y *_{231} x$
4:	$(z *_{231} y) *_{132} y = z$		
5:	$x *_{231} (z * x) = z$		
6:	$(z *_{132} y) *_{231} y = z$		

This set of equations is terminating and confluent when read as a set of left-to-right reductions. This set of equations was used in the present study.

That these equations suffice to characterize quasigroups can be shown by proving the cancellation laws, i.e., $a_1 = a_2$ and $b_1 = b_2$ can be proved from $a_1 * b = a_2 * b$ and $a * b_1 = a * b_2$, respectively.

5 Short Conjugate-Orthogonal Identities

The Knuth-Bendix procedure[1] can be applied to constraints in the form of equations, called *quasigroup identities.* A quasigroup identity is said to be *nontrivial* if it is consistent with the specification of a Latin square. A quasigroup identity is called a *short conjugate-orthogonal identity* in [3] if it is of form $a(x, y) * b(x, y) = x$, where $a, b \in \{*, *_{213}, *_{132}, *_{312}, *_{231}, *_{321}\}$. The a and b conjugates of $*$ are orthogonal.

[1] Actually, we use the *unfailing* Knuth-Bendix procedure to cope with the problem of some derived equalities being unorientable.

	$*_{321}$	$*_{132}$	$*_{213}$	$*$	$*_{231}$	$*_{312}$
$*_{312}$	$QG9$	$QG8$	$QG8$	$QG5$	$QG5$	—
$*_{231}$	$QG8$	$QG6$	$QG8$	$QG7$	—	—
$*$	$QG8$	$QG8$	$QG3$	—	$QG4$	—
$*_{213}$	$QG5$	$QG7$	—	$QG4$	$QG5$	—
$*_{132}$	$QG5$	—	$QG4$	$QG5$	$QG7$	—
$*_{321}$	—	—	—	—	—	—

Table 2: Short Conjugate-Orthogonal Identities

Identity	Conjugate-Implicants	Orthogonal Conjugates
$QG3$	$QG0$	$* \perp *_{213}$, $*_{231} \perp *_{321}$, $*_{132} \perp *_{312}$
$QG4$	$QG0, QG2$	$* \perp *_{213}$, $*_{231} \perp *_{312}$, $*_{132} \perp *_{321}$
$QG5$	$QG1, QG2$	$* \perp *_{231} \perp *_{213} \perp *_{321} \perp *$, $* \perp *_{312}$, $*_{132} \perp *_{213}$
$QG6$	$QG1$	$* \perp *_{132} \perp *_{231} \perp *_{213} \perp *_{312} \perp *_{321} \perp *$
$QG7$	$QG1, QG2$	$* \perp *_{231} \perp *_{132} \perp *_{213} \perp *_{321} \perp *_{312} \perp *$
$QG8$	$QG0, QG1$	$* \perp *_{132} \perp *_{231} \perp *_{321} \perp *_{312} \perp *_{213} \perp *$
$QG9$	$QG1$	$* \perp *_{321}$, $*_{213} \perp *_{231}$

Table 3: Conjugate-Orthogonality Results for $QG3$–$QG9$

Theorem 2 ([3, 1]) *Any nontrivial short conjugate-orthogonal identity is conjugate-equivalent to one of the following:*

Code Name[2]	Identity
$QG3$	$(x*y)*(y*x) = x$
$QG4$	$(y*x)*(x*y) = x$
$QG5$	$((y*x)*y)*y = x$
$QG6$	$(x*y)*y = x*(x*y)$
$QG7$	$(y*x)*y = x*(y*x)$
$QG8$	$x*(x*y) = y*x$
$QG9$	$((x*y)*y)*y = x$

Theorem 2 can be verified easily by the Knuth-Bendix procedure with the results in Table 2. Each location in the table corresponds to a short conjugate-orthogonal identity; its value is either the code name "QGi" of the identity that is conjugate-equivalent to it or "—" if the identity is trivial. For example, the identity $(x *_{312} y) * (x *_{321} y) = x$ is conjugate-equivalent to $QG9$. Construction of this table required 57 proofs using the Knuth-Bendix procedure (none took more than 5 seconds of CPU time). Each trivial identity required the derivation of $x = y$ from the quasigroup axioms plus the short conjugate-orthogonal identity. Each nontrivial identity required two proofs: that QGi is a conjugate-implicant of the identity, and that the identity is a conjugate-implicant of QGi.

Superimposing Tables 1 and 2, we can determine which of $QG0$–$QG2$ are conjugate-implicants of $QG3$–$QG9$ (Table 3).

[2]This extends the nomenclature $QG1$–$QG7$ introduced in [4].

These relationships had not been exhaustively studied before and two of these results are noteworthy. The fact that a conjugate of $QG4$ satisfies $QG2$ was observed by Stickel in 1994. This observation lead to the positive solution of the previously open problem of the existence of $(3,1,2)$-COILS(12)—an idempotent quasigroup of order 12 that satisfies $QG2$. Bennett then proved the hitherto unnoticed theorem that $QG2$ is a conjugate-implicant of $QG4$, which we have now verified by the Knuth-Bendix procedure. The fact that a conjugate of $QG7$ satisfies $QG1$ is a new result, which was discovered by the Knuth-Bendix procedure in this study.

The third column of Table 3 shows the situation in more detail. It lists for each identity which pairs of conjugates we found to be orthogonal. The expression $a_1 \perp \cdots \perp a_n$ means a_i is conjugate orthogonal to a_{i+1} $(1 \leq i < n)$.

Let $|t|$ denote the number of variable occurrences in term t. We call $(|u|,|v|)$ the *type* of the identity $u = v$. For example, four identities in Theorem 2 are of type $(4,1)$, one of type $(3,2)$, and two of type $(3,3)$.

It is natural to inquire about existence of conjugate-equivalent identities of various types. For example, is each of $QG3$–$QG9$ conjugate-equivalent to a type $(4,1)$ identity?

Here is the classification of some type $(4,1)$ identities proved by the Knuth-Bendix procedure:

$(x*y)*(y*x) = x$ is $QG3$

$(y*x)*(x*y) = x$ is $QG4$
$(x*(y*x))*y = x$ is conjugate-equivalent to $QG4$
$y*((x*y)*x) = x$ is conjugate-equivalent to $QG4$

$((y*x)*y)*y = x$ is $QG5$
$(y*(x*y))*y = x$ is logically equivalent to $QG5$
$y*((x*y)*y) = x$ is logically equivalent to $QG5$
$(y*(y*x))*y = x$ is conjugate-equivalent to $QG5$
$y*((y*x)*y) = x$ is conjugate-equivalent to $QG5$
$y*(y*(x*y)) = x$ is conjugate-equivalent to $QG5$
$y*(x*(x*y)) = x$ is conjugate-equivalent to $QG5$
$((y*x)*x)*y = x$ is conjugate-equivalent to $QG5$

$((x*y)*x)*y = x$ is conjugate-equivalent to $QG7$
$y*(x*(y*x)) = x$ is conjugate-equivalent to $QG7$

$(x*(x*y))*y = x$ is conjugate-equivalent to $QG8$
$y*((y*x)*x) = x$ is conjugate-equivalent to $QG8$

$((x*y)*y)*y = x$ is $QG9$
$y*(y*(y*x)) = x$ is conjugate-equivalent to $QG9$

We believe that none of this is significant since $QG3$–$QG9$ have been extensively studied. The possibility that $QG3$–$QG9$ are equivalent or conjugate-equivalent to additional type $(4,1)$ identities cannot be ruled out by our results so far, since the search spaces were not always fully explored (and may be infinite). We were disappointed at not finding a type $(4,1)$ identity for $QG6$, the only exception.

So far, we have just studied short conjugate-orthogonal identities. The following theorem describes an infinite set of identities that guarantee orthogonality of at least one pair of conjugates.

Theorem 3 ([3]) *Let $*_{ijk}$ and $*_{abc}$ be conjugate operations on S. Then $*_{ijk}$ is orthogonal to $*_{abc}$ if and only if there is a quasigroup word $w(u,v)$ such that $w((x *_{ijk} y),(x *_{abc} y)) = x$ holds identically.*

Short conjugate-orthogonal identities are those for which $w(u,v) = uv$ (i.e., $u * v$). The next ones to try might be $u(uv)$, $u(vu)$, etc.

Just as we were able to verify properties of short conjugate-orthogonal identities, and even discover minor new properties, automated term rewriting techniques should be valuable for discovering properties of large numbers of identities not previously examined.

6 Conclusion

We have demonstrated the applicability of automated term rewriting techniques to reasoning about quasigroup identities. We verified the theorem that reduced all short conjugate-orthogonal identities to a list of seven conjugate-equivalent identities. We explored in more detail than ever before which pairs of conjugates are orthogonal for each of these identities. This process verified a recently discovered relationship (that $QG2$ is a conjugate-implicant of $QG4$) and discovered a new one (that $QG1$ is a conjugate-implicant of $QG7$). We can often prove logical or conjugate-equivalence among identities allowing us to search for equivalent identities of a desired form. We are encouraged to believe that automated term rewriting techniques will allow us to usefully explore classes of identities not previously considered.

References

[1] Bennett, F.: The spectra of a variety of quasigroups and related combinatorial designs. *Discrete Math.* **34** (1987): 43-64.

[2] Bennett, F., Zhu, L.: Conjugate-orthogonal Latin squares and related structures, J. Dinitz & D. Stinson (eds), *Contemporary Design Theory: A Collection of Surveys.* John Wiley & Sons, 1992.

[3] Evans, T.: Algebraic structures associated with Latin squares and orthogonal arrays. *Proc. of Conf. on Algebraic Aspects of Combinatorics. Congr. Numer.* **13** (1975): 31-52.

[4] Fujita, M., Slaney, J., Bennett, F.: Automatic generation of some results in finite algebra, *Proc. International Joint Conference on Artificial Intelligence*, 1993.

[5] McCune, W.: A Davis-Putnam program and its application to finite first-order model search: quasigroup existence problems. Preprint, Division of MCS, Argonne National Laboratory, 1994.

[6] Slaney, J., Fujita, M., Stickel, M.: Automated reasoning and exhaustive search: Quasigroup existence problems. To appear in *Computers and Mathematics with Applications*, 1994.

[7] Zhang, H.: Herky: High-performance rewriting techniques in RRL. In Kapur, D.: (ed.): Proc. of 1992 International Conference of Automated Deduction. Saratoga, NY. Lecture Notes in Artificial Intelligence, 607, Springer-Verlag. pp. 696–700.

[8] Zhang, H., Hsiang, J.: Solving open quasigroup problems by propositional reasoning. To appear in *Proc. of International Computer Symposium*, Taiwan, December 1994.

[9] Zhang, H., Bonacina, M. P.: Cumulating search in a distributed computing environment: a case study in parallel satisfiability. Proc. of the First International Symposium on Parallel Symbolic Computation. Sept. 26–28, 1994, Linz, Austria.

[10] Zhang, H., Stickel, M.: Implementing the Davis-Putnam algorithm by tries. Technical Report, Dept. of Computer Science, The University of Iowa, 1994.

[11] Zhang, H., Stickel, M.: Problem set: studying quasigroup identities by rewriting techniques. Submitted to *Sixth International Conference on Rewriting Techniques and Applications,* Kaiserslautern, Germany, April 1995.

[12] Zhang, J.: Search for idempotent models of quasigroup identities, Typescript, Institute of Software, Academia Sinica, Beijing, 1991.