Automated Equational Deduction with Otter

William McCune
Argonne National Laboratory

R. Padmanabhan
University of Manitoba

DRAFT August 8, 1995

Contents

1 Introduction **1**
- 1.1 Algebras and Equational Logic . . . 2
  - 1.1.1 Outside of Equational Logic . . . 3
  - 1.1.2 Birkhoff's Subdirect Decomposition Theorem . . . 4
- 1.2 First-order and Higher-order Proofs . . . 4
- 1.3 The Use of OTTER and MACE . . . 5
- 1.4 Organization of the Monograph . . . 6

2 OTTER and MACE **7**
- 2.1 Definitions . . . 7
- 2.2 Otter . . . 9
  - 2.2.1 The Main Loop . . . 10
  - 2.2.2 General Strategies . . . 10
  - 2.2.3 Equational Theorems . . . 14
  - 2.2.4 Equational Theorems with the Rule $=\!(gL)\!\Rightarrow$ . . . 15
  - 2.2.5 Theorems with Deduction Rules . . . 17
  - 2.2.6 Example Input Files and Proofs . . . 18
  - 2.2.7 Trustworthiness of OTTER . . . 22
- 2.3 MACE . . . 23
  - 2.3.1 Trustworthiness of MACE . . . 25

3 Uniqueness of Algebraic Laws **27**
- 3.1 Background . . . 27
  - 3.1.1 The Rigidity Lemma and the Rule $=\!(gL)\!\Rightarrow$ . . . 27
  - 3.1.2 Equations and Cubic Curves . . . 27
- 3.2 The Median Law . . . 30
- 3.3 Group-like Laws . . . 33
- 3.4 Uniqueness of n-ary Steiner Laws . . . 38
- 3.5 Group Laws on a Quartic Curve . . . 44

4 $=\!(gL)\!\Rightarrow$ in Other Algebras **47**
- 4.1 Equations Consistent with $=\!(gL)\!\Rightarrow$ . . . 47
  - 4.1.1 Abelian Groups . . . 47
  - 4.1.2 Quasigroups . . . 52

4.1.3 Boolean Groups 55
4.2 Equations Strictly Inconsistent with $=\!(gL)\!\Rightarrow$ 56
4.3 Quasigroups and Overlay Conditions 58
4.4 Closure Conditions and $=\!(gL)\!\Rightarrow$ 60
4.5 Cancellative Semigroups and $=\!(gL)\!\Rightarrow$ 70
4.6 A Discovery Rule 73

5 Semigroups 75
5.1 A Conjecture in Cancellative Semigroups 75
5.2 Theorems Supporting the Conjecture 76
5.3 Meta-Abelian CS and the Quotient Condition 81

6 Independent Self-Dual Bases for Group Theory 85
6.1 Tarski's Interpolation Theorem 85
6.2 Self-Dual Equational Bases for Group Theory 85
6.3 Self-Dual Schemas for Subvarieties of Group Theory 92
6.4 Other Results in Self-Dual Equational Bases 95

7 Lattice-like Algebras 97
7.1 Equational Theory of Lattices 97
7.2 Presence of Jónsson Polynomials 103
7.2.1 A Reduction Schema 103
7.3 A Short Single Identity for Lattices 105
7.4 Weakly Associative Lattices 106
7.4.1 Uniqueness of $\wedge$ in WAL 108
7.4.2 A Single Axiom for WAL 110
7.5 Quasilattices 112
7.6 Near Lattices (NL) and Transitive Near Lattices (TNL) 125
7.7 Boolean Algebras 127
7.7.1 Frink's Theorem 127
7.7.2 Padmanabhan's Self-Dual Basis 128
7.7.3 Algebras of Set Difference 130
7.7.4 Robbins Algebra 133
7.7.5 Ternary Boolean Algebra 136

8 Miscellaneous Topics 139
8.1 Inverse Loops and Moufang Loops 139
8.1.1 Bases for Moufang Loops 140
8.1.2 Single Axioms for Inverse Loops and Moufang Loops . . . 148
8.2 Quasigroups 154
8.3 Other Algebras 159

A Open Questions **161**
A.1 Uniqueness of Algebraic Laws 161
A.2 $=\!(gL)\!\Rightarrow$ in Other Algebras 161
A.3 Semigroups 162
A.4 Independent Self-Dual Bases 162
A.5 Lattice-like Algebras 162
A.6 Miscellaneous Topics 162

B Theorems Proved **165**

Bibliography **166**

Index **169**

Preface

This monograph is intended to demonstrate that automated deduction is starting to become a practical tool for working mathematicians. It contains a set of problems and theorems that arose in correspondence between the authors starting early in 1993. One of us (RP), a mathematician working in universal algebra and geometry, contacted the other (WM), a computer scientist working in automated deduction, after reading a survey article by Larry Wos on applications of automated reasoning. [[continue this thread.]]

[[What else to add?]]

OTTER (version 3.0.4) and MACE (version 1.0.2) are the two computer programs that made this work possible. Both programs are in the public domain and are available by anonymous FTP and through the World Wide Web (WWW). See one of

ftp://info.mcs.anl.gov/pub/Otter/README
http://www.mcs.anl.gov/home/mccune/ar

for information on obtaining the programs. The primary documentation for the programs are [19] and [17, 18]; these are included with the programs when obtained by FTP.

We also have the following WWW document associated with this work.

http://www.mcs.anl.gov/home/mccune/ar/monograph

All of the OTTER and MACE input files and proofs are available through that page.

Special thanks go to Larry Wos and to Ross Overbeek. Larry introduced the notions of strategy and simplification to automated deduction and invented the inference rule paramodulation for equality; all three of those concepts are at the center of this work. Ross is due a lot of the credit for OTTER's basic design and high performance, because in building OTTER, McCune borrowed so heavily from Ross's eariler theorem provers and ideas.

[[Who else to thank??]]

McCune was supported by the Office of Scientific Computing, U.S. Department of Energy, under Contract W-31-109-Eng-38, and Padmanabhan was supported by the University of Manitoba and by an operating grant from NSERC of Canada (#A8215).

October ??, 1995

W. McCune
mccune@mcs.anl.gov

R. Padmanabhan
padman@cc.umanitoba.ca

Chapter 1

Introduction

This monograph contains a collection of theorems and problems in equational logic and in logics close to equational logic. Some are easy, some are difficult, and some are still open. We have attacked nearly all of the problems with the automated deduction system OTTER, and many of the resulting proofs are presented in the following chapters. Many previously open problems were solved by OTTER, and many more new problems arose and were solved by OTTER during the course of this work.

About half of the theorems and problems are in several areas of universal algebra, including lattice theory, Boolean algebra, groups, quasigroups, loops, and semigroups; these are about axiomatizations of algebras, relationships between various algebras, investigations of new algebras, finding proofs simpler than those previously known, finding new equational descriptions satisfying certain pre-assigned syntactic properties, and finding first-order proofs where previous proofs had been model theoretic or higher order. The other half of the problems are related to algebraic geometry; these use an equational inference rule, implemented for the first time in OTTER, that captures a generalization principle of cubic curves in the complex projective plane.

In this work, the program OTTER was used to *find* proofs rather than to check proofs supplied by the user or to complete proofs outlined by the user. OTTER is programmable in the sense that the user can specify inference rules and supply parameters to restrict and direct the search for proofs, and we freely used these features. But we did not use any knowledge about proofs when giving problems to OTTER; in nearly all cases the user did not know a proof of the theorem in question. Nor did we use much knowledge about the algebras under study; in most cases, the user had little or none. We also made some use of a complementary program called MACE, which searches for small finite models and counterexamples. Although not particularly powerful, MACE made several important contributions to this work.[1]

[1] We apologize if the reader is offended by our anthropomorphism about OTTER and MACE, but we view them as assistants. In fact, we considered making OTTER a coauthor.

1.1 Algebras and Equational Logic

[[RP: you are welcome to rewrite some of this material.]]

The material in this section follows Tarski's 1968 paper on equational logic [39]. An *algebra* is a system $< A, O_1, \ldots, O_n >$ consisting of a nonempty set A and a finite sequence of finitary operations from A to A. The sequence of arities of $O_1, \ldots, O_n$ is the *type* of the algebra. For example, a group might be $< G, \cdot, ', e >$ with type $< 2, 1, 0 >$. If the type of an algebra or class of algebras is clear from the context, e.g., if it is specified by a set of equations, we may omit mention of the type. To specify classes of algebras and to prove theorems about them, we can use equational logic.

Equational logic. A logic is typically specified by a language of formulas and rules of inference over formulas. The language of an equational logic consists of a set of function symbols of fixed arity (including constants) and an unlimited supply of variables. (OTTER distinguishes variables from constants with the following rule: it is a variable iff it starts with a member of $\{u, v, w, x, y, z\}$; we use the same convention here.) Formulas are simply equations, in which all variables are interpreted as being universally quantified. From another view, equational logic is that part of predicate logic with equality in which equations are the only formulas. In the terminology of automated theorem proving (Sec. 2.1), an equation is a unit equality clause.

The *equational theory* of a class of algebras is the set of equations that are satisfied in all algebras of the class. A *variety* is a class of algebras that consists of all models of some set of equations. A *basis* for a theory is a set of formulas from which all formulas of the theory can be derived by the rules of inference. A basis is *independent* if none of its members can be derived from the remaining equations. An n-basis is a basis with n elements.

There has been great interest in simple bases and bases with particular properties (see Tarski's paper [39] for an excellent survey), and many of our theorems are in those areas. For example, we study (1) one-based theories, including the existence of simple single axioms, (2) self-dual independent bases, with several different notions of the dual of an equation, (3) cardinalities of independent bases, including self-dual bases, and (4) bases in terms of nonstandard operations.

A standard set of inference rules for equational logic is Birkhoff's, listed in Table 1.1. Birkhoff's rules are sound and deduction-complete [2]; that is, an

Table 1.1: Birkhoff's Inference Rules for Equational Logic

$\dfrac{}{t = t}$	Reflexivity
$\dfrac{t_1 = t_2}{t_2 = t_1}$	Symmetry
$\dfrac{t_1 = t_2,\ t_2 = t_3}{t_1 = t_3}$	Transitivity
$\dfrac{f(x) = g(x)}{f(t) = g(t)}$	Substitution
$\dfrac{t_1 = t_2}{f[t_1] = f[t_2]}$	Replacement

equation E is a model-theoretic consequence of a set Σ of equations if and only if E can be derived from Σ br Birkhoff's rules.

Although of theoretical interest, Birkhoff's rules have not been useful in searching automatically for proofs of theorems in equational logic, because no one has found effective ways of controlling the use of the substitution and replacement rules. Instead, we use *paramodulation*[36], a rule that combines substitution with a different kind of replacement, in particular, replacing a term with an equal term. See Table 1.1, where σ is a most general substitution

Table 1.2: Paramodulation for Equational Logic

$\dfrac{}{x = x}$	Reflexivity
$\dfrac{t_1 = t_2,\ P[s]\ (\text{with } t_1\sigma \equiv s\sigma)}{(P[t_2])\sigma}$	Paramodulation

of terms for variables such that $t_1\sigma$ is identical to $s\sigma$, and $P[s]$ is an equation or negated equation containing a term s. (Paramodulation is ordinarily defined for first-order predicate logic with equality. See Sec. 2.1 for clarification.) Paramodulation is not deduction-complete, because there is no substitution rule; for example, $f(t,t) = t$ cannot be derived from $f(x,x) = x$. It is, however, *refutation*-complete; that is, if $\Sigma \models \{t_1 = t_2\}$, then $\Sigma \cup \{t_1' \neq t_2'\} \vdash \{t \neq t\}$ for some term t, where $t_1' \neq t_2'$ is the *denial* of $t_1 = t_2$, obtained by replacing all variables with new (Skolem) constants.

1.1.1 Outside of Equational Logic

We deviate from equational logic in several ways; all but the last listed here are still within first-order predicate logic with equality First, we occasionally

include deduction rules, for example left cancellation, $x \cdot y = x \cdot z \rightarrow y = z$, as axioms. In some cases, for example the theory of cancellative semigroups, it is necessary, because there is no equational axiomatization. In other cases it leads to more effective searches for proofs; for example, quasigroups can be defined equationally, but because cancellation holds for quasigoups, we may include it as a deduction rule. Second, we prove some theorems involving existential quantification. For example, to prove that an operation is a quasigroup, we prefer to show left and right cancellation and the existence of left and right solutions, rather than the (more awkward) equational axioms for quasigroups (see Thms. #MFL-4, #MFL-5, and #MFL-6, p. 143). Third, we occasionally make simple transformations to a representation in predicate logic. For example, for Thm. #CS-4, (p. 78), to prove $t_1 = t_2$, we assert $P(t_1')$, deny $P(t_2')$, then derive a contradiction. The purpose of the transformation in this case is to achieve a particular highly constrained bidirectional search strategy.

Finally, many of the theorems in this work involve Padmanabhan's inference rule $=(gL)\Rightarrow$, which is based on a property of cubic curves in the complex projective plane. We refer to $=(gL)\Rightarrow$ as an first-order equational rule, because it derives equations from equations; however, it is outside of ordinary equational logic, because it cannot be axiomatized with equations. The beauty of the rule is that it can be used to construct elegant proofs of some interesting and useful theorems that ordinarily require higher-order notions from algebraic geometry. See Sec. 2.2.4 for details of OTTER's implementation of $=(gL)\Rightarrow$, and see Sec. ?? for the mathematical discussion of the rule.

1.1.2 Birkhoff's Subdirect Decomposition Theorem

[[RP: please write this section.]]

1.2 First-order and Higher-order Proofs

By the completeness of equational logic, if an equational statement is a theorem, there must exist an equational proof of it. However, equational theorems are frequently proved with model theoretic or set theoretic arguments; for example, [[RP: need some examples.]].

Proofs involving such higher-order notions frequently give no insight into equational proofs, and one of our goals in this work is to find equational proofs of theorems whose previously known proofs have been higher order. Why? (1) We are better at automating searches in lower logics. When faced with an open equational problem about which we have little insight, our only practical choice is an automated first-order search. Experience with known theorems will give us insight into open problems. (2) It is currently much more difficult to rigorously formalize higher-order notions. As formal verification becomes more important throughout mathematics, science, and engineering, lower level proofs may be regarded as more trustworthy because the inference rules are simpler. (3) We simply like to work without using unnecessary machinery.

We give here an example of a theorem whose previously known proofs are higher-order. First we list a proof found by OTTER (after several failed attempts with various search strategies); then, we give the mathematical background of the theorem and a higher-order proof.

Theorem #MED-1. The type is (2,0) with nullary e.

$$\left\{ \begin{array}{l} \cdot \text{ is cancellataive} \\ (xy)(zu) = (xz)(yu) \\ ee = e \end{array} \right\} \Rightarrow \{(x(yz))((uv)w) = (x(uz))((yv)w)\}.$$

Proof (found by Otter 3.0.3l on gyro at 141.38 seconds).

1	$x = x$	
2	$x \cdot y = z,\ x \cdot u = z \ \rightarrow\ y = u$	
3	$x \cdot y = z,\ u \cdot y = z \ \rightarrow\ x = u$	
4	$(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u)$	
5	$e \cdot e = e$	
7	$(A \cdot (D \cdot C)) \cdot ((B \cdot E) \cdot F) = (A \cdot (B \cdot C)) \cdot ((D \cdot E) \cdot F) \ \rightarrow\ \square$	
8	$((x \cdot y) \cdot (z \cdot u)) \cdot (v \cdot w) = ((x \cdot z) \cdot v) \cdot ((y \cdot u) \cdot w)$	[4 → 4]
9	$(x \cdot y) \cdot ((z \cdot u) \cdot (v \cdot w)) = (x \cdot (z \cdot v)) \cdot (y \cdot (u \cdot w))$	[4 → 4]
10	$((x \cdot y) \cdot z) \cdot ((u \cdot v) \cdot w) = ((x \cdot u) \cdot (y \cdot v)) \cdot (z \cdot w)$	[flip 8]
13,12	$(x \cdot e) \cdot (y \cdot e) = (x \cdot y) \cdot e$	[5 → 4, flip]
15,14	$(e \cdot x) \cdot (e \cdot y) = e \cdot (x \cdot y)$	[5 → 4, flip]
16	$(e \cdot x) \cdot e = e \cdot (x \cdot e)$	[5 → 12, flip]
27	$((e \cdot x) \cdot y) \cdot (e \cdot z) = (e \cdot (x \cdot e)) \cdot (y \cdot z)$	[16 → 4, flip]
30	$(x \cdot (e \cdot y)) \cdot (z \cdot (e \cdot u)) = (x \cdot z) \cdot (e \cdot (y \cdot u))$	[14 → 4, flip]
33,32	$((e \cdot x) \cdot y) \cdot ((e \cdot z) \cdot u) = (e \cdot (x \cdot z)) \cdot (y \cdot u)$	[14 → 4, flip]
74	$((x \cdot y) \cdot (z \cdot u)) \cdot e = ((x \cdot z) \cdot (y \cdot u)) \cdot e$	[5 → 8 :13]
81	$(e \cdot (x \cdot e)) \cdot ((e \cdot y) \cdot z) = e \cdot ((x \cdot y) \cdot z)$	[14 → 27 :15, flip]
147	$(x \cdot ((y \cdot z) \cdot (u \cdot v))) \cdot e = (x \cdot ((y \cdot u) \cdot (z \cdot v))) \cdot e$	[74 → 12 :13]
193	$(e \cdot (x \cdot y)) \cdot ((z \cdot u) \cdot v) = (e \cdot (z \cdot y)) \cdot ((x \cdot u) \cdot v)$	[14 → 10 :33]
238,237	$(x \cdot (y \cdot e)) \cdot ((e \cdot z) \cdot (u \cdot v)) = (x \cdot (y \cdot u)) \cdot (e \cdot (z \cdot v))$	[9 → 30]
306	$x \cdot ((y \cdot z) \cdot (u \cdot v)) = x \cdot ((y \cdot u) \cdot (z \cdot v))$	[3,1,147]
369	$e \cdot ((x \cdot (y \cdot z)) \cdot ((u \cdot v) \cdot w)) = e \cdot ((x \cdot (y \cdot v)) \cdot ((u \cdot z) \cdot w))$	[193 → 81 :238,15]
485	$(x \cdot (y \cdot z)) \cdot ((u \cdot v) \cdot w) = (x \cdot (u \cdot z)) \cdot ((y \cdot v) \cdot w)$	[2,306,369]
486	$\square$	[485,7]

[[Note to RP: give background and higher-order proof.]]

1.3 The Use of OTTER and MACE

[[Mention other successes (Kunen, Wos, Veroff, Quaife).]]

[[non-interactive, but used interactively.]]

[[Cover how we search for single axioms.]]

1.4 Organization of the Monograph

[[RP: what do you think about marking theorems that are new or where we give the first first-order proof? something like the following.]]

•**Theorem A.** This is a new result.

°**Theorem B.** This is the first known first-order proof.

Chapter 2

OTTER and MACE

OTTER [19] is a program that searches for proofs, and MACE [17, 18] is a program that searches for small finite counterexamples. Both apply to statements in first-order logic with equality. OTTER is more powerful and flexible at its task than MACE is at its task (consequently, OTTER is more difficult to use). When searching for a proof with OTTER the user typically formulates a search strategy and makes several attempts, modifying the strategy along the way. When searching for a counterexample with MACE, the user simply supplies a statement of the conjecture; if the conjecture is not too complex, and if there exist small finite models, then MACE will find them. For many of our conjectures (quasigroup problems in particular), we know that counterexamples, if they exist, must be infinite; MACE is useless in such cases. But the two programs nicely complement one another in many other cases.

The following descriptions of the two programs are informal. See the manuals and [42] for more formal and detailed presentations. First, we define some terms of automated theorem proving.

2.1 Definitions

These definitions are biased toward OTTER and equational theorem proving.

A *term* is either a variable, a constant, or the application of an n-ary function symbol to n terms.

An *atom* is the application of an n-ary predicate symbol to n terms. Nearly all atoms in this work will be equalities.

A *literal* is either an atom or the negation of an atom.

A *clause* is a disjunction of literals. The variables in a clause are implicitly universally quantified.

A *unit clause* contains exactly one literal. Most of the clauses in this work are unit equality clauses, that is, equations.

The *empty clause* contains no literals and represents a contradiction.

A *Horn clause* has at most one positive literal. All of the clauses associated with this work are Horn clauses.

Two terms or atoms *unify* if there is a substitution of terms for variables that makes the terms or atoms identical. When we speak of a *unifying substitution*, we refer to the most general unifying substitution.

An *equational deduction rule* is a non-unit Horn clause containing some number, say n, of negative equalities (the antecedents) and one positive equality (the consequent). It is frequently written as an implication,

$$s_1 = t_1 \ \& \ \cdots \ \& \ s_n = t_n \ \rightarrow \ s = t,$$

and is typically used by OTTER with the inference rule hyperresolution.

The inference rule *hyperresolution* (for equational deduction rules) takes an equational deduction rule with n antecedents and n equality unit clauses, and derives, if possible, the appropriate instance of the consequent.

Paramodulation (for unit equality clauses) is an inference rule that combines variable instantiation (by unification) and equality substitution into one step. Consider $t = s$ and let $P[t']$ be a positive or negative equality containing a term t'. If t and t' unify, with unifying substitution σ, then paramodulation *from* $t = s$ *into* $P[t']$ yields the paramodulant $\sigma(P[s])$. For example, from $uu' = e$ into $x(x'y) = y$, we can derive $xe = x''$ by unifying uu' and $x'y$.

Unit conflict is a trivial inference rule the derives the empty clause (a contradiction) from two unifying unit clauses of opposite sign. All OTTER proofs are by contradiction.

A *demodulator* is a positive equality unit, $t_1 = t_2$, that is used as a rewrite rule to rewrite instances of t_1 to the corresponding instances of t_2.

Demodulation is the process of repeatedly rewriting a clause with a set of demodulators until no more rewriting steps can be applied. A desirable property of a set of demodulators is that demodulation with the set terminates on all terms to which it is applied.

Forward demodulation is demodulation applied to newly inferred clauses. OTTER always performs forward demodulation when demodulators are present.

Back demodulation occurs when a newly inferred equality is added to the set of demodulators. All clauses that can be rewritten with the new demodulator are demodulated with the (extended) set of demodulators. Back demodulation is optional in OTTER.

Skolemization is a process of eliminating existentially quantified variables from a formula by replacing them with *Skolem constants* and *Skolem functions*. The resulting formula is equiconsistent with the original formula. In this work, Skolemization is used mainly to assert the denials of conclusions. For example, when proving commutativity, the conclusion is $\forall x \forall y(xy = yx)$, its negation is $\exists x \exists y(xy \neq yx)$, and the Skolemized negation is $AB \neq BA$, where A and B are new symbols, that is, Skolem constants. In other words, to deny the conclusion, we simply assert that there are two elements, A and B, that do not commute.

Knuth-Bendix completion is a method for attempting to transform a set of equalities into a *complete set of reductions*, that is, a set of rewrite rules that

produces canonical forms. Although we are not concerned in this work with complete sets of reductions, the mechanics of some of our search strategies are similar to Knuth-Bendix completion. See Sec. 2.2.3.

2.2 Otter

OTTER is a resolution/paramodulation theorem-proving program that applies to statements in first-order logic with equality. OTTER operates on clauses, so if the statements supplied by the user are not clauses, OTTER immediately translates them with Skolemization (to eliminate existential quantifiers) and conjunctive normal form (CNF) conversion. This work focuses mainly on equational logic, and equations are clauses already, so CNF conversion is not necessary. We search for proofs by contradiction, and Skolemization is used here mainly to deny the conclusion of the conjecture.

OTTER is not interactive; the user prepares an input file which contains a denial of the conjecture and a specification of a search strategy, then runs OTTER and receives an output file. (OTTER has a primitive interactive mode, but it was not used for this work.) If the output file does not contain a proof, the user examines the output, modifies the input, and tries again for a proof. Most trivial theorems are proved within the first few attempts, and most difficult theorems require some iteration, resulting in the development of a specialized search strategy. For this work, we did not use OTTER as a proof checker; that is, the strategies were not designed to lead OTTER directly to particular proofs. Rather, the strategies were designed to guide the program toward a particular *type* of proof or to avoid search paths that seem to be worthless.

Because of the iterative way in which OTTER is typically used, we do not think of it as an "automatic" theorem prover. However, OTTER does have a mode, the *autonomous mode*, that allows the user to supply simply a denial of the conjecture; the program does a simple syntactic analysis of the conjecture, decides on a simple strategy, and searches for a proof. Although not used in this work, the autonomous mode can be used by OTTER to prove many of the easy theorems we present.

The real, practical strength of OTTER is the ability to quickly explore large search spaces. Strategies are used mainly to restrict the search rather than to carefully guide it, resulting in a search less focused than with some of the other automated theorem provers, which use heuristics to carefully plan and control the search for a proof.

The theorems we present fall into two main classes: ordinary equational theorems, and equational theorems with the rule $=(gL)\Rightarrow$. In some cases we also add deduction rules such as cancellation or various closure conditions (Sec. 4.4). The strategies we use for ordinary equational theorems (both with and without deduction rules) are simpler, more uniform, and better understood than our strategies for $=(gL)\Rightarrow$; before going into detail about particular strategies in Sections 2.2.3 and 2.2.4, we present some general features of OTTER.

2.2.1 The Main Loop

OTTER maintains three primary lists of clauses.

`usable`. These clauses are able to participate in the search through application of inference rules.

`sos` (set of support). These clauses are waiting to participate in the search through application of inference rules. A subset (possibly empty) of `sos` occurs also in list `demodulators`; members of that subset can participate in the search through rewriting (demodulation).

`demodulators`. All of these clauses are unit equalities. They are applied as rewrite rules to all inferred clauses.

In the input file, the user typically partitions the statement of the conjecture into `usable` and `sos`; if any equalities are present, they may be inserted into `demodulators` also. OTTER's highest-level operation is a simple loop:

Repeat

1. Select a clause, the *given clause*, from `sos`.
2. Move the given clause from `sos` to `usable`.
3. Draw inferences from the given clause using other clauses in `usable`. With each inferred clause, rewrite it with `demodulators` and decide if it should be retained; if retained, append it so `sos`, and if it should be a rewrite rule, append it to `demodulators`.

Until a proof is found or a resource is exhausted.

The five main determinants of the search are (1) the initial partition into `usable` and `sos`, (2) the method for selecting the given clause, (3) the inference rules that are applied, (4) the rules for retention of inferred clauses, and (5) the rules for deciding whether inferred equalities are to be rewrite rules. These are considered to be part of the search strategy and are covered in some detail in the following subsection.

2.2.2 General Strategies

As mentioned above, use of OTTER frequently involves iteration through a sequence of searches, and part of the iteration is toward achieving a *well-behaved* search. The notion of a well-behaved search is not precise, and recognizing one is largely a matter of experience in finding proofs with OTTER. However, we can list here some ways in which searches can be ill behaved. One determines the behavior of a search by examining the output file.

- The `sos` list grows to rapidly. This wastes time and memory, because most `sos` clauses will never participate in the search.
- The program focuses on many trivial variants of clauses, because they are smaller than other, useful clauses.

- The program is not using, or not using to the desired extent, some of the inference rules that are enabled.
- A bidirectional search is desired, but the given clauses that are selected force the search to be in one direction only.
- The program is wasting time making checks or performing other operations that have little or no effect on the search.

To adjust the behavior of a search, one changes the specification of one or more strategies. The rest of this subsection contains summaries of OTTER's most important general strategies.

Set of Support

One of the earliest strategies for automated theorem proving is the set of support strategy [43], which is designed to prevent lines of reasoning. The set of support requires that the input clauses be partitioned into two sets, S (clauses with support) and T (those without support); the strategy requires that all lines of reasoning start with a member of S. That is, no inference is drawn entirely from clauses in T.

OTTER's main loop can be viewed as a simple implementation of the set of support strategy. The initial `sos` list is S, and the initial `usable` list is T. Because the clauses in the initial `usable` list never occur in the `sos` list, and because each inference is started with the given clause, which is selected from the `sos list`, no inference is made in which all of the participants are in the initial `usable` list. If the user wishes to do without the set of support strategy, then he or she simply places all input clauses in the `sos` list.

The primary motivation for the set of support strategy is to focus the reasoning on the problem at hand instead of on the general theory. Many theorems formulate naturally as axioms of a theory, special hypotheses, and a conclusion. The standard recommendation for partitioning the input into S (supported clauses) and T (non-supported clauses) is to place the axioms of the theory into T and clauses corresponding to the special hypotheses and denial of the conclusion into S. The result is that all lines of reasoning start with the hypotheses and the conclusion.

However, our experience has shown that the set of support strategy is not particularly effective for two classes of theory: (1) equational and nearly-equational theories, and (2) theories with few axioms and few concepts. The theories on which we focus in this work fall into both classes, so for the most part, we do without the set of support strategy.

Selecting the Given Clause

Selection of the given clause has a great effect on the character and outcome of the search; it is the "next path to explore". Since new clauses are appended to the `sos` list, selecting the first `sos` clause leads to breadth-first search (occasionally

useful), and taking the last leads to depth-first search (rarely useful). OTTER's default method, however, is to select the best clause in the `sos` list as the given clause. For example, if a simple identity is derived, it is usually best to use it right away. The default measure of "best" , and the one used for this work, is simply the length of the clause; if the user has other ideas about what is best, he or she can use OTTER's weighting mechanism to specify rules for assigning weights to clauses.

For most of the theorems and conjectures in this work, we use a selection method that is a combination of best-first and breadth-first. One of OTTER's parameters, `pick_given_ratio`, can be used to specify the ratio; a value of n means n parts best-first to 1 part breadth-first; that is, through n iterations of the main loop, the best clause is taken, then in the next iteration, the first is used, and so on. With this method, OTTER focuses mainly on the small clauses, while occasionally allowing a larger, richer clause to participate in the search, to "mix things up".

Demodulation (Rewriting)

The list `demodulators` contains a set of directed equalities that are used as rewrite rules. When a new clause is inferred, one of the first processes applied to it is forward demodulation, in which the clause is rewritten, as much as possible, with the members of `demodulators`. The primary motivation for demodulation is to reduce redundancy by canonicalizing clauses. For example, if the theory has a left identity, $ex = x$, then it is usually wasteful to retain both $(xy)z = x(yz)$ and $(xy)(ez) = x(yz)$; with $ex = x$ as a demodulator, the second will be demodulated to an equality identical to the first and will be deleted.

Equalities can become demodulators in three ways: (1) demodulators can be specified in the input file, (2) input equalities in `sos` or `usable` can be copied into `demodulators`, and (3) derived equalities can be copied into `demodulators`. Alternatives (2) and (3), which apply only if certain flags are set, can also cause the new demodulator to rewrite previously retained clauses, through back demodulation.

Retaining Inferred Clauses

After a newly inferred clause is demodulated and possibly rewritten in other ways, OTTER must decide whether it is to be retained. Forward subsumption is nearly always applied; that is, if the new clause is subsumed by any of OTTER's existing clauses, then it is discarded. Also, the user can assign limits on several measures, including number of variables, number of literals, and the weight of clause. A limit on the weight of retained clauses is nearly always used for difficult theorems.

As when selecting the given clause, the default weight (which we use unless stated otherwise) is the length of new clause. If there is no limit on the weight of retained clauses, or if the limit is too high, then the `sos` list will grow very rapidly; most of the `sos` clauses will simply be wasting space, with little chance of

participating in the search. Also, if back demodulation is enabled, when newly derived equalities are adjoined as demodulators, a lot of time will be wasted attempting to rewrite all of the `sos` clauses. If the limit is too low, then the `sos` list will be exhausted and the search will terminate. The typical strategy, and the one used in this work, is to start with a low limit and make several test runs, adjusting the limit, until a well-behaved search is achieved. (This iterative process explains the apparently arbitrary weight limits specified in many of the input files associated with this work.)

Forward, Backward, and Bidirectional Searches

Most of the theorems and conjectures in this work fit the template

$$E \cup D \Rightarrow C,$$

where E and C are sets of equalities, D is a set of deduction rules, and "$\Rightarrow$" may include an extension to the theory.

In a forward search, one reasons from $E \cup D$, and derives additional equalities, succeeding if all members of C are derived. An easy (but possibly risky) way to have OTTER conduct a forward search is to place the denials of the conclusions C in an auxiliary list called `passive`. Clauses in `passive` do not participate actively in the search, but if an equality that conflicts with a member of `passive`, then a proof will be reported and printed. This method is risky, however, if the members of C are complex enough to be rewritten by a demodulator. For example, suppose e is a constant, the denial of $(ex)x = yy$ is in `passive`, and the equality $ex = x$ is derived and adjoined as a demodulator. If $(ex)x = yy$ is derived later, it will be demodulated to $xx = yy$ before the unit conflict check with passive, and the proof will be missed. Therefore, only non-simplifiable clauses should be placed in `passive`.

In a backward search, one reasons from the denial of C (assume C is a singleton), using members of E and D to derive negated equalities, until a contradiction with a member of E is derived. To have OTTER conduct a backward search one can simply start the search with $E \cup D$ in list `usable` and the denial of C in `sos`. All derived clauses will be negative. (If D is nonempty, then they will have to be used to derive negative clauses with the inference rule UR-resolution [42].) *However, purely backward searches are ineffective for nearly all theories in which equality plays a major role*; deriving and using equalities is simply too important.

In a bidirectional search, one reasons both forward and backward. To achieve a bidirectional search with OTTER, one can place a subset of E in the list `sos`; both positive and negative equalities can be derived. However, it can be difficult to achieve the desired balance between forward and backward search, because OTTER uses a single method for selecting the given clause, and both positive and negative clauses must be selected.

Most of the searches and most of the proofs in this work are either forward or mostly-forward bidirectional. If C was a simple singleton equality, its denial was

usually placed in the list `passive`, resulting in a forward search (proof); otherwise, its denial was placed in list `usable`, resulting in a forward or bidirectional search (proof).

Problem Formulation

Although it is arguable whether problem formulation is a search strategy, from a practical view, it falls in with the other strategies presented in this section.

One usually has choices in the statement of the theorem or conjecture, and OTTER can be sensitive to these choices. We list three examples. First, given an equational theory E, which axiomatization of E should be used? We usually find it best to use an axiomatization that includes simple identities; in some cases we prefer to use single axioms.

Second, should dependent identities be included? Consider group theory in terms of product, inverse, and identity e. Three logically equivalent alternatives are the following.

$$\{ex = x,\ x'x = x,\ (xy)z = x(yz)\}$$
$$\{ex = x,\ xe = e,\ x'x = x,\ xx' = e,\ (xy)z = x(yz)\}$$
$$\{ex = x,\ xe = e,\ x'x = x,\ xx' = e,\ (xy)z = x(yz),\ e' = e,\ x'' = x,\ (xy)' = y'x',\ x(x'y) = y,\ x'(xy) = y\}$$

In addition, should cancellation be included as a deduction rule? We don't have easy answers; it usually depends on the situation and requires some experimentation to achieve a well-behaved search.

Finally, consider the following two forms of the deduction rule for left cancellation:

$$xy = xz \ \rightarrow\ y = z$$
$$xy = u\ \&\ xz = u \ \rightarrow\ y = z$$

The first form, although more natural, is less effective than the second. Both rules apply to the identity $ab = ac$ (assuming the presence of $x = x$ for use with the second rule), but only the second rule applies to the pair $\{ab = d, ac = d\}$.

2.2.3 Equational Theorems

Many of our proof searches in equational theories use strategies that are similar to the Knuth-Bendix completion method [14]. Because the method is well known, we review it here and state how it differs from our OTTER strategies.

Knuth-Bendix completion

Knuth-Bendix completion is a method for attempting to transform a set of equalities E in to an equivalent set of rewrite rules R such that rewriting with R terminates on all terms and produces a canonical form. Rewriting with R is a decision procedure for equality of terms in the theory of E. (Thus, the existence of R is undecidable.) The set R is called a *complete set of reductions*.

The method uses an ordering, say $\succ$, on terms to orient equalities into rewrite rules and to guarantee that rewriting terminates; each member of R satisfies *left-side* $\succ$ *right-side*. The following summarizes the method.

1. All equalities, whether members of E or derived, must be orientable into rules as *left-side* $\succ$ *right-side*; otherwise the method fails.

2. New equalities are inferred by paramodulation from left sides of rules into right sides of rules, then simplified with the current set of rules.

3. When a new (simplified) equality is derived and oriented into a rule, it is used to rewrite all known rules.

4. The method succeeds if no new paramodulants (left into left) can be derived.

If the method fails, then a different term ordering may lead to success.

The OTTER strategy we typically use for equational theorems is quite similar to the Knuth-Bendix method; the main differences are (1) our goal is to prove theorems, (2) instead of failing when a non-orientable equality is derived, we continue, using if for paramodulation, but not for rewriting, (3) we typically impose a limit on the size of retained clauses, and (4) we can paramodulate into negative clauses as well as positive ones, resulting in a bidirectional search.

(Historical remark: The roots of our current equational rules and strategies are in the methods used by Larry Wos and Ross Overbeek in the late 1960's and early 1970's. Those methods were developed independently from the Knuth-Bendix method (at about the same time) and were aimed at proving theorems rather than at finding a complete set of reductions.)

2.2.4 Equational Theorems with the Rule $=(gL)\Rightarrow$

This section contains a description of OTTER's implementation of the derivation rule $=(gL)\Rightarrow$ and some practical information on its use. The rule $=(gL)\Rightarrow$ is presented mathematically in Sec. ??. This section can be skipped during the first reading of this document.

From the operational point of view of OTTER, $=(gL)\Rightarrow$ is implemented in two ways: as an inference rule and as a rewrite rule. Application of $=(gL)\Rightarrow$ requires the equality to have identical terms in two positions. When used as an inference rule, the identical terms occur implicitly through the use of unification (in analogy to the inference rules resolution and paramodulation). Let $F[a_1, x]$ represent a term in that contains a subterm a_1 at a particular position, with x representing everything else in the term. Suppose we have $F[a_1, x] = F[a_2, y]$, (i.e., a_1, and a_2 are in corresponding positions and occur in the same nest of symbols), with a_1 and a_2 unifiable. By $=(gL)\Rightarrow$ we infer $F[z, x'] = F[z, y']$, where z is a new variable, and x' and y' are the appropriate instances of x and y. For example, from

$$f(f(x, y), f(z, f(x, z))) = f(u, f(y, u)),$$

we can derive

$$f(f(x,y),f(z,w)) = f(f(x,z),f(y,w))$$

with $=\!(gL)\!\Rightarrow$ by unifying u and $f(x,z)$ and introducing the new variable w.

When used as a rewrite rule, $=\!(gL)\!\Rightarrow$ is applied automatically to all pairs of identical terms in appropriate positions, in analogy to ordinary rewriting. The equality $F[a,x] = F[a,y]$ is rewritten by $=\!(gL)\!\Rightarrow$ to $F[z,x] = F[z,y]$, where z is a new variable. For example, from

$$f(e,e,e,e) = f(e,e,x,f(e,e,x,e)),$$

we can derive

$$f(y,z,e,e) = f(y,z,x,f(e,e,x,e))$$

by two applications of $=\!(gL)\!\Rightarrow$ as a rewrite rule: to the first occurrences of e on each side, then to the second occurrences of e.

The user has the options of applying $=\!(gL)\!\Rightarrow$ as an inference rule, as a rewrite rule before ordinary rewriting, as a rewrite rule after ordinary rewriting, or any combination of these.

Strategies for use with $=\!(gL)\!\Rightarrow$

OTTER's implementation of $=\!(gL)\!\Rightarrow$ can be difficult to work with, because it does not fit well with our ordinary strategies for equational deduction (activated with the OTTER flag `knuth_bendix`). The main reason is that in many cases, the positions at which $=\!(gL)\!\Rightarrow$ is effectively and usefully applied occur in *simplifiable* terms. With our ordinary strategies, the simplifiable terms are eliminated by demodulation before $=\!(gL)\!\Rightarrow$ can be applied. Consider, for example, the theorem

$$\{ex = xe = x\} \;=\!(gL)\!\Rightarrow\; \{xy = yx\}.$$

and the following proof (found by Otter 3.0.3b on merlin.mcs.anl.gov at 17.07 seconds).

2	$e \cdot x = x$	
3	$x \cdot e = x$	
4	$B \cdot A \neq A \cdot B$	
5	$(e \cdot e) \cdot x = x$	[2 → 2]
7	$(x \cdot e) \cdot e = x$	[3 → 3]
47	$(x \cdot e) \cdot e = (e \cdot e) \cdot x$	[5 → 7]
812	$(x \cdot y) \cdot e = (e \cdot y) \cdot x$	[(gL) 47]
827	$(e \cdot x) \cdot y = y \cdot x$	[3 → 812, flip]
899	$x \cdot y = y \cdot x$	[2 → 827]
900	$\Box$	[899,4]

Note the following points about the preceding proof.

- The notation for the justification of each step is explained in Sec. 2.2.6

- The positions in clause 47 at which $=(gL)\Rightarrow$ applies (to derive clause 812) occur in terms that can be simplified by clauses 2 and 3; in fact, if clauses 2 and 3 become demodulators (as in our ordinary strategies), everything that OTTER derives is demodulated to $x = x$, and the search terminates without finding a proof.

- The proof is quite simple, but OTTER required 17 seconds to find it on a fast computer. (A simple proof like this but without $=(gL)\Rightarrow$ would be found immediately with our ordinary equational strategies.)

- The derivation of clauses 5, 7, and 47 involve paramodulation from a variable, a process that is never allowed with our ordinary equational strategies but is frequently required with $=(gL)\Rightarrow$.

Our basic strategy for use with $=(gL)\Rightarrow$ allows unrestricted paramodulation from both sides of equalities and from and into variables, and it does not use any demodulation. Such a strategy (which produced the preceding proof) usually results in a very redundant search, due mostly to the lack of demodulation, and it takes a long time to find proofs.

In many cases, however, we can use demodulation with our basic $=(gL)\Rightarrow$ strategy. (Such cases usually have a richer set of axioms than the preceding example.) So when faced with a new $=(gL)\Rightarrow$ conjecture, we typically start with full demodulation as in our ordinary equational strategy, then iteratively restrict demodulation (in successive OTTER runs) until a well-behaved search is achieved.

Our search strategies for $=(gL)\Rightarrow$ are still quite primitive; there is a lot of room for research in this area.

2.2.5 Theorems with Deduction Rules

Some of the theories we deal with are specified by axiom sets that contain equational deduction rules (implications) as well as equalities. An example is left cancellation (in its more useful form):

$$xy = u \;\&\; xz = u \;\rightarrow\; y = z.$$

We use the following OTTER flags whenever equational deduction rules are present.

```
set(hyper_res). set(unit_deletion).
set(para_from_units_only). set(para_into_units_only).
set(output_sequent).
```

The flag `hyper_res` enables the inference rule hyperresolution, `unit_deletion` says to delete an antecedent when justified by a derived equation, the paramodulation flags disallow paramodulation from or into nonunit clauses (the deduction rules), and `output_sequent` causes deduction rules to be printed as implications instead of as disjunctions of literals.

Multiple Goals

If the equational theorem or conjecture we are trying to prove, say $E \Rightarrow C$, has multiple goals (i.e., if C is not a singleton), then the denial of C is a nonunit negative clause. For example, if we are trying to prove that E is commutative and associative, the denial would be

$$AB \neq BA \;\mid\; (AB)C \neq A(BC),$$

where A, B, and C are Skolem constants. This can be viewed as the deduction rule

$$AB = BA,\ (AB)C = A(BC) \;\rightarrow\; \Box,$$

where $\Box$ represents falsehood. If commutativity and associativity are derived, then hyperresolution with that deduction rule gives a contradiction. Also, the goals can be rewritten with derived demodulators (and individual goals can be removed from the denial with the *unit deletion* process) before hyperresolution produces a contradiction.

2.2.6 Example Input Files and Proofs

This section contains two examples of OTTER input files and proofs, with some explanation of the input language and the proof format.

Ordinary Equational Logic

Consider the basic theorem that groups satisfying $xx = e$ are commutative. The following annotated input file causes OTTER to find a proof.

```
%%%%%%%%%%%%%%%%%%%%  Basic options

  op(400, xfx, [*,+,^,v,/,\,#]).  % Declare some standard infix operations.
  op(300,yf,@).                   % Postfix operator.

  clear(print_kept).       % Disable printing of retained clauses.
  clear(print_new_demod).  % Disable printing of new demodulators.
  clear(print_back_demod). % Disable printing of back demodulated clauses.

  assign(pick_given_ratio, 4).  % 4 best-first : 1 breadth-first.
  assign(max_mem, 20000).       % Stop if more than 20 megabytes are required.

  %%%%%%%%%%%%%%%%%%%%  Standard for equational problems

  set(knuth_bendix).    % Specify the Knuth-Bendix search strategy.

  %%%%%%%%%%%%%%%%%%%%  Modifications to strategy

  %%%%%%%%%%%%%%%%%%%%  Clauses

  list(usable).              % The usable list.
```

```
x = x.
end_of_list.

list(sos).                  % The sos list.
e * x = x.                  % Left identity.
x@ * x = e.                 % Left inverse.
(x * y) * z = x * (y * z).  % Associativity.
x * x = e.                  % The special hypothesis.
end_of_list.

list(passive).              % The passive list.
A * B != B * A.             % Denial of commutativity.
end_of_list.
```

Note the following points about the input file.

- The first part of the input file, through the "Modifications to strategy" is our standard header for ordinary equational problems. This theorem is easy enough so that no modifications are required. For many theorems, the only addition to the strategy is the parameter `max_weight` (as explained in Sec. 2.2.2).
- OTTER requires the clause "`x = x`" to be present when the inference rule paramodulation is used. (The operational reason is so that a contradiction can be found when $t \neq t$, for some t, is derived. The main reason is historical, due to the original definition of paramodulation.)
- OTTER's rule for distinguishing variables from constants is that variables start with (lower case) `u`–`z`. Our convention for naming Skolem constants is to use `A`, `B`, `C`, ...
- For OTTER, we use "`!=`" instead of "$\neq$".
- The denial of the conclusion is placed in the passive list, because we wish a forward proof; in this case it is safe in the passive list, because no derived clause can simplify it (Sec. 2.2.2).

If we run OTTER with the preceding input file, it quickly finds a proof. We use a simple program to extract the proof from the output file and translate it into the following form.

Proof (found by Otter 3.0.3l on lutra.mcs.anl.gov at 0.25 seconds).

1	$A \cdot B \neq B \cdot A$	
4,3	$e \cdot x = x$	
7	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	
9	$x \cdot x = e$	
11	$x \cdot (x \cdot y) = y$	[9 → 7 :4, flip]
15	$x \cdot (y \cdot (x \cdot y)) = e$	[9 → 7, flip]
18,17	$x \cdot e = x$	[9 → 11]

25	$x \cdot (y \cdot x) = y$	[15 → 11 :18, flip]
29	$x \cdot y = y \cdot x$	[25 → 11]
30	□	[29,1]

The clause numbers in the proof are not sequential, because they reflect the sequence of *retained* clauses. Some clauses are identified with two numbers; the first is cited when the clause is used as a demodulator, and the second when it is used with an inference rule (paramodulation or hyperresolution).

Each derived clause has a justification. The notation "$m \rightarrow n$" indicates paramodulation from m into n; ": $i, j, k, \ldots$" indicates rewriting with the demodulators $i, j, k, \ldots$; and ",flip" indicates that equality was reversed (usually so that the complex sides occurs on the left).

An Example with $=(gL)\Rightarrow$

Consider the theorem that a cancellative semigroup satisfying $=(gL)\Rightarrow$ must be commutative. OTTER finds a proof with the following input file.

```
%%%%%%%%%%%%%%%%%%%%%  Basic options

op(400, xfx, [*,+,^,v,/,\,#]).  % Declare some standard infix operations.
op(300,yf,@).                   % Postfix operator.

clear(print_kept).       % Disable printing of retained clauses.
clear(print_new_demod).  % Disable printing of new demodulators.
clear(print_back_demod). % Disable printing of back demodulated clauses.

assign(pick_given_ratio, 4).    % 4 best-first : 1 breadth-first.
assign(max_mem, 20000).         % Stop if more 16 megabytes are required.

%%%%%%%%%%%%%%%%%%%%%  Standard for (gL) problems

set(geometric_rule).     % Apply =(gL)=> as an inference rule.
set(geometric_rewrite_before).  % Apply =(gL)=> as an rewrite rule
                                % before ordinary demodulation.
set(para_from).          % Paramodulate from the given clause.
set(para_into).          % Paramodulate into the given clause.
set(para_from_vars).     % Allow paramodulation into variables.
set(para_into_vars).     % Allow paramodulation from variables.
set(order_eq).           % Orient equalities.
set(back_demod).         % Apply back demodulation.
set(process_input).      % Process input clauses as if derived.
set(lrpo).               % Orient equalities with LRPO procedure.

%%%%%%%%%%%%%%%%%%%%%  Standard options for hyperresolution

set(output_sequent).        % Output nonunit clauses as implications.
set(hyper_res).             % Apply the inference rule hyperresolution.
```

```
set(order_history).        % Given clause is listed first in just. list.
set(unit_deletion).        % Existing units simplify new nonunits.
set(para_from_units_only). % Disable paramodulation from nonunits.
set(para_into_units_only). % Disable paramodulation into nonunits.

%%%%%%%%%%%%%%%%%%%%  Modifications to strategy

clear(dynamic_demod).      % Disable demodulation.

%%%%%%%%%%%%%%%%%%%%  Clauses

list(usable).
x = x.
x * y != u | x * z != u | y = z.  % left cancellation
y * x != u | z * x != u | y = z.  % right cancellation
end_of_list.

list(sos).
(x * y) * z = x * (y * z).
end_of_list.

list(passive).
B * A != A * B.
end_of_list.
```

The first part of the input file, through "Modifications to strategy" is standard for $=(gL)\Rightarrow$ searches. Demodulation was found to constrain the search too much, so it was disabled. The preceding input file leads to the following proof.

Proof (found by Otter 3.0.3l on peace.mcs.anl.gov at 22.21 seconds).

1	$B \cdot A = A \cdot B \ \rightarrow \ \Box$	
3	$x \cdot y = z,\ x \cdot u = z \ \rightarrow \ y = u$	
4	$x \cdot y = z,\ u \cdot y = z \ \rightarrow \ x = u$	
5	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	
7	$((x \cdot (y \cdot z)) \cdot u) \cdot v = ((x \cdot y) \cdot z) \cdot (u \cdot v)$	$[5 \rightarrow 5]$
11	$(x \cdot (y \cdot z)) \cdot u = (x \cdot y) \cdot (z \cdot u)$	$[5 \rightarrow 5]$
1687	$((x \cdot (y \cdot z)) \cdot u) \cdot v = ((x \cdot y) \cdot u) \cdot (z \cdot v)$	[(gL) 7]
2076	$(x \cdot (y \cdot z)) \cdot u = (x \cdot z) \cdot (y \cdot u)$	$[11 \rightarrow 1687$:(gL)]
2123	$(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u)$	$[7 \rightarrow 1687$:(gL)]
2887	$x \cdot (y \cdot z) = x \cdot (z \cdot y)$	[4,11,2076]
4307	$x \cdot y = y \cdot x$	[3,2123,2887]
4308	$\Box$	[4307,1]

The justification "[(gL)" indicates the use of $=(gL)\Rightarrow$ as an inference rule, and ":(gL)" indicates its use as an rewrite rule. Hyperresolution with a deduction rule is indicated by a sequence of clause identifiers at the beginning of

the justification, for example, clauses 2887 and 4307. Note also the the flag `output_sequent` causes the denial, clause 1, to be written as an implication. (The preceding theorem is Thm. #CS-GL-1 in Sec. 4.5; it is a significant new result that demonstrates the machine-oriented nature of $=(gL)\Rightarrow$ —the proof is short, but it is not intuitive and not one that would likely be found by a mathematician.)

2.2.7 Trustworthiness of OTTER

OTTERis a large and complex program, with many optimizations and experimental features, coded in a low level programming language (C). It certainly has some unknown bugs. Rather that to try to formally verify OTTER, our approach to the problem of soundness is to have another program check OTTER's proofs. This approach is gaining acceptance in the automated deduction community [1, 35], because verification of large low-level programs will not be practical within the next few years (decades?), but, as this work demonstrates, we are already starting to rely on automatically generated proofs.

If OTTER's flag `build_proof_object` is set, and if it finds a proof, then a very detailed *proof object* will be output along with the ordinary proof. The proof object is not meant for human consumption; It's purpose is to be read and checked by an independent program, the *checker*. The proof object has enough detail and its steps are at such a low level that the checker can be a very simple program; for example, it doesn't have to handle term unification or matching, because variable substitutions are explicit and done as separate steps. We list here the proof object corresponding to the 5-step proof above that $x^2 = e$ groups are commutative.

```
(
  (1 (input) ((not (= (* (A) (B)) (* (B) (A))))))
  (2 (input) ((= (* (e) v0) v0)))
  (3 (input) ((= (* (* v0 v1) v2) (* v0 (* v1 v2)))))
  (4 (input) ((= (* v0 v0) (e))))
  (5 (instantiate 4 ((v0 . v65))) ((= (* v65 v65) (e))))
  (6 (instantiate 3 ((v0 . v65)(v1 . v65)(v2 . v66))) ((= (* (* v65 v65) v66) (* v65 (* v65 v66)))))
  (7 (paramod 5 (1 1) 6 (1 1 1)) ((= (* (e) v66) (* v65 (* v65 v66)))))
  (8 (instantiate 2 ((v0 . v66))) ((= (* (e) v66) v66)))
  (9 (paramod 8 (1 1) 7 (1 1)) ((= v66 (* v65 (* v65 v66)))))
  (10 (flip 9 (1)) ((= (* v65 (* v65 v66)) v66)))
  (11 (instantiate 10 ((v65 . v0)(v66 . v1))) ((= (* v0 (* v0 v1)) v1)))
  (12 (instantiate 4 ((v0 . (* v64 v65)))) ((= (* (* v64 v65) (* v64 v65)) (e))))
  (13 (instantiate 3 ((v0 . v64)(v1 . v65)(v2 . (* v64 v65)))) ((= (* (* v64 v65) (* v64 v65)) (* v64 (* v65 (* v64 v
  (14 (paramod 12 (1 1) 13 (1 1)) ((= (e) (* v64 (* v65 (* v64 v65))))))
  (15 (flip 14 (1)) ((= (* v64 (* v65 (* v64 v65))) (e))))
  (16 (instantiate 15 ((v64 . v0)(v65 . v1))) ((= (* v0 (* v1 (* v0 v1))) (e))))
  (17 (instantiate 4 ((v0 . v65))) ((= (* v65 v65) (e))))
  (18 (instantiate 11 ((v0 . v65)(v1 . v65))) ((= (* v65 (* v65 v65)) v65)))
  (19 (paramod 17 (1 1) 18 (1 1 2)) ((= (* v65 (e)) v65)))
  (20 (instantiate 19 ((v65 . v0))) ((= (* v0 (e)) v0)))
  (21 (instantiate 16 ((v0 . v64))) ((= (* v64 (* v1 (* v64 v1))) (e))))
  (22 (instantiate 11 ((v0 . v64)(v1 . (* v1 (* v64 v1))))) ((= (* v64 (* v64 (* v1 (* v64 v1)))) (* v1 (* v64 v1)))
  (23 (paramod 21 (1 1) 22 (1 1 2)) ((= (* v64 (e)) (* v1 (* v64 v1)))))
  (24 (instantiate 20 ((v0 . v64))) ((= (* v64 (e)) v64)))
  (25 (paramod 24 (1 1) 23 (1 1)) ((= v64 (* v1 (* v64 v1)))))
  (26 (flip 25 (1)) ((= (* v1 (* v64 v1)) v64)))
  (27 (instantiate 26 ((v1 . v0)(v64 . v1))) ((= (* v0 (* v1 v0)) v1)))
  (28 (instantiate 27 ((v0 . v64))) ((= (* v64 (* v1 v64)) v1)))
```

```
  (29 (instantiate 11 ((v0 . v64)(v1 . (* v1 v64)))) ((= (* v64 (* v64 (* v1 v64))) (* v1 v64))))
  (30 (paramod 28 (1 1) 29 (1 1 2)) ((= (* v64 v1) (* v1 v64))))
  (31 (instantiate 30 ((v64 . v0))) ((= (* v0 v1) (* v1 v0))))
  (32 (instantiate 31 ((v0 . (A))(v1 . (B)))) ((= (* (A) (B)) (* (B) (A)))))
  (33 (resolve 1 (1) 32 (1)) ())
)
```

A checker for OTTER proof objects has been written in the language of the Boyer-Moore logic [3, 4], and all of the non- $=(gL)\Rightarrow$ OTTER proofs in this work have been checked with it. (The checker cannot yet handle $=(gL)\Rightarrow$ inferences.)

Of course, the correctness of the checker is now in question. The goal of formally verifying the checker (say, with the Boyer-Moore prover) is certainly within reach, but that has not yet been attempted. However, it is just a few pages of of high-level code, and it has been carefully read by an outside expert in the area.

2.3 MACE

The program MACE (Models And Counter-Examples) [17, 18] is used to search for finite models of formulas or sets of clauses. When the input is interpreted as the denial of a conjecture, any models found are counterexamples of the conjecture.

MACE is easy to use. Its input language is the same as OTTER's, and few decisions need to be made when using it; the search algorithm, unlike OTTER's, is not adjustable by the user. To run MACE, the user takes the following steps.

1. Prepare a set of clauses. These are usually the same as the clauses prepared for OTTER. If an equivalent set of simpler clauses is known, that should be used instead. (The key parameter is the length of the longest clause.) If very simple lemmas are known, they should be included as well.

2. Declare properties of operations. The two properties currently accepted by MACE are "quasigroup" for binary operations, and "bijection" for unary operations. These declarations speed the search; the clauses that specify the declared properties can be (should be) omitted.

3. Assign constants. To reduce the generation of isomorphic models, the user can assign constants in the clauses to elements of the domain. (If the domain has size n, its elements are named $0, 1, \cdots, n-1$.)

4. Specify a domain size. Each MACE search is for models of a fixed size. The user typically makes a sequence of searches, starting with a small size, then increasing it, until a model is found or until resources are exhausted. MACE is complete: if the search for a given domain size terminates without models, then there are none of that size.

MACE is quite limited, both in the size of clauses it can handle and in the size of domain it can search. (The space it uses is proportional to n^{c+v}, where n is the domain size, c is the length of the longest clause, and v is the number of

variables in the longest clause.) If the clauses are very simple, MACE may be able to complete searches of sizes 10–12 in a reasonable time; examples of the longest clauses that MACE can handle are the following.

$$x \cdot y = u \cdot v,\ x \cdot w = z \cdot v \ \rightarrow\ u \cdot w = z \cdot y$$
$$x \cdot (((x \cdot y) \cdot z')' \cdot y)' = z$$

With such clauses, MACE can search for models of size at most 4 or 5.

An Example of a MACE Search

The following input file asks MACE to search for a non-commutative group.

```
op(400, xfx, [*,+,^,v,/,\,#]).  % Declare some standard infix operations.
op(300,yf,@).                   % Postfix operator.

set(dp_transform).

list(usable).
e * x = x.                  % left identity
x@ * x = e.                 % left inverse
(x * y) * z = x * (y * z).  % associativity
A * B != B * A.             % denial of commutativity
end_of_list.

list(passive).
assign(e, 0).   % The group identity is element 0.
assign(A, 1).   % The non-commuting elements are 1 and 2.
assign(B, 2).
end_of_list.
```

If we run a sequence of MACE searches specifying sizes $3, 4, \ldots$, the first model found has size six, as expected, because the smallest non-commutative group is order six. The following output is produced.

Model. The clauses have the following model (found by MACE 1.1.0 on peace.mcs.anl.gov at 2.61 seconds).

```
* :
     | 0 1 2 3 4 5
   --+------------
   0 | 0 1 2 3 4 5
   1 | 1 0 3 2 5 4
   2 | 2 4 0 5 1 3
   3 | 3 5 1 4 0 2
   4 | 4 2 5 0 3 1
   5 | 5 3 4 1 2 0

@ :
0 1 2 3 4 5
---------------
0 1 2 4 3 5
```

If we include the (dependent) clauses $\{x * e = x, x * g(x) = e\}$, or if we declare "*" to be a quasigroup and "g" to be a bijection, a model is found in a bit less

time. If we omit the assignments of the constants e, A, and B, a model is found in about a minute.

MACE is a primitive program; in this work, it has made useful discoveries in only a few cases. In some of the cases where we cite its use, a mathematician familiar with the area could have found a model with little work. However, the program is useful to non-mathematicians, and model-searching programs are likely to become more powerful in the near future.

2.3.1 Trustworthiness of MACE

MACE has not been formally verified in any way. Although models found by MACE can be checked without much difficulty (in fact with a special OTTER strategy), we have not yet done so in this work. A more difficult problem arises when the interest is in showing that there are no models of a given size. In this case, the user has to trust MACE; but we have not faced that problem in this work.

Chapter 3

Uniqueness of Algebraic Laws

[[RP: need motivation, definition of gL, difference of gL and rigidity lemma, soundness of otter's implementation, etc. Some references are [30, 28].]]

3.1 Background

3.1.1 The Rigidity Lemma and the Rule $=\!(gL)\!\Rightarrow$

We have the model-theoretic question of whether one can extract some first order properties from the theory of projective curves and formulate and prove the various uniqueness theorems within the framework of first order logic with equality. And the answer, an emphatic *yes*, is in the rigidity lemma, a powerful local-to-global principle valid for morphisms of complete varieties:

> Let X be a projective curve and Y and Z be irreducible algebraic varieties, all defined over an algebraically closed field k. Let f be a regular mapping from $X \times Y$ into Z such that $f(X \times \{y_0\})$ is a singleton z_0 for some $y_0 \in Y$. Then $f(X \times \{y\})$ is a singleton for every $y \in Y$.

Proofs of this basic fact may be found in [37, p. 152], [23, p. 104], or in [38, p. 156].

3.1.2 Equations and Cubic Curves

In Table 3.1 we list some of the correspondence between geometric and algebraic concepts, and Fig. 3.1 shows the chord-tangent operation on a cubic curve.

Table 3.1: Equationally Definable Concepts in Cubic Curves

Geometry	Algebra
points	elements
chords	$\{P,\ Q,\ P \cdot Q\}$
tangents	$\{P,\ P \cdot P\}$
P, Q, R colinnear	$R = P \cdot Q$
P lies on the tangent at Q	$P = Q \cdot Q$
inflection point	idempotent elments
singular point	absorbing element
nonsingular curve	cancellation law
conic	$\{P, Q, R, S, T, f(P, Q, R, S, T)\}$
sextatic point P	$P = f(P, P, P, P, P)$
configuration theorem	identity or implication

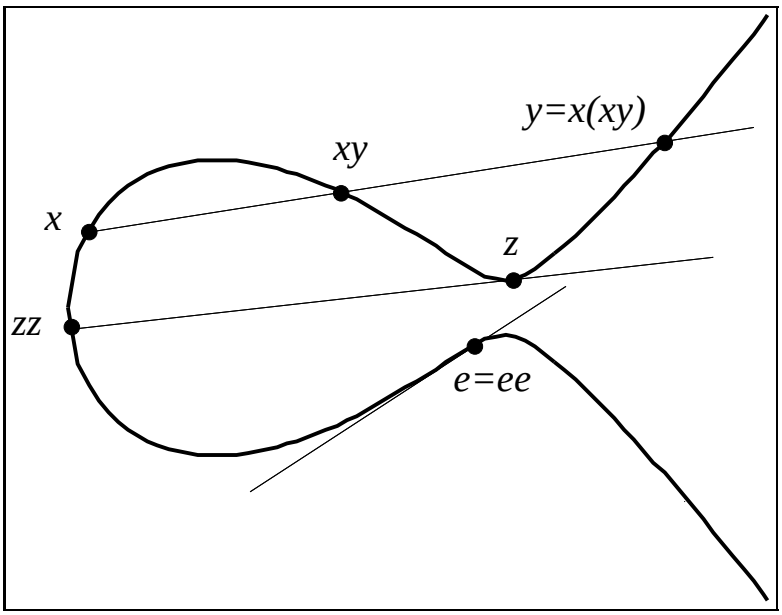

Figure 3.1: Chord-Tangent Operation on a Cubic Curve.

The following configuration theorem is a simple consequence of a Steiner law and $=(gL)\Rightarrow$. The conclusion $S \cdot S = R \cdot Q$ means that the tangent at point S is parallel to line RQ. See Fig. 3.2.

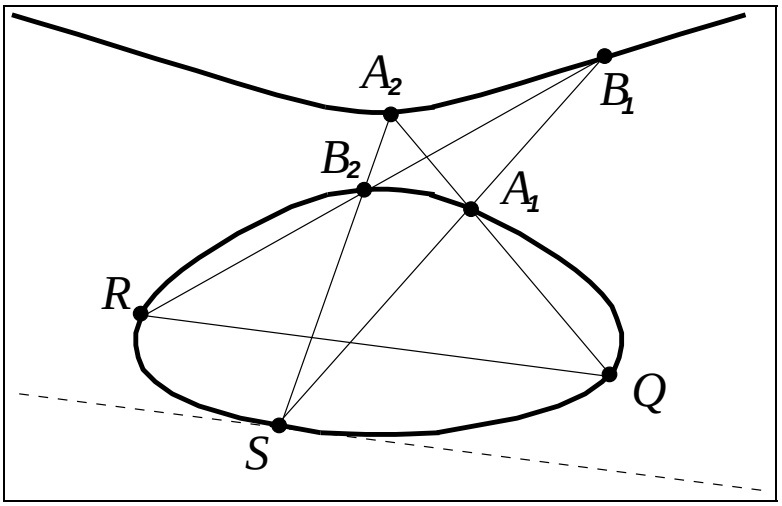

Figure 3.2: Configuration for Thm #GEO-1.

Theorem #GEO-1.

$$\{x \cdot (y \cdot x) = y\} \ =\!(gL)\!\Rightarrow \ \left\{ \left[\begin{array}{l} A_1 \cdot A_2 = Q \\ B_1 \cdot B_2 = R \\ A_1 \cdot B_1 = S \\ A_2 \cdot B_2 = S \end{array} \right] \rightarrow S \cdot S = Q \cdot R \right\}.$$

(In the statement of the theorem, $A_1, A_2, B_1, B_2, P, Q, R$ are variables, and in the proof below, they are Skolem constants.)

Proof (found by Otter 3.0.3l on gyro at 27.02 seconds).

1	$S \cdot S \neq Q \cdot R$	
3	$x \cdot (y \cdot x) = y$	
4	$A_1 \cdot A_2 = Q$	
5	$B_1 \cdot B_2 = R$	
6	$A_1 \cdot B_1 = S$	
7	$A_2 \cdot B_2 = S$	
13	$(x \cdot y) \cdot x = y$	$[3 \rightarrow 3]$
18	$A_2 \cdot Q = A_1$	$[4 \rightarrow 3]$
25	$B_2 \cdot R = B_1$	$[5 \rightarrow 3]$
32	$B_1 \cdot S = A_1$	$[6 \rightarrow 3]$
40	$B_2 \cdot S = A_2$	$[7 \rightarrow 3]$
134	$(B_2 \cdot R) \cdot S = A_1$	$[25 \rightarrow 32]$
171	$(B_2 \cdot S) \cdot Q = A_1$	$[40 \rightarrow 18]$
1849	$(x \cdot S) \cdot Q = (x \cdot R) \cdot S$	$[134 \rightarrow 171$:(gL)$]$
2161	$(Q \cdot R) \cdot S = S$	$[13 \rightarrow 1849$, flip$]$
6976	$S \cdot S = Q \cdot R$	$[2161 \rightarrow 3]$

6977 □ [6976,1]

3.2 The Median Law

The median law is

$$(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u).$$

We first give a Padmanabhan's proof that two Steiner laws (gL)-imply the median law.

Theorem #MED-0.

$$\left\{ \begin{array}{l} x(yx) = y \\ (yz)z = y \end{array} \right\} \Rightarrow (gL) \Rightarrow \{(xy)(zu) = (xz)(yu)\}$$

Proof. Define the 5-ary composite operation f by

$$f(x, y, z, t, u) = ((xy)(zt))(u((xz)(yt))).$$

Now we have, by the law $x(yx) = y$, $f(x, c, c, t, d) = d$ for all x. Thus by the rule (gL), the 5-ary expression $f(x, y, z, t, u)$ does not depend upon x *for all* y, z, t, u. In particular, we have

$$\begin{array}{lll} f(x,y,z,t,u) & = f(x_1,y,z,t,u) & \forall x \forall x_1 \\ ((xy)(zt))(u((xz)(yt))) & = ((x_1y)(zt))(u((x_1z)(yt))) & \forall x \forall x_1 \\ & = (((yz)y)(zt))(u(((yz)z)(yt))) & \text{letting } x_1 = yz \\ & = t(ut) & \text{by the Steiner laws} \\ & = u & \\ & = ((xz)(yt))(u((xz)(yt))) & \end{array}$$

and hence one right-cancellation of the common term $(u((xz)(yt)))$ immediately yields the desired median law $(xy)(zt) = (xz)(yt)$.

Let us now apply this to the geometry of plane cubic curves without any further reference to the geometry or the topology of curves.

Corollary. *Every binary morphism "$\cdot$" defined on a nonsingular cubic curve* Γ *over an algebraically closed field satisfying the Steiner quasigroup identities must be medial (see Fig. 3.3).*

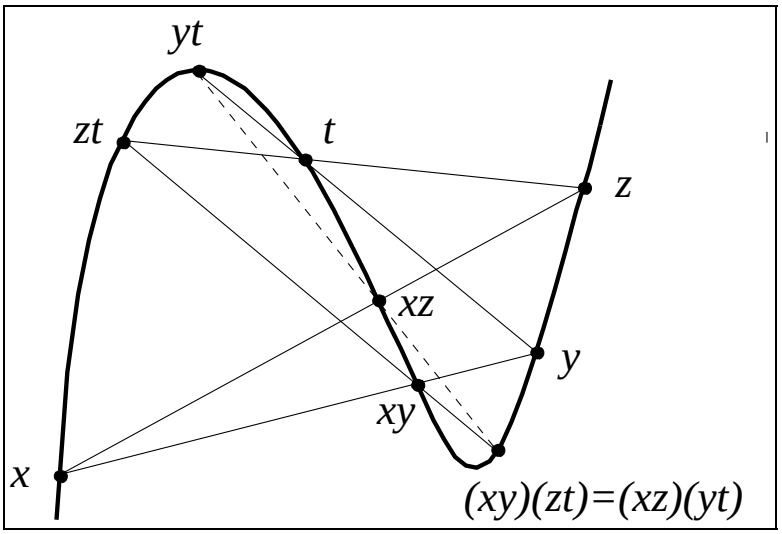

Figure 3.3: The Median Law

Proof. A nonsingular cubic curve is an Abelian variety and hence, as mentioned in the introduction, satisfies (the rigidity lemma and consequently) the rule (gL) for all morphisms.

Historical remark. This corollary was first proved for plane cubic curves by I. M. S. Etherington using the classical Bezout theorem (see [6]). In [28], Padmanabhan gave a proof for elliptic curves over an arbitrary algebraically closed field k (see also Knapp [13, p. 67–74]).

The next three theorems, all first proved by OTTER, show that the median law can be (gL)-derived from weaker hypotheses than those in Thm. #MED-0.

Theorem #MED-3.

$$\{x(yx) = y\} \ \Rightarrow(gL)\Rightarrow \ \{(xy)(zu) = (xz)(yu)\}.$$

Proof (found by Otter 3.0.3l on gyro at 23.93 seconds).

2	$x \cdot (y \cdot x) = y$	
3	$(A \cdot C) \cdot (B \cdot D) \neq (A \cdot B) \cdot (C \cdot D)$	
4	$(x \cdot (y \cdot x)) \cdot (z \cdot y) = z$	$[2 \rightarrow 2]$
9	$(x \cdot y) \cdot x = y$	$[2 \rightarrow 2]$
38	$(x \cdot (y \cdot x)) \cdot (z \cdot y) = (u \cdot z) \cdot u$	$[9 \rightarrow 4]$
369	$(x \cdot (y \cdot z)) \cdot (u \cdot y) = (x \cdot u) \cdot z$	[(gL) 38]
371	$(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u)$	$[2 \rightarrow 369]$
372	$\Box$	[371,3]

Theorem #MED-4. The type is (2,0) with nullary e.

$$\{x(ex) = e\} \ =(gL)\Rightarrow\ \{(xy)(zu) = (xz)(yu)\}.$$

Proof (found by Otter 3.0.3l on gyro at 1.27 seconds).

2	$x \cdot (e \cdot x) = e$	
4	$(A \cdot C) \cdot (B \cdot D) \neq (A \cdot B) \cdot (C \cdot D)$	
7	$x \cdot (y \cdot x) = z \cdot (y \cdot z)$	[2 → 2 :(gL)]
8	$(x \cdot y) \cdot (z \cdot (x \cdot z)) = u \cdot (y \cdot u)$	[7 → 7]
67	$(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u)$	[(gL) 8]
68	□	[67,4]

Theorem #MED-5. The type is (2,0) with nullary e.

$$\left\{ \begin{array}{l} e(ex) = x \\ ee = e \\ e(xe) = (ex)e \end{array} \right\} \ =(gL)\Rightarrow\ \{(xy)(zu) = (xz)(yu)\}$$

Proof (found by Otter 3.0.3l on gyro at 15.72 seconds).

3,2	$e \cdot (e \cdot x) = x$	
4	$e \cdot e = e$	
6	$e \cdot (x \cdot e) = (e \cdot x) \cdot e$	
7	$(e \cdot x) \cdot e = e \cdot (x \cdot e)$	[flip 6]
9	$(A \cdot C) \cdot (B \cdot D) \neq (A \cdot B) \cdot (C \cdot D)$	
10	$(e \cdot x) \cdot (e \cdot y) = e \cdot (x \cdot y)$	[4 → 7 :(gL)]
12	$(x \cdot y) \cdot e = (x \cdot e) \cdot (y \cdot e)$	[4 → 7 :(gL)]
23	$x \cdot (y \cdot e) = e \cdot (y \cdot (x \cdot e))$	[7 → 10 :(gL) :3]
25	$(x \cdot e) \cdot (y \cdot e) = (x \cdot y) \cdot e$	[12 → 2 :3]
28	$x \cdot ((y \cdot e) \cdot z) = e \cdot ((y \cdot x) \cdot z)$	[12 → 23 :(gL)]
29	$e \cdot (x \cdot (y \cdot e)) = y \cdot (x \cdot e)$	[23 → 2 :3]
49	$x \cdot ((y \cdot z) \cdot e) = e \cdot ((y \cdot x) \cdot (z \cdot e))$	[25 → 28]
66	$(x \cdot y) \cdot (z \cdot e) = (x \cdot z) \cdot (y \cdot e)$	[49 → 29 :3]
67	$(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u)$	[2 → 66 :(gL) :3]
68	□	[67,9]

[[Need background for this theorem. Relationship to #Thm MED-1 in the introduction.]]

Theorem #MED-2. The type is (2,0) with nullary e.

$$\left\{ \begin{array}{l} (xy)(zu) = (xz)(yu) \\ ee = e \end{array} \right\} \ =(gL)\Rightarrow\ \{(x(yz))((uv)w) = (x(uz))((yv)w)\}.$$

Proof (found by Otter 3.0.3l on gyro at 2.26 seconds).

2	$(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u)$	
4,3	$e \cdot e = e$	
5	$(A \cdot (D \cdot C)) \cdot ((B \cdot E) \cdot F) \neq (A \cdot (B \cdot C)) \cdot ((D \cdot E) \cdot F)$	
6	$(A \cdot (B \cdot C)) \cdot ((D \cdot E) \cdot F) \neq (A \cdot (D \cdot C)) \cdot ((B \cdot E) \cdot F)$	[flip 5]
7	$((x \cdot y) \cdot (z \cdot u)) \cdot (v \cdot w) = ((x \cdot z) \cdot v) \cdot ((y \cdot u) \cdot w)$	[2 → 2]
11	$(x \cdot e) \cdot (y \cdot e) = (x \cdot y) \cdot e$	[3 → 2]
17	$(e \cdot x) \cdot e = e \cdot (x \cdot e)$	[3 → 11 :4,4, flip]
54,53	$((e \cdot x) \cdot y) \cdot (e \cdot z) = (e \cdot (x \cdot e)) \cdot (y \cdot z)$	[17 → 2]
128	$(x \cdot (y \cdot z)) \cdot ((u \cdot v) \cdot w) = (x \cdot (u \cdot z)) \cdot ((y \cdot v) \cdot w)$	[17 → 7 :54 :(gL) :(gL)]
129	□	[128,6]

3.3 Group-like Laws

[[RP: Need introduction to this section. You once mentioned that one of these results is due to Mumford. Do you have a reference?]]

Theorem #ABGT-5. The type is (2,0) with nullary e.

$$\{ex = xe = x\} \Rightarrow_{(gL)} \{xy = yx\}.$$

Proof (found by Otter 3.0.3l on gyro at 34.89 seconds).

1	$B \cdot A \neq A \cdot B$	
3	$e \cdot x = x$	
4	$x \cdot e = x$	
5	$(e \cdot e) \cdot x = x$	[3 → 3]
7	$(x \cdot e) \cdot e = x$	[4 → 4]
83	$(x \cdot y) \cdot e = (e \cdot y) \cdot x$	[5 → 7 :(gL)]
384	$x \cdot y = (e \cdot y) \cdot x$	[4 → 83]
948	$x \cdot y = y \cdot x$	[3 → 384]
949	□	[948,1]

Theorem #ABGT-6. The type is (2,0) with nullary e.

$$\{ex = xe = x\} \Rightarrow_{(gL)} \{(xy)z = x(yz)\}.$$

Proof (found by Otter 3.0.3l on gyro at 0.97 seconds).

2	$e \cdot x = x$	
3	$x \cdot e = x$	
4	$(A \cdot B) \cdot C \neq A \cdot (B \cdot C)$	
8	$(e \cdot x) \cdot e = x$	[2 → 3]
95	$(A \cdot (B \cdot C)) \cdot e \neq (A \cdot B) \cdot C$	[3 → 4, flip]

175	$(e \cdot x) \cdot y = x \cdot y$	[3 → 8 :(gL)]
302	$(x \cdot (y \cdot z)) \cdot e = (x \cdot y) \cdot z$	[8 → 175 :(gL), flip]
303	□	[302,95]

The next theorem is also a corollay of Thm. #ABGT-5. Note that this proof is longer and uses more concepts than the proof of #ABGT-5; but it is found much more quickly, because the additional richness of the language allows the use of demodulation with derived equalities, which reduces redundancy in the search (Sec. 2.2.4).

Theorem #ABGT-4. Group theory $\Rightarrow(gL)\Rightarrow$ Abelian group theory.

Proof (found by Otter 3.0.3l on gyro at 4.52 seconds).

2	$e \cdot x = x$	
3	$x \cdot e = x$	
4	$x' \cdot x = e$	
5	$x \cdot x' = e$	
6	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	
7	$B \cdot A \neq A \cdot B$	
21	$e \cdot x = x \cdot e$	[3 → 2]
26	$(x \cdot e)' \cdot x = e$	[3 → 4]
30	$(e \cdot x)' \cdot x = e$	[2 → 4]
41,40	$e' = e$	[3 → 4]
45	$x' \cdot x = e \cdot e$	[3 → 4]
48,47	$(e \cdot e)' = e$	[3 → 40]
56,55	$x \cdot (x \cdot e)' = e$	[3 → 5]
85,84	$x \cdot (e \cdot y) = x \cdot y$	[3 → 6, flip]
102,101	$(x \cdot y) \cdot z = e \cdot (x \cdot (y \cdot z))$	[2 → 6]
103	$(x \cdot y)' \cdot x = (z \cdot y)' \cdot z$	[26 → 26 :(gL)]
104	$(x \cdot y)' \cdot y = (x \cdot z)' \cdot z$	[30 → 30 :(gL)]
106,105	$(x \cdot y)' \cdot x = e \cdot y'$	[45 → 103 :48, flip]
112,111	$(x \cdot e)' \cdot e = e \cdot x'$	[21 → 103 :106]
116,115	$(e \cdot x)' = e \cdot x'$	[3 → 103 :106]
119,118	$(x \cdot y)' \cdot y = e \cdot x'$	[55 → 104 :56,112, flip]
120	$e \cdot x'' = e \cdot x$	[45 → 104 :116,41,102,85,85,119, flip]
137,136	$x'' = e \cdot x$	[2 → 120]
140	$e \cdot (x \cdot y) = e \cdot (y \cdot x)$	[105 → 118 :116,137,85,102,85,137,85]
144	$x \cdot y = e \cdot (y \cdot x)$	[2 → 140]
155	$x \cdot y = y \cdot x$	[2 → 144]
156	□	[155,7]

Theorem #UAL-3. Under (gL), two inversive groupoids with a common identity must be identical. That is,

$$\left\{\begin{array}{ll} f(e,x)=x, & F(e,x)=x \\ f(x,e)=x, & F(x,e)=x \\ f(g(x),x)=e, & F(G(x),x)=e \\ f(x,g(x))=e, & F(x,G(x))=e \end{array}\right\} \Rightarrow(gL)\Rightarrow \left\{\begin{array}{l} f(x,y)=F(x,y) \\ g(x)=G(x) \end{array}\right\}.$$

Proof (found by Otter 3.0.3l on gyro at 13.90 seconds).

2	$f(e,x)=x$	
3	$f(x,e)=x$	
4	$f(g(x),x)=e$	
5	$f(x,g(x))=e$	
6	$F(e,x)=x$	
7	$F(x,e)=x$	
8	$F(G(x),x)=e$	
9	$F(x,G(x))=e$	
10	$f(A,B)=F(A,B),\ g(A)=G(A)\ \rightarrow\ \Box$	
28,27	$f(x,e)=F(e,x)$	[3 → 6, flip]
32,31	$f(e,x)=F(e,x)$	[2 → 6, flip]
40	$F(e,x)=F(x,e)$	[7 → 6]
41	$f(g(F(x,e)),x)=e$	[7 → 4]
43	$f(g(x),F(x,e))=e$	[7 → 4]
82	$f(x,F(e,g(x)))=e$	[6 → 5]
94,93	$F(x,f(y,g(y)))=x$	[5 → 7]
112,111	$G(e)=e$	[5 → 8 :94]
139,138	$G(F(G(x),x))=e$	[8 → 111]
144	$F(e,g(e))=e$	[111 → 5 :112,32]
176	$F(G(x),x)=F(y,G(y))$	[9 → 8]
184,183	$F(F(x,G(x)),y)=y$	[9 → 6]
186,185	$g(e)=e$	[9 → 144 :184]
214,213	$f(F(G(x),x),y)=F(e,y)$	[8 → 31]
231	$f(g(F(x,y)),x)=f(g(F(z,y)),z)$	[41 → 41 :(gL)]
236,235	$f(g(F(x,y)),x)=F(e,g(y))$	[9 → 231 :184,28, flip]
243	$F(e,g(F(x,e)))=F(e,g(x))$	[40 → 231 :28,236]
248,247	$F(e,g(x))=F(e,G(x))$	[8 → 231 :186,32,236, flip]
268,267	$F(x,g(F(y,e)))=F(x,g(y))$	[243 :(gL)]
277	$f(x,F(e,G(x)))=e$	[82 :248]
289	$f(g(x),F(x,y))=f(g(z),F(z,y))$	[43 → 43 :(gL)]
291,290	$g(x)=F(e,G(x))$	[9 → 267 :268,184,248]
292	$f(F(e,G(x)),F(x,y))=f(F(e,G(z)),F(z,y))$	[289 :291,291]
311	$f(A,B)=F(A,B)\ \rightarrow\ \Box$	[10 :291 :6]
312	$f(F(A,e),B)=F(A,B)\ \rightarrow\ \Box$	[7 → 311]
350,349	$f(x,G(x))=e$	[9 → 277 :184]
409	$f(F(x,G(y)),F(y,z))=f(F(x,G(u)),F(u,z))$	[292 :(gL)]

443,442	$f(F(x,G(y)),F(y,z)) = f(F(x,e),F(e,z))$	[349 → 409 :350,112, flip]
446,445	$f(F(x,e),F(e,y)) = f(F(x,e),y)$	[176 → 409 :139,184,443, flip]
449,448	$f(F(x,e),y) = F(e,F(x,y))$	[176 → 409 :214,443,446, flip]
478	$F(e,F(A,B)) = F(A,B) \rightarrow \square$	[312 :449]
479	$\square$	[478,6]

Corollary #UAL-3a. Under (gL), two groups with a common identity must be identical.

The following theorem generalizes the uniqueness of the group law on a curve into a first order sentence. The context is that + has a unit element e.

[[RP: note that we prove a more general identity than in the statemet of the theorem. Also, please clarify the motivation.]]

Theorem #UAL-5. The type is (2,2,0) with $+$, $\cdot$, and e as the three operations.

$$\left\{ \begin{array}{l} x + e = x \\ e + x = x \\ x \cdot (y \cdot x) = y \end{array} \right\} \Rightarrow (gL) \Rightarrow \{x + z = ((e \cdot e) \cdot x) \cdot (z \cdot e)\}.$$

Proof (found by Otter 3.0.3l on gyro at 54.24 seconds).

2	$x + e = x$	
3	$e + x = x$	
4	$x \cdot (y \cdot x) = y$	
5	$((e \cdot e) \cdot A) \cdot (B \cdot e) \neq A + B$	
10	$(e + x) \cdot (y \cdot x) = y$	[3 → 4]
14	$(x + e) \cdot (y \cdot x) = y$	[2 → 4]
29	$(x \cdot y) \cdot x = y$	[4 → 4]
61	$(x + y) \cdot (z \cdot y) = (x + u) \cdot (z \cdot u)$	[10 → 10 :(gL)]
73	$x \cdot (y \cdot e) = (x + z) \cdot (y \cdot z)$	[2 → 61]
77	$(x + y) \cdot ((z \cdot u) \cdot y) = (x + z) \cdot u$	[29 → 61]
112	$(x + y) \cdot (z \cdot x) = (u + y) \cdot (z \cdot u)$	[14 → 14 :(gL)]
133	$(x + y) \cdot z = (u + y) \cdot ((x \cdot z) \cdot u)$	[29 → 112]
179	$(x + y) \cdot ((e \cdot z) \cdot y) = x \cdot z$	[29 → 73, flip]
327	$(x + y) \cdot z = (y + x) \cdot z$	[77 → 133]
349	$x \cdot ((y + z) \cdot x) = z + y$	[327 → 4]
377	$((e \cdot x) \cdot y) \cdot (z \cdot x) = y + z$	[179 → 349]
378	$\square$	[377,5]

[[What is the background for the rest of this section??]]

Theorem #MCV-1.

$$\left\{ \begin{array}{l} p(x,y,y) = x \\ p(x,x,y) = y \end{array} \right\} \Rightarrow (gL) \Rightarrow \{p(x,y,p(z,u,v)) = p(v,u,p(x,y,z))\}.$$

Proof (found by Otter 3.0.3l on gyro at 16.83 seconds).

2	$p(x,y,y) = x$	
3	$p(x,x,y) = y$	
4	$p(A,B,p(C,D,E)) \neq p(E,D,p(A,B,C))$	
25	$p(x,x,y) = p(y,z,z)$	$[2 \rightarrow 3]$
70	$p(x,y,z) = p(z,y,x)$	[(gL) 25]
98	$p(x,x,p(y,z,u)) = p(u,z,y)$	$[3 \rightarrow 70]$
99	$p(p(x,y,z),u,u) = p(z,y,x)$	$[2 \rightarrow 70]$
135	$p(p(C,D,E),B,A) \neq p(E,D,p(A,B,C))$	$[70 \rightarrow 4]$
183	$p(x,y,p(z,u,y)) = p(x,u,z)$	[(gL) 98]
291	$p(p(x,y,z),x,u) = p(z,y,u)$	[(gL) 99]
304	$p(p(x,y,z),u,v) = p(z,y,p(v,u,x))$	$[183 \rightarrow 291]$
305	$\Box$	[304,135]

Theorem #UAL-6. The type is (3,3) with two ternary operations M_1 and M_2.

$$\left\{ \begin{array}{l} M_1(x,y,y) = x,\ M_1(x,x,z) = z \\ M_2(x,y,y) = x,\ M_2(x,x,z) = z \end{array} \right\} \Rightarrow (gL) \Rightarrow \ \{M_1(x,y,z) = M_2(x,y,z)\}.$$

Proof (found by Otter 3.0.3l on gyro at 100.97 seconds).

2	$M_1(x,y,y) = x$	
3	$M_1(x,x,z) = z$	
4	$M_2(x,y,y) = x$	
5	$M_2(x,x,z) = z$	
6	$M_2(A,B,C) \neq M_1(A,B,C)$	
15	$M_1(x,x,y) = M_1(y,z,z)$	$[2 \rightarrow 3]$
30	$M_1(x,y,M_2(y,z,z)) = x$	$[4 \rightarrow 2]$
37	$M_2(x,x,y) = M_2(y,z,z)$	$[4 \rightarrow 5]$
51	$M_1(x,y,z) = M_1(z,y,x)$	[(gL) 15]
52	$M_1(x,y,M_2(z,z,u)) = M_1(u,y,x)$	$[5 \rightarrow 51$, flip]
60	$M_2(x,y,z) = M_2(z,y,x)$	[(gL) 37]
65	$M_2(x,x,M_2(y,z,u)) = M_2(u,z,y)$	$[5 \rightarrow 60]$
71	$M_1(x,y,M_2(z,z,u)) = M_1(u,y,M_2(v,v,x))$	$[5 \rightarrow 52]$
419	$M_2(x,y,M_2(z,x,u)) = M_2(u,y,z)$	[(gL) 65]
516	$M_2(x,y,M_2(y,x,z)) = z$	$[4 \rightarrow 419]$
937	$M_1(x,y,M_2(z,u,v)) = M_1(v,y,M_2(z,u,x))$	[(gL) 71]
964	$M_1(x,y,M_2(y,x,z)) = z$	$[30 \rightarrow 937$, flip]
989	$M_2(x,y,z) = M_1(x,y,z)$	$[516 \rightarrow 964$, flip]
990	$\Box$	[989,6]

Corollary #UAL-7. The type is (2,2) with binary operations $\cdot$ and $\sharp$. Define the ternary Mal'cev terms as

$$M_1(x,y,z) = ((y \cdot y) \cdot x) \cdot (z \cdot y)$$
$$M_2(x,y,z) = ((y \sharp y) \sharp x) \sharp (z \sharp y).$$

Then

$$\left\{ \begin{array}{l} x \cdot (y \cdot x) = y \\ x \sharp (y \sharp x) = y \end{array} \right\} \Rightarrow (gL) \Rightarrow \{M_1(x,y,z) = M_2(x,y,z)\}.$$

We have been unable to get OTTER to prove this directly in a single search without a highly specialized strategy—so specialized that it is essentially proof checking; however, the result follows easily from Thm. #UAL-6.

3.4 Uniqueness of n-ary Steiner Laws

Some of the material in this section is presented also in [31], where we give an equational characterization of the conic construction on a cubic curve. The key result in that paper, which we also resent here, is the uniqueness of the 5-ary Steiner law under (gL); from there we have the well-known theorem in geometry that given five points of intersection between a cubic and a conic, the sixth point can be found by a simple ruler construction. (See the end of this section.)

We start with the uniqueness of the binary Steiner law.

Theorem #UAL-1. The type of theory is (2,2,0) with two binary operations and nullary e.

$$\left\{ \begin{array}{ll} f(x,y) = f(y,x), & g(x,y) = g(y,x) \\ f(x,f(y,x)) = y, & g(x,g(y,x)) = y \\ f(e,e) = e), & g(e,e) = e) \end{array} \right\} \Rightarrow (gL) \Rightarrow \{f(x,y) = g(x,y)\}$$

Proof (found by Otter 3.0.3l on gyro at 156.05 seconds).

2	$f(x,y) = f(y,x)$	
3	$f(x,f(y,x)) = y$	
4	$f(e,e) = e$	
5	$g(x,y) = g(y,x)$	
6	$g(x,g(y,x)) = y$	
7	$g(e,e) = e$	
8	$g(A,B) \neq f(A,B)$	
9	$f(e,e) = e$	
10	$f(x,f(y,x)) = y$	
11	$f(x,g(e,e)) = f(e,x)$	$[7 \rightarrow 2]$
15	$f(x,f(x,y)) = y$	$[2 \rightarrow 3]$
22	$g(x,g(x,y)) = y$	$[5 \rightarrow 6]$
48	$g(x,y) = f(z,f(z,g(y,x)))$	$[15 \rightarrow 5]$
106	$f(x,g(e,e)) = f(e,g(y,g(y,x)))$	$[22 \rightarrow 11]$

493	$f(e,g(x,g(e,y))) = f(y,g(x,e))$	[4 → 106 :(gL) :9, flip]
500	$f(x,g(x,e)) = e$	[6 → 493 :9, flip]
536	$f(x,g(x,y)) = f(z,g(z,y))$	[500 → 500 :(gL)]
551	$g(e,x) = f(x,e)$	[500 → 48]
860	$f(x,g(x,y)) = y$	[551 → 536 :10]
983	$g(x,y) = f(x,y)$	[22 → 860, flip]
984	$\Box$	[983,8]

The next three theorems, #STN-3, #STN-4, and #STN-5, show that for arities 3, 4, and 5, the universal Steiner law can be replaced with a weaker form in the presence of idempotence and permutation identities. In [33] we prove the corresponding general theorem for all arities.

Problem #STN-3. The type is (3,0), with ternary f and nullary e.

$$\left\{ \begin{array}{l} f(w,x,y) = f(w,y,x) \\ f(e,e,e) = e \\ f(e,x,f(e,x,y)) = y \end{array} \right\} \Rightarrow_{(gL)} \{f(w,x,f(w,x,y)) = y\}.$$

The conclusion is the universal ternary Steiner law.

Proof (found by Otter 3.0.3l on gyro at 2.66 seconds).

1	$f(A,B,f(A,B,C)) \neq C$	
3	$f(x,y,z) = f(x,z,y)$	
4	$f(e,e,e) = e$	
7,6	$f(e,x,f(e,x,y)) = y$	
9,8	$f(e,x,f(e,y,x)) = y$	[3 → 6]
12	$f(x,e,e) = f(x,y,f(e,y,e))$	[6 → 4 :(gL)]
20	$f(e,x,f(y,f(z,e,e),x)) = f(z,u,f(y,u,e))$	[8 → 12 :(gL)]
282	$f(e,e,x) = f(y,f(y,e,e),x)$	[(gL) 20]
347	$f(x,y,f(x,y,e)) = e$	[282 → 20 :9, flip]
422	$f(x,y,f(x,y,z)) = z$	[6 → 347 :(gL) :7]
424	$\Box$	[422,1]

Theorem #STN-4. The type is (4,0), with 4-ary f and nullary e.

$$\left\{ \begin{array}{l} f(v,w,x,y) = f(v,w,y,x) \\ f(e,e,e,e) = e \\ f(e,e,x,f(e,e,x,y)) = y \end{array} \right\} \Rightarrow_{(gL)} \{f(v,w,x,f(v,w,x,y)) = y\}.$$

The conclusion is the universal 4-ary Steiner law.

Proof (found by Otter 3.0.3l on gyro at 3.23 seconds).

1	$f(D,A,B,f(D,A,B,C)) \neq C$	
3	$f(x,y,z,u) = f(x,y,u,z)$	
4	$f(e,e,e,e) = e$	
6	$f(e,e,x,f(e,e,x,y)) = y$	
11,10	$f(e,e,f(e,e,x,y),x) = y$	[3 → 6]
12	$f(x,y,e,e) = f(x,y,z,f(e,e,z,e))$	[6 → 4 :(gL) :(gL)]
17	$f(x,y,z,f(u,v,z,w)) = f(x,y,v_6,f(u,v,v_6,w))$	[12 → 12 :(gL) :(gL) :(gL)]
34	$f(x,y,f(z,u,v,w),v) = f(x,y,v_6,f(z,u,v_6,w))$	[3 → 17]
120	$f(x,y,z,f(u,v,f(u,v,w,v_6),v_6)) = f(x,y,z,w)$	[(gL) 34, flip]
134	$f(x,y,f(x,y,z,u),u) = z$	[120 → 10 :11, flip]
167	$f(x,y,z,f(x,y,z,u)) = u$	[34 → 134]
169	□	[167,1]

Theorem #STN-5. The type is (5,0), with 5-ary f and nullary e.

$$\left\{ \begin{array}{l} f(u,v,w,x,y) = f(u,v,w,y,x) \\ f(e,e,e,e,e) = e \\ f(e,e,e,x,f(e,e,e,x,y)) = y \end{array} \right\} \Rightarrow(gL)\Rightarrow \{f(u,v,w,x,f(u,v,w,x,y)) = y\}.$$

The conclusion is the universal 5-ary Steiner law.

Proof (found by Otter 3.0.3l on gyro at 3.89 seconds).

1	$f(E,D,A,B,f(E,D,A,B,C)) \neq C$	
3	$f(x,y,z,u,v) = f(x,y,z,v,u)$	
4	$f(e,e,e,e,e) = e$	
7,6	$f(e,e,e,x,f(e,e,e,x,y)) = y$	
9,8	$f(e,e,e,x,f(e,e,e,y,x)) = y$	[3 → 6]
12	$f(x,y,z,e,e) = f(x,y,z,u,f(e,e,e,u,e))$	[6 → 4 :(gL) :(gL) :(gL)]
20	$f(e,e,e,x,f(y,z,u,f(v,w,v_6,e,e),x)) = f(v,w,v_6,v_7,f(y,z,u,v_7,e))$	[8 → 12 :(gL) :(gL)
223	$f(e,e,e,e,x) = f(y,z,u,f(y,z,u,e,e),x)$	[(gL) 20]
277	$f(x,y,z,u,f(x,y,z,u,e)) = e$	[223 → 20 :9, flip]
340	$f(x,y,z,u,f(x,y,z,u,v)) = v$	[6 → 277 :(gL) :7]
342	□	[340,1]

The following lemma leads to the uniqueness of the 5-ary Steiner law, the main result of this section.

Lemma #UAL-4a. The type is (5,5,0), with nullary e.

$$\left\{ \begin{array}{l} f(u,v,w,x,y) = f(u,v,w,y,x) \\ f(e,e,e,e,e) = e \\ f(u,v,w,x,f(u,v,w,x,y)) = y \\ g(u,v,w,x,y) = g(u,v,w,y,x) \\ g(e,e,e,e,e) = e \\ g(u,v,w,x,g(u,v,w,x,y)) = y \end{array} \right\} \Rightarrow(gL)\Rightarrow \{f(x1,x2,x3,y,g(x4,x5,x6,y,x7)) = f(x1,x2,x3,z$$

Proof (found by Otter 3.0.3l on gyro at 22.26 seconds).

2 $f(u,v,w,x,y) = f(u,v,w,y,x)$
5 $g(u,v,w,x,y) = g(u,v,w,y,x)$
6 $g(e,e,e,e,e) = e$
7 $g(u,v,w,x,g(u,v,w,x,y)) = y$
8 $f(A_1,A_2,A_3,B,g(A_4,A_5,A_6,B,A_7)) \neq f(A_1,A_2,A_3,C,g(A_4,A_5,A_6,C,A_7))$
10 $f(x,y,z,u,g(e,e,e,e,e)) = f(x,y,z,e,u)$ [6 → 2]
14 $f(x,y,z,e,g(u,v,w,v_6,g(u,v,w,v_6,v_7))) = f(x,y,z,v_7,g(e,e,e,e,e))$ [7 → 10, flip]
20 $f(x,y,z,e,g(u,v,w,v_6,g(u,v,w,v_7,v_6))) = f(x,y,z,v_7,g(e,e,e,e,e))$ [5 → 14]
24 $f(x,y,z,e,g(u,v,w,v_6,g(u,v,w,e,v_7))) = f(x,y,z,v_7,g(e,e,e,v_6,e))$ [(gL) 14]
45 $f(x,y,z,e,g(u,v,w,e,v_6)) = f(x,y,z,v_7,g(u,v,w,v_7,v_6))$ [20 → 24 :(gL) :(gL) :(gL) :(gL)]
52 $f(x,y,z,u,g(v,w,v_6,u,v_7)) = f(x,y,z,v_8,g(v,w,v_6,v_8,v_7))$ [45 → 45]
53 □ [52,8]

Theorem #UAL-4b. The type is (5,5,0), with nullary e.

$$\left\{\begin{array}{l} \text{full symmetey of } f \\ f(e,e,e,e,e) = e \\ f(e,e,e,x,f(e,e,e,x,y)) = y \\ \text{full symmetey of } g \\ g(e,e,e,e,e) = e \\ g(e,e,e,x,g(e,e,e,x,y)) = y \end{array}\right\} \Rightarrow_{(gL)} \{g(x,y,z,u,v) = f(x,y,z,u,v)\}.$$

By Thm. #STN-5, we may also assume the universal 5-ary Steiner laws for f and for g:

$$f(u,v,w,x,f(u,v,w,x,y)) = y$$
$$g(u,v,w,x,g(u,v,w,x,y)) = y.$$

By Lem. #UAL-4a, we include the identity

$$f(x_1,x_2,x_3,y,g(x_4,x_5,x_6,y,x_7)) = f(x_1,x_2,x_3,z,g(x_4,x_5,x_6,z,x_7)).$$

Proof (found by Otter 3.0.3l on gyro at 3.82 seconds).

2 $g(x,y,z,u,v) = f(x,y,z,u,v) \rightarrow g(y,z,u,v,x) = f(y,z,u,v,x)$
3 $f(e,e,e,e,e) = e$
4 $f(u,v,w,x,f(u,v,w,x,y)) = y$
5 $g(e,e,e,e,e) = e$
6 $g(u,v,w,x,g(u,v,w,x,y)) = y$
7 $f(x_1,x_2,x_3,y,g(x_4,x_5,x_6,y,x_7)) = f(x_1,x_2,x_3,z,g(x_4,x_5,x_6,z,x_7))$
8 $g(A,B,C,D,E) = f(A,B,C,D,E) \rightarrow$ □
10 $f(e,e,e,e,g(e,e,e,e,e)) = e$ [5 → 3]
11 $f(e,e,e,x,g(e,e,e,x,e)) = e$ [7 → 10]
12 $g(e,e,e,x,e) = f(e,e,e,x,e)$ [11 → 4, flip]
13 $g(e,e,x,e,e) = f(e,e,x,e,e)$ [2,12]

15	$f(e,e,x,e,g(e,e,x,e,e)) = e$	[13 → 4]
18	$f(e,e,x,y,g(e,e,x,y,e)) = e$	[7 → 15]
19	$g(e,e,x,y,e) = f(e,e,x,y,e)$	[18 → 4, flip]
20	$g(e,x,y,e,e) = f(e,x,y,e,e)$	[2,19]
22	$f(e,x,y,e,g(e,x,y,e,e)) = e$	[20 → 4]
25	$f(e,x,y,z,g(e,x,y,z,e)) = e$	[7 → 22]
26	$g(e,x,y,z,e) = f(e,x,y,z,e)$	[25 → 4, flip]
27	$g(x,y,z,e,e) = f(x,y,z,e,e)$	[2,26]
29	$f(x,y,z,e,g(x,y,z,e,e)) = e$	[27 → 4]
32	$f(x,y,z,u,g(x,y,z,u,e)) = e$	[7 → 29]
33	$g(x,y,z,u,e) = f(x,y,z,u,e)$	[32 → 4, flip]
34	$g(x,y,z,e,u) = f(x,y,z,e,u)$	[2,33]
36	$f(x,y,z,e,g(x,y,z,e,u)) = u$	[6 → 34, flip]
39	$f(x,y,z,u,g(x,y,z,u,v)) = v$	[7 → 36]
40	$g(x,y,z,u,v) = f(x,y,z,u,v)$	[6 → 39, flip]
41	$\square$	[40,8]

The above OTTER proofs of Thms. #UAL-1, #UAL-4a, and #UAL-4b were found with specialized search strategies. The first OTTER proof of #UAL-1, which was found with a straightforward strategy, required about 38 hours. Because it is an important theorem, and because we planned to attack problems of a similar nature (e.g., higher arities), we devised some strategies would lead OTTER quickly to a proof. The strategy that led to the above proof of #UAL-1 (in a few minutes) discards clauses containg left associated terms and prefers clauses with variables.

Commutativity of a binary operation usually causes a minor explosion in the search space, and full permutability of a higher-arity operation is nearly always disasterous, especially when used with OTTER's prolific and redundant strategies for $=\!(gL)\!\Rightarrow$. So when RP first asked WM to find a proof of the 5-ary Steiner conjecture (Thm. #UAL-4b), the response was "not a chance". Eight months later, RP asked again, and we went back to the binary case (Thm. #UAL-1) for clues; we reduced the search time from 38 hours to several minutes by studying the form of the 38-hour proof. Although the cases with nice geometric interpretations are arities $3m + 2$ ($m \geq 0$), we conjectured that the analogous theorems hold for all arities, and tried the ternary case next. After adjusting the search strategy, a proof was found, and we noticed that the universal Steiner law is a natural lemma for the theorem, and proved the corresponding lemmas (Thms. #STN-4 and #STN-5) separately for the 4-ary and 5-ary cases.

The key strategies were to discard clauses that are not right associated, and to severely limit the use of symmetry. For the 4-ary and 5-ary cases, we directed the searches toward the form of proof we expected, and proofs were found. The first proof of the 5-ary universal Steiner law (Thm. #STN-5) took half an hour (length 13), and the first 5-ary uniqueness proof (Thm. #UAL-4b) took 23 hours (length 46).

The strategies were refined further while studying the proofs and working

out a proof (by hand) that the analogous proofs hold for all arities. Lemma #UAL-4a was separated from the main proof at that time. The proofs above are the product of the specialized strategies. Independently, we found (entirely by hand) a higher-order proof for all arities. (The n-ary proofs will appear elsewhere [33].)

Corollary #UAL-2. The type is (5,2,0), with nullary e.

$$\left\{\begin{array}{l} \text{full symmetry of } f \\ f(e,e,e,e,e) = e \\ f(e,e,e,x,f(e,e,e,x,y)) = y \\ h(x,y) = h(y,x) \\ h(e,e) = e \\ h(x,h(x,y)) = y \end{array}\right\} \Rightarrow_{(gL)} \{h(h(h(x,y),h(z,u)),v) = f(x,y,z,u,v)\}.$$

This follows from Thm. #UAL-4a. Define $g(x,y,z,u,v)$ as $h(h(h(x,y),h(z,u)),v)$; then g satisfies the hypotheses of Thm. #UAL-4.

Fig. 3.4 is a geometric interpretation of Thm. #UAL-4b. Let Γ be a

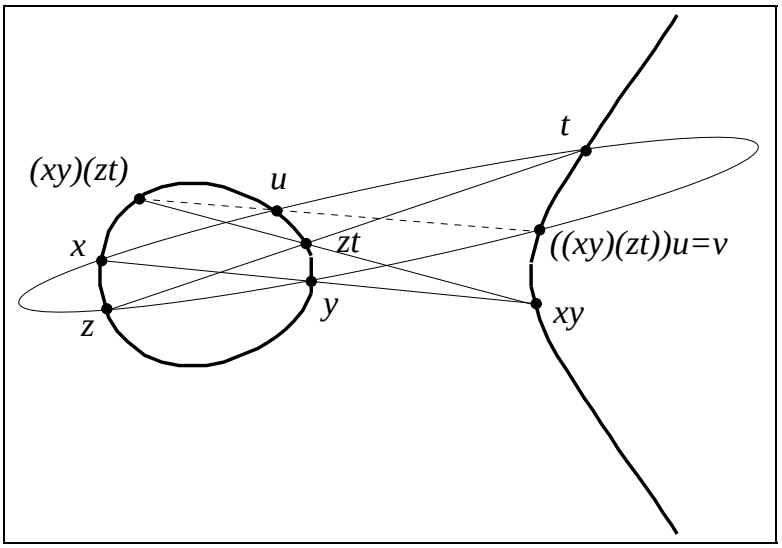

Figure 3.4: The Conic Construction on a Cubic Curve

non-singular cubic curve, and let x,y,z,t,u be five points on the curve. Let Q be the unique conic determined by the 5 points. By the Bezout theorem of classical geometry, we have $|\Gamma \cap Q| = 6$, counting multiplicities. Now let $F(x,y,z,t,u)$ be the 5-ary morphism on Γ defined by the complete intersection cycle $\Gamma \cap Q$ $\{x,y,z,t,u,F(x,y,z,t,u)\}$. By Corollary #UAL-2, we know that the unique sixth point $F(x,y,z,t,u)$ can be found by a simple ruler construction as shown. (A proof using the rigidity lemma was given by N. S. Mendelsohn, R. Padmanabhan and B. Wolk in [22]). See [22] for more detail.

3.5 Group Laws on a Quartic Curve

[[RP: Need introduction to this section.]]

Theorem #QUART-1. The type is (3).

$$\left\{ \begin{array}{l} f(x,y,f(x,y,z)) = z \\ f(x,y,z) = f(x,z,y) \end{array} \right\} =(gL)\Rightarrow \{f(x,y,f(x,z,u)) = f(u,y,f(u,z,u))\}.$$

The first version of this problem had a different conclusion: $f(x,y,f(x,z,t)) = f(u,y,f(u,z,t))$. OTTER was unable to prove the first version, then RP found the following counterexample. Define $f(x,y,z)$ as $ax+by+cz$ in an Abelian group. Such an algebra is always a (gL)-algebra. The first identity $f(x,y,f(x,y,z)) = z$ demands that $a+ac=0$, $b+bc=0$ and $c^2=1$. Thus $c=-1$ would satisfy all the conditions without the number a being 0. Now the second identity $f(x,y,z) = f(x,z,y)$ demands that $b=c$. Hence choose $b=c=-1$ and $a=2$, say. Now, $f(x,y,f(z,x,t)) = 2x-y-(2z-x-t) = x-y-2z-t$ which is not independent of x in the Abelian group of integers! Thus our goal is not a consequence of the assumptions. However, the following identity is true in this model: $f(x,y,f(x,z,t)) = f(u,y,f(u,z,t)$ because the LHS reduces to $2x-y-(2x-z-t) = z-y+t$ which is independent of x. So the corrected formulation of Thm. #QUART-1 is given above.

Proof (found by Otter 3.0.3l on gyro at 2.07 seconds).

2	$f(x,y,f(x,y,z)) = z$	
4	$f(A,B,f(A,C,D)) \neq f(E,B,f(E,C,D))$	
10	$f(x,y,f(x,y,z)) = f(u,v,f(u,v,z))$	$[2 \rightarrow 2]$
163	$f(x,y,f(x,z,u)) = f(v,y,f(v,z,u))$	[(gL) 10]
164	$\Box$	[163,4]

Theorem #QUART-2.

$$\left\{ \begin{array}{l} f(x,y,f(x,y,z)) = z \\ f(x,y,z) = f(x,z,y) \\ p(z,y,v) = f(x,y,f(x,z,v)) \end{array} \right\} =(gL)\Rightarrow \{p(x,y,p(z,v,u)) = p(u,v,p(x,y,z))\}$$

Background: guided by the intution gained through the model described for the previous problem, we suspect that $p(z,y,v) := f(x,y,f(x,z,v))$ must behave like the ternary Mal'cev polynomial $z-y+v$ in Abelian groups! Thms. #QUART-1 and #QUART-2, taken together, construct a synthetic group law $+$ on a quartic curve Γ such that if four points P,Q,R,S on Γ are collinear, then $P+Q+R+S = E$ under the group law.

By Thm. #MCV-1, it is sufficient to prove $p(x,y,y) = p(y,y,x) = x$.

Proof (found by Otter 3.0.3l on gyro at 1577.70 seconds).

2	$f(x,y,f(x,y,z)) = z$	
3	$f(x,y,z) = f(x,z,y)$	
4	$p(z,y,v) = f(x,y,f(x,z,v))$	
5	$p(A,B,p(C,D,E)) \neq p(E,D,p(A,B,C))$	
6	$f(x,y,f(x,z,y)) = z$	$[3 \to 2]$
7	$p(x,y,y) = x$	$[6 \to 4]$
8	$p(x,x,y) = y$	$[2 \to 4]$
14	$p(x,x,y) = p(y,z,z)$	$[7 \to 8]$
78	$p(x,y,z) = p(z,y,x)$	[(gL) 14]
88	$p(x,y,p(z,u,u)) = p(z,y,x)$	$[7 \to 78]$
90	$p(x,x,p(y,z,u)) = p(u,z,y)$	$[8 \to 78]$
272	$p(x,y,p(z,u,y)) = p(x,u,z)$	[(gL) 90]
286	$p(x,y,p(z,u,y)) = p(z,u,p(x,v,v))$	$[88 \to 272]$
538	$p(x,y,p(z,u,v)) = p(z,u,p(x,y,v))$	[(gL) 286]
541	$p(x,y,p(z,u,v)) = p(v,u,p(x,y,z))$	$[78 \to 538]$
542	$\square$	[541,5]

Chapter 4

$=\!(gL)\!\Rightarrow$ in Other Algebras

4.1 Equations Consistent with $=\!(gL)\!\Rightarrow$

[[Need background for this section.]]

[[RP: Because of the title of this section, the reader might think that we are proving consistency with (gL). We probably need an into to explain this.]]

4.1.1 Abelian Groups

Theorem #ABGT-1. The type of theory is (2,0), with operations $\mid$ and e. Let

$$A = \left\{ \begin{array}{l} x \mid x = e \\ e \mid (e \mid x) = x \\ e \mid x = x \mid e \end{array} \right\}.$$

Then A $=\!(gL)\!\Rightarrow$ {all Abelian group axioms satisfied by both left division $\backslash$ and right-division /}. In view of [8], it is enough to derive, using the rule $=\!(gL)\!\Rightarrow$, the following single identity from the axiom set A: $(x \mid y) \mid (((x \mid z) \mid (u \mid u)) \mid y) = z$.

Proof (found by Otter 3.0.3l on gyro at 2.66 seconds).

3,2	$x \mid x = e$	
5,4	$e \mid (e \mid x) = x$	
7,6	$(x \mid e) \mid e = x$	
8	$e \mid (x \mid e) = (e \mid x) \mid e$	
9	$(e \mid x) \mid e = e \mid (x \mid e)$	[flip 8]
11	$(A \mid B) \mid (((A \mid C) \mid (D \mid D)) \mid B) \neq C$	
12	$(A \mid B) \mid (((A \mid C) \mid e) \mid B) \neq C$	[copy,11 :3]
13	$(e \mid x) \mid (e \mid y) = e \mid (x \mid y)$	[6 $\rightarrow$ 9 :(gL) :3]
15	$(x \mid y) \mid e = (x \mid e) \mid (y \mid e)$	[4 $\rightarrow$ 9 :(gL) :3]
23,22	$(e \mid x) \mid y = e \mid (x \mid (e \mid y))$	[4 $\rightarrow$ 13]
24	$(x \mid y) \mid (e \mid z) = (x \mid e) \mid (y \mid z)$	[4 $\rightarrow$ 13 :(gL) :3]

25	$x \mid (y \mid (e \mid z)) = e \mid (y \mid (x \mid z))$	[13 → 13 :(gL) :5]
26	$x \mid (y \mid e) = e \mid (y \mid (x \mid e))$	[9 → 13 :(gL) :5]
27	$((x \mid y) \mid z) \mid e = ((x \mid e) \mid z) \mid y$	[15 → 15 :(gL) :7]
39	$(A \mid B) \mid (((A \mid e) \mid (C \mid e)) \mid B) \neq C$	[15 → 12]
53,52	$(x \mid y) \mid e = e \mid (y \mid x)$	[15 → 26 :7]
67,66	$((x \mid e) \mid y) \mid z = e \mid (y \mid (x \mid z))$	[27 :53, flip]
71	$(A \mid B) \mid (e \mid ((C \mid e) \mid (A \mid B))) \neq C$	[39 :67]
80	$(x \mid y) \mid (e \mid y) = x$	[2 → 24 :53,5]
113	$x \mid e = y \mid (e \mid (x \mid y))$	[2 → 25 :23,5]
137,136	$(x \mid (y \mid z)) \mid z = (x \mid e) \mid y$	[80 → 24 :5]
183	$x \mid (e \mid ((y \mid e) \mid x)) = y$	[113 → 113 :53,137,3,5, flip]
185	□	[183,71]

Theorem #ABGT-2.

$$\left\{ \begin{array}{l} x/e = x \\ x/x = e \end{array} \right\} \; =\!(gL)\!\Rightarrow \; \text{Abelian group theory,}$$

with x/y as right division. It is enough to derive one of the single axioms defining abelian groups with $x/y = x - y$. (Note: the first axioms were $\{x/e = x, e/(e/x) = x\}$. OTTER failed to find a proof, then RP found a couterexample and added axiom $x/x = e$ to kill the unwanted model $x + 3y$ (mod 8). OTTER then found a proof, but the proof did not use $e/(e/x) = x$. Hence the current formulation of the theorem.)

Proof (found by Otter 3.0.3l on gyro at 131.92 seconds).

2	$x/e = x$	
3	$x/x = e$	
5	$A/((B/C)/(B/A)) \neq C$	
10	$(x/e)/e = x$	[2 → 2]
15	$x/(x/e) = e$	[2 → 3]
17	$x/(y/y) = x$	[3 → 2]
152	$x/(x/y) = z/(z/y)$	[15 → 15 :(gL)]
634	$x/(x/y) = y$	[17 → 152, flip]
858	$(x/e)/(x/y) = y$	[2 → 634]
884	$x/((x/y)/e) = y$	[2 → 634]
9245	$(x/y)/(x/z) = (z/y)/e$	[10 → 858 :(gL)]
11150	$x/((y/z)/(y/x)) = z$	[9245 → 884]
11151	□	[11150,5]

Theorem #ABGT-3.

$$\left\{ \begin{array}{l} x/(x/y) = y \\ x/x = e \end{array} \right\} \; =\!(gL)\!\Rightarrow \; \text{Abelian group theory.}$$

Here, x/y is right division. It is sufficient to prove any of the single axioms for Abeilan groups in terms of right division.

Proof (found by Otter 3.0.3l on gyro at 13.24 seconds).

2	$x/x = e$	
3	$x/(x/y) = y$	
8	$(A/((A/B)/C))/B \neq C$	
22	$x/e = x$	[2 → 3]
26	$(x/e)/e = x$	[22 → 22]
27	$(x/(x/y))/e = y$	[3 → 22]
167	$(x/e)/y = x/y$	[22 → 26 :(gL)]
239	$((x/y)/z)/e = (x/z)/y$	[26 → 167 :(gL), flip]
3177	$(x/((x/y)/z))/y = z$	[239 → 27]
3178	□	[3177,8]

In each of the next two theorems, the right-hand side is a single identity for Abelian groups in terms of the double inversion operation [16]. The context is Theorem 3 of [30]. Let e be an inflection point on the curve Γ. Then the binary morphism xy of chord-tangent construction on Γ is completely characterized by the single identity. See Fig. 3.1 on page 28.

Theorem #ABGT-7. The type is (2,0) with nullary e.

$$\left\{ \begin{array}{l} x(yx) = y \\ ex = xe \\ ee = e \end{array} \right\} \begin{array}{c} =\!(gL)\!\Rightarrow \\ \Leftarrow \end{array} \{(x((z(xy))(ey)))(ee) = z\}.$$

Proof ($\Rightarrow$) found by Otter 3.0.3l on gyro at 7.24 seconds.

1	$x = x$	
3,2	$e \cdot e = e$	
4	$e \cdot x = x \cdot e$	
6,5	$x \cdot (y \cdot x) = y$	
7	$(A \cdot ((C \cdot (A \cdot B)) \cdot (e \cdot B))) \cdot (e \cdot e) \neq C$	
8	$(A \cdot ((C \cdot (A \cdot B)) \cdot (e \cdot B))) \cdot e \neq C$	[copy,7 :3]
13	$(e \cdot x) \cdot (y \cdot (x \cdot e)) = y$	[4 → 5]
19,18	$(x \cdot y) \cdot x = y$	[5 → 5]
21,20	$e \cdot (e \cdot x) = x$	[4 → 5]
22	$x \cdot (x \cdot e) = e$	[4 → 5]
35	$x \cdot (x \cdot y) = y$	[20 → 22 :(gL) :21]
41	$(x \cdot y) \cdot y = x$	[18 → 35]
43	$x \cdot y = y \cdot x$	[5 → 35]
44	$(x \cdot y) \cdot (z \cdot (y \cdot u)) = (x \cdot v) \cdot (z \cdot (v \cdot u))$	[13 → 13 :(gL) :(gL)]
46	$(e \cdot x) \cdot y = (x \cdot e) \cdot y$	[18 → 13]
54	$(A \cdot (((A \cdot B) \cdot C) \cdot (e \cdot B))) \cdot e \neq C$	[43 → 8]

65,64	$(x \cdot y) \cdot (z \cdot (y \cdot x)) = z$	[43 → 5]
84	$(x \cdot y) \cdot z = (x \cdot u) \cdot (y \cdot (u \cdot z))$	[35 → 44]
129,128	$((x \cdot y) \cdot e) \cdot z = (e \cdot (y \cdot x)) \cdot z$	[43 → 46, flip]
473	$e \cdot ((((A \cdot B) \cdot C) \cdot (e \cdot B)) \cdot A) \neq C$	[64 → 54 :129,65]
540,539	$((x \cdot y) \cdot z) \cdot u = x \cdot (z \cdot (y \cdot u))$	[41 → 84]
593	$C \neq C$	[473 :540,6,19,6]
594	□	[593,1]

Proof ($\Leftarrow$) found by Otter 3.0.3l on gyro at 0.55 seconds.

1	$x = x$	
2	$e \cdot e = e,\ e \cdot A = A \cdot e,\ A \cdot (B \cdot A) = B\ \rightarrow$ □	
4,3	$(x \cdot ((y \cdot (x \cdot z)) \cdot (e \cdot z))) \cdot (e \cdot e) = y$	
5	$(e \cdot (x \cdot (e \cdot e))) \cdot (e \cdot e) = y \cdot ((x \cdot (y \cdot z)) \cdot (e \cdot z))$	[3 → 3]
7	$x \cdot ((y \cdot (x \cdot z)) \cdot (e \cdot z)) = u \cdot ((y \cdot (u \cdot v)) \cdot (e \cdot v))$	[5 → 5]
8	$x \cdot (((y \cdot (e \cdot e)) \cdot (x \cdot z)) \cdot (e \cdot z)) = y$	[3 → 5, flip]
11,10	$(e \cdot x) \cdot (e \cdot e) = e \cdot (x \cdot (e \cdot e))$	[5 → 3 :4]
13,12	$e \cdot (((x \cdot (e \cdot y)) \cdot (e \cdot y)) \cdot (e \cdot e)) = x$	[3 → 10, flip]
14	$(x \cdot (e \cdot ((x \cdot e) \cdot (e \cdot e)))) \cdot (e \cdot e) = e$	[10 → 3]
16	$e \cdot (e \cdot (e \cdot (e \cdot (e \cdot (e \cdot (e \cdot e)))))) = e$	[10 → 8 :11,11,11,11,11]
19,18	$e \cdot (((x \cdot y) \cdot y) \cdot (e \cdot e)) = x$	[12 → 12 :13]
20	$e \cdot (((x \cdot (e \cdot e)) \cdot y) \cdot y) = x$	[18 → 8 :19]
24	$((x \cdot e) \cdot x) \cdot (e \cdot e) = e$	[18 → 14]
27,26	$e \cdot (e \cdot e) = e$	[24 → 24]
29,28	$e \cdot e = e$	[16 :27,27,27]
30	$((x \cdot e) \cdot x) \cdot e = e$	[24 :29]
34	$e \cdot (((x \cdot e) \cdot y) \cdot y) = x$	[20 :29]
36	$e \cdot (((x \cdot y) \cdot y) \cdot e) = x$	[18 :29]
41,40	$(e \cdot x) \cdot e = e \cdot (x \cdot e)$	[10 :29,29]
44	$(x \cdot ((y \cdot (x \cdot z)) \cdot (e \cdot z))) \cdot e = y$	[3 :29]
46	$e \cdot A = A \cdot e,\ A \cdot (B \cdot A) = B\ \rightarrow$ □	[2 :29 :1]
47	$e \cdot ((e \cdot x) \cdot x) = (y \cdot e) \cdot y$	[30 → 34]
49,48	$e \cdot ((e \cdot x) \cdot x) = e$	[28 → 34]
50	$(x \cdot e) \cdot x = e$	[flip 47 :49]
53,52	$e \cdot (e \cdot x) = x$	[50 → 34]
54	$((x \cdot e) \cdot y) \cdot y = e \cdot x$	[34 → 52, flip]
62	$(e \cdot x) \cdot x = e$	[48 → 52 :29, flip]
64	$x \cdot (e \cdot x) = e$	[52 → 62]
67,66	$x \cdot ((y \cdot (x \cdot z)) \cdot (e \cdot z)) = e \cdot y$	[64 → 7 :53, flip]
68	$x \cdot ((y \cdot e) \cdot x) = e \cdot y$	[64 → 7 :53,67]
71,70	$e \cdot (x \cdot e) = x$	[44 :67,41]
75,74	$(x \cdot y) \cdot y = x$	[36 :71]
76	$x \cdot e = e \cdot x$	[54 :75]
77	$e \cdot x = x \cdot e$	[flip 76]
109,108	$x \cdot (y \cdot x) = y$	[74 → 68 :71]
112	□	[46 :109 :77,1]

Theorem #ABGT-8.

$$\left\{ \begin{array}{l} ee = e \\ (xe)e = x \\ x(xy) = y \end{array} \right\} \begin{array}{c} =(gL)\Rightarrow \\ \Longleftarrow \end{array} \{(x(((xy)z)(ye)))(ee) = z\}.$$

Proof ($\Rightarrow$) found by Otter 3.0.3l on gyro at 12.14 seconds.

1	$x = x$	
3,2	$e \cdot e = e$	
5,4	$(x \cdot e) \cdot e = x$	
7,6	$x \cdot (y \cdot x) = y$	
8	$(A \cdot (((A \cdot B) \cdot C) \cdot (B \cdot e))) \cdot (e \cdot e) \neq C$	
9	$(A \cdot (((A \cdot B) \cdot C) \cdot (B \cdot e))) \cdot e \neq C$	[copy,8 :3]
11,10	$(x \cdot y) \cdot x = y$	[6 → 6]
12	$e \cdot x = x \cdot e$	[4 → 6]
14,13	$x \cdot (x \cdot e) = e$	[4 → 10]
17,16	$e \cdot (e \cdot x) = x$	[12 → 12 :5]
30	$x \cdot (x \cdot y) = z \cdot (z \cdot y)$	[13 → 13 :(gL)]
34,33	$x \cdot (x \cdot y) = y$	[13 → 30 :14,17, flip]
39	$(x \cdot y) \cdot y = x$	[10 → 30 :34]
41	$x \cdot y = y \cdot x$	[6 → 30 :34]
45	$(x \cdot y) \cdot z = z \cdot (y \cdot x)$	[41 → 41]
121	$(x \cdot y) \cdot (z \cdot u) = (u \cdot z) \cdot (y \cdot x)$	[41 → 45]
126	$e \cdot ((((A \cdot B) \cdot C) \cdot (B \cdot e)) \cdot A) \neq C$	[45 → 9]
218	$(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u)$	[(gL) 121]
222,221	$((x \cdot y) \cdot z) \cdot (y \cdot u) = x \cdot (z \cdot u)$	[39 → 218, flip]
250	$C \neq C$	[126 :222,11,7]
251	$\Box$	[250,1]

Proof ($\Leftarrow$) found by Otter 3.0.3l on gyro at 0.38 seconds.

1	$x = x$	
2	$e \cdot e = e,\ (A \cdot e) \cdot e = A,\ A \cdot (B \cdot A) = B \ \rightarrow\ \Box$	
3	$(x \cdot (((x \cdot y) \cdot z) \cdot (y \cdot e))) \cdot (e \cdot e) = z$	
8,7	$(((x \cdot e) \cdot y) \cdot z) \cdot (y \cdot e) = (x \cdot z) \cdot (e \cdot e)$	[3 → 3, flip]
10	$x \cdot (((y \cdot x) \cdot (e \cdot e)) \cdot e) = (y \cdot (e \cdot e)) \cdot (e \cdot e)$	[3 → 7 :8]
14,13	$((x \cdot e) \cdot ((x \cdot y) \cdot (e \cdot e))) \cdot (e \cdot e) = y$	[7 → 3]
15	$(e \cdot e) \cdot ((x \cdot (e \cdot e)) \cdot e) = x \cdot (e \cdot e)$	[13 → 10 :14]
18,17	$(e \cdot e) \cdot (x \cdot e) = x$	[13 → 15 :14]
23	$((e \cdot e) \cdot e) \cdot (e \cdot e) = e$	[17 → 13]
29,28	$(e \cdot (x \cdot (e \cdot e))) \cdot (e \cdot e) = x \cdot e$	[17 → 3]
35	$((e \cdot e) \cdot e) \cdot e = e$	[23 → 28 :18, flip]
40,39	$(e \cdot e) \cdot e = e$	[17 → 28 :18, flip]

41	$(((x \cdot e) \cdot e) \cdot y) \cdot e = (x \cdot y) \cdot e$	[7 → 28 :29, flip]
46,45	$e \cdot e = e$	[35 :40]
54,53	$e \cdot (x \cdot e) = x$	[17 :46]
58	$x \cdot (((y \cdot x) \cdot e) \cdot e) = (y \cdot e) \cdot e$	[10 :46,46,46]
65	$(A \cdot e) \cdot e = A,\ A \cdot (B \cdot A) = B \ \rightarrow\ \Box$	[2 :46 :1]
68	$((x \cdot e) \cdot e) \cdot y = x \cdot y$	[41 → 53 :54, flip]
87,86	$(x \cdot e) \cdot e = x$	[68 → 53 :54, flip]
90	$A \cdot (B \cdot A) = B \ \rightarrow\ \Box$	[65 :87 :1]
91	$x \cdot (y \cdot x) = y$	[58 :87,87]
93	$\Box$	[91,90]

[[Background for the following?]]

Theorem #STN-1.

$$\{x(y(yx)) = yx, \text{cancellation}\} \ =\!(gL)\!\Rightarrow\ \ \{x(xy) = yx\}.$$

Proof (found by Otter 3.0.3l on gyro at 0.44 seconds).

1	$A \cdot (A \cdot B) = B \cdot A \ \rightarrow\ \Box$	
4	$x \cdot y = z,\ u \cdot y = z \ \rightarrow\ x = u$	
6,5	$x \cdot (y \cdot (y \cdot x)) = y \cdot x$	
9	$(x \cdot y) \cdot (z \cdot (z \cdot u)) = z \cdot (y \cdot (x \cdot u))$	[5 → 5 :(gL) :6]
10	$(x \cdot (x \cdot y)) \cdot (y \cdot z) = y \cdot (x \cdot z)$	[5 → 5 :(gL)]
33	$x \cdot (x \cdot y) = y \cdot x$	[4,10,9]
34	$\Box$	[33,1]

4.1.2 Quasigroups

[[RP: please give motivation and check the following.]]

Consider type (2,0) with nullary e, and let

$$\text{A1} = \left\{ \begin{array}{l} (xe)e = x \\ e(ex) = x \\ ee = e \\ e(xe) = (ex)e \end{array} \right\}, \qquad \text{A2} = \text{A1} \cup \{((xx)e)(xx) = e\}.$$

We first asked OTTER to prove

$$\text{A2} \ =\!(gL)\!\Rightarrow\ \left\{ \begin{array}{l} (xy)(zt) = (xz)(yt) \\ ((xx)y)(xx) = y \end{array} \right\}.$$

OTTER failed, but we noticed several interesting (gL)-consequences of axioms A2, including

$$(x((xy)x))x = y, \qquad (5)$$
$$x((x(yx))x) = y. \qquad (6)$$

E-mail from RP to WWM, 4 November, 1994:

Here what we want is already obtained by Otter, namely the two identities (5) and (6). The only purpose of this problem is to prove that any (gL)-algebra satisfying the axioms A2 must also satisfy all the identities true for all the three interpretations

$$a \cdot b = a - b,\ a \cdot b = -a + b,\ \text{or } a \cdot b = -a - b$$

in Abelian groups. What you have obtained is a basis for the equational theory of algebras of type (2,0) satisfying all the identities common to above three operations in abelian groups. This is because the two identities (5) and (6) imply the two cancellation laws and make the algebra a quasigroup at the same time. David Kelly and myself do already have such a basis (last line in Kelly-RP table) but our set involved four variables. The above result shows that, modulo (gL), we can define the same equational theory by a set of *one*-variable sentences, i.e. the axioms A2. That is a *new* result and that was the intent of the problem.

Now coming to the actual problem posed as above, is $((xx)y)(xx) = y$ a (gL)-consequence? Unfortunately, no. Interpret $x \cdot y$ as $x - y$ and e as 0, the zero in an Abelian group. This is a (gL)-algebra satisfying all the axioms (A2). This is also medial. However, $((x \cdot x) \cdot y) \cdot (x \cdot x) = (0 \cdot y) \cdot 0 = (-y) \cdot 0 = -y \neq y$ as claimed in the conclusion. No wonder OTTER could not derive this. I will write a new proof for the following.

Theorem. A (gL)-algebra of type (2,0) satisfies all the identities common to the three operations

$$a \cdot b = a - b,\ a \cdot b = -a + b,\ \text{or } a \cdot b = -a - b$$

iff it satisfies the one variable identities

$$\text{A2} = \left\{ \begin{array}{l} (xe)e = x \\ e(ex) = x \\ ee = e \\ e(xe) = (ex)e \\ ((xx)e)(xx) = e \end{array} \right\}.$$

The crucial step in the new proof will be the two identities (5) and (6).

From the above example, we can make the conjecture [Thm. #QGT-2 below] that

$$\text{A2}\ =\!(gL)\!\Rightarrow\ \{((xx)y)(xx) = (ey)e\},$$

because this identity is valid for all the three models. Thus this forms a test case. This was the original intention of the problem.

Theorem #QGT-1.

$$\text{A2} \;=\!(gL)\!\Rightarrow\; \left\{ \begin{array}{l} (x((xy)x))x = y \\ x((x(yx))x) = y \end{array} \right\}$$

Proof (found by Otter 3.0.3l on gyro at 85.81 seconds).

1	$x = x$	
2	$(A \cdot ((A \cdot B) \cdot A)) \cdot A = B,\ A \cdot ((A \cdot (B \cdot A)) \cdot A) = B \ \rightarrow\ \square$	
4,3	$(x \cdot e) \cdot e = x$	
6,5	$e \cdot (e \cdot x) = x$	
8,7	$e \cdot e = e$	
9	$e \cdot (x \cdot e) = (e \cdot x) \cdot e$	
10	$(e \cdot x) \cdot e = e \cdot (x \cdot e)$	[flip 9]
12	$((x \cdot x) \cdot e) \cdot (x \cdot x) = e$	
14	$(e \cdot x) \cdot (e \cdot y) = e \cdot (x \cdot y)$	[7 → 10 :(gL)]
16	$(x \cdot y) \cdot e = (x \cdot e) \cdot (y \cdot e)$	[7 → 10 :(gL)]
24,23	$(e \cdot x) \cdot y = e \cdot (x \cdot (e \cdot y))$	[5 → 14]
25	$(x \cdot y) \cdot (e \cdot z) = (x \cdot e) \cdot (y \cdot z)$	[7 → 14 :(gL)]
27	$x \cdot (y \cdot e) = e \cdot (y \cdot (x \cdot e))$	[10 → 14 :(gL) :6]
30	$((x \cdot x) \cdot y) \cdot (x \cdot x) = e \cdot (y \cdot e)$	[3 → 12 :(gL) :24,8]
63	$x \cdot y = e \cdot ((y \cdot e) \cdot (x \cdot e))$	[3 → 27]
66,65	$(x \cdot y) \cdot e = e \cdot (y \cdot x)$	[16 → 27 :4]
74	$(x \cdot e) \cdot (y \cdot e) = e \cdot (y \cdot x)$	[3 → 27]
108,107	$((x \cdot y) \cdot z) \cdot (e \cdot u) = e \cdot (z \cdot (e \cdot ((y \cdot x) \cdot u)))$	[65 → 25 :(gL) :24]
111	$x \cdot ((y \cdot z) \cdot u) = z \cdot ((y \cdot x) \cdot u)$	[25 → 25 :108,24,6,6,66,6]
160	$(x \cdot x) \cdot (y \cdot (x \cdot x)) = e \cdot (y \cdot e)$	[30 → 30 :(gL) :66,6]
175	$(x \cdot y) \cdot (z \cdot e) = e \cdot (y \cdot (e \cdot (z \cdot x)))$	[7 → 74 :(gL) :24]
294,293	$(x \cdot x) \cdot ((x \cdot x) \cdot y) = y$	[65 → 160 :(gL) :6]
411	$(x \cdot (x \cdot x)) \cdot (x \cdot e) = e$	[160 → 175 :8,8,8]
445	$(x \cdot (x \cdot x)) \cdot (x \cdot y) = y$	[293 → 411 :(gL) :294]
467	$(x \cdot y) \cdot ((y \cdot y) \cdot y) = x$	[63 → 445 :66,66,24,6,6]
645	$(x \cdot ((y \cdot y) \cdot y)) \cdot y = x$	[467 → 467 :294]
1087,1086	$x \cdot ((x \cdot (y \cdot x)) \cdot x) = y$	[467 → 111, flip]
1102	$(A \cdot ((A \cdot B) \cdot A)) \cdot A = B \ \rightarrow\ \square$	[2 :1087 :1]
1106	$(x \cdot ((x \cdot y) \cdot x)) \cdot x = y$	[111 → 645]
1108	$\square$	[1106,1102]

Theorem #QGT-2.

$$\text{A2} \;=\!(gL)\!\Rightarrow\; \{((xx)y)(xx) = (ey)e\}.$$

Proof (found by Otter 3.0.3l on gyro at 0.29 seconds).

2	$((A \cdot A) \cdot B) \cdot (A \cdot A) \neq (e \cdot B) \cdot e$

3	$(x \cdot e) \cdot e = x$	
5	$e \cdot (e \cdot x) = x$	
8,7	$e \cdot e = e$	
9	$e \cdot (x \cdot e) = (e \cdot x) \cdot e$	
11,10	$(e \cdot x) \cdot e = e \cdot (x \cdot e)$	[flip 9]
12	$((x \cdot x) \cdot e) \cdot (x \cdot x) = e$	
14	$((A \cdot A) \cdot B) \cdot (A \cdot A) \neq e \cdot (B \cdot e)$	[2 :11]
15	$(e \cdot x) \cdot (e \cdot y) = e \cdot (x \cdot y)$	[7 → 10 :(gL)]
25,24	$(e \cdot x) \cdot y = e \cdot (x \cdot (e \cdot y))$	[5 → 15]
31	$((x \cdot x) \cdot y) \cdot (x \cdot x) = e \cdot (y \cdot e)$	[3 → 12 :(gL) :25,8]
33	$\Box$	[31,14]

4.1.3 Boolean Groups

Theorem #TBG-1. The pair of identities $\{p(x,x,x) = x, p(x,y,p(z,u,v)) = p(y,z,p(u,v,x))\}$ is a (gL)-basis for the variety of Boolean groups, where $p(x,y,z)$ is $x + (y + z)$. It is sufficient to derive a basis for Boolean groups as follows.

$$\left\{ \begin{array}{l} p(x,x,x) = x \\ p(x,y,p(z,u,v)) = p(y,z,p(u,v,x)) \\ p(x,y,z) = x + (y + z) \end{array} \right\} \; =\!(gL)\!\Rightarrow \; \left\{ \begin{array}{l} (x + y) + z = x + (y + z) \\ x + x = y + y \\ x + (y + y) = x \end{array} \right\}.$$

Proof (found by Otter 3.0.3l on gyro at 10.29 seconds).

1	$x = x$	
2	$(A + B) + C = A + (B + C),\ B + B = A + A,\ A + (B + B) = A \ \rightarrow \ \Box$	
3	$p(x,x,x) = x$	
4	$p(x,y,p(z,u,v)) = p(y,z,p(u,v,x))$	
5	$p(x,y,z) = x + (y + z)$	
7,6	$(x + (x + x)) + (x + x) = x$	[3 → 3 :5,5]
13,12	$x + (x + x) = x$	[3 → 6 :5,7]
14	$x + (y + z) = y + (z + (z + (z + x)))$	[3 → 4 :5,5,5]
16,15	$x + (y + (z + (x + x))) = y + (z + x)$	[3 → 4 :5,5,5]
17	$x + (y + z) = y + (x + z)$	[(gL) 4 :5,5]
20,19	$x + (y + (x + x)) = y + x$	[12 → 17, flip]
26,25	$(x + x) + (y + x) = y + x$	[12 → 14 :13]
32	$x + (y + (y + (y + z))) = z + (x + y)$	[14 → 12 :13]
35,34	$(x + x) + ((x + x) + y) = x + (x + y)$	[19 → 19 :(gL)]
36	$x + (x + (y + x)) = y + x$	[17 → 19]
38	$x + (x + (x + (x + (x + y)))) = y + x$	[14 → 19]
43,42	$(x + x) + x = x$	[12 → 19 :26,13]
56	$((x + x) + y) + (x + x) = (x + y) + x$	[42 → 12 :(gL) :43]
61,60	$((x + y) + (x + y)) + z = (y + y) + z$	[25 → 25 :(gL)]
65,64	$(x + x) + (y + (z + x)) = y + (z + x)$	[19 → 25 :(gL) :61,20]
68,67	$(x + y) + ((x + y) + z) = y + (y + z)$	[25 → 34 :26,26,26,26,61,61,35,26, flip]

76,75	$x + ((y + x) + x) = y + x$	[14 → 36 :68,13]
80	$(x + (y + y)) + (y + y) = (x + y) + y$	[36 → 56 :65,20]
84	$(x + (y + y)) + y = (x + y) + (y + y)$	[12 → 56 :(gL) :26, flip]
96,95	$(x + y) + (z + y) = x + (y + (z + y))$	[12 → 75 :(gL) :13,16]
99	$((x + y) + y) + (x + (x + y)) = x + y$	[75 → 75 :76,96,76]
110	$(x + (y + y)) + y = x + y$	[84 :96,13]
125,124	$(x + (y + y)) + z = x + z$	[42 → 110 :(gL) :43]
143,142	$(x + y) + y = x + (y + y)$	[80 :125, flip]
145,144	$x + (x + (x + y)) = x + y$	[99 :143,125]
148	$x + y = y + x$	[38 :145,145]
149	$x + (y + z) = z + (x + y)$	[32 :145]
167	$x + (y + (z + y)) = x + z$	[36 → 148 :(gL)]
170,169	$x + (y + (z + z)) = x + y$	[19 → 148 :(gL)]
176,175	$(x + y) + z = x + (y + z)$	[15 → 148 :170, flip]
194	$x + (y + (x + z)) = y + z$	[36 → 148 :(gL) :176,176]
197,196	$x + (y + (y + z)) = x + z$	[19 → 148 :(gL) :176,176]
209	$B + B = A + A,\ A + (B + B) = A\ \rightarrow\ \Box$	[2 :176 :1]
222,221	$x + (y + y) = x$	[12 → 167 :176,197]
224	$B + B = A + A\ \rightarrow\ \Box$	[209 :222 :1]
231,230	$x + (y + x) = y$	[149 → 221]
236	$x + x = A + A\ \rightarrow\ \Box$	[194 → 224 :231]
237	$\Box$	[236,221]

The preceding theorem arose by accident as we were trying to write axioms for semilattices in terms of a ternary operation p. Semilattices are inconsistent with $=\!(gL)\!\Rightarrow$ (Thm. #LT-6), so we expected OTTER to derive $x = y$ from our identities. OTTER failed to do this, and we noticed instead that p was shown to be a minority polynomial, $p(x, x, y) = p(x, y, x) = p(y, x, x) = y$. We soon realized that what we had written was in fact a (gL)-basis for Boolean groups in terms of a ternary operation, a system we had not previously considered. Note also that the preceding OTTER proof shows that a nonregular identity can be derived by $=\!(gL)\!\Rightarrow$ from a set of regular identities; this cannot happen in ordinary equational logic. (An identity is *regular* if the same set of variables occurs on both sides of the equal sign).

4.2 Equations Strictly Inconsistent with $=\!(gL)\!\Rightarrow$

The philosophy behind the Thms. #PIX-1, #MAJ-4, #LT-6, and #LT-6a (all previously known) is that there are no polynomially defined semilattice or lattice laws on say, the reals, rationals or the complex numbers. Hence, modulo the process $=\!(gL)\!\Rightarrow$, a semilattice will be "crushed" into a singleton! The validity of the implication made in Thm. #PIX-1 was proved by Padmanabhan, actually via Thm. #MAJ-4.

The following theorem shows that any theory that contains a term satisfying the so-called Pixley properties **??**, which characterize the permutability and distributivity of congruences of an equational class of algebras, is inconsistent with $=\!(gL)\!\Rightarrow$. An example is Boolean algebra, with $p(x,y,z) = xy' + xz + y'z$.

Theorem #PIX-1.

$$\{p(y,y,x) = p(x,z,z) = p(x,u,x) = x\} \;=\!(gL)\!\Rightarrow\; \{x = y\}.$$

Proof (found by Otter 3.0.3l on gyro at 0.11 seconds).

1	$B \neq A$	
4,3	$p(x,x,y) = y$	
6,5	$p(x,y,y) = x$	
7	$p(x,y,x) = x$	
11,10	$p(x,y,z) = x$	[5 → 7 :(gL) :6,6]
12	$x = y$	[3 → 7 :(gL) :4,11,4]
13	$\Box$	[12,1]

The next theorem says that no theory containing a ternary majority polynomial [26] will satisfy the rule $=\!(gL)\!\Rightarrow$. In particular, lattice theory does not satisfy this rule.

Theorem #MAJ-4.

$$\{p(x,x,y) = p(x,y,x) = p(y,x,x) = x\} \;=\!(gL)\!\Rightarrow\; \{x = y\}.$$

Proof (found by Otter 3.0.3l on gyro at 0.27 seconds).

1	$B \neq A$	
3	$p(x,x,y) = x$	
4	$p(x,y,x) = x$	
5	$p(x,y,y) = y$	
11	$p(x,y,z) = p(x,y,u)$	[3 → 3 :(gL)]
41	$p(x,y,z) = x$	[4 → 11, flip]
53	$p(x,y,z) = p(u,y,z)$	[5 → 5 :(gL)]
65	$p(x,y,z) = u$	[53 → 41]
66	$x = y$	[65 → 65]
67	$\Box$	[66,1]

The following theorem shows directly that any theory containing a semilattice operation is inconsistent with $=\!(gL)\!\Rightarrow$.

Theorem #LT-6. Semilattice on a cubic curve.

$$\left\{ \begin{array}{l} x \cdot x = x \\ x \cdot (y \cdot z) = y \cdot (z \cdot x) \end{array} \right\} \; =\!(gL)\!\Rightarrow \; \{x = y\}.$$

Proof (found by Otter 3.0.3l on gyro at 0.11 seconds).

1	$B \neq A$	
4,3	$x \cdot x = x$	
5	$x \cdot (y \cdot z) = y \cdot (z \cdot x)$	
10	$x \cdot (y \cdot (z \cdot y)) = x \cdot y$	[3 $\rightarrow$ 5 :(gL), flip]
12	$(x \cdot y) \cdot (z \cdot u) = z \cdot (y \cdot (u \cdot x))$	[5 $\rightarrow$ 5]
15,14	$x \cdot (y \cdot x) = y \cdot x$	[3 $\rightarrow$ 5]
21,20	$x \cdot (y \cdot z) = x \cdot z$	[10 :15]
25,24	$x \cdot y = y$	[14 :21,4, flip]
26	$x = y$	[12 :25,25,25,25,25,25]
27	$\Box$	[26,1]

The next theorem shows that a fragment of Boolean algebra satisfying some set difference properties is inconsistent with $=\!(gL)\!\Rightarrow$.

Theorem #LT-6a.

$$\left\{ \begin{array}{l} x - (y - x) = x \\ x - (x - y) = y - (y - x) \end{array} \right\} \; =\!(gL)\!\Rightarrow \; \{x = y\}.$$

Proof (found by Otter 3.0.3l on gyro at 0.26 seconds).

1	$A \neq B$	
4,3	$x - (y - x) = x$	
5	$x - (x - y) = y - (y - x)$	
8,7	$(x - y) - z = x - z$	[3 $\rightarrow$ 3 :(gL)]
10,9	$x - (y - (z - u)) = x - u$	[3 $\rightarrow$ 7 :(gL), flip]
16,15	$x - x = x$	[5 $\rightarrow$ 5 :10,8,8,4]
18,17	$x - y = y$	[3 $\rightarrow$ 5 :16,8,16, flip]
19	$x = y$	[7 $\rightarrow$ 5 :18,18,18,18,18]
20	$\Box$	[19,1]

4.3 Quasigroups and Overlay Conditions

[[RP: we need an introduction]].

Theorem #OC-GL-1. Binary overlay for quasigroup.

$$\left\{\begin{array}{l} \cdot \text{ is a quasigroup} \\ g(x,e) = f(x,e) \\ g(e,x) = f(e,x) \end{array}\right\} \Rightarrow (gL) \Rightarrow \{g(x,y) = f(x,y)\}.$$

Proof (found by Otter 3.0.3l on gyro at 56.88 seconds).

1	$g(A,B) \neq f(A,B)$	
6,5	$x\backslash(x \cdot y) = y$	
7	$(x/y) \cdot y = x$	
9	$(x \cdot y)/y = x$	
11	$g(x,e) = f(x,e)$	
12	$g(e,x) = f(e,x)$	
13	$(x/y)\backslash x = y$	[7 → 5]
17	$(x \cdot g(y,e))/f(y,e) = x$	[11 → 9]
33	$(x \cdot g(e,y))/f(e,y) = x$	[12 → 9]
65	$(x \cdot g(y,z))/f(y,u) = (x \cdot g(v,z))/f(v,u)$	[17 → 17 :(gL) :(gL)]
124	$(x \cdot g(y,z))/f(y,z) = x$	[65 → 33]
592	$g(x,y) = f(x,y)$	[124 → 13 :6]
593	$\square$	[592,1]

Corollary #OC-GL-2. Binary overlay with Steiner law.

$$\left\{\begin{array}{l} x \cdot (y \cdot x) = y \\ g(x,e) = f(x,e) \\ g(e,x) = f(e,x) \end{array}\right\} \Rightarrow (gL) \Rightarrow \{g(x,y) = f(x,y)\}.$$

This follows immediately from Thm. #OC-GL-1, because the Steiner law implies that "$\cdot$" is a quasigroup.

Theorem #OC-GL-3. Ternary overlay for quasigroup.

$$\left\{\begin{array}{l} \cdot \text{ is a quasigroup} \\ g(x,e,e) = f(x,e,e) \\ g(e,x,e) = f(e,x,e) \\ g(e,e,x) = f(e,e,x) \end{array}\right\} \Rightarrow (gL) \Rightarrow \{g(x,y,z) = f(x,y,z)\}.$$

Proof (found by Otter 3.0.3l on gyro at 711.36 seconds).

1	$g(A,B,C) \neq f(A,B,C)$
6,5	$x\backslash(x \cdot y) = y$
7	$(x/y) \cdot y = x$
9	$(x \cdot y)/y = x$
11	$g(x,e,e) = f(x,e,e)$

12	$g(e,x,e) = f(e,x,e)$	
13	$g(e,e,x) = f(e,e,x)$	
14	$(x/y)\backslash x = y$	[7 → 5]
18	$(x \cdot g(y,e,e))/f(y,e,e) = x$	[11 → 9]
42	$(x \cdot g(e,y,e))/f(e,y,e) = x$	[12 → 9]
66	$(x \cdot g(e,e,y))/f(e,e,y) = x$	[13 → 9]
90	$(x \cdot g(y,z,u))/f(y,v,w) = (x \cdot g(v_6,z,u))/f(v_6,v,w)$	[18 → 18 :(gL) :(gL) :(gL) :(gL)]
107	$((x \cdot g(y,z,u))/f(y,v,w))\backslash(x \cdot g(v_6,z,u)) = f(v_6,v,w)$	[90 → 14]
224	$(x \cdot g(y,z,e))/f(y,z,e) = x$	[90 → 42]
406	$(x \cdot g(y,z,u))/f(v,w,u) = (x \cdot g(y,z,v_6))/f(v,w,v_6)$	[66 → 66 :(gL) :(gL) :(gL) :(gL)]
1602	$(x \cdot g(y,z,u))/f(y,z,u) = x$	[224 → 406, flip]
2470	$g(x,y,z) = f(x,y,z)$	[1602 → 107 :6]
2471	□	[2470,1]

Corollary #OC-GL-4. Ternary overlay with Steiner law.

$$\left\{ \begin{array}{l} x \cdot (y \cdot x) = y \\ g(x,e,e) = f(x,e,e) \\ g(e,x,e) = f(e,x,e) \\ g(e,e,x) = f(e,e,x) \end{array} \right\} =\!(gL)\!\Rightarrow \{g(x,y,z) = f(x,y,z)\}.$$

This follows immediately from Thm. #OC-GL-3, because the Steiner law implies that "$\cdot$" is a quasigroup.

4.4 Closure Conditions and $=\!(gL)\!\Rightarrow$

[[Need introduction.]] [[These theorems don't use $=\!(gL)\!\Rightarrow$, so why are they in this chapter??]]

Thomsen Closure Condition (TC)

$$\left\{ \begin{array}{l} z_1 \cdot x = z_2 \cdot y \\ z_1 \cdot z = z_3 \cdot y \end{array} \right\} \Rightarrow \{z_2 \cdot z = z_3 \cdot x\}.$$

Reidemeister Closure Condition (RC)

$$\left\{ \begin{array}{l} z_1 \cdot x = z_2 \cdot y \\ z_3 \cdot x = z_4 \cdot y \\ z_1 \cdot u = z_2 \cdot v \end{array} \right\} \Rightarrow \{z_3 \cdot u = z_4 \cdot v\}.$$

Theorem #TC-2.

$$\left\{ \begin{array}{l} \text{TC} \\ \text{quasigroup} \end{array} \right\} \Rightarrow \text{RC}.$$

Proof (found by Otter 3.0.3l on gyro at 5.37 seconds).

1	$x = x$	
2	$x \cdot y = z,\ u \cdot v = z,\ x \cdot w = v_6,\ v_7 \cdot v = v_6 \ \rightarrow\ u \cdot w = v_7 \cdot y$	
3	$x \cdot (x \backslash y) = y$	
6,5	$x \backslash (x \cdot y) = y$	
7	$(x/y) \cdot y = x$	
11	$C_4 \cdot A = C_3 \cdot B$	
13	$C_2 \cdot A = C_1 \cdot B$	
15	$C_4 \cdot F = C_3 \cdot E$	
17	$C_2 \cdot F = C_1 \cdot E \ \rightarrow\ \square$	
31	$C_4 \cdot (C_3 \backslash x) = (x/A) \cdot B$	[2,3,7,1,11, flip]
85	$C_2 \cdot (C_1 \backslash x) = (x/A) \cdot B$	[2,3,7,1,13, flip]
1078	$C_2 \cdot F = C_1 \cdot E$	[2,15,3,31,85 :6, flip]
1080	$\square$	[1078,17]

Theorem #TC-3.

$$\left\{ \begin{array}{l} \text{TC} \\ e \cdot x = x \\ x \cdot e = x \end{array} \right\} \Rightarrow \text{RC.}$$

Proof (found by Otter 3.0.3l on gyro at 2.33 seconds).

1	$x = x$	
2	$x \cdot y = z,\ u \cdot v = z,\ x \cdot w = v_6,\ v_7 \cdot v = v_6 \ \rightarrow\ u \cdot w = v_7 \cdot y$	
3	$e \cdot x = x$	
5	$x \cdot e = x$	
7	$C_4 \cdot A = C_3 \cdot B$	
9	$C_2 \cdot A = C_1 \cdot B$	
11	$C_4 \cdot F = C_3 \cdot E$	
13	$C_2 \cdot F = C_1 \cdot E \ \rightarrow\ \square$	
15	$x \cdot y = y \cdot x$	[2,3,5,3,5]
40	$C_4 \cdot C_1 = C_2 \cdot C_3$	[2,15,9,15,7, flip]
77	$E \cdot C_1 = C_2 \cdot F$	[2,11,15,40,1]
207	$C_2 \cdot F = C_1 \cdot E$	[15 $\rightarrow$ 77, flip]
209	$\square$	[207,13]

Theorem #TC-4.

$$\left\{ \begin{array}{l} \text{TC} \\ x \cdot e = x \end{array} \right\} \Rightarrow \text{RC.}$$

Counterexample. The clauses

$$x = x$$

$z_1 \cdot x \neq u | z_2 \cdot y \neq u | z_1 \cdot z \neq w | z_3 \cdot y \neq w | z_2 \cdot z = z_3 \cdot x$
$x \cdot e = x$
$C_4 \cdot A = C_3 \cdot B$
$C_2 \cdot A = C_1 \cdot B$
$C_4 \cdot F = C_3 \cdot E$
$C_2 \cdot F \neq C_1 \cdot E$

have the following model (found by MACE 1.1.0 on gyro at 0.87 seconds).

```
* :
      | 0 1 2
   --+------
   0  | 0 0 0
   1  | 1 1 2
   2  | 2 2 1
e: 0
C4: 0
A: 0
C3: 0
B: 0
C2: 1
C1: 1
F: 0
E: 2
end_of_model
```

Theorem #TC-5.

$$\left\{ \begin{array}{l} \text{TC} \\ (x \cdot e) \cdot e = x \\ e \cdot (e \cdot x) = x \end{array} \right\} \Rightarrow \text{RC}.$$

Proof (found by Otter 3.0.3l on gyro at 57.18 seconds).

1	$x = x$	
2	$x \cdot y = z,\ u \cdot v = z,\ x \cdot w = v_6,\ v_7 \cdot v = v_6 \ \rightarrow\ u \cdot w = v_7 \cdot y$	
4,3	$(x \cdot e) \cdot e = x$	
6,5	$e \cdot (e \cdot x) = x$	
7	$C_4 \cdot A = C_3 \cdot B$	
9	$C_2 \cdot A = C_1 \cdot B$	
11	$C_4 \cdot F = C_3 \cdot E$	
13	$C_2 \cdot F = C_1 \cdot E \ \rightarrow\ \square$	
20	$((e \cdot x) \cdot e) \cdot (e \cdot (y \cdot e)) = y \cdot x$	[2,1,3,5,1]
22	$x \cdot y = ((e \cdot y) \cdot e) \cdot (e \cdot (x \cdot e))$	[2,5,1,1,3]
39	$((e \cdot E) \cdot e) \cdot A = ((e \cdot B) \cdot e) \cdot F$	[2,11,20,7,20]
60	$((e \cdot E) \cdot e) \cdot (e \cdot (C_1 \cdot e)) = C_2 \cdot F$	[2,20,9,1,39, flip]
70	$C_2 \cdot F = C_1 \cdot E$	[22 → 60 :6,4,4,6, flip]

72 $\square$ [70,13]

Theorem #TC-6.

$$\left\{ \begin{array}{l} \text{TC} \\ ((x \cdot e) \cdot e) \cdot e = x \\ e \cdot (e \cdot (e \cdot x)) = x \end{array} \right\} \Rightarrow \text{RC}.$$

Proof (found by Otter 3.0.3l on gyro at 74.72 seconds).

1 $x = x$
2 $x \cdot y = z,\ u \cdot v = z,\ x \cdot w = v_6,\ v_7 \cdot v = v_6 \ \rightarrow\ u \cdot w = v_7 \cdot y$
4,3 $((x \cdot e) \cdot e) \cdot e = x$
6,5 $e \cdot (e \cdot (e \cdot x)) = x$
7 $C_4 \cdot A = C_3 \cdot B$
9 $C_2 \cdot A = C_1 \cdot B$
11 $C_4 \cdot F = C_3 \cdot E$
13 $C_2 \cdot F = C_1 \cdot E \ \rightarrow\ \square$
14 $(((x \cdot y) \cdot e) \cdot e) \cdot z = (((x \cdot z) \cdot e) \cdot e) \cdot y$ [2,1,3,1,3]
18,17 $(((C_2 \cdot x) \cdot e) \cdot e) \cdot A = (((C_1 \cdot B) \cdot e) \cdot e) \cdot x$ [2,1,3,9,3]
33 $x \cdot (e \cdot (e \cdot y)) = ((y \cdot e) \cdot e) \cdot (e \cdot (e \cdot (x \cdot e)))$ [2,5,1,5,3]
36 $(((e \cdot x) \cdot e) \cdot e) \cdot (e \cdot (e \cdot (y \cdot e))) = y \cdot x$ [2,1,3,5,1]
293 $(((e \cdot E) \cdot e) \cdot e) \cdot A = (((e \cdot B) \cdot e) \cdot e) \cdot F$ [2,11,36,7,36]
418,417 $(((e \cdot E) \cdot e) \cdot e) \cdot (e \cdot (e \cdot (C_1 \cdot B))) = (((C_2 \cdot F) \cdot e) \cdot e) \cdot B$ [2,36,17,36,293 :4,6,4, flip]
423 $(((C_2 \cdot F) \cdot e) \cdot e) \cdot B = (((C_1 \cdot B) \cdot e) \cdot e) \cdot E$ [2,33,17,293,293 :4,6,18,418, flip]
515 $C_2 \cdot F = C_1 \cdot E$ [2,3,14,3,423 :4,4, flip]
517 $\square$ [515,13]

Theorem #TC-7.

$$\left\{ \begin{array}{l} \text{TC} \\ \text{semilattice} \end{array} \right\} \Rightarrow \{x = y\}.$$

Proof (found by Otter 3.0.3l on gyro at 0.40 seconds).

1 $x = x$
2 $x \cdot y = z,\ u \cdot v = z,\ x \cdot w = v_6,\ v_7 \cdot v = v_6 \ \rightarrow\ u \cdot w = v_7 \cdot y$
4,3 $x \cdot x = x$
5 $x \cdot y = y \cdot x$
7,6 $(x \cdot y) \cdot z = x \cdot (y \cdot z)$
8 $B = A \ \rightarrow\ \square$
24 $x \cdot (x \cdot y) = x \cdot y$ [2,6,3,6,1 :7,4]
27,26 $x \cdot (y \cdot x) = y \cdot x$ [2,5,3,6,1 :7,4]
43,42 $x \cdot y = y$ [2,5,3,5,24 :7,27,4]

44	$x = y$	[2,5,1,3,24 :43,43,43]
45	□	[44,8]

Theorem #RC-1.

$$\left\{ \begin{array}{l} \text{RC} \\ \text{semilattice} \end{array} \right\} \Rightarrow \{x = y\}.$$

Proof (found by Otter 3.0.3l on gyro at 0.55 seconds).

1	$x = x$	
2	$x \cdot y = z,\ u \cdot v = z,\ w \cdot y = v_6,\ v_7 \cdot v = v_6,\ x \cdot v_8 = v_9,\ u \cdot v_{10} = v_9\ \rightarrow\ w \cdot v_8 = v_7 \cdot v_{10}$	
4,3	$x \cdot x = x$	
5	$x \cdot y = y \cdot x$	
7,6	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	
8	$B = A\ \rightarrow$ □	
9	$x \cdot (y \cdot x) = y \cdot x$	[2,5,3,5,3,1,5 :7,4]
16,15	$x \cdot y = y$	[2,9,9,9,3,1,9 :4,4,7,4, flip]
17	$x = y$	[2,9,9,5,5,5,9 :16,16,16]
18	□	[17,8]

Theorem #TC-8.

$$\left\{ \begin{array}{l} \text{TC} \\ m(x,y,z) = ((y \cdot y) \cdot x) \cdot (z \cdot y) \\ x \cdot (y \cdot x) = y \end{array} \right\} \Rightarrow \{m(x,y,m(z,u,v)) = m(m(x,y,z),u,v)\}.$$

Proof (found by Otter 3.0.3l on gyro at 15.49 seconds).

1	$x = x$	
2	$x \cdot y = z,\ u \cdot v = z,\ x \cdot w = v_6,\ v_7 \cdot v = v_6\ \rightarrow\ u \cdot w = v_7 \cdot y$	
4,3	$m(x,y,z) = ((y \cdot y) \cdot x) \cdot (z \cdot y)$	
5	$x \cdot (y \cdot x) = y$	
7	$m(A,B,m(C,D,E)) = m(m(A,B,C),D,E)\ \rightarrow$ □	
8	$((B \cdot B) \cdot A) \cdot ((((D \cdot D) \cdot C) \cdot (E \cdot D)) \cdot B) = ((D \cdot D) \cdot (((B \cdot B) \cdot A) \cdot (C \cdot B))) \cdot (E \cdot D)$ -	
14	$(x \cdot y) \cdot x = y$	[5 → 5]
17	$(x \cdot ((y \cdot z) \cdot u)) \cdot y = (x \cdot z) \cdot u$	[2,14,14,1,14, flip]
19	$x \cdot (y \cdot (z \cdot u)) = ((u \cdot x) \cdot y) \cdot z$	[2,14,5,5,14]
784	$x \cdot (((y \cdot z) \cdot u) \cdot v) = (y \cdot ((((v \cdot w) \cdot x) \cdot z) \cdot u)) \cdot w$	[2,1,5,5,17]
1734,1733	$(x \cdot ((((y \cdot z) \cdot u) \cdot v) \cdot w)) \cdot z = (x \cdot (u \cdot (v \cdot y))) \cdot w$	[19 → 17]
1752	$x \cdot (((y \cdot z) \cdot u) \cdot v) = (y \cdot (x \cdot (z \cdot v))) \cdot u$	[784 :1734]
1753	□	[1752,8]

Theorem #TC-9.

$$\left\{ \begin{array}{l} \text{TC} \\ x \cdot (y \cdot x) = y \end{array} \right\} \Rightarrow \{(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u)\}.$$

Proof (found by Otter 3.0.3l on gyro at 0.11 seconds).

2	$x \cdot y = z,\ u \cdot v = z,\ x \cdot w = v_6,\ v_7 \cdot v = v_6 \ \rightarrow\ u \cdot w = v_7 \cdot y$	
3	$x \cdot (y \cdot x) = y$	
5	$(A \cdot C) \cdot (B \cdot D) = (A \cdot B) \cdot (C \cdot D) \ \rightarrow\ \Box$	
11	$(x \cdot y) \cdot x = y$	[3 → 3]
19	$(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u)$	[2,3,11,3,11]
20	$\Box$	[19,5]

[[In the following, the conclusion is equivalent to the median law. SHould we change it?]]

Theorem #RC-2.

$$\left\{ \begin{array}{l} \text{RC} \\ x \cdot y = y \cdot x \\ x \cdot (y \cdot x) = y \end{array} \right\} \Rightarrow \{((x \cdot y) \cdot z) \cdot (u \cdot x) = y \cdot (z \cdot u)\}.$$

Proof (found by Otter 3.0.3l on gyro at 9.56 seconds).

2	$x \cdot y = z,\ u \cdot v = z,\ w \cdot y = v_6,\ v_7 \cdot v = v_6,\ x \cdot v_8 = v_9,\ u \cdot v_{10} = v_9 \ \rightarrow\ w \cdot v_8 = v_7 \cdot v_{10}$	
3	$x \cdot y = y \cdot x$	
4	$x \cdot (y \cdot x) = y$	
6	$((A \cdot B) \cdot C) \cdot (D \cdot A) = B \cdot (C \cdot D) \ \rightarrow\ \Box$	
68	$(x \cdot y) \cdot x = y$	[4 → 4]
70	$x \cdot (x \cdot y) = y$	[3 → 4]
1006	$((x \cdot y) \cdot z) \cdot (u \cdot x) = y \cdot (z \cdot u)$	[2,70,70,68,4,4,70]
1008	$\Box$	[1006,6]

Theorem #RC-3.

$$\left\{ \begin{array}{l} \text{RC} \\ x \cdot e = x \\ e \cdot x = x \end{array} \right\} \Rightarrow \{(x \cdot y) \cdot z = x \cdot (y \cdot z)\}.$$

Proof (found by Otter 3.0.3l on gyro at 0.21 seconds).

1	$x = x$
2	$x \cdot y = z,\ u \cdot v = z,\ w \cdot y = v_6,\ v_7 \cdot v = v_6,\ x \cdot v_8 = v_9,\ u \cdot v_{10} = v_9 \ \rightarrow\ w \cdot v_8 = v_7 \cdot v_{10}$
3	$x \cdot e = x$

5	$e \cdot x = x$	
7	$(A \cdot B) \cdot C = A \cdot (B \cdot C) \ \rightarrow \ \square$	
8	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	[2,3,5,3,1,1,5]
10	$\square$	[8,7]

Theorem #RC-4.

$$\left\{ \begin{array}{l} \text{RC} \\ x \cdot e = x \\ x \cdot (x \cdot y) = y \end{array} \right\} \Rightarrow \{(x \cdot (e \cdot y)) \cdot (e \cdot c) = x \cdot (e \cdot (y \cdot (e \cdot c)))\}.$$

Proof (found by Otter 3.0.3l on gyro at 0.11 seconds).

1	$x = x$	
2	$x \cdot y = z, \ u \cdot v = z, \ w \cdot y = v_6, \ v_7 \cdot v = v_6, \ x \cdot v_8 = v_9, \ u \cdot v_{10} = v_9 \ \rightarrow \ w \cdot v_8 = v_7 \cdot v_{10}$	
3	$x \cdot e = x$	
5	$x \cdot (x \cdot y) = y$	
7	$(A \cdot (e \cdot B)) \cdot (e \cdot C) = A \cdot (e \cdot (B \cdot (e \cdot C))) \ \rightarrow \ \square$	
12	$(x \cdot (y \cdot z)) \cdot u = x \cdot (y \cdot (z \cdot u))$	[2,3,5,3,1,1,5]
14	$\square$	[12,7]

Theorem #TC-10.

$$\left\{ \begin{array}{l} \text{TC} \\ e \cdot e = e \\ (x \cdot e) \cdot e = x \\ x \cdot (x \cdot y) = y \end{array} \right\} \Rightarrow \{(x \cdot (((x \cdot y) \cdot z) \cdot (y \cdot e))) \cdot (e \cdot e) = z\}.$$

The conclusion is a single axiom for Abelian groups in terms of $-x - y$.

Proof (found by Otter 3.0.3l on gyro at 1.19 seconds).

1	$x = x$	
2	$x \cdot y = z, \ u \cdot v = z, \ x \cdot w = v_6, \ v_7 \cdot v = v_6 \ \rightarrow \ u \cdot w = v_7 \cdot y$	
4,3	$e \cdot e = e$	
6,5	$(x \cdot e) \cdot e = x$	
7	$x \cdot (y \cdot x) = y$	
9	$(A \cdot (((A \cdot B) \cdot C) \cdot (B \cdot e))) \cdot (e \cdot e) = C \ \rightarrow \ \square$	
10	$(A \cdot (((A \cdot B) \cdot C) \cdot (B \cdot e))) \cdot e = C \ \rightarrow \ \square$	[copy,9 :4]
30	$e \cdot x = x \cdot e$	[2,5,3,7,1 :4,6]
39,38	$(x \cdot y) \cdot x = y$	[7 → 7]
50	$x \cdot y = y \cdot x$	[2,30,5,30,5 :6,6]
55,54	$(x \cdot y) \cdot y = x$	[2,38,38,5,38 :6, flip]
180,179	$(((x \cdot y) \cdot z) \cdot u) \cdot x = z \cdot (u \cdot y)$	[2,7,38,50,7]
195	$C = C \ \rightarrow \ \square$	[50 → 10 :180,39,55]
196	$\square$	[195,1]

Theorem #TC-11.

$$\left\{ \begin{array}{l} \text{TC} \\ e \cdot x = x \\ x \cdot e = x \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} x \cdot y = y \cdot x \\ (x \cdot y) \cdot z = x \cdot (y \cdot z) \end{array} \right\}.$$

Proof (found by Otter 3.0.3l on gyro at 0.57 seconds).

1	$x = x$	
2	$x \cdot y = z,\ u \cdot v = z,\ x \cdot w = v_6,\ v_7 \cdot v = v_6 \ \rightarrow\ u \cdot w = v_7 \cdot y$	
3	$B \cdot A = A \cdot B,\ (A \cdot B) \cdot C = A \cdot (B \cdot C) \ \rightarrow\ \Box$	
4	$e \cdot x = x$	
7,6	$x \cdot e = x$	
8	$x \cdot (y \cdot z) = y \cdot (x \cdot z)$	[2,4,1,4,1]
9	$x \cdot y = y \cdot x$	[2,4,6,4,6]
32,31	$(x \cdot y) \cdot z = y \cdot (x \cdot z)$	[2,6,9,8,9 :7, flip]
45	$\Box$	[3 :32 :9,8]

Theorem #TC-12.

$$\left\{ \begin{array}{l} \text{TC} \\ p(x,y) = e \cdot (y \cdot x) \\ x \cdot (y \cdot x) = y \\ x \cdot e = e \cdot x \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} p(x,y) = p(y,x) \\ p(p(x,y),z) = p(x,p(y,z)) \end{array} \right\}.$$

Proof (found by Otter 3.0.3l on gyro at 2.20 seconds).

1	$x = x$	
2	$x \cdot y = z,\ u \cdot v = z,\ x \cdot w = v_6,\ v_7 \cdot v = v_6 \ \rightarrow\ u \cdot w = v_7 \cdot y$	
4,3	$p(x,y) = e \cdot (y \cdot x)$	
5	$x \cdot (y \cdot x) = y$	
7	$x \cdot e = e \cdot x$	
8	$p(A,B) = p(B,A),\ p(p(A,B),C) = p(A,p(B,C)) \ \rightarrow\ \Box$	
9	$e \cdot (B \cdot A) = e \cdot (A \cdot B),\ e \cdot ((e \cdot (C \cdot B)) \cdot A) = e \cdot (C \cdot (e \cdot (B \cdot A))) \ \rightarrow\ \Box$	[copy,8 :4,4,4,4,4,4, flip]
17,16	$(x \cdot y) \cdot x = y$	[5 → 5]
19	$x \cdot y = y \cdot x$	[2,5,7,1,7 :17]
115	$x \cdot (x \cdot y) = y$	[16 → 19, flip]
117	$(x \cdot y) \cdot y = x$	[5 → 19, flip]
119	$x \cdot (y \cdot z) = x \cdot (z \cdot y)$	[2,115,115,5,115]
243,242	$(x \cdot (y \cdot z)) \cdot u = y \cdot (x \cdot (z \cdot u))$	[2,117,115,5,117, flip]
348	$\Box$	[9 :243 :119,1]

Theorem #RC-5. Do all quasigroups satisfy RC?

Counterexample. The clauses

$C_4 \cdot A = C_3 \cdot B$
$C_2 \cdot A = C_1 \cdot B$
$C_4 \cdot F = C_3 \cdot E$
$C_2 \cdot F \neq C_1 \cdot E$

```
properties(_*_, quasigroup).
```

have the following quasigroup model (found by MACE 1.1.0 on gyro at 7.19 seconds).

```
* :
     | 0 1 2 3 4
   --+----------
   0 | 0 1 2 3 4
   1 | 1 4 0 2 3
   2 | 2 3 1 4 0
   3 | 3 0 4 1 2
   4 | 4 2 3 0 1
C4: 0
A: 0
C3: 1
B: 2
C2: 1
C1: 2
F: 1
E: 0
end_of_model
```

Theorem #TC-13. Cancellative medial algebras satisfy TC.

$$\left\{ \begin{array}{l} (x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u) \\ \text{cancellation} \end{array} \right\} \Rightarrow \text{TC}.$$

Proof (found by Otter 3.0.3l on gyro at 1.11 seconds).

2	$x \cdot y = z,\ x \cdot u = z \ \rightarrow\ y = u$	
4	$(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u)$	
5	$C_3 \cdot A = C_2 \cdot B$	
7	$C_3 \cdot D = C_1 \cdot B$	
9	$C_2 \cdot D = C_1 \cdot A \ \rightarrow\ \square$	
14	$(x \cdot y) \cdot (C_2 \cdot B) = (x \cdot C_3) \cdot (y \cdot A)$	[5 → 4]
17	$(x \cdot C_3) \cdot (y \cdot A) = (x \cdot y) \cdot (C_2 \cdot B)$	[flip 14]
18	$(x \cdot y) \cdot (C_1 \cdot B) = (x \cdot C_3) \cdot (y \cdot D)$	[7 → 4]
101	$(x \cdot C_3) \cdot (y \cdot D) = (x \cdot C_1) \cdot (y \cdot B)$	[4 → 18, flip]
235	$C_2 \cdot D = C_1 \cdot A$	[2,17,101, flip]
237	$\square$	[235,9]

The last two theorems of this section show that the two set subtraction identites shown to be inconsistent with $=(gL)\Rightarrow$ in Thm. #LT-6a above are also inconsistent with RC and with TC.

Theorem #RC-0.

$$\left\{ \begin{array}{l} \text{RC} \\ x-(y-x)=x \\ x-(x-y)=y-(y-x) \end{array} \right\} \Rightarrow \{x=y\}.$$

Proof (found by Otter 3.0.3l on gyro at 0.88 seconds).

1	$A=B \ \rightarrow \ \square$	
2	$x=x$	
3	$x-y=z,\ u-v=z,\ w-y=v_6,\ v_7-v=v_6,\ x-v_8=v_9,\ u-v_{10}=v_9 \ \rightarrow \ w-v_8=v_7-v_{10}$	
5,4	$x-(y-x)=x$	
6	$x-(x-y)=y-(y-x)$	
9,8	$(x-y)-y=x-y$	[4 → 4]
15,14	$x-(y-(z-u))=x-u$	[3,8,8,2,8,4,8 :9]
17,16	$(x-y)-z=x-z$	[3,2,2,8,2,8,8]
23,22	$x-y=x$	[3,16,6,6,6,2,6 :17,5,15, flip]
24	$x=y$	[3,16,6,6,2,16,6 :23,23,23,23]
25	$\square$	[24,1]

Theorem #TC-0.

$$\left\{ \begin{array}{l} \text{TC} \\ x-(y-x)=x \\ x-(x-y)=y-(y-x) \end{array} \right\} \Rightarrow \{x=y\}.$$

Proof (found by Otter 3.0.3l on gyro at 0.85 seconds).

1	$A=B \ \rightarrow \ \square$	
2	$x=x$	
3	$x-y=z,\ u-v=z,\ x-w=v_6,\ v_7-v=v_6 \ \rightarrow \ u-w=v_7-y$	
5,4	$x-(y-x)=x$	
6	$x-(x-y)=y-(y-x)$	
9,8	$(x-y)-y=x-y$	[4 → 4]
11,10	$x-(y-(x-z))=x-z$	[3,8,2,4,8 :9]
14	$(x-y)-((x-y)-z)=z-y$	[3,8,4,2,6]
41,40	$(x-y)-(z-((u-y)-v))=(u-y)-v$	[3,10,10,14,14 :11, flip]
44,43	$(x-y)-((z-y)-x)=x-y$	[3,10,2,8,14 :9,41, flip]
49,48	$x-y=x$	[3,14,10,14,4 :5,44, flip]
50	$x=y$	[3,14,8,14,8 :49,49,49,49,49,49,49,49]
51	$\square$	[50,1]

4.5 Cancellative Semigroups and $=\!(gL)\!\Rightarrow$

[[Give an example of a cancellative Algebra satisfying the 4-var assoc. law but not associative.]]

Theorem #CS-GL-1.

$$\{\text{Cancellative Semigroup}\} \;=\!(gL)\!\Rightarrow\; \{xy = yx\}.$$

Proof (found by Otter 3.0.3l on gyro at 5.99 seconds).

2	$x \cdot y = u,\ x \cdot z = u \ \rightarrow\ y = z$	
3	$y \cdot x = u,\ z \cdot x = u \ \rightarrow\ y = z$	
4	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	
5	$B \cdot A = A \cdot B \ \rightarrow\ \Box$	
6	$(((x \cdot y) \cdot z) \cdot u) \cdot v = (x \cdot (y \cdot z)) \cdot (u \cdot v)$	[4 → 4]
11	$(x \cdot (y \cdot z)) \cdot u = (x \cdot y) \cdot (z \cdot u)$	[4 → 4]
432	$(((x \cdot y) \cdot z) \cdot u) \cdot v = (x \cdot u) \cdot ((y \cdot z) \cdot v)$	[(gL) 6]
433	$((x \cdot y) \cdot z) \cdot u = x \cdot (u \cdot (y \cdot z))$	[3,11,432, flip]
1205	$x \cdot y = y \cdot x$	[2,432,433]
1206	$\Box$	[1205,5]

E-mail from RP to WWM, 11 May, 1993:

> The proof of
>
> $$\{\text{CS}\} \;=\!(gL)\!\Rightarrow\; \{xy = yx\},$$
>
> is especially excellent. This means that not only a group law, but even a cancellative semigroup law on a projective curve must be commutatiave! This is a new result.
>
> Now the commutative law has only two variables and $=\!(gL)\!\Rightarrow$ is an inference rule. Believing in the cosmic orderliness of mathematics, one can ask the question whether the two cancellation laws along with the set of all two-variable consequences of associativity will already (gL)-imply $xy = yx$.

The following theorem answers the question, using just two of the three tow-variable instances of associativity.

Theorem #CS-GL-9.

$$\left\{ \begin{array}{l} x(yx) = (xy)x \\ x(xy) = (xx)y \\ \text{cancellation} \end{array} \right\} \;=\!(gL)\!\Rightarrow\; \{xy = yx\}$$

Proof (found by Otter 3.0.3l on gyro at 1.41 seconds).

1	$B \cdot A = A \cdot B \ \rightarrow \ \Box$	
2	$x = x$	
3	$x \cdot y = z,\ x \cdot u = z \ \rightarrow \ y = u$	
4	$x \cdot y = z,\ u \cdot y = z \ \rightarrow \ x = u$	
5	$(x \cdot x) \cdot y = x \cdot (x \cdot y)$	
6	$(x \cdot y) \cdot x = x \cdot (y \cdot x)$	
12	$(x \cdot x) \cdot (y \cdot z) = x \cdot ((x \cdot y) \cdot z)$	[6 → 5 :(gL)]
13	$x \cdot ((y \cdot z) \cdot u) = x \cdot (y \cdot (z \cdot u))$	[5 → 12 :(gL), flip]
14	$(x \cdot x) \cdot (y \cdot z) = x \cdot (y \cdot (x \cdot z))$	[5 → 12 :(gL)]
19	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	[3,2,13, flip]
22	$(x \cdot y) \cdot z = y \cdot (x \cdot z)$	[3,12,14, flip]
38	$x \cdot y = y \cdot x$	[4,19,22]
39	$\Box$	[38,1]

The next few theorems generalize Thm. #CS-GL-1, the commutativity of cancellative semigroups under (gL), to weaker forms of associativity.

Theorem #CS-GL-2. The type is (2).

$$\left\{ \begin{array}{l} \text{cancellation} \\ x(y(zu)) = ((xy)z)u \end{array} \right\} \ =\!(gL)\!\Rightarrow \ \{xy = yx\}.$$

Proof (found by Otter 3.0.3l on gyro at 18.16 seconds).

1	$B \cdot A = A \cdot B \ \rightarrow \ \Box$	
2	$x = x$	
3	$x \cdot y = z,\ x \cdot u = z \ \rightarrow \ y = u$	
4	$x \cdot y = z,\ u \cdot y = z \ \rightarrow \ x = u$	
5	$x \cdot (y \cdot (z \cdot u)) = ((x \cdot y) \cdot z) \cdot u$	
6	$((x \cdot y) \cdot z) \cdot u = x \cdot (y \cdot (z \cdot u))$	[flip 5]
7	$((((x \cdot y) \cdot z) \cdot u) \cdot v) \cdot w = x \cdot ((y \cdot (z \cdot u)) \cdot (v \cdot w))$	[6 → 6]
8	$((x \cdot (y \cdot (z \cdot u))) \cdot v) \cdot w = ((x \cdot y) \cdot z) \cdot (u \cdot (v \cdot w))$	[6 → 6]
14	$((x \cdot y) \cdot z) \cdot (u \cdot v) = x \cdot (((y \cdot z) \cdot u) \cdot v)$	[6 → 6]
38	$((x \cdot y) \cdot z) \cdot (u \cdot v) = x \cdot ((y \cdot (z \cdot u)) \cdot v)$	[6 → 7 :(gL)]
42	$x \cdot (((y \cdot z) \cdot u) \cdot v) = x \cdot ((y \cdot (z \cdot u)) \cdot v)$	[14 → 38]
53	$((x \cdot y) \cdot z) \cdot u = (x \cdot (y \cdot z)) \cdot u$	[3,2,42, flip]
63	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	[4,2,53, flip]
111	$((x \cdot (y \cdot (z \cdot u))) \cdot v) \cdot w = ((x \cdot y) \cdot v) \cdot (u \cdot (z \cdot w))$	[(gL) 8]
125	$(x \cdot (y \cdot z)) \cdot u = (x \cdot y) \cdot (z \cdot u)$	[63 → 63]
273	$(x \cdot y) \cdot (z \cdot (u \cdot v)) = (x \cdot u) \cdot (z \cdot (y \cdot v))$	[8 → 111 :(gL)]
453	$(x \cdot y) \cdot z = y \cdot (x \cdot z)$	[3,273,125, flip]
540	$x \cdot y = y \cdot x$	[4,63,453]
541	$\Box$	[540,1]

Theorem #CS-GL-3. The type is (2).

$$\left\{ \begin{array}{l} \text{cancellation} \\ x(y(z(uv))) = (((xy)z)u)v \end{array} \right\} =\!(gL)\!\Rightarrow \{xy = yx\}.$$

Proof (found by Otter 3.0.3l on gyro at 15.86 seconds).

1	$B \cdot A = A \cdot B \ \rightarrow\ \Box$	
3	$x \cdot y = z,\ x \cdot u = z \ \rightarrow\ y = u$	
4	$x \cdot y = z,\ u \cdot y = z \ \rightarrow\ x = u$	
5	$x \cdot (y \cdot (z \cdot (u \cdot v))) = (((x \cdot y) \cdot z) \cdot u) \cdot v$	
6	$(((x \cdot y) \cdot z) \cdot u) \cdot v = x \cdot (y \cdot (z \cdot (u \cdot v)))$	[flip 5]
7	$((x \cdot (y \cdot (z \cdot (u \cdot v)))) \cdot w) \cdot v_6 = ((x \cdot y) \cdot z) \cdot (u \cdot (v \cdot (w \cdot v_6)))$	[6 $\rightarrow$ 6]
8	$(x \cdot (y \cdot (z \cdot (u \cdot v)))) \cdot w = (x \cdot y) \cdot (z \cdot (u \cdot (v \cdot w)))$	[6 $\rightarrow$ 6]
25	$((x \cdot (y \cdot (z \cdot (u \cdot v)))) \cdot w) \cdot v_6 = ((x \cdot y) \cdot w) \cdot (u \cdot (v \cdot (z \cdot v_6)))$	[(gL) 7]
32	$(x \cdot (y \cdot (z \cdot (u \cdot v)))) \cdot w = (x \cdot y) \cdot (w \cdot (u \cdot (v \cdot z)))$	[4,8,25, flip]
33	$(x \cdot (y \cdot (z \cdot u))) \cdot v = (x \cdot (y \cdot (v \cdot u))) \cdot z$	[4,7,25 :(gL)]
37	$(x \cdot y) \cdot (z \cdot (u \cdot (v \cdot w))) = (x \cdot v) \cdot (z \cdot (u \cdot (y \cdot w)))$	[7 $\rightarrow$ 25 :(gL)]
56	$x \cdot (y \cdot (z \cdot (u \cdot v))) = x \cdot (v \cdot (z \cdot (u \cdot y)))$	[8 $\rightarrow$ 32 :(gL)]
61	$x \cdot (y \cdot (z \cdot u)) = u \cdot (y \cdot (z \cdot x))$	[3,33,56]
208	$x \cdot y = y \cdot x$	[4,61,37]
209	$\Box$	[208,1]

Theorem #CS-GL-4. The type is (2).

$$\left\{ \begin{array}{l} \text{cancellation} \\ x(y(zu)) = (xy)(zu) \end{array} \right\} =\!(gL)\!\Rightarrow \{xy = yx\}.$$

Proof (found by Otter 3.0.3l on gyro at 0.53 seconds).

1	$B \cdot A = A \cdot B \ \rightarrow\ \Box$	
3	$x \cdot y = z,\ x \cdot u = z \ \rightarrow\ y = u$	
4	$x \cdot y = z,\ u \cdot y = z \ \rightarrow\ x = u$	
5	$x \cdot (y \cdot (z \cdot u)) = (x \cdot y) \cdot (z \cdot u)$	
6	$(x \cdot y) \cdot (z \cdot u) = x \cdot (y \cdot (z \cdot u))$	[flip 5]
13	$(x \cdot y) \cdot (z \cdot u) = x \cdot ((y \cdot z) \cdot u)$	[6 $\rightarrow$ 6 :(gL)]
15	$(x \cdot y) \cdot (z \cdot u) = x \cdot (z \cdot (y \cdot u))$	[(gL) 6]
42	$(x \cdot y) \cdot z = y \cdot (x \cdot z)$	[3,13,15, flip]
91	$x \cdot y = y \cdot x$	[4,15,42]
92	$\Box$	[91,1]

Example #CS-GL-5. The type is (2).

$$\left\{ \begin{array}{l} \text{cancellation} \\ x(y(zu)) = (x(yz))u \end{array} \right\} =\!(gL)\!\Rightarrow \{xy = yx\}.$$

Counterexample. The clauses

$(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u)$ % medial law
$x \cdot (y \cdot (z \cdot u)) = (x \cdot (y \cdot z)) \cdot u$
$B \cdot A \neq A \cdot B$

```
properties(_*_, quasigroup).
```

have the following model (found by MACE 1.1.0 on gyro at 3.01 seconds).

```
* :
      | 0 1 2
   ---+------
   0  | 0 2 1
   1  | 1 0 2
   2  | 2 1 0
B: 1
A: 0
end_of_model
```

Note that the model in the preceding example is $x \cdot y = x + 2y$ (mod3) and hence is (gL).

Theorem #CS-GL-6. The type is (2).

$$\left\{ \begin{array}{l} \text{cancellation} \\ (x(yz))u = (xy)(zu) \end{array} \right\} =\!(gL)\!\Rightarrow\ \{xy = yx\}.$$

Proof (found by Otter 3.0.3l on gyro at 2.32 seconds).

1	$B \cdot A = A \cdot B \ \rightarrow\ \square$	
3	$x \cdot y = z,\ x \cdot u = z \ \rightarrow\ y = u$	
4	$x \cdot y = z,\ u \cdot y = z \ \rightarrow\ x = u$	
5	$(x \cdot (y \cdot z)) \cdot u = (x \cdot y) \cdot (z \cdot u)$	
8	$((x \cdot (y \cdot z)) \cdot u) \cdot v = ((x \cdot y) \cdot z) \cdot (u \cdot v)$	[5 → 5]
24	$((x \cdot (y \cdot z)) \cdot u) \cdot v = ((x \cdot y) \cdot u) \cdot (z \cdot v)$	[(gL) 8]
29	$(x \cdot (y \cdot z)) \cdot u = (x \cdot z) \cdot (y \cdot u)$	[5 → 24 :(gL)]
32	$(x \cdot y) \cdot (z \cdot u) = (x \cdot z) \cdot (y \cdot u)$	[8 → 24 :(gL)]
67	$x \cdot (y \cdot z) = x \cdot (z \cdot y)$	[4,5,29]
183	$x \cdot y = y \cdot x$	[3,32,67]
184	$\square$	[183,1]

4.6 A Discovery Rule

[[Examples and a small table.]]

Chapter 5

Semigroups

5.1 A Conjecture in Cancellative Semigroups

Electronic mail (with a little editiing) from RP to WM, May 7, 1993:

> Let me now state more problems for Otter all in one area: this time it is semigroups. These are based on an uproved conjecture of mine. So, any negative solution will disprove my conjecture once and for all. But every positive solution, apart from being a new theorem in Mathematics will generalize the corresponding result from group theory. It will thus strengthen the conjecture and also may pave way for the general proof. So much for the preamble.
>
> Groups are of type $< 2, 1, 0 >$ with an associative multiplication, an inverse and an identity element. The semigroup of a group is, of course, cancellative: $ab = ac \Rightarrow a'ab = a'ac \Rightarrow b = c$. The cancellative law, as a first order property, is within the language of type (2). This is the backdrop of my conjecture.
>
> *Conjecture.* Let A be a nonempty set of axioms of type (2) and let a be an axiom of the same type. If every group satisfying A also satisfies a, then every cancellative semigroup satisfying A must satisfy a as well. To put it more formally, let GT be the axioms of group theory and CS be the associative law and the two cancellation laws. Then
>
> $$\text{if } (A, \text{GT} \Rightarrow a) \text{ then } (A, \text{CS} \Rightarrow a).$$
>
> From the computational point of view, this conjecture says that if one uses the luxury of the richer language of group theory {associativity, inverse and identity} to derive a from A, then one can do the same thing within the limited language of just one binary operation which is associative and cancellative. Over the past ten years, I have mentioned this problem to many famous group theorists (including S.I. Adjan, B.H. Neumann, Sevrin, Narain Gupta and many others).

No one believed it right away and tried to give counter examples. But none of the examples really worked and the problem is still open. I too believe that this may not true and the only way is to find a counterexample of a rather difficult nature.

For our purpose, all we need to do is to pick up "good" A's in the language of one binary operation implying a non-trivial a in groups and try to prove it under the milder hypothesis of just CS. Over the years, I have collected some examples. Naturally, OTTER can play a very useful role here.

5.2 Theorems Supporting the Conjecture

Theorem #CS-1.

$$\{\text{CS},\ xyzyx = yxzxy\} \Rightarrow \{xyyx = yxxy\}.$$

(In groups, simply substitute $z = e$ to derive the right-hand side.) There is a second order reason for this: such semigroups can be imbedded in groups satisfying the same identity and hence are OK. The imbedding theorem was proved by A. I. Mal'cev, B. H. Neumann, and others around the 1950's. A first order proof was given by Padmanabhan.

Proof (found by Otter 3.0.3l on gyro at 7.00 seconds).

1	$A \cdot B \cdot B \cdot A = B \cdot A \cdot A \cdot B \ \rightarrow\ \Box$	
2	$x = x$	
3	$x \cdot y = z,\ x \cdot u = z \ \rightarrow\ y = u$	
6,5	$(x \cdot y) \cdot z = x \cdot y \cdot z$	
7	$x \cdot y \cdot z \cdot y \cdot x = y \cdot x \cdot z \cdot x \cdot y$	
11	$x \cdot y \cdot z \cdot u \cdot y \cdot x = y \cdot x \cdot z \cdot u \cdot x \cdot y$	[5 → 7 :6]
17	$x \cdot y \cdot z \cdot y \cdot x \cdot u = y \cdot x \cdot z \cdot x \cdot y \cdot u$	[7 → 5 :6,6,6,6,6,6,6]
22	$x \cdot y \cdot z \cdot u \cdot v \cdot y \cdot x = y \cdot x \cdot z \cdot u \cdot v \cdot x \cdot y$	[5 → 11 :6]
262	$x \cdot y \cdot x \cdot z \cdot z \cdot x = x \cdot y \cdot z \cdot x \cdot x \cdot z$	[3,17,22]
329	$x \cdot y \cdot z \cdot z \cdot y = x \cdot z \cdot y \cdot y \cdot z$	[3,2,262]
376	$x \cdot y \cdot y \cdot x = y \cdot x \cdot x \cdot y$	[3,2,329]
377	$\Box$	[376,1]

Theorem #CS-2.

$$\{\text{Group Theory},\ z[x,y] = [x,y]z\} \Rightarrow \{xyyx = yxxy\}$$

Here $[x,y]$ stands for the commutator $x'y'xy$. In other words, the identity in question says that the commutators commute. These are the so-called meta-abelian groups. Thm. #CS-1 can also be used to prove this.

Proof (found by Otter 3.0.3l on gyro at 5.30 seconds).

1	$A \cdot (B \cdot (B \cdot A)) \neq B \cdot (A \cdot (A \cdot B))$	
4,3	$e \cdot x = x$	
8,7	$x' \cdot x = e$	
12,11	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	
16,15	$x'' = x$	
18,17	$(x \cdot y)' = y' \cdot x'$	
20,19	$x' \cdot (x \cdot y) = y$	
22,21	$x \cdot (x' \cdot y) = y$	
23	$h(x,y) = x' \cdot (y' \cdot (x \cdot y))$	
24	$x \cdot h(y,z) = h(y,z) \cdot x$	
25	$x' \cdot (y' \cdot (x \cdot y)) = h(x,y)$	[flip 23]
26	$h(x,y) \cdot z = z \cdot h(x,y)$	[flip 24]
28	$x \cdot (y \cdot h(z,u)) = h(z,u) \cdot (x \cdot y)$	[11 → 24]
39	$x' \cdot (y' \cdot (x \cdot (y \cdot z))) = z \cdot h(x,y)$	[23 → 26 :12,12,12]
66,65	$h(h(x,y),z) = e$	[26 → 25 :20,8, flip]
81	$x \cdot h(x,y) = y' \cdot (x \cdot y)$	[25 → 21]
85	$x' \cdot (y \cdot x) = y \cdot h(y,x)$	[flip 81]
203	$x \cdot (y \cdot h(y,x)) = y \cdot x$	[85 → 21]
206	$h(x,y) = h(y', x \cdot y)$	[85 → 25 :16,18,12,20,22]
208	$h(x', y \cdot x) = h(y,x)$	[flip 206]
247	$x \cdot (h(y,x) \cdot y) = y \cdot x$	[24 → 203]
251	$h(x,y) \cdot (y \cdot x) = x \cdot y$	[28 → 203]
264	$x \cdot h(y,x) = x \cdot h(x',y)$	[85 → 39 :16,20]
383	$h(x' \cdot y', x \cdot y) = e$	[251 → 208 :18,66]
546	$h(x,y) = h(y,x')$	[264 → 21 :16,22]
559	$h(x \cdot y, y \cdot x) = e$	[383 → 546 :18,16,16, flip]
775	$x \cdot (y \cdot (y \cdot x)) = y \cdot (x \cdot (x \cdot y))$	[559 → 247 :4,12,12]
776	□	[775,1]

Theorem #CS-3.

$$\{\text{CS},\ xy^2 = y^2x\} \Rightarrow \{(xy)^4 = x^4y^4\}.$$

This was previously proved by Padmanabhan (unpublished).

In fact, OTTER proves a stronger theorem, $xyxyzyxu = zxxxyyyu$, without using the cancellation laws.

Proof (found by Otter 3.0.3l on gyro at 187.61 seconds).

1	$A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B \neq A \cdot A \cdot A \cdot A \cdot B \cdot B \cdot B \cdot B$	
4,3	$(x \cdot y) \cdot z = x \cdot y \cdot z$	
5	$x \cdot y \cdot y = y \cdot y \cdot x$	
8	$x \cdot y \cdot z \cdot y \cdot z = y \cdot z \cdot y \cdot z \cdot x$	[3 → 5 :4,4]
13	$x \cdot x \cdot y \cdot z = y \cdot x \cdot x \cdot z$	[5 → 3 :4,4,4]
14	$x \cdot y \cdot y \cdot z = y \cdot y \cdot x \cdot z$	[flip 13]
48	$x \cdot y \cdot x \cdot y \cdot z \cdot u = z \cdot x \cdot y \cdot x \cdot y \cdot u$	[8 → 3 :4,4,4,4,4,4,4]

50	$x \cdot y \cdot z \cdot y \cdot z \cdot u = y \cdot z \cdot y \cdot z \cdot x \cdot u$	[flip 48]
78	$x \cdot y \cdot z \cdot z \cdot y \cdot u = y \cdot y \cdot x \cdot z \cdot z \cdot u$	[14 → 14]
3988	$x \cdot y \cdot y \cdot y \cdot z \cdot z \cdot z \cdot u = y \cdot z \cdot y \cdot z \cdot x \cdot z \cdot y \cdot u$	[78 → 50]
4008	$x \cdot y \cdot x \cdot y \cdot z \cdot y \cdot x \cdot u = z \cdot x \cdot x \cdot x \cdot y \cdot y \cdot y \cdot u$	[flip 3988]
4009	□	[4008,1]

Theorem #CS-4.

$$\{\text{CS},\ xy^3 = y^3x\} \Rightarrow \{(xy)^9 = x^9y^9\}.$$

The analogous statement for group theory was first proved by Narain Gupta in 1969.

In fact, we prove this for ordinary semigroups, without cancellation. (This is a difficult problem for Otter, and we use a very specialized search strategy. [[It might be worth while to include a description of how the strategy was developed.]])

Proof (found by Otter 3.0.3l on gyro at 202.47 seconds).

2	$(x \cdot y) \cdot z = x \cdot y \cdot z$	
3	$x \cdot y \cdot y \cdot y = y \cdot y \cdot y \cdot x$	
4	$p(A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B)$	
5	$-p(A \cdot A \cdot A \cdot A \cdot A \cdot A \cdot A \cdot A \cdot A \cdot B \cdot B \cdot B \cdot B \cdot B \cdot B \cdot B \cdot B)$	
6	$(x \cdot y) \cdot z = x \cdot y \cdot z$	
8	$x \cdot y \cdot z \cdot y \cdot z \cdot y \cdot z = y \cdot z \cdot y \cdot z \cdot y \cdot z \cdot x$	[2 → 3 :6,6,6,6,6,6,6]
9	$x \cdot y \cdot z \cdot z \cdot z = z \cdot z \cdot z \cdot x \cdot y$	[2 → 3]
12	$x \cdot x \cdot x \cdot y \cdot z = y \cdot x \cdot x \cdot x \cdot z$	[3 → 2 :6,6,6,6,6]
15	$x \cdot x \cdot x \cdot y = y \cdot x \cdot x \cdot x$	[3 → 2 :6]
16	$x \cdot y \cdot y \cdot y \cdot z = y \cdot y \cdot y \cdot x \cdot z$	[3 → 2 :6,6,6,6,6]
20	$x \cdot y \cdot z \cdot u \cdot y \cdot z \cdot u \cdot y \cdot z \cdot u = y \cdot z \cdot u \cdot y \cdot z \cdot u \cdot y \cdot z \cdot u \cdot x$	[2 → 8 :6,6,6,6,6,6]
22	$x \cdot y \cdot z \cdot u \cdot z \cdot u \cdot z \cdot u = z \cdot u \cdot z \cdot u \cdot z \cdot u \cdot x \cdot y$	[2 → 8]
40	$p(A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A)$	[8 → 4]
42	$x \cdot y \cdot x \cdot y \cdot x \cdot y \cdot z = z \cdot x \cdot y \cdot x \cdot y \cdot x \cdot y$	[8 → 2 :6]
65	$p(A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A)$	[8 → 40 :6,6,6,6,6,6]
69	$p(A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot B \cdot A \cdot B \cdot A \cdot B \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot A)$	[8 → 65]
92	$p(B \cdot A \cdot B \cdot A \cdot B \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot A \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B)$	[8 → 69 :6,6,6,6,6,6,6,6,6,6,6
98	$x \cdot x \cdot x \cdot y \cdot z \cdot u \cdot u \cdot u = u \cdot x \cdot x \cdot x \cdot u \cdot u \cdot y \cdot z$	[9 → 12]
144	$p(B \cdot A \cdot B \cdot A \cdot B \cdot B \cdot A \cdot B \cdot A \cdot A \cdot A \cdot A \cdot B \cdot B \cdot A \cdot B \cdot A \cdot B)$	[12 → 92]
174	$p(B \cdot A \cdot B \cdot A \cdot B \cdot B \cdot A \cdot A \cdot A \cdot A \cdot B \cdot A \cdot B \cdot B \cdot A \cdot B \cdot A \cdot B)$	[12 → 144]
176	$p(B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot A \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot B \cdot A \cdot B \cdot A \cdot B)$	[12 → 174]
180	$p(A \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot B \cdot A \cdot B \cdot A \cdot B \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A)$	[8 → 176 :6,6,6,6,6,6,6,6,6,6
272	$p(A \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot B \cdot A \cdot B \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot A \cdot B)$	[22 → 180]
296	$p(A \cdot A \cdot B \cdot A \cdot A \cdot B \cdot A \cdot A \cdot B \cdot B \cdot A \cdot B \cdot B \cdot A \cdot B \cdot B \cdot A \cdot B)$	[20 → 272 :6,6,6,6]
351	$p(A \cdot A \cdot B \cdot A \cdot A \cdot B \cdot A \cdot A \cdot B \cdot B \cdot B \cdot A \cdot B \cdot B \cdot A \cdot B \cdot B \cdot A)$	[20 → 296]
390	$p(A \cdot A \cdot B \cdot A \cdot A \cdot B \cdot A \cdot A \cdot A \cdot B \cdot B \cdot B \cdot B \cdot B \cdot A \cdot B \cdot B \cdot A)$	[16 → 351]
449	$p(A \cdot A \cdot B \cdot A \cdot A \cdot B \cdot B \cdot B \cdot B \cdot B \cdot B \cdot A \cdot B \cdot B \cdot A \cdot A \cdot A \cdot A)$	[15 → 390 :6,6,6,6,6,6,6,6,6]

687 $p(A \cdot A \cdot B \cdot A \cdot A \cdot A \cdot B \cdot B \cdot A \cdot A \cdot A \cdot A \cdot B \cdot B \cdot B \cdot B \cdot B)$ [42 → 449 :6,6,6,6,6,6]
2438 $p(A \cdot A \cdot A \cdot A \cdot A \cdot A \cdot A \cdot A \cdot A \cdot B \cdot B \cdot B \cdot B \cdot B \cdot B \cdot B \cdot B)$ [98 → 687 :6,6,6,6,6,6,6,6]
2439 □ [2438,5]

Theorem #CS-5.

$$\{\text{CS},\ xy^4 = y^4x\} \Rightarrow \{(xy)^4 = (yx)^4\}.$$

Proof (found by Otter 3.0.3l on gyro at 4.60 seconds).

1 $B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A = A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B \ \rightarrow$ □
2 $x = x$
3 $x \cdot y = z,\ x \cdot u = z \ \rightarrow \ y = u$
6,5 $(x \cdot y) \cdot z = x \cdot y \cdot z$
7 $x \cdot y \cdot y \cdot y \cdot y = y \cdot y \cdot y \cdot y \cdot x$
10 $x \cdot y \cdot z \cdot y \cdot z \cdot y \cdot z \cdot y \cdot z = y \cdot z \cdot y \cdot z \cdot y \cdot z \cdot y \cdot z \cdot x$ [5 → 7 :6,6,6,6,6,6]
211 $x \cdot y \cdot x \cdot y \cdot x \cdot y \cdot x \cdot y = y \cdot x \cdot y \cdot x \cdot y \cdot x \cdot y \cdot x$ [3,2,10]
212 □ [211,1]

Theorem #CS-5a.

$$\{\text{CS},\ xy^n = y^nx\} \Rightarrow \{(xy)^n = (yx)^n\}.$$

This theorem is outside the scope of Otter, because it requires induction. However, OTTER easily proves the statment for $n = 2, 3, 4, 5$, and it is easy to construct a proof by hand of the general theorem by looking at the OTTER proofs.

Proof.

$$\begin{array}{rll} xy^n & = y^nx & \text{[hypothesis]} \\ x(xw)^n & = (xw)^nx & \text{[set } y = xw\text{]} \\ & = x(wx)^n & \text{[change power notation]} \\ (xw)^n & = (wx)^n & \text{[cancel } x\text{]} \end{array}$$

Theorem #CS-7. The type is (2).

$$\left\{ \begin{array}{l} (xy)z = x(yz) \\ xyzu = yzux \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} (xy)^3 = x^3y^3 \\ x^3y^3 = y^3x^3 \end{array} \right\}.$$

Proof (found by Otter 3.0.3l on gyro at 4.95 seconds).

4 $A \cdot B \cdot A \cdot B \cdot A \cdot B = A \cdot A \cdot A \cdot B \cdot B \cdot B,\ B \cdot B \cdot B \cdot A \cdot A \cdot A = A \cdot A \cdot A \cdot B \cdot B \cdot B \ \rightarrow$ □
6,5 $(x \cdot y) \cdot z = x \cdot y \cdot z$
7 $x \cdot y \cdot z \cdot u = y \cdot z \cdot u \cdot x$
8 $x \cdot y \cdot z \cdot u = u \cdot x \cdot y \cdot z$ [flip 7]

9	$x \cdot y \cdot z \cdot u \cdot v \cdot w = y \cdot w \cdot z \cdot u \cdot v \cdot x$	[7 → 7 :6,6]
22	$x \cdot y \cdot z \cdot u = z \cdot u \cdot x \cdot y$	[7 → 8]
111	$x \cdot y \cdot z \cdot u \cdot v \cdot w = v \cdot u \cdot w \cdot y \cdot z \cdot x$	[22 → 9 :6]
134	$x \cdot y \cdot z \cdot u \cdot v \cdot w = w \cdot u \cdot v \cdot y \cdot x \cdot z$	[flip 111]
373	$x \cdot y \cdot z \cdot u \cdot v \cdot w = z \cdot w \cdot y \cdot u \cdot x \cdot v$	[8 → 134 :6]
412	$x \cdot y \cdot z \cdot u \cdot v \cdot w = v \cdot z \cdot x \cdot u \cdot w \cdot y$	[flip 373]
462	□	[4,412,134]

Theorem #CS-8. The type is (2).

$$\left\{ \begin{array}{l} (xy)z = x(yz) \\ xyzuv = yzuvx \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} (xy)^4 = x^4y^4 \\ x^4y^4 = y^4x^4 \end{array} \right\}.$$

Proof (found by Otter 3.0.3l on gyro at 269.24 seconds).

4	$A \cdot B \cdot A \cdot B \cdot A \cdot B \cdot A \cdot B = A \cdot A \cdot A \cdot A \cdot B \cdot B \cdot B \cdot B,\ B \cdot B \cdot B \cdot B \cdot A \cdot A \cdot A \cdot A = A \cdot A$	
6,5	$(x \cdot y) \cdot z = x \cdot y \cdot z$	
7	$x \cdot y \cdot z \cdot u \cdot v = y \cdot z \cdot u \cdot v \cdot x$	
8	$x \cdot y \cdot z \cdot u \cdot v = v \cdot x \cdot y \cdot z \cdot u$	[flip 7]
9	$x \cdot y \cdot z \cdot u \cdot v \cdot w \cdot v_6 \cdot v_7 = y \cdot z \cdot v_7 \cdot u \cdot v \cdot w \cdot v_6 \cdot x$	[7 → 7 :6,6,6]
13	$x \cdot y \cdot z \cdot u \cdot v \cdot w = z \cdot u \cdot v \cdot w \cdot x \cdot y$	[5 → 7]
14	$x \cdot y \cdot z \cdot u \cdot v \cdot w \cdot v_6 \cdot v_7 = v_7 \cdot x \cdot y \cdot u \cdot v \cdot w \cdot v_6 \cdot z$	[flip 9]
34	$x \cdot y \cdot z \cdot u \cdot v \cdot w = z \cdot u \cdot v \cdot w \cdot y \cdot x$	[8 → 7 :6]
37	$x \cdot y \cdot z \cdot u \cdot v \cdot w = w \cdot v \cdot x \cdot y \cdot z \cdot u$	[flip 34]
2779	$x \cdot y \cdot z \cdot u \cdot v \cdot w \cdot v_6 \cdot v_7 = v \cdot w \cdot v_6 \cdot v_7 \cdot u \cdot z \cdot x \cdot y$	[37 → 13 :6,6]
2799	$x \cdot y \cdot z \cdot u \cdot v \cdot w \cdot v_6 \cdot v_7 = z \cdot x \cdot v \cdot v_6 \cdot v_7 \cdot u \cdot y \cdot w$	[37 → 14 :6]
3136	□	[4,2799,2779]

The last three theorems in this section are stated for arbitrary parameter n, so they are outside of OTTER's scope. (OTTER easily proved all of the particular cases we gave to it.) The proofs are left as exercises for the reader.

Theorem #CS-9. The type is (2).

$$\left\{ \begin{array}{l} (xy)z = x(yz) \\ x_1x_2 \cdots x_n = x_2 \cdots x_nx_1 \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} \forall m \geq \lceil n/2 \rceil, x^my^m = y^mx^m \\ \forall m \geq n-1, (xy)^m = x^my^m \end{array} \right\}.$$

Theorem #CS-11. The type is (2).

$$\left\{ \begin{array}{l} \text{CS} \\ x_1x_2 \cdots x_n = x_2 \cdots x_nx_1 \end{array} \right\} \Rightarrow \{xy = yx\}.$$

Theorem #CS-14. The type is (2).

$$\left\{ \begin{array}{l} \text{CS} \\ x^ny = yz^n \end{array} \right\} \Rightarrow \{x^ny = y\}.$$

5.3 Meta-Abelian CS and the Quotient Condition

A classical result of Mal'cev (1939) says that the following theorem does not hold for cancellative semigroups. Note that this theorem does not satisfy the conditions of Padmanabhan's conjecture.

Theorem #GT-1. Let $a, b, c, d, a_0, b_0, c_0, d_0$ be nullary constants.

$$\left\{ \begin{array}{l} \mathrm{GT} \\ aa_0 = bb_0 \\ ca_0 = db_0 \\ ac_0 = bd_0 \end{array} \right\} \Rightarrow \{cc_0 = dd_0\}$$

Proof (found by Otter 3.0.3l on gyro at 0.36 seconds).

1	$d \cdot d_0 \neq c \cdot c_0$	
4,3	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	
15	$x' \cdot (x \cdot y) = y$	
18,17	$x \cdot (x' \cdot y) = y$	
23	$a \cdot a_0 = b \cdot b_0$	
24	$b \cdot b_0 = a \cdot a_0$	[flip 23]
26	$c \cdot a_0 = d \cdot b_0$	
27	$d \cdot b_0 = c \cdot a_0$	[flip 26]
29	$a \cdot c_0 = b \cdot d_0$	
30	$b \cdot d_0 = a \cdot c_0$	[flip 29]
32	$b \cdot (b_0 \cdot x) = a \cdot (a_0 \cdot x)$	[24 → 3 :4, flip]
34	$d \cdot (b_0 \cdot x) = c \cdot (a_0 \cdot x)$	[27 → 3 :4, flip]
44	$b' \cdot (a \cdot c_0) = d_0$	[30 → 15]
62	$b' \cdot (a \cdot (a_0 \cdot x)) = b_0 \cdot x$	[32 → 15]
97,96	$b' \cdot (a \cdot x) = b_0 \cdot ({a_0}' \cdot x)$	[17 → 62]
106	$b_0 \cdot ({a_0}' \cdot c_0) = d_0$	[44 :97]
114	$d \cdot d_0 = c \cdot c_0$	[106 → 34 :18]
116	$\square$	[114,1]

[[WWM: Remember to rerun the following without hints.]]
[[RP: what is the motivation for this theorem??]]

Theorem #CS-15. Let $a, b, c, d, a_0, b_0, c_0, d_0$ be nullary constants.

$$\left\{ \begin{array}{l} \mathrm{CS} \\ x * y * z * y * x = y * x * z * x * y \\ aa_0 = bb_0 \\ ca_0 = db_0 \\ ac_0 = bd_0 \end{array} \right\} \Rightarrow \{cc_0 = dd_0\}.$$

Proof (found by Otter 3.0.3l on gyro at 7.42 seconds).

1	$d \cdot d_0 = c \cdot c_0 \ \rightarrow \ \square$	
60	$x = x$	
61	$x \cdot y = z,\ x \cdot u = z \ \rightarrow \ y = u$	
64,63	$(x \cdot y) \cdot z = x \cdot y \cdot z$	
65	$x \cdot y \cdot z \cdot y \cdot x = y \cdot x \cdot z \cdot x \cdot y$	
66	$b \cdot b_0 = a \cdot a_0$	
69,68	$d \cdot b_0 = c \cdot a_0$	
71,70	$b \cdot d_0 = a \cdot c_0$	
73,72	$b \cdot d_0 \cdot x = a \cdot c_0 \cdot x$	[70 → 63 :64, flip]
75,74	$d \cdot b_0 \cdot x = c \cdot a_0 \cdot x$	[68 → 63 :64, flip]
77,76	$b \cdot b_0 \cdot x = a \cdot a_0 \cdot x$	[66 → 63 :64, flip]
82	$b_0 \cdot d \cdot x \cdot c \cdot a_0 = c \cdot a_0 \cdot x \cdot b_0 \cdot d$	[68 → 65 :75]
84	$b_0 \cdot b \cdot x \cdot a \cdot a_0 = a \cdot a_0 \cdot x \cdot b_0 \cdot b$	[66 → 65 :77]
89	$x \cdot d_0 \cdot a \cdot c_0 \cdot x = d_0 \cdot x \cdot b \cdot x \cdot d_0$	[72 → 65]
90	$x \cdot y \cdot z \cdot u \cdot y \cdot x = y \cdot x \cdot z \cdot u \cdot x \cdot y$	[63 → 65 :64]
98	$a \cdot c_0 \cdot x \cdot d_0 \cdot b = d_0 \cdot b \cdot x \cdot a \cdot c_0$	[72 → 65 :71]
107	$b \cdot x \cdot b_0 \cdot y \cdot b_0 \cdot x = a \cdot a_0 \cdot x \cdot y \cdot x \cdot b_0$	[65 → 76]
110	$x \cdot y \cdot z \cdot y \cdot x \cdot u = y \cdot x \cdot z \cdot x \cdot y \cdot u$	[65 → 63 :64,64,64,64,64,64,64]
123	$c \cdot a_0 \cdot x \cdot b_0 \cdot d \cdot y = b_0 \cdot d \cdot x \cdot c \cdot a_0 \cdot y$	[82 → 63 :64,64,64,64,64,64,64]
138	$a \cdot a_0 \cdot x \cdot b_0 \cdot b \cdot y = b_0 \cdot b \cdot x \cdot a \cdot a_0 \cdot y$	[84 → 63 :64,64,64,64,64,64,64]
152	$d_0 \cdot x \cdot b \cdot x \cdot d_0 \cdot y = x \cdot d_0 \cdot a \cdot c_0 \cdot x \cdot y$	[89 → 63 :64,64,64,64,64,64,64]
153	$x \cdot d_0 \cdot a \cdot c_0 \cdot x \cdot y = d_0 \cdot x \cdot b \cdot x \cdot d_0 \cdot y$	[flip 152]
155	$x \cdot b_0 \cdot y \cdot a \cdot a_0 \cdot x = b_0 \cdot x \cdot y \cdot b \cdot x \cdot b_0$	[76 → 90]
158	$x \cdot y \cdot z \cdot u \cdot v \cdot y \cdot x = y \cdot x \cdot z \cdot u \cdot v \cdot x \cdot y$	[63 → 90 :64]
180	$d_0 \cdot b \cdot x \cdot a \cdot c_0 \cdot y = a \cdot c_0 \cdot x \cdot d_0 \cdot b \cdot y$	[98 → 63 :64,64,64,64,64,64,64]
181	$a \cdot c_0 \cdot x \cdot d_0 \cdot b \cdot y = d_0 \cdot b \cdot x \cdot a \cdot c_0 \cdot y$	[flip 180]
184	$a \cdot a_0 \cdot d_0 \cdot x \cdot d_0 \cdot b_0 = a \cdot c_0 \cdot b_0 \cdot x \cdot b_0 \cdot d_0$	[72 → 107, flip]
243,242	$b_0 \cdot d \cdot b \cdot c \cdot a_0 \cdot x = c \cdot a_0 \cdot a \cdot a_0 \cdot d \cdot x$	[76 → 123, flip]
259	$a \cdot a_0 \cdot x \cdot b_0 \cdot a \cdot c_0 = b_0 \cdot b \cdot x \cdot a \cdot a_0 \cdot d_0$	[70 → 138]
289,288	$d_0 \cdot d \cdot b \cdot d \cdot d_0 \cdot b_0 = d \cdot d_0 \cdot a \cdot c_0 \cdot c \cdot a_0$	[68 → 153, flip]
302	$x \cdot b_0 \cdot y \cdot z \cdot a \cdot a_0 \cdot x = b_0 \cdot x \cdot y \cdot z \cdot b \cdot x \cdot b_0$	[63 → 155 :64]
307	$b_0 \cdot x \cdot y \cdot z \cdot b \cdot x \cdot b_0 = x \cdot b_0 \cdot y \cdot z \cdot a \cdot a_0 \cdot x$	[flip 302]
336	$x \cdot y \cdot z \cdot u \cdot z \cdot y \cdot x = z \cdot x \cdot y \cdot u \cdot y \cdot x \cdot z$	[110 → 158]
389	$a \cdot c_0 \cdot x \cdot d_0 \cdot a \cdot a_0 = d_0 \cdot b \cdot x \cdot a \cdot c_0 \cdot b_0$	[66 → 181]
402	$a_0 \cdot d_0 \cdot x \cdot d_0 \cdot b_0 = c_0 \cdot b_0 \cdot x \cdot b_0 \cdot d_0$	[61,60,184, flip]
416	$c_0 \cdot b_0 \cdot b \cdot x \cdot a \cdot a_0 \cdot d_0 = a \cdot c_0 \cdot a_0 \cdot x \cdot b_0 \cdot c_0 \cdot a$	[259 → 158]
417	$a \cdot c_0 \cdot a_0 \cdot x \cdot b_0 \cdot c_0 \cdot a = c_0 \cdot b_0 \cdot b \cdot x \cdot a \cdot a_0 \cdot d_0$	[flip 416]
469	$x \cdot y \cdot z \cdot u \cdot z \cdot y \cdot x = z \cdot y \cdot x \cdot u \cdot x \cdot y \cdot z$	[158 → 336]
491	$a_0 \cdot d_0 \cdot b \cdot x \cdot a \cdot c_0 \cdot b_0 = a \cdot a_0 \cdot c_0 \cdot x \cdot d_0 \cdot a_0 \cdot a$	[389 → 158]
492	$a \cdot a_0 \cdot c_0 \cdot x \cdot d_0 \cdot a_0 \cdot a = a_0 \cdot d_0 \cdot b \cdot x \cdot a \cdot c_0 \cdot b_0$	[flip 491]
495	$a_0 \cdot d_0 \cdot x \cdot y \cdot d_0 \cdot b_0 = c_0 \cdot b_0 \cdot x \cdot y \cdot b_0 \cdot d_0$	[63 → 402 :64]
556	$a_0 \cdot d_0 \cdot x \cdot a \cdot c_0 \cdot b_0 = c_0 \cdot b_0 \cdot x \cdot a \cdot a_0 \cdot d_0$	[72 → 495 :77]
558	$a_0 \cdot d_0 \cdot x \cdot y \cdot z \cdot d_0 \cdot b_0 = c_0 \cdot b_0 \cdot x \cdot y \cdot z \cdot b_0 \cdot d_0$	[63 → 495 :64]
571,570	$a_0 \cdot d_0 \cdot x \cdot y \cdot a \cdot c_0 \cdot b_0 = c_0 \cdot b_0 \cdot x \cdot y \cdot a \cdot a_0 \cdot d_0$	[63 → 556 :64]
576	$a \cdot a_0 \cdot c_0 \cdot x \cdot d_0 \cdot a_0 \cdot a = c_0 \cdot b_0 \cdot b \cdot x \cdot a \cdot a_0 \cdot d_0$	[492 :571]

586	$a_0 \cdot d \cdot d_0 \cdot a \cdot c_0 \cdot c \cdot a_0 = c_0 \cdot c \cdot a_0 \cdot a \cdot a_0 \cdot d \cdot d_0$	[288 → 558 :75,243]
602	$c_0 \cdot a_0 \cdot x \cdot b_0 \cdot c_0 \cdot a = a_0 \cdot c_0 \cdot x \cdot d_0 \cdot a_0 \cdot a$	[61,417,576]
604	$a_0 \cdot c_0 \cdot d \cdot d_0 \cdot a_0 \cdot a = c_0 \cdot a_0 \cdot c \cdot a_0 \cdot c_0 \cdot a$	[74 → 602, flip]
614	$c_0 \cdot d \cdot d_0 \cdot a_0 \cdot a = c_0 \cdot c \cdot c_0 \cdot a_0 \cdot a$	[61,110,604, flip]
616	$d \cdot d_0 \cdot a_0 \cdot a = c \cdot c_0 \cdot a_0 \cdot a$	[61,60,614, flip]
629	$a_0 \cdot a \cdot d \cdot d_0 \cdot a \cdot a_0 = a \cdot a_0 \cdot c \cdot c_0 \cdot a_0 \cdot a$	[616 → 90, flip]
636	$a \cdot d \cdot d_0 \cdot a \cdot a_0 = a \cdot c \cdot c_0 \cdot a \cdot a_0$	[61,90,629, flip]
638	$d \cdot d_0 \cdot a \cdot a_0 = c \cdot c_0 \cdot a \cdot a_0$	[61,60,636, flip]
649	$d \cdot d_0 \cdot a \cdot a_0 \cdot x = c \cdot c_0 \cdot a \cdot a_0 \cdot x$	[638 → 63 :64,64,64,64,64, flip]
668	$b_0 \cdot x \cdot d \cdot d_0 \cdot b \cdot x \cdot b_0 = x \cdot b_0 \cdot c \cdot c_0 \cdot a \cdot a_0 \cdot x$	[649 → 302, flip]
676	$x \cdot d \cdot d_0 \cdot b \cdot x \cdot b_0 = x \cdot c \cdot c_0 \cdot b \cdot x \cdot b_0$	[61,307,668, flip]
678	$d \cdot d_0 \cdot b \cdot x \cdot b_0 = c \cdot c_0 \cdot b \cdot x \cdot b_0$	[61,60,676, flip]
684	$d \cdot d_0 \cdot b \cdot x \cdot y \cdot b_0 = c \cdot c_0 \cdot b \cdot x \cdot y \cdot b_0$	[63 → 678 :64]
703,702	$d \cdot d_0 \cdot a \cdot c_0 \cdot c \cdot a_0 = c \cdot c_0 \cdot a \cdot c_0 \cdot c \cdot a_0$	[110 → 684 :289,69,73]
704	$c_0 \cdot c \cdot a_0 \cdot a \cdot a_0 \cdot d \cdot d_0 = a_0 \cdot c \cdot c_0 \cdot a \cdot c_0 \cdot c \cdot a_0$	[586 :703, flip]
724	$c \cdot a_0 \cdot a \cdot a_0 \cdot d \cdot d_0 = c \cdot a_0 \cdot a \cdot a_0 \cdot c \cdot c_0$	[61,469,704, flip]
728	$a_0 \cdot a \cdot a_0 \cdot d \cdot d_0 = a_0 \cdot a \cdot a_0 \cdot c \cdot c_0$	[61,60,724, flip]
730	$a \cdot a_0 \cdot d \cdot d_0 = a \cdot a_0 \cdot c \cdot c_0$	[61,60,728, flip]
734	$a_0 \cdot d \cdot d_0 = a_0 \cdot c \cdot c_0$	[61,60,730, flip]
736	$d \cdot d_0 = c \cdot c_0$	[61,60,734, flip]
738	$\square$	[736,1]

Chapter 6

Independent Self-Dual Bases for Group Theory

We write about two different types of dual identites in this monograph. The first type applies to algebras with two operations, such as lattice theory; there, the dual of an identity is obtained by replacing all occurrences of each operation with the other. The second type, which we use in this chapter, applies to algebras with one binary operation. Here, the dual of an identity is obtained by simultaneously flipping the arguments of all occurrences of the binary operation; informally, the dual of an identity is its mirror image. For the rest of this chapter, we refer to the second type of dual operation. We write $\widetilde{I}$ for the dual of an identity I.

A set S of identities is self-dual if $I \in S \Rightarrow \widetilde{I} \in S$ (modulo renaming of variables). An identity I is self-dual if $I \equiv \widetilde{I}$. For example, the associative law $(xy)z = x(yz)$ is self-dual, for if we write it backwards then rename variables, the result is what we started with.

6.1 Tarski's Interpolation Theorem

6.2 Self-Dual Equational Bases for Group Theory

Thm. #DUAL-GT-2 presents a self-dual 2-basis for the variety of groups, and Thm. #DUAL-GT-3 shows its independence. Thms. #DUAL-GT-3 and #DUAL-GT-4 are the analogous results for Abelian groups. These two 2-bases were found by techniques similar to those presented by McCune in [16]: a large number of candidate bases were generated, and each was given to OTTER to search for a proof.

Theorem #DUAL-GT-1. The type is (2,1).

$$\left\{ \begin{array}{l} ((x \cdot y) \cdot z) \cdot (y \cdot z)' = x \\ (z \cdot y)' \cdot (z \cdot (y \cdot x)) = x \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} x \cdot x' = y \cdot y' \\ x \cdot (y \cdot y') = x \\ (x \cdot y) \cdot z = x \cdot (y \cdot z) \end{array} \right\}.$$

($\Leftarrow$) is trivial, because the right-hand side is a well-known basis for group theory. The proof of ($\Rightarrow$) follows.

Proof (found by Otter 3.0.3k on gyro at 0.52 seconds).

1	$x = x$	
2	$B \cdot B' = A \cdot A',\ A \cdot (B \cdot B') = A,\ (A \cdot B) \cdot C = A \cdot (B \cdot C)\ \rightarrow\ \Box$	
3	$((x \cdot y) \cdot z) \cdot (y \cdot z)' = x$	
6,5	$(x \cdot y)' \cdot (x \cdot (y \cdot z)) = z$	
7	$(x \cdot y) \cdot ((z \cdot u)' \cdot y)' = (x \cdot z) \cdot u$	[3 → 3]
8	$x \cdot (y \cdot (z \cdot y)')' = x \cdot z$	[3 → 3]
12	$(x \cdot y) \cdot z = (x \cdot u) \cdot ((y \cdot z)' \cdot u)'$	[flip 7]
35	$((x \cdot y) \cdot (z \cdot y)') \cdot z = x$	[3 → 8, flip]
37	$(x \cdot (y \cdot x)')' = y$	[8 → 5 :6, flip]
43	$((x \cdot y)' \cdot x)' = y$	[37 → 37]
45	$x \cdot (y \cdot ((x \cdot y)' \cdot z)) = z$	[37 → 5]
48,47	$(x' \cdot (y \cdot z)')' = y \cdot (z \cdot x)$	[5 → 43]
52,51	$x \cdot ((y \cdot x)' \cdot (y \cdot z)) = z$	[43 → 5]
63	$(x \cdot y) \cdot (z \cdot y)' = (x \cdot (u \cdot z)') \cdot u$	[43 → 7]
75,74	$(x \cdot y) \cdot (z \cdot ((y \cdot z)' \cdot u)) = x \cdot u$	[7 → 37 :48]
98	$((x \cdot ((y \cdot z) \cdot (u \cdot z)')) \cdot u) \cdot y' = x$	[35 → 3]
119,118	$(x \cdot y) \cdot (z' \cdot y)' = x \cdot z$	[45 → 7 :75]
137,136	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	[12 :119]
143,142	$x \cdot (y \cdot y') = x$	[98 :137,137,137,137,137,137,137,137,52]
182	$x \cdot (y \cdot (z \cdot y)') = x \cdot ((u \cdot z)' \cdot u)$	[63 :137,137]
193	$B \cdot B' = A \cdot A'\ \rightarrow\ \Box$	[2 :143,137 :1,1]
196	$x \cdot (y \cdot (x \cdot y)') = z \cdot z'$	[142 → 45]
200,199	$(x \cdot y)' \cdot x = y'$	[142 → 5]
203	$x \cdot x' = y \cdot (z \cdot (y \cdot z)')$	[flip 196]
205,204	$x \cdot (y \cdot (z \cdot y)') = x \cdot z'$	[182 :200]
210	$x \cdot x' = y \cdot y'$	[flip 203 :205]
211	$\Box$	[210,193]

Example #DUAL-GT-2. The set

$$\left\{ \begin{array}{l} ((x \cdot y) \cdot z) \cdot (y \cdot z)' = x \\ (z \cdot y)' \cdot (z \cdot (y \cdot x)) = x \end{array} \right\}$$

is an independent self-dual basis for group theory.

Proof. By #Thm. DUAL-GT-1, the set is a basis for group theory; it is self-dual by inspection. Independence follows from the non-group model below, which

satisfies the first identity and not the second. (Also, it is well-known that a single identity for group theory must have at least 3 occurrences of inverse [15]).

The clauses

$$((x \cdot y) \cdot z) \cdot (y \cdot z)' = x$$
$$(C \cdot B)' \cdot (C \cdot (B \cdot A)) \neq A$$

have the following model (found by MACE 1.1.0 on gyro at 0.27 seconds).

```
* :
      | 0 1 2
   --+------
   0  | 0 0 0
   1  | 1 1 1
   2  | 2 2 2
@ :
      0 1 2
   ---------
      0 0 0
C: 0
B: 0
A: 1
end_of_model
```

Theorem #DUAL-GT-3.

$$\left\{ \begin{array}{l} (z \cdot (x \cdot y)) \cdot (y \cdot z)' = x \\ (z \cdot y)' \cdot ((y \cdot x) \cdot z) = x \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} x \cdot x' = y \cdot y' \\ x \cdot (y \cdot y') = x \\ (x \cdot y) \cdot z = x \cdot (y \cdot z) \\ x \cdot y = y \cdot x \end{array} \right\}.$$

($\Leftarrow$) is trivial, because the right-hand side is a well-known basis for Abelian group theory. The proof of ($\Rightarrow$) follows.

Proof (found by Otter 3.0.3k on gyro at 1.55 seconds).

1	$x = x$	
2	$B \cdot B' = A \cdot A',\ A \cdot (B \cdot B') = A,\ (A \cdot B) \cdot C = A \cdot (B \cdot C),\ B \cdot A = A \cdot B \ \rightarrow\ \Box$	
3	$(x \cdot (y \cdot z)) \cdot (z \cdot x)' = y$	
5	$(x \cdot y)' \cdot ((y \cdot z) \cdot x) = z$	
7	$(x \cdot y) \cdot ((z \cdot u)' \cdot x)' = u \cdot (y \cdot z)$	[3 → 3]
17	$((x \cdot y)' \cdot y)' \cdot z = z \cdot x$	[3 → 5]
20	$x \cdot y = ((y \cdot z)' \cdot z)' \cdot x$	[flip 17]
23	$x \cdot (y \cdot (y \cdot z)')' = z \cdot x$	[5 → 3]
26	$x \cdot y = y \cdot (z \cdot (z \cdot x)')'$	[flip 23]
31	$((x \cdot y) \cdot (z \cdot x)') \cdot z = y$	[5 → 17, flip]
62,61	$((x \cdot (y \cdot z))' \cdot y)' = z \cdot x$	[31 → 31, flip]
95	$(((x \cdot y)' \cdot y)' \cdot z)' \cdot ((x \cdot u) \cdot z) = u$	[20 → 5]

126	$x \cdot ((y \cdot (z \cdot x)') \cdot z) = y$	[31 → 7 :62, flip]
171	$x \cdot (((((y \cdot x)' \cdot z)' \cdot z)' \cdot u) \cdot y) = u$	[20 → 126]
173	$x \cdot (((y \cdot x)' \cdot z) \cdot y) = ((z \cdot u)' \cdot u)'$	[17 → 126]
183,182	$(x \cdot (x \cdot y)')' = y$	[5 → 126]
184	$((x \cdot y)' \cdot y)' = z \cdot (((u \cdot z)' \cdot x) \cdot u)$	[flip 173]
185	$x \cdot y = y \cdot x$	[26 :183]
198	$(((x \cdot (y \cdot z)') \cdot y) \cdot (u \cdot z)) \cdot x' = u$	[126 → 3]
212,211	$((x \cdot y)' \cdot y)' \cdot z = x \cdot z$	[20 → 185]
223,222	$x \cdot (((y \cdot x)' \cdot z) \cdot y) = z$	[171 :212]
245	$(x \cdot y)' \cdot ((x \cdot z) \cdot y) = z$	[95 :212]
255	$((x \cdot y)' \cdot y)' = x$	[184 :223]
257	$(x \cdot (y \cdot x)')' = y$	[185 → 182]
294,293	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	[255 → 7]
330,329	$(x \cdot y)' \cdot (x \cdot (z \cdot y)) = z$	[245 :294]
353	$x \cdot (y \cdot x') = y$	[198 :294,294,294,330,294]
423	$B \cdot B' = A \cdot A',\ A \cdot (B \cdot B') = A \ \rightarrow\ \square$	[2 :294 :1,185]
458	$x \cdot (x' \cdot y) = y$	[185 → 353]
465,464	$(x \cdot y')' = y \cdot x'$	[353 → 182]
482,481	$x \cdot (y \cdot y') = x$	[257 :465,294]
492	$B \cdot B' = A \cdot A' \ \rightarrow\ \square$	[423 :482 :1]
526	$x \cdot x' = y \cdot y'$	[481 → 458]
527	$\square$	[526,492]

Example #DUAL-GT-4. The set

$$\left\{ \begin{array}{l} (z \cdot (x \cdot y)) \cdot (y \cdot z)' = x \\ (z \cdot y)' \cdot ((y \cdot x) \cdot z) = x \end{array} \right\}$$

is an independent self-dual basis for Abelian group theory.

Proof. By #Thm. DUAL-GT-2, the set is a basis for group theory; it is self-dual by inspection. The following noncommutative model of the first identity, and the dual model of the second identity show independence.

The clauses

$$(z \cdot (x \cdot y)) \cdot (y \cdot z)' = x$$
$$1 \cdot 2 \neq 2 \cdot 1$$

have the following model (found by MACE 1.1.0 on gyro at 0.14 seconds).

```
* :
    | 0 1 2
  --+------
  0 | 0 1 2
  1 | 2 0 1
  2 | 1 2 0
```

```
@ :
        0 1 2
     ---------
        0 2 1
end_of_model
```

The next few theorems present a 3-basis and a 4-basis for (ordinary) groups; both are independent and self-dual. These bases were found by "trial and error": we conjectured several variations, giving each to OTTER to search for a proof.

Theorem #DUAL-GT-5.

$$\left\{ \begin{array}{l} x \cdot (x' \cdot y) = y \\ (x \cdot y') \cdot y = x \\ (x \cdot y) \cdot ((z \cdot z') \cdot u) = (x \cdot (v' \cdot v)) \cdot (y \cdot u) \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} x \cdot x' = y \cdot y' \\ x \cdot (y \cdot y') = x \\ (x \cdot y) \cdot z = x \cdot (y \cdot z) \end{array} \right\}.$$

($\Leftarrow$) is trivial, because the right-hand side is a well-known basis for group theory. The proof of ($\Rightarrow$) follows.

Proof (found by Otter 3.0.3k on gyro at 0.49 seconds).

1	$x = x$	
2	$B \cdot B' = A \cdot A',\ A \cdot (B \cdot B') = A,\ (A \cdot B) \cdot C = A \cdot (B \cdot C)\ \rightarrow\ \Box$	
4,3	$x \cdot (x' \cdot y) = y$	
6,5	$(x \cdot y') \cdot y = x$	
7	$(x \cdot y) \cdot ((z \cdot z') \cdot u) = (x \cdot (v' \cdot v)) \cdot (y \cdot u)$	
8	$(x \cdot (y' \cdot y)) \cdot (z \cdot u) = (x \cdot z) \cdot ((v \cdot v') \cdot u)$	[flip 7]
9	$x'' \cdot y = x \cdot y$	[3 $\rightarrow$ 3, flip]
14,13	$x'' = x$	[9 $\rightarrow$ 5 :6, flip]
15	$x' \cdot (x \cdot y) = y$	[9 $\rightarrow$ 3]
17	$(x \cdot y) \cdot y' = x$	[13 $\rightarrow$ 5]
27	$(x \cdot y) \cdot z = (x \cdot (u' \cdot u)) \cdot (y \cdot z)$	[5 $\rightarrow$ 7]
38	$(x \cdot (y' \cdot y)) \cdot (z \cdot u) = (x \cdot z) \cdot u$	[flip 27]
42	$x \cdot (y \cdot x)' = y'$	[15 $\rightarrow$ 17]
50	$(x \cdot y)' = y' \cdot x'$	[17 $\rightarrow$ 42, flip]
65	$(x \cdot (y \cdot z)) \cdot (z' \cdot y') = x$	[50 $\rightarrow$ 17]
80	$(x \cdot ((y \cdot z) \cdot u)) \cdot (u' \cdot (z' \cdot y')) = x$	[50 $\rightarrow$ 65]
91,90	$(x \cdot y) \cdot ((z \cdot z') \cdot u) = x \cdot (y \cdot u)$	[15 $\rightarrow$ 8 :14, flip]
99,98	$x \cdot (y' \cdot y) = x$	[65 $\rightarrow$ 8 :14,91, flip]
118,117	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	[38 :99, flip]
120,119	$x \cdot (y \cdot y') = x$	[80 :118,118,118,118,4,4]
121	$B \cdot B' = A \cdot A'\ \rightarrow\ \Box$	[2 :120,118 :1,1]
125	$x \cdot x' = y \cdot y'$	[119 $\rightarrow$ 3]
126	$\Box$	[125,121]

Theorem #DUAL-GT-6. The set

$$\left\{ \begin{array}{l} x \cdot (x' \cdot y) = y \\ (x \cdot y') \cdot y = x \\ (x \cdot y) \cdot ((z \cdot z') \cdot u) = (x \cdot (v' \cdot v)) \cdot (y \cdot u) \end{array} \right\}$$

is an independent self-dual basis for group theory.

Proof. By #Thm. DUAL-GT-5, the set is a basis for group theory; it is self-dual by inspection. To prove independence, we show that no two members are a basis for group theory. The first two are not a basis, because three variables are required in any basis, the first and third are not a basis, as shown by the nongroup MACE example below, and the dual example holds for the second and third.

The third identity is too complex for the current version of MACE, so we add the additional constraint $x \cdot x' = y' \cdot y = 0$, which allows us to simplify the identity.

The clauses

$x \cdot (x' \cdot y) = y$
$(x \cdot y) \cdot (0 \cdot z) = (x \cdot 0) \cdot (y \cdot z)$
$x \cdot x' = 0$
$x' \cdot x = 0$
$1 \cdot 2 \neq 2 \cdot 1$

have the following model (found by MACE 1.1.0 on gyro at 0.71 seconds).

```
* :
     | 0 1 2
   --+------
   0 | 0 2 1
   1 | 1 0 2
   2 | 2 1 0
@ :
       0 1 2
   ---------
       0 1 2
end_of_model
```

Theorem #DUAL-GT-7.

$$\left\{ \begin{array}{l} x \cdot (x' \cdot y) = y \\ (y \cdot x') \cdot x = y \\ x \cdot x' = y' \cdot y \\ ((x \cdot (y \cdot z)) \cdot y) \cdot u = x \cdot (y \cdot ((z \cdot y) \cdot u)) \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} x \cdot x' = y \cdot y' \\ x \cdot (y \cdot y') = x \\ (x \cdot y) \cdot z = x \cdot (y \cdot z) \end{array} \right\}.$$

($\Leftarrow$) is trivial, because the right-hand side is a well-known basis for group theory. The proof of ($\Rightarrow$) follows.

Proof (found by Otter 3.0.3k on gyro at 0.18 seconds).

1	$x = x$	
2	$B \cdot B' = A \cdot A',\ A \cdot (B \cdot B') = A,\ (A \cdot B) \cdot C = A \cdot (B \cdot C) \ \rightarrow\ \Box$	
3	$x \cdot (x' \cdot y) = y$	
5	$(x \cdot y') \cdot y = x$	
7	$((x \cdot (y \cdot z)) \cdot y) \cdot u = x \cdot (y \cdot ((z \cdot y) \cdot u))$	
9	$x \cdot x' = y' \cdot y$	
17,16	$(x' \cdot x) \cdot y = y$	[9 → 5]
18	$x \cdot (y' \cdot y) = x''$	[9 → 3]
19	$x'' = x \cdot (y' \cdot y)$	[flip 18]
22,21	$x'' = x$	[5 → 16]
27,26	$x \cdot (y' \cdot y) = x$	[19 :22, flip]
28	$(x \cdot y) \cdot y' = x$	[21 → 5]
35,34	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	[16 → 7 :27,27,17]
44,43	$x \cdot (y \cdot y') = x$	[28 :35]
45	$B \cdot B' = A \cdot A' \ \rightarrow\ \Box$	[2 :44,35 :1,1]
51	$x \cdot x' = y \cdot y'$	[43 → 3]
52	$\Box$	[51,45]

Theorem #DUAL-GT-8. The set

$$\left\{ \begin{array}{ll} (1) & x \cdot (x' \cdot y) = y \\ (2) & (y \cdot x') \cdot x = y \\ (3) & x \cdot x' = y' \cdot y \\ (4) & ((x \cdot (y \cdot z)) \cdot y) \cdot u = x \cdot (y \cdot ((z \cdot y) \cdot u)) \end{array} \right\}$$

is an independent self-dual basis for group theory.

Proof. By #Thm. DUAL-GT-6, the set is a basis for group theory; it is self-dual by inspection. To prove independence, we show that no three members are a basis for group theory. The set {1,2,3} is not a basis, because three variables are required in any basis, {1,3,4} is not a basis by the first MACE example below; {2,3,4} is not a basis by dual model; and {1,2,4} is not a basis by the second MACE example below.

The clauses

$x \cdot (x' \cdot y) = y$
$x \cdot x' = y' \cdot y$
$((x \cdot (y \cdot z)) \cdot y) \cdot u = x \cdot (y \cdot ((z \cdot y) \cdot u))$
$(1 \cdot 2') \cdot 2 \neq 1$

have the following model (found by MACE 1.1.0 on gyro at 28.35 seconds).

```
* :
    | 0 1 2
  --+------
  0 | 0 2 1
```

```
      1 | 1 0 2
      2 | 2 1 0
 @ :
          0 1 2
      ---------
          0 1 2
end_of_model
```

The clauses

$x \cdot (x' \cdot y) = y$
$(y \cdot x') \cdot x = y$
$((x \cdot (y \cdot z)) \cdot y) \cdot u = x \cdot (y \cdot ((z \cdot y) \cdot u))$
$1 \cdot 1' \neq 2' \cdot 2$

have the following model (found by MACE 1.1.0 on gyro at 26.09 seconds).

```
 * :
        | 0 1 2
      --+------
      0 | 0 2 1
      1 | 2 1 0
      2 | 1 0 2
 @ :
          0 1 2
      ---------
          0 1 2
end_of_model
```

6.3 Self-Dual Schemas for Subvarieties of Group Theory

In this section, we given Neumann-type schemas [9, 24] for equational subvarieties of groups. In particular, we give bases containing meta-terms G and F, that can be replaced with terms specifying the subvariety of interest. The resulting basis is self-dual. Any equational subvariety of groups can be specified with an equation $\alpha = e$, where e is the group identity; the term α and its dual, always with fresh variables, replace the meta-terms. After Thm. #DUAL-GT-9 below, we say more about how this works and give an example.

Here we consider bases of cardinalities 2, 3, and 4. (In [33], we extend these to all finite cardinalities ≥ 2, and show independence of all the resulting bases.) These bases were found by considering the 2-, 3-, and 4-bases in the preceding section and conjecturing various positions for the meta-terms. OTTER found proofs without much difficulty.

Theorem #DUAL-GT-9.

$$\left\{ \begin{array}{l} ((x\cdot y)\cdot(D_1\cdot z))\cdot(y\cdot(D_1\cdot z))' = x \\ ((x\cdot D_2)\cdot y)'\cdot((x\cdot D_2)\cdot(y\cdot z)) = z \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} x\cdot x' = y\cdot y' \\ x\cdot(y\cdot y') = x \\ (x\cdot y)\cdot z = x\cdot(y\cdot z) \end{array} \right\}.$$

Proof (found by Otter 3.0.3k on gyro at 2.70 seconds).

1	$x = x$	
2	$B\cdot B' = A\cdot A',\ A\cdot(B\cdot B') = A,\ (A\cdot B)\cdot C = A\cdot(B\cdot C)\ \rightarrow\ \square$	
3	$((x\cdot y)\cdot(D\cdot z))\cdot(y\cdot(D\cdot z))' = x$	
5	$((x\cdot F)\cdot y)'\cdot((x\cdot F)\cdot(y\cdot z)) = z$	
7	$(x\cdot(D\cdot y))\cdot((z\cdot(D\cdot u))'\cdot(D\cdot y))' = (x\cdot z)\cdot(D\cdot u)$	[3 → 3]
16,15	$((x\cdot(y\cdot(D\cdot z))')\cdot y)\cdot(D\cdot z) = x$	[3 → 7, flip]
28,27	$(((x\cdot(F\cdot(D\cdot y))')\cdot F)\cdot D)'\cdot x = y$	[15 → 5]
45	$(x\cdot y)'\cdot(x\cdot(y\cdot z)) = z$	[27 → 5 :28]
99	$((x\cdot y)'\cdot x)'\cdot z = y\cdot z$	[45 → 45]
139,138	$x\cdot((y\cdot x)'\cdot(y\cdot z)) = z$	[45 → 99, flip]
140	$((x\cdot y)'\cdot x)' = y$	[99 → 15 :16, flip]
144	$(x'\cdot(y\cdot z)')' = y\cdot(z\cdot x)$	[45 → 140]
154	$(x\cdot(y\cdot x)')' = y$	[140 → 140]
170	$x\cdot(y\cdot((x\cdot y)'\cdot z)) = z$	[154 → 45]
276	$((x\cdot(y\cdot z)')\cdot y)\cdot z = x$	[138 → 15 :139]
279	$((x\cdot y)\cdot z)\cdot(y\cdot z)' = x$	[138 → 3 :139]
309	$((x\cdot y)\cdot(z\cdot y)')\cdot z = x$	[140 → 276]
419	$x'\cdot(((x\cdot y)\cdot(z\cdot y)')\cdot(z\cdot u)) = u$	[309 → 45]
435,434	$x\cdot(y'\cdot y) = x$	[154 → 144, flip]
480	$(x\cdot y')\cdot y = x$	[276 → 434 :435, flip]
489	$((x'\cdot x)\cdot y')' = y$	[434 → 154]
493	$(x\cdot y)\cdot y' = x$	[434 → 279 :435]
521,520	$(x\cdot y)\cdot z = x\cdot(y\cdot z)$	[279 → 480, flip]
553,552	$x\cdot(y\cdot y') = x$	[493 :521]
556	$(x'\cdot(x\cdot y'))' = y$	[489 :521]
580,579	$x'\cdot(x\cdot y) = y$	[419 :521,521,521,139]
634	$B\cdot B' = A\cdot A'\ \rightarrow\ \square$	[2 :553,521 :1,1]
635	$x'' = x$	[556 :580]
648,647	$x\cdot(y\cdot x)' = y'$	[154 → 635, flip]
675	$x\cdot x' = y\cdot y'$	[552 → 170 :648]
676	$\square$	[675,634]

Theorem #DUAL-GT-10.

$$\left\{ \begin{array}{l} x\cdot(x'\cdot y) = y \\ (x\cdot y')\cdot y = x \\ ((x\cdot D_1)\cdot y)\cdot(D_2\cdot z) = (x\cdot D_1)\cdot(y\cdot(D_2\cdot z)) \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} x\cdot x' = y\cdot y' \\ x\cdot(y\cdot y') = x \\ (x\cdot y)\cdot z = x\cdot(y\cdot z) \end{array} \right\}.$$

Proof (found by Otter 3.0.3k on gyro at 0.23 seconds).

1	$x = x$	
2	$B \cdot B' = A \cdot A',\ A \cdot (B \cdot B') = A,\ (A \cdot B) \cdot C = A \cdot (B \cdot C)\ \rightarrow\ \square$	
4,3	$x \cdot (x' \cdot y) = y$	
6,5	$(x \cdot y') \cdot y = x$	
7	$((x \cdot D) \cdot y) \cdot (F \cdot z) = (x \cdot D) \cdot (y \cdot (F \cdot z))$	
9	$x'' \cdot y = x \cdot y$	[3 → 3, flip]
13	$x'' = x$	[9 → 5 :6, flip]
15	$x' \cdot (x \cdot y) = y$	[9 → 3]
17	$(x \cdot y) \cdot y' = x$	[13 → 5]
21	$(x \cdot y) \cdot (F \cdot z) = x \cdot (y \cdot (F \cdot z))$	[5 → 7 :6]
27	$x \cdot (y \cdot x)' = y'$	[15 → 17]
31	$(x \cdot y)' = y' \cdot x'$	[17 → 27, flip]
35	$(x \cdot (y \cdot z)) \cdot (z' \cdot y') = x$	[31 → 17]
54,53	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	[3 → 21 :4]
58,57	$x \cdot (y \cdot y') = x$	[35 :54,54,4]
59	$B \cdot B' = A \cdot A'\ \rightarrow\ \square$	[2 :58,54 :1,1]
63	$x \cdot x' = y \cdot y'$	[57 → 3]
64	$\square$	[63,59]

Theorem #DUAL-GT-11.

$$\left\{ \begin{array}{l} x \cdot (x' \cdot y) = y \\ (x \cdot y') \cdot y = x \\ x' \cdot x = y \cdot y' \\ ((x \cdot (D_1 \cdot y)) \cdot D_2) \cdot z = x \cdot (D_1 \cdot ((y \cdot D_2) \cdot z)) \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} x \cdot x' = y \cdot y' \\ x \cdot (y \cdot y') = x \\ (x \cdot y) \cdot z = x \cdot (y \cdot z) \end{array} \right\}.$$

Proof (found by Otter 3.0.3k on gyro at 3.31 seconds).

1	$x = x$	
2	$B \cdot B' = A \cdot A',\ A \cdot (B \cdot B') = A,\ (A \cdot B) \cdot C = A \cdot (B \cdot C)\ \rightarrow\ \square$	
3	$x \cdot (x' \cdot y) = y$	
5	$(x \cdot y') \cdot y = x$	
7	$x' \cdot x = y \cdot y'$	
8	$((x \cdot (D \cdot y)) \cdot F) \cdot z = x \cdot (D \cdot ((y \cdot F) \cdot z))$	
15	$x \cdot x' = y \cdot y'$	[7 → 7]
16	$(x \cdot x') \cdot y = y''$	[7 → 5]
18,17	$x \cdot (y \cdot y') = x$	[7 → 3]
19	$x'' = (y \cdot y') \cdot x$	[flip 16]
20	$(A \cdot B) \cdot C = A \cdot (B \cdot C)\ \rightarrow\ \square$	[2 :18 :15,1]
25,24	$x'' = x$	[3 → 17]
28,27	$(x \cdot x') \cdot y = y$	[19 :25, flip]
31	$(x \cdot y) \cdot y' = x$	[24 → 5]
33	$x' \cdot (x \cdot y) = y$	[24 → 3]
37	$((x \cdot y) \cdot F) \cdot z = x \cdot (D \cdot (((D' \cdot y) \cdot F) \cdot z))$	[3 → 8]
38	$(x \cdot F) \cdot y = x \cdot (D \cdot ((D' \cdot F) \cdot y))$	[17 → 8]

48	$x \cdot (D \cdot ((D' \cdot F) \cdot y)) = (x \cdot F) \cdot y$	[flip 38]
52,51	$(x' \cdot x) \cdot y = y$	[24 → 27]
61	$(x \cdot y)' \cdot x = y'$	[31 → 33]
76,75	$(x \cdot y)' = y' \cdot x'$	[33 → 61, flip]
94	$(x' \cdot y') \cdot ((y \cdot x) \cdot z) = z$	[75 → 33]
160,159	$D \cdot (((D' \cdot x) \cdot F) \cdot y) = (x \cdot F) \cdot y$	[51 → 37 :52, flip]
167,166	$x \cdot ((x' \cdot F) \cdot y) = F \cdot y$	[15 → 37 :28,160, flip]
173,172	$x \cdot (((x' \cdot y) \cdot F) \cdot z) = (y \cdot F) \cdot z$	[3 → 37 :160, flip]
181	$x \cdot ((y \cdot F) \cdot ((F' \cdot (y' \cdot x')) \cdot z)) = z$	[3 → 37 :76,76,173, flip]
195,194	$(x \cdot F) \cdot y = x \cdot (F \cdot y)$	[48 :167, flip]
215	$x \cdot (y \cdot (F \cdot ((F' \cdot (y' \cdot x')) \cdot z))) = z$	[181 :195]
233	$x \cdot (F \cdot ((F' \cdot x') \cdot y)) = y$	[3 → 194 :76, flip]
380	$(x' \cdot y) \cdot ((y' \cdot x) \cdot z) = z$	[24 → 94]
420,419	$F \cdot ((F' \cdot x) \cdot y) = x \cdot y$	[233 → 3 :25, flip]
423	$x \cdot (y \cdot ((y' \cdot x') \cdot z)) = z$	[215 :420]
563	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	[380 → 423 :25, flip]
565	□	[563,20]

6.4 Other Results in Self-Dual Equational Bases

Chapter 7

Lattice-like Algebras

7.1 Equational Theory of Lattices

[[Need a short introduction to this chapter. What are the theorems about??]]

The following six identities form a basis for lattice theory (LT).

$$x \wedge y = y \wedge x, \qquad x \vee y = y \vee x, \qquad \text{(commutativity)}$$
$$(x \wedge y) \wedge z = x \wedge (y \wedge z), \qquad (x \vee y) \vee z = x \vee (y \vee z), \qquad \text{(associativity)}$$
$$x \wedge (x \vee y) = x, \qquad x \vee (x \wedge y) = x, \qquad \text{(absorption)}$$

Note that the basis is self-dual, that is, it contains all of its dual identities. Three MACE runs easily show the basis to be independent. The two idempotence laws,

$$x \wedge x = x, \qquad x \vee x = x, \qquad \text{(idempotence)}$$

can be trivially derived from the two absorption laws, and we generally include the idempotence laws when using this basis.

We start with the following basic theorem about distributivity, which is usually proved (easily) with the model-theoretic $M_5 - N_5$ argument [**?**].

Theorem #LT-1. In lattice theory, a distributive law implies its dual.

$$\{\text{LT}, x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)\} \Rightarrow \{x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)\}$$

Proof (found by Otter 3.0.3l on gyro at 4.02 seconds).

4	$x \wedge y = y \wedge x$
6,5	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$
9	$x \vee y = y \vee x$
10	$(x \vee y) \vee z = x \vee (y \vee z)$
12	$x \wedge (x \vee y) = x$
14	$x \vee (x \wedge y) = x$
16	$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$

17	$(x \wedge y) \vee (x \wedge z) = x \wedge (y \vee z)$	[flip 16]
19	$A \vee (B \wedge C) \neq (A \vee B) \wedge (A \vee C)$	
20	$x \wedge (y \vee x) = x$	[9 → 12]
22	$(x \vee y) \wedge x = x$	[4 → 12]
35	$x \vee (y \wedge x) = x$	[4 → 14]
39	$x \wedge (y \wedge x) = x \wedge y$	[14 → 20 :6]
53	$(x \wedge y) \vee y = y$	[9 → 35]
55	$x \vee ((y \wedge x) \vee z) = x \vee z$	[35 → 10, flip]
70	$(x \vee (y \vee z)) \wedge (x \vee y) = x \vee y$	[10 → 22]
91,90	$x \vee ((x \vee y) \wedge z) = (x \vee y) \wedge (x \vee z)$	[22 → 17]
145	$A \vee (C \wedge B) \neq (A \vee B) \wedge (A \vee C)$	[4 → 19]
346,345	$x \vee (y \wedge (x \vee z)) = x \vee (y \wedge z)$	[17 → 55]
502,501	$(x \vee y) \wedge (x \vee (z \wedge y)) = x \vee (z \wedge y)$	[53 → 70]
816	$x \vee (y \wedge z) = (x \vee z) \wedge (x \vee y)$	[39 → 90 :91,346,502, flip]
818	$\Box$	[816,145]

It was previously known that the following self-dual identity can be used to express distributivity in lattice theory.

$$(x \wedge y) \vee (y \wedge z) \vee (x \wedge z) = (x \vee y) \wedge (y \vee z) \wedge (x \vee z)$$

The following theorem gives us an alternate identity.

Theorem #LT-1c. A new self-dual form of distributivity for lattice theory.

$$\{\text{LT}, (((x \wedge y) \vee z) \wedge y) \vee (z \wedge x) = (((x \vee y) \wedge z) \vee y) \wedge (z \vee x)\} \Rightarrow \{x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)\}$$

Proof (found by Otter 3.0.3l on gyro at 11.43 seconds).

3,2	$x \wedge x = x$	
4	$x \wedge y = y \wedge x$	
6,5	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$	
8,7	$x \vee x = x$	
9	$x \vee y = y \vee x$	
11,10	$(x \vee y) \vee z = x \vee (y \vee z)$	
12	$x \wedge (x \vee y) = x$	
15,14	$x \vee (x \wedge y) = x$	
16	$(((x \wedge y) \vee z) \wedge y) \vee (z \wedge x) = (((x \vee y) \wedge z) \vee y) \wedge (z \vee x)$	
20	$A \vee (B \wedge C) \neq (A \vee B) \wedge (A \vee C)$	
21	$x \wedge (y \wedge z) = y \wedge (x \wedge z)$	[4 → 5 :6]
22	$x \wedge (x \wedge y) = x \wedge y$	[2 → 5, flip]
29,28	$x \wedge (y \vee x) = x$	[9 → 12]
33,32	$(x \vee y) \wedge x = x$	[4 → 12]
36	$x \vee (y \vee z) = y \vee (x \vee z)$	[9 → 10 :11]
38,37	$x \vee (x \vee y) = x \vee y$	[7 → 10, flip]
47	$x \vee (y \wedge x) = x$	[4 → 14]

51	$(x \wedge y) \vee x = x$	[9 → 14]
53	$x \vee ((x \wedge y) \vee z) = x \vee z$	[14 → 10, flip]
56,55	$x \wedge (y \wedge x) = x \wedge y$	[14 → 28 :6]
57	$x \wedge (y \vee (z \vee x)) = x$	[10 → 28]
61	$(x \vee y) \wedge y = y$	[4 → 28]
67	$(((x \wedge y) \vee z) \wedge x) \vee (z \wedge y) = (((y \vee x) \wedge z) \vee x) \wedge (z \vee y)$	[4 → 16]
76	$((((x \vee y) \wedge z) \vee x) \wedge z) \vee x = (x \vee z) \wedge (x \vee y)$	[12 → 16 :11,33,38]
89	$(((x \vee (y \vee x)) \wedge z) \vee x) \wedge (z \vee (x \vee y)) = x \vee (z \wedge (x \vee y))$	[32 → 16 :33,11, flip]
92,91	$x \vee (y \vee x) = x \vee y$	[32 → 14 :11]
94,93	$(x \vee y) \wedge (x \wedge z) = x \wedge z$	[32 → 5, flip]
95	$(((x \vee y) \wedge z) \vee x) \wedge (z \vee (x \vee y)) = x \vee (z \wedge (x \vee y))$	[89 :92]
110,109	$x \vee ((y \wedge x) \vee z) = x \vee z$	[47 → 10, flip]
118	$(((x \vee y) \wedge z) \vee y) \wedge (z \wedge x) = z \wedge x$	[16 → 61 :6,94]
122	$(((x \vee y) \wedge z) \vee y) \wedge (z \vee (x \vee y)) = y \vee (z \wedge (x \vee y))$	[61 → 16 :33,11,8, flip]
127	$(B \wedge C) \vee A \neq (A \vee B) \wedge (A \vee C)$	[9 → 20]
141,140	$(x \vee y) \wedge (z \wedge y) = z \wedge y$	[61 → 21, flip]
142	$(x \vee y) \wedge (z \wedge x) = z \wedge x$	[32 → 21, flip]
207,206	$(x \vee y) \wedge (z \vee (y \vee x)) = x \vee y$	[91 → 57]
559,558	$((x \wedge y) \vee z) \wedge (u \vee (y \vee z)) = (x \wedge y) \vee z$	[109 → 57]
696,695	$(x \vee (y \wedge z)) \wedge (z \wedge y) = z \wedge y$	[55 → 140 :56]
747,746	$((x \wedge y) \vee z) \wedge (y \wedge x) = y \wedge x$	[55 → 142 :56]
936	$(x \wedge y) \vee (z \vee ((((y \vee x) \wedge z) \vee x) \wedge (z \vee y))) = (x \wedge y) \vee z$	[67 → 53 :11,11,15]
1222,1221	$(x \wedge (y \vee z)) \vee y = (y \vee (x \wedge (y \vee z))) \wedge (y \vee z)$	[55 → 76 :747]
1224,1223	$((x \vee y) \wedge z) \vee x = (x \vee ((x \vee y) \wedge z)) \wedge (x \vee y)$	[22 → 76 :33]
1226,1225	$(x \vee ((x \vee y) \wedge z)) \wedge (x \vee y) = (x \vee z) \wedge (x \vee y)$	[4 → 76 :1222,6,696,1224]
1234,1233	$x \vee ((x \vee y) \wedge z) = (x \vee z) \wedge (x \vee y)$	[9 → 76 :1224,1226,6,141]
1246,1245	$x \vee (y \wedge (x \vee z)) = (x \vee y) \wedge (x \vee z)$	[95 :1224,1234,6,3,6,29, flip]
1248,1247	$((x \vee y) \wedge z) \vee x = (x \vee z) \wedge (x \vee y)$	[1223 :1234,6,3]
1254,1253	$(x \wedge y) \vee ((z \vee x) \wedge (z \vee y)) = (x \wedge y) \vee z$	[936 :1246,110]
2199	$(x \wedge y) \vee (((y \vee z) \wedge x) \vee z) = ((y \vee z) \wedge x) \vee z$	[118 → 51]
2238,2237	$x \vee (y \wedge (z \vee x)) = (x \vee y) \wedge (x \vee z)$	[9 → 122 :1248,6,207, flip]
2265,2264	$((x \vee y) \wedge z) \vee y = (y \vee z) \wedge (y \vee x)$	[36 → 122 :559,2238]
2280	$(x \wedge y) \vee z = (z \vee x) \wedge (z \vee y)$	[2199 :2265,1254,2265]
2281	$\square$	[2280,127]

[[Note: First euqational proof of N5 problem. We need some background here.]]

Theorem #LT-N5. The lattice theory N_5 problem (suggested by David Kelly).

Proof (found by Otter 3.0.3l on gyro at 101.64 seconds).

1	$x = x$
2	$x \vee x = x$
5,4	$x \wedge x = x$

6	$x \vee y = y \vee x$	
7	$x \wedge y = y \wedge x$	
9,8	$(x \vee y) \vee z = x \vee (y \vee z)$	
11,10	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$	
13,12	$x \wedge (x \vee y) = x$	
15,14	$x \vee (x \wedge y) = x$	
16	$x \wedge (y \vee (z \wedge (x \vee u))) = (x \wedge (y \vee (x \wedge z))) \vee (x \wedge ((x \wedge y) \vee (z \wedge u)))$	
17	$(x \wedge (y \vee (x \wedge z))) \vee (x \wedge ((x \wedge y) \vee (z \wedge u))) = x \wedge (y \vee (z \wedge (x \vee u)))$ [flip 16]	
19	$x \vee (y \wedge (z \vee (x \wedge u))) = (x \vee (y \wedge (x \vee z))) \wedge (x \vee ((x \vee y) \wedge (z \vee u)))$	
20	$(x \vee (y \wedge z)) \wedge (z \vee (x \wedge y)) = (z \wedge (x \vee (y \wedge z))) \vee (x \wedge (y \vee z))$	
21	$(x \wedge (y \vee (z \wedge x))) \vee (y \wedge (z \vee x)) = (y \vee (z \wedge x)) \wedge (x \vee (y \wedge z))$ [flip 20]	
23	$a \wedge ((b \vee c) \wedge (b \vee d)) \neq (a \wedge ((b \vee c) \wedge (b \vee d))) \wedge ((a \wedge (b \vee (c \wedge d))) \vee ((a \wedge c) \vee (a \wedge d)))$	
24	$a \wedge ((b \vee c) \wedge ((b \vee d) \wedge ((a \wedge (b \vee (c \wedge d))) \vee ((a \wedge c) \vee (a \wedge d))))) \neq a \wedge ((b \vee c) \wedge (b \vee d))$ [
25	$(x \vee (y \wedge (x \vee z))) \wedge (x \vee ((x \vee y) \wedge (z \vee u))) = x \vee (y \wedge (z \vee (x \wedge u)))$ [flip 19]	
26	$x \wedge (y \vee x) = x$	$[6 \to 12]$
28	$(x \vee y) \wedge x = x$	$[7 \to 12]$
30	$x \vee (y \vee z) = y \vee (x \vee z)$	$[6 \to 8 :9]$
32,31	$x \vee (x \vee y) = x \vee y$	$[2 \to 8, \text{flip}]$
33	$x \vee (y \vee z) = y \vee (z \vee x)$	$[6 \to 8]$
36	$x \vee (y \vee z) = z \vee (x \vee y)$	[flip 33]
40,39	$x \vee (y \wedge x) = x$	$[7 \to 14]$
43	$(x \wedge y) \vee x = x$	$[6 \to 14]$
45	$x \vee ((x \wedge y) \vee z) = x \vee z$	$[14 \to 8, \text{flip}]$
48,47	$x \wedge (y \wedge x) = x \wedge y$	$[14 \to 26 :11]$
50,49	$x \wedge (y \vee (z \vee x)) = x$	$[8 \to 26]$
51	$(x \vee y) \wedge y = y$	$[7 \to 26]$
55	$x \vee (y \vee x) = x \vee y$	$[28 \to 14 :9]$
59	$(x \wedge y) \vee y = y$	$[6 \to 39]$
62,61	$x \vee ((y \wedge x) \vee z) = x \vee z$	$[39 \to 8, \text{flip}]$
63	$(x \vee y) \wedge (x \wedge z) = x \wedge z$	$[28 \to 10, \text{flip}]$
69	$x \wedge (y \wedge z) = y \wedge (x \wedge z)$	$[7 \to 10 :11]$
71,70	$x \wedge (x \wedge y) = x \wedge y$	$[4 \to 10, \text{flip}]$
76	$x \wedge (y \wedge z) = y \wedge (z \wedge x)$	$[7 \to 10]$
77	$x \wedge (y \wedge z) = z \wedge (x \wedge y)$	[flip 76]
78	$x \vee (y \wedge (z \wedge x)) = x$	$[10 \to 39]$
83,82	$(x \wedge (y \wedge z)) \vee (x \wedge y) = x \wedge y$	$[10 \to 43]$
86	$(x \vee (y \vee z)) \wedge z = z$	$[8 \to 51]$
90	$(x \wedge (y \wedge z)) \vee z = z$	$[10 \to 59]$
92	$(x \wedge y) \vee (y \vee z) = y \vee z$	$[59 \to 8, \text{flip}]$
104	$(x \wedge (y \vee (z \wedge x))) \vee (x \wedge ((x \wedge y) \vee (z \wedge u))) = x \wedge (y \vee (z \wedge (x \vee u)))$ $[7 \to 17]$	
112	$(x \wedge (y \vee (z \vee (x \wedge u)))) \vee (x \wedge ((x \wedge (y \vee z)) \vee (u \wedge v))) = x \wedge (y \vee (z \vee (u \wedge (x \vee v))))$ [8 −	
126	$(x \wedge (y \vee (x \wedge z))) \vee (x \wedge ((y \wedge x) \vee (z \wedge u))) = x \wedge (y \vee (z \wedge (x \vee u)))$ $[7 \to 17]$	
128	$(x \wedge (y \vee (x \wedge (z \vee u)))) \vee (x \wedge ((x \wedge y) \vee u)) = x \wedge (y \vee ((z \vee u) \wedge (x \vee u)))$ $[51 \to 17]$	
132	$(x \wedge (y \vee (x \wedge z))) \vee (x \wedge ((x \wedge y) \vee z)) = x \wedge (y \vee z)$	$[26 \to 17 :50]$
167,166	$x \wedge (y \wedge (z \wedge x)) = x \wedge (y \wedge z)$	$[10 \to 47]$

168	$(x \wedge y) \vee (y \wedge x) = x \wedge y$	[47 → 39]
175,174	$x \wedge (y \wedge (x \wedge z)) = x \wedge (y \wedge z)$	[47 → 10 :11,11, flip]
189,188	$x \wedge (y \wedge (z \vee x)) = x \wedge y$	[14 → 49 :11]
192	$x \wedge (y \vee (x \vee z)) = x$	[6 → 49]
210	$(x \vee y) \wedge (y \vee x) = x \vee y$	[55 → 26]
242,241	$x \vee (y \wedge (x \wedge z)) = x$	[43 → 19 :11,15,40,11,13]
273	$x \vee (y \vee (z \wedge x)) = x \vee y$	[12 → 78 :9]
295	$(x \vee (y \vee z)) \wedge y = y$	[6 → 86]
305	$(x \wedge y) \vee (z \vee y) = z \vee y$	[26 → 90]
361	$(x \wedge y) \vee (y \wedge (x \wedge z)) = y \wedge x$	[43 → 21 :48,11,11,11,189,11,83,11,11,11,167,242,11,5]
409	$(x \vee (y \wedge z)) \wedge ((z \vee (x \wedge y)) \wedge (x \wedge (y \vee z))) = x \wedge (y \vee z)$	[21 → 51 :11]
481,480	$x \vee (y \vee (x \wedge z)) = y \vee x$	[14 → 30, flip]
487	$x \vee ((y \wedge (x \vee z)) \vee z) = x \vee z$	[59 → 30, flip]
527	$x \vee (y \vee z) = z \vee (y \vee x)$	[6 → 33]
576,575	$x \wedge (y \wedge (x \vee z)) = x \wedge y$	[45 → 192 :11]
578,577	$((x \wedge y) \vee z) \wedge (x \vee z) = (x \wedge y) \vee z$	[45 → 26]
626	$x \vee (y \wedge ((x \wedge z) \vee (x \wedge u))) = x$	[14 → 25 :40,13, flip]
644	$((x \wedge y) \vee (x \wedge ((x \wedge y) \vee z))) \wedge ((x \wedge y) \vee (x \wedge (z \vee u))) = (x \wedge y) \vee (x \wedge (z \vee (x \wedge (y \wedge u))))$	[43 → 25 :11]
686	$(x \wedge y) \vee (x \wedge (z \vee (x \wedge (y \wedge u)))) = ((x \wedge y) \vee (x \wedge ((x \wedge y) \vee z))) \wedge ((x \wedge y) \vee (x \wedge (z \vee u)))$	[flip 644]
824,823	$(x \vee y) \wedge (z \wedge (x \wedge u)) = z \wedge (x \wedge u)$	[63 → 69, flip]
835	$x \wedge (((x \wedge y) \vee z) \wedge y) = x \wedge y$	[28 → 69, flip]
840	$(x \vee (y \wedge z)) \wedge (y \wedge (z \vee x)) = y \wedge (z \vee x)$	[409 :824]
1109	$x \wedge (y \wedge (z \vee (y \wedge x))) = x \wedge y$	[168 → 49 :11]
1121,1120	$((x \wedge y) \vee z) \wedge (u \wedge (y \vee z)) = ((x \wedge y) \vee z) \wedge u$	[61 → 188]
1123,1122	$(x \vee y) \wedge (z \wedge (y \vee x)) = (x \vee y) \wedge z$	[55 → 188]
1129,1128	$(x \vee y) \wedge (z \wedge (y \vee (u \vee x))) = (x \vee y) \wedge z$	[36 → 188]
1156,1155	$(x \wedge y) \vee (y \wedge (z \vee x)) = y \wedge (z \vee x)$	[188 → 59]
1271	$x \wedge (y \vee z) = (z \vee y) \wedge x$	[210 → 77 :1123]
1272	$(x \vee y) \wedge z = z \wedge (y \vee x)$	[flip 1271]
1341,1340	$(x \vee (y \wedge z)) \wedge (u \wedge (z \vee x)) = (x \vee (y \wedge z)) \wedge u$	[273 → 188]
1351	$(x \vee (y \wedge z)) \wedge y = y \wedge (z \vee x)$	[840 :1341]
1916	$a \wedge ((b \vee c) \wedge ((b \vee d) \wedge ((a \wedge d) \vee ((a \wedge c) \vee (a \wedge (b \vee (c \wedge d))))))) \neq a \wedge ((b \vee c) \wedge (b \vee d))$	[527 → 24]
1971,1970	$(x \wedge y) \vee (z \vee (y \wedge (x \vee u))) = z \vee (y \wedge (x \vee u))$	[575 → 305]
2231,2230	$(x \wedge y) \vee (x \wedge (z \vee (y \vee u))) = x \wedge (z \vee (y \vee u))$	[295 → 82]
2243,2242	$(x \wedge (y \wedge z)) \vee (x \wedge (y \vee u)) = x \wedge (y \vee u)$	[63 → 82]
2247,2246	$(x \wedge y) \vee (x \wedge (z \vee y)) = x \wedge (z \vee y)$	[51 → 82]
3172,3171	$(x \wedge y) \vee (x \wedge ((x \wedge (y \wedge z)) \vee (y \wedge u))) = x \wedge y$	[82 → 104 :48,175,2243,576]
3853	$(x \wedge ((x \wedge y) \vee z)) \vee (x \wedge ((x \wedge ((x \wedge y) \vee z)) \vee (y \wedge u))) = x \wedge (z \vee (y \wedge (x \vee u)))$	[55 → 112 :1971]
4053,4052	$(x \wedge (y \vee (x \wedge z))) \vee (x \wedge z) = (y \vee (x \wedge z)) \wedge x$	[51 → 361]
5139	$(x \wedge y) \vee (z \wedge (u \vee (x \wedge (z \vee y)))) = (x \wedge y) \vee (z \wedge (u \vee (z \wedge x)))$	[126 → 273 :9,1971,9,1971]
5159	$(x \wedge y) \vee (z \wedge (u \vee (z \wedge x))) = (x \wedge y) \vee (z \wedge (u \vee (x \wedge (z \vee y))))$	[flip 5139]
5530,5529	$x \vee (y \wedge ((y \wedge x) \vee z)) = x \vee (y \wedge (x \vee z))$	[128 → 487 :578,62, flip]
6026	$x \wedge (((y \wedge z) \vee (y \wedge u)) \wedge y) = x \wedge ((y \wedge z) \vee (y \wedge u))$	[626 → 26 :11]
6072,6071	$x \wedge (y \wedge ((x \wedge z) \vee (x \wedge u))) = y \wedge ((x \wedge z) \vee (x \wedge u))$	[626 → 51]
6739,6738	$(x \vee (y \wedge (x \vee z))) \wedge y = y \wedge (x \vee z)$	[92 → 132 :4053,32]

6830,6829 $x \wedge (y \vee (x \wedge (y \vee z))) = x \wedge (y \vee z)$ [132 → 132 :71,9,2247,5530,71,4053,6739,9,2247,5530,
6857 $((x \wedge y) \vee z) \wedge ((x \wedge (y \vee (x \wedge z))) \vee (x \wedge ((x \wedge y) \vee (z \vee u)))) = ((x \wedge y) \vee z) \wedge x$ [132 → 1
7082,7081 $(x \wedge y) \vee (x \wedge ((x \wedge y) \vee z)) = x \wedge ((x \wedge y) \vee z)$ [835 → 82]
7141 $x \wedge ((x \wedge ((x \wedge y) \vee z)) \vee (y \wedge u)) = x \wedge (z \vee (y \wedge (x \vee u)))$ [3853 :7082]
7189 $(x \wedge y) \vee (x \wedge (z \vee (x \wedge (y \wedge u)))) = ((x \wedge y) \vee z) \wedge ((x \wedge y) \vee (x \wedge (z \vee u)))$ [686 :7082,11,6
8277 $(x \wedge y) \vee (y \wedge (z \vee (y \wedge x))) = y \wedge (z \vee (y \wedge x))$ [1109 → 59]
9238,9237 $((x \wedge y) \vee z) \wedge x = x \wedge (y \vee z)$ [6 → 1351]
9241,9240 $x \wedge ((x \wedge y) \vee z) = x \wedge (y \vee z)$ [1272 → 1351]
9397,9396 $x \wedge ((y \wedge z) \vee (y \wedge u)) = x \wedge (y \wedge (z \vee (y \wedge u)))$ [6026 :9238, flip]
9603,9602 $x \wedge (y \vee (z \wedge (x \vee u))) = x \wedge (y \vee z)$ [7141 :9241,9241,9,481, flip]
9965,9964 $((x \wedge y) \vee z) \wedge (x \wedge (y \vee (z \vee u))) = x \wedge (y \vee z)$ [6857 :9241,9397,9,2231,6830,9238]
10254 $(x \wedge y) \vee (x \wedge (z \vee (x \wedge (y \wedge u)))) = ((x \wedge y) \vee z) \wedge (x \wedge (y \vee (x \wedge (z \vee u))))$ [7189 :9397]
10762,10761 $(x \wedge y) \vee (z \wedge (u \vee (z \wedge x))) = (x \wedge y) \vee (z \wedge (u \vee x))$ [5159 :9603]
10966,10965 $x \wedge (y \vee (x \wedge z)) = x \wedge (y \vee z)$ [8277 :10762,1156, flip]
11208,11207 $(x \wedge y) \vee (x \wedge (z \vee (y \wedge u))) = x \wedge (y \vee z)$ [10254 :10966,10966,9965]
11311,11310 $x \wedge ((y \wedge z) \vee (y \wedge u)) = x \wedge (y \wedge (z \vee u))$ [9396 :10966]
11477 $a \wedge ((b \vee c) \wedge (b \vee d)) \neq a \wedge ((b \vee c) \wedge (b \vee d))$ [1916 :11208,11311,1129,167]
11478 $\Box$ [11477,1]

The following four absorption identities, due to R. McKenzie [21], are a basis for lattice theory.

$$y \vee (x \wedge (y \wedge z)) = y, \qquad y \wedge (x \vee (y \vee z)) = y, \qquad \text{(L1,L2)}$$
$$((x \wedge y) \vee (y \wedge z)) \vee y = y, \qquad ((x \vee y) \wedge (y \vee z)) \wedge y = y. \qquad \text{(L3,L4)}$$

The next theorem gives us a new and simpler absorption basis.

Theorem #LT-2. The following set is an absorption basis for lattice theory.

$$\left\{ \begin{array}{ll} y \wedge (x \vee (y \vee z)) = y & \text{(L2)} \\ ((x \wedge y) \vee (y \wedge z)) \vee y = y & \text{(L3)} \\ ((y \vee x) \wedge (y \vee z)) \wedge y = y & \text{(L4}') \end{array} \right\}.$$

It is sufficient to prove (L1) and (L4) of the McKenzie basis.

Proof (found by Otter 3.0.3l on gyro at 7.95 seconds).

1 $x = x$
2 $B \vee (A \wedge (B \wedge C)) = B,\ ((A \vee B) \wedge (B \vee C)) \wedge B = B \ \rightarrow \ \Box$
3 $x \wedge (y \vee (x \vee z)) = x$
5 $((x \wedge y) \vee (y \wedge z)) \vee y = y$
7 $((x \vee y) \wedge (x \vee z)) \wedge x = x$
11 $((x \wedge y) \vee y) \vee y = y$ [3 → 5]
14,13 $x \wedge (x \vee y) = x$ [5 → 3]
37 $(x \vee y) \wedge x = x$ [3 → 7]
41 $(x \vee x) \vee x = x$ [7 → 11]
43 $(x \vee (x \wedge y)) \vee x = x$ [7 → 5]

59	$x \wedge ((y \wedge x) \vee x) = (y \wedge x) \vee x$	[11 → 37]
70,69	$x \vee x = x$	[41 → 37 :14, flip]
76,75	$x \wedge (y \vee x) = x$	[41 → 3 :70,70]
77	$(x \wedge y) \vee y = y$	[59 :76, flip]
91	$x \vee (y \vee x) = y \vee x$	[75 → 77]
99	$x \wedge (y \wedge x) = y \wedge x$	[77 → 37]
109	$(x \wedge y) \wedge (z \vee y) = x \wedge y$	[77 → 3]
116,115	$x \vee (x \wedge y) = x$	[43 → 37 :14, flip]
146,145	$((x \vee y) \wedge (y \vee z)) \wedge y = y$	[91 → 7]
153	$B \vee (A \wedge (B \wedge C)) = B \ \rightarrow \ \square$	[2 :146 :1]
202	$x \vee (y \wedge x) = x$	[99 → 115]
474	$(x \vee y) \vee (z \wedge y) = x \vee y$	[109 → 202]
1504	$x \vee (y \wedge (x \wedge z)) = x$	[115 → 474 :116]
1506	$\square$	[1504,153]

7.2 Presence of Jónsson Polynomials

A term in three variables, say $p(x, y, z)$, is a *ternary majority polynomial* (Jónsson polynomial [10]) for a theory if it satisfies $p(x, x, y) = p(x, y, x) = p(y, x, x) = y$ in the theory. For example, the each of following is a ternary majority polynomial for lattice theory:

$$(x \wedge y) \vee (y \wedge z) \vee (x \wedge z),$$
$$(x \wedge z) \vee (y \wedge (x \vee z)).$$

7.2.1 A Reduction Schema

With the following theorem we can construct single axioms for many theories, including lattice theory.

Theorem #MAJ-1. Majority polynomial single axiom (from [26]).

$$\left\{ \begin{array}{l} p(x,y,y) = y \\ p(y,x,y) = y \\ p(y,y,x) = y \\ f(y) = y. \end{array} \right\} \Leftrightarrow \{p(p(x,y,y),u,p(p(x,y,y),f(y),z)) = y\}.$$

($\Rightarrow$) is trivial by simplification. The proof of ($\Leftarrow$) follows.

Proof (found by Otter 3.0.3l on gyro at 0.08 seconds).

1	$x = x$	
2	$p(A,A,B) = A,\ p(A,B,A) = A,\ p(B,A,A) = A,\ f(A) = A \ \rightarrow \ \square$	
3	$p(p(x,y,y),z,p(p(x,y,y),f(y),u)) = y$	
8,7	$p(p(x,y,y),z,y) = y$	[3 → 3]
10,9	$p(x,y,x) = x$	[7 → 7]
11	$p(x,y,p(p(z,x,x),f(x),u)) = p(p(z,x,x),f(x),u)$	[3 → 7]

13	$p(A,A,B)=A,\ p(B,A,A)=A,\ f(A)=A\ \rightarrow\ \Box$	[2 :10 :1]
15,14	$p(x,y,p(x,f(x),z))=x$	[7 → 3 :8]
17,16	$p(x,y,y)=y$	[9 → 3 :10]
18	$p(A,A,B)=A,\ f(A)=A\ \rightarrow\ \Box$	[13 :17 :1]
19	$p(x,f(x),y)=x$	[11 :17,15,17, flip]
22,21	$f(x)=x$	[16 → 19]
24,23	$p(x,x,y)=x$	[19 :22]
25	$\Box$	[18 :24,22 :1,1]

With Theorem #MAJ-1 we can construct a single axiom for any theory that admits a ternary majority polynomial and can be axiomatized with absorption identities. The method and proof are given in [26]. Lattice theory qualifies, with majority polynomial $p(x,y,z)=(x\wedge z)\vee(y\wedge(x\vee z))$ and the four identities of McKenzie. Bundling the identities as

$$f(y)=p(p(\mathrm{L1}(y),\mathrm{L2}(y),u),p(\mathrm{L3}(y),\mathrm{L4}(y),u),v),$$

then substituting this into the single axiom above, then expanding to obtain the single axiom in terms of $\wedge$ and $\vee$ produces a single axiom of weight 259 with 7 variables (see [26]). The motivation for the next several theorems is to find a shorter single axiom for lattice theory. (Parts of this work are also reported in [20]). We first give a new single axiom schema that handles two absorption identities.

Theorem #MAJ-2. Majority polynomial single axiom with two absorption identities.

$$\left\{\begin{array}{l} p(x,y,y)=y \\ p(y,x,y)=y \\ p(y,y,x)=y \\ f(y)=y \\ g(y)=y \end{array}\right\} \Leftrightarrow \{p(p(x,y,y),p(x,p(y,z,f(y)),g(y)),u)=y\}.$$

($\Rightarrow$) is trivial by simplification. The proof of ($\Leftarrow$) follows.

Proof (found by Otter 3.0.3l on gyro at 0.74 seconds).

1	$x=x$
2	$p(A,A,B)=A,\ p(A,B,A)=A,\ p(B,A,A)=A,\ f(A)=A,\ g(A)=A\ \rightarrow\ \Box$
4,3	$p(p(x,y,y),p(x,p(y,z,f(y)),g(y)),u)=y$
5	$p(x,p(p(y,x,x),p(p(y,p(x,z,f(x)),g(x)),u,f(p(y,p(x,z,f(x)),g(x)))),g(p(y,p(x,z,f(x))$
7	$p(p(x,p(y,z,z),p(y,z,z)),p(x,z,g(p(y,z,z))),u)=p(y,z,z)$ [3 → 3]
12,11	$p(p(x,y,y),p(x,p(z,p(y,u,f(y)),g(y)),g(y)),v)=y$ [3 → 7 :4,4,4]
25	$p(p(p(x,y,y),y,y),y,z)=y$ [3 → 11]
29	$p(p(x,y,y),p(x,p(z,p(u,p(y,v,f(y)),g(y)),g(y)),g(y)),w)=y$ [11 → 7 :12,12,12]
42,41	$p(x,x,y)=x$ [25 → 25]
43	$p(A,B,A)=A,\ p(B,A,A)=A,\ f(A)=A,\ g(A)=A\ \rightarrow\ \Box$ [2 :42 :1]

64 $p(p(x,y,y),p(p(x,y,y),y,g(p(x,y,y))),z) = p(x,y,y)$ [41 → 7]
68 $p(x,p(x,p(y,p(x,z,f(x)),g(x)),g(x)),u) = x$ [41 → 11]
82 $p(p(x,p(y,z,f(y)),g(y)),p(y,p(p(p(x,y,y),p(p(x,p(y,z,f(y)),g(y)),u,f(p(x,p(y,z,f(y)),g(y))))),g(p(x,p(
91,90 $p(x,p(y,z,f(y)),g(y)) = y$ [41 → 5 :4,42, flip]
95,94 $p(x,p(y,x,g(x)),z) = p(y,x,g(x))$ [41 → 5 :42,42,91,42]
103,102 $p(x,p(x,y,f(x)),z) = p(x,y,f(x))$ [41 → 5 :42,42,91,42]
107,106 $p(x,y,f(x)) = x$ [82 :91,91,91,91,91,91,91,91,91,91,91,91,91,103,103,91,91,91,91]
115,114 $p(x,y,g(y)) = y$ [68 :107,95,95]
117,116 $p(p(x,y,y),y,z) = y$ [29 :107,115,115,115]
121,120 $p(x,y,y) = y$ [64 :117,117, flip]
122 $p(A,B,A) = A,\ f(A) = A,\ g(A) = A \rightarrow \square$ [43 :121 :1]
124,123 $f(x) = x$ [120 → 106]
125 $p(A,B,A) = A,\ g(A) = A \rightarrow \square$ [122 :124 :1]
127,126 $p(x,y,x) = x$ [106 :124]
128 $g(A) = A \rightarrow \square$ [125 :127 :1]
129 $g(x) = x$ [114 → 126, flip]
131 $\square$ [129,128]

With the absorption basis {L2,L3,L4′}, the axiom schema of Thm. #MAJ-2, and the same majority polymonmial as above, we can substitute $p(\mathrm{L3}(y), \mathrm{L4}'(y), u)$ for $f(y)$ and $\mathrm{L2}(y)$ for $g(y)$, obtaining a single identity for LT of length 119, again with 7 variables.

7.3 A Short Single Identity for Lattices

To build a simpler single identity for LT, we can use the fact that the three identities

$$\begin{array}{l}(x \wedge y) \vee (x \wedge (x \vee y)) = x \\ (x \wedge x) \vee (y \wedge (x \vee x)) = x \\ (x \wedge y) \vee (y \wedge (x \vee y)) = y\end{array} \qquad \text{(B)}$$

hold, given the axiom schema of Thm. #MAJ-2 and the majority polynomial

$$p(x,y,z) = (x \wedge z) \vee (y \wedge (x \vee z)).$$

We first show that if we add (L3) and one other identity to (B), we obtain a basis for LT.

Theorem #LT-3. Another absorption basis for LT.

$$\left\{\begin{array}{ll}(x \wedge y) \vee (x \wedge (x \vee y)) = x & \\ (x \wedge x) \vee (y \wedge (x \vee x)) = x & \\ (x \wedge y) \vee (y \wedge (x \vee y)) = y & \\ ((x \wedge y) \vee (y \wedge z)) \vee y = y & \text{(L3)} \\ ((x \vee (y \vee z)) \wedge (u \vee y)) \wedge y = y & \end{array}\right\} \Rightarrow \left\{\begin{array}{ll} y \wedge (x \vee (y \vee z)) = y & \text{(L2)} \\ ((y \vee x) \wedge (y \vee z)) \wedge y = y & \text{(L4}') \end{array}\right\}$$

Proof (found by Otter 3.0.3l on gyro at 1.48 seconds).

1	$x = x$	
2	$B \wedge (A \vee (B \vee C)) = B,\ ((B \vee A) \wedge (B \vee C)) \wedge B = B\ \rightarrow\ \Box$	
3	$(x \wedge y) \vee (x \wedge (x \vee y)) = x$	
5	$(x \wedge x) \vee (y \wedge (x \vee x)) = x$	
7	$(x \wedge y) \vee (y \wedge (x \vee y)) = y$	
9	$((x \wedge y) \vee (y \wedge z)) \vee y = y$	
11	$((x \vee (y \vee z)) \wedge (u \vee y)) \wedge y = y$	
13	$((x \wedge y) \wedge (x \wedge (x \vee y))) \vee ((x \wedge y) \wedge x) = x \wedge y$	$[3 \rightarrow 3]$
26,25	$x \vee x = x$	$[7 \rightarrow 9]$
31	$(x \wedge x) \vee (y \wedge x) = x$	[5 :26]
42,41	$x \wedge x = x$	$[25 \rightarrow 7$:26]
43	$x \vee (y \wedge x) = x$	[31 :42]
57	$((x \vee y) \wedge (z \vee x)) \wedge x = x$	$[25 \rightarrow 11]$
59	$((x \vee (y \vee z)) \wedge y) \wedge y = y$	$[25 \rightarrow 11]$
67	$(x \vee (x \wedge y)) \vee x = x$	$[11 \rightarrow 9]$
77	$(x \wedge y) \vee y = y$	$[43 \rightarrow 9]$
80,79	$(x \wedge y) \wedge y = x \wedge y$	$[77 \rightarrow 3$:26]
82,81	$(x \vee (y \vee z)) \wedge y = y$	[59 :80]
105	$(x \vee (x \wedge y)) \wedge x = x \vee (x \wedge y)$	[67 → 3 :26]
122,121	$(x \vee y) \wedge x = x$	$[77 \rightarrow 81]$
123	$x \vee (x \wedge y) = x$	[105 :122, flip]
127	$(x \wedge ((y \vee (x \vee z)) \wedge ((y \vee (x \vee z)) \vee x))) \vee (x \wedge (y \vee (x \vee z))) = x$	$[81 \rightarrow 13$:82,82]
169	$(x \vee y) \vee x = x \vee y$	$[121 \rightarrow 123]$
174,173	$(x \vee (y \vee z)) \vee y = x \vee (y \vee z)$	$[81 \rightarrow 123]$
188,187	$x \wedge (y \vee (x \vee z)) = x$	[127 :174,42,26]
199	$((B \vee A) \wedge (B \vee C)) \wedge B = B\ \rightarrow\ \Box$	[2 :188 :1]
414	$((x \vee y) \wedge (x \vee z)) \wedge x = x$	$[169 \rightarrow 57]$
416	$\Box$	[414,199]

Theorem #LT-4. A short single axiom for LT.

We use the majority polynomial $p(x, y, z) = (x \wedge z) \vee (y \wedge (x \vee z))$. With the axiom schema axiom of Prob. #MAJ-2, we substitute the two additional identities from Prob. #LT-3. (The three identities (B) need not be used in the construction, because they are already satisfied.) When the schema is expanded with the majority polynomial and written in terms of $\wedge$ and $\vee$, it has length 79, with 7 variables:

$$(((x \wedge y) \vee (y \wedge (x \vee y))) \wedge z) \vee (((x \wedge (((x_1 \wedge y) \vee (y \wedge x_2)) \vee y)) \vee (((y \wedge (((x_1 \vee (y \vee x_2)) \wedge (x_3 \vee y)) \wedge y)) \vee (u \wedge (y \vee (((x_1 \vee (y \vee x_2)) \wedge (x_3 \vee y)) \wedge y)))) \wedge (x \vee (((x_1 \wedge y) \vee (y \wedge x_2)) \vee y)))) \wedge (((x \wedge y) \vee (y \wedge (x \vee y))) \vee z)) = y.$$

7.4 Weakly Associative Lattices

The following set is a basis for the variety of weakly assosiative lattices (WAL).

$x \wedge x = x,$	$x \vee x = x,$	(W1,W1′)
$x \wedge y = y \wedge x,$	$x \vee y = y \vee x,$	(W2,W2′)
$((x \vee z) \wedge (y \vee z)) \wedge z = z,$	$((x \wedge z) \vee (y \wedge z)) \vee z = z.$	(W3,W3′)

First we show that by adding an absoprtion law to WAL, we obtain LT. The proof can be compared to the (mathematician's) proof presented in [20].

Theorem #WAL-1.

$$\{\text{WAL},\ x \wedge (y \vee (x \vee z)) = x\} \Rightarrow \{\text{LT}\}$$

It is sufficient to derive the associative laws for $\wedge$ and $\vee$.

Proof (found by Otter 3.0.3l on gyro at 267.63 seconds).

1	$x = x$	
2	$(A \wedge B) \wedge C = A \wedge (B \wedge C),\ (A \vee B) \vee C = A \vee (B \vee C)\ \rightarrow\ \square$	
3	$x \wedge x = x$	
5	$x \wedge y = y \wedge x$	
6	$((x \vee y) \wedge (z \vee y)) \wedge y = y$	
8	$x \vee x = x$	
10	$x \vee y = y \vee x$	
11	$((x \wedge y) \vee (z \wedge y)) \vee y = y$	
13	$x \wedge (y \vee (x \vee z)) = x$	
15	$x \wedge (y \vee (z \vee x)) = x$	$[10 \rightarrow 13]$
17	$x \wedge (y \vee x) = x$	$[8 \rightarrow 13]$
19	$x \wedge ((x \vee y) \vee z) = x$	$[10 \rightarrow 13]$
21	$x \wedge (x \vee y) = x$	$[8 \rightarrow 13]$
31	$(x \vee y) \wedge y = y$	$[3 \rightarrow 6]$
33	$x \wedge ((y \vee x) \wedge (z \vee x)) = x$	$[5 \rightarrow 6]$
35	$(x \vee y) \wedge x = x$	$[5 \rightarrow 21]$
39	$(x \vee (y \wedge (x \vee z))) \vee (x \vee z) = x \vee z$	$[21 \rightarrow 11]$
49	$((x \wedge (y \vee z)) \vee z) \vee (y \vee z) = y \vee z$	$[17 \rightarrow 11]$
53	$(x \wedge y) \vee y = y$	$[8 \rightarrow 11]$
65	$x \vee (y \vee (x \vee z)) = y \vee (x \vee z)$	$[13 \rightarrow 53]$
67	$(x \wedge y) \vee x = x$	$[5 \rightarrow 53]$
70,69	$x \vee (y \wedge x) = x$	$[10 \rightarrow 53]$
71	$(x \wedge y) \wedge (z \vee y) = x \wedge y$	$[53 \rightarrow 13]$
73	$x \wedge (y \wedge x) = y \wedge x$	$[53 \rightarrow 35]$
80,79	$x \vee (x \wedge y) = x$	$[10 \rightarrow 67]$
85	$(x \wedge y) \wedge x = x \wedge y$	$[67 \rightarrow 21]$
93	$((x \vee (y \wedge z)) \wedge z) \wedge (y \wedge z) = y \wedge z$	$[69 \rightarrow 6]$
110,109	$x \vee (y \vee (z \vee x)) = y \vee (z \vee x)$	$[15 \rightarrow 53]$
111	$(x \wedge y) \wedge (x \vee z) = x \wedge y$	$[67 \rightarrow 19]$
153	$(x \wedge y) \wedge (x \wedge (z \vee (x \wedge y))) = x \wedge y$	$[79 \rightarrow 33]$
157	$(x \wedge y) \wedge ((z \vee (x \wedge y)) \wedge x) = x \wedge y$	$[79 \rightarrow 33]$
195	$(x \vee y) \vee (x \vee (z \vee y)) = x \vee (z \vee y)$	$[15 \rightarrow 39]$
197	$(x \vee y) \vee (x \vee (y \vee z)) = x \vee (y \vee z)$	$[13 \rightarrow 39]$

231	$(x \vee y) \vee (z \wedge y) = x \vee y$	[71 → 69]
434,433	$((x \wedge y) \vee z) \vee (x \vee z) = x \vee z$	[111 → 49]
539	$x \vee (y \wedge (x \wedge z)) = x$	[79 → 231 :80]
541	$x \vee (y \wedge (z \wedge x)) = x$	[69 → 231 :70]
629	$x \vee ((y \wedge x) \wedge z) = x$	[85 → 541]
727	$x \vee (y \vee z) = x \vee (z \vee y)$	[10 → 65 :110]
1036	$(x \wedge y) \wedge ((z \wedge x) \wedge y) = (z \wedge x) \wedge y$	[629 → 93]
1421	$(x \vee y) \vee z = z \vee (y \vee x)$	[10 → 727]
1423	$x \vee (y \vee z) = (z \vee y) \vee x$	[flip 1421]
2968,2967	$(x \wedge y) \wedge (x \wedge (z \vee y)) = x \wedge y$	[231 → 153]
3194,3193	$(x \wedge (y \wedge z)) \wedge (z \wedge x) = x \wedge (y \wedge z)$	[541 → 157]
3196,3195	$(x \wedge (y \wedge z)) \wedge (y \wedge x) = x \wedge (y \wedge z)$	[539 → 157]
3200,3199	$(x \wedge y) \wedge ((z \vee y) \wedge x) = x \wedge y$	[231 → 157]
4876,4875	$((x \vee y) \vee z) \vee (z \vee y) = z \vee (x \vee y)$	[1423 → 195]
5085	$x \vee ((x \wedge y) \vee z) = x \vee z$	[433 → 197 :4876,434]
5196,5195	$(x \vee y) \vee (x \vee z) = (x \vee y) \vee z$	[35 → 5085]
5198,5197	$(x \vee y) \vee (y \vee z) = (x \vee y) \vee z$	[31 → 5085]
5282,5281	$(x \vee y) \vee z = x \vee (y \vee z)$	[197 :5196,5198]
5737	$(A \wedge B) \wedge C = A \wedge (B \wedge C) \ \rightarrow \ \Box$	[2 :5282 :1]
5741	$C \wedge (A \wedge B) = A \wedge (B \wedge C) \ \rightarrow \ \Box$	[5 → 5737]
8492	$x \wedge ((y \vee x) \wedge z) = z \wedge x$	[3199 → 1036 :3194,3200]
8495,8494	$x \wedge (y \wedge (z \vee x)) = y \wedge x$	[2967 → 1036 :3196,2968]
8573	$(x \wedge y) \wedge (y \wedge z) = z \wedge (x \wedge y)$	[69 → 8492]
8580	$(x \wedge (y \vee z)) \wedge z = x \wedge z$	[73 → 8492 :8495, flip]
8607	$x \wedge (y \wedge z) = (y \wedge z) \wedge (z \wedge x)$	[flip 8573]
8842,8841	$(x \wedge y) \wedge (y \wedge z) = x \wedge (y \wedge z)$	[79 → 8580]
8853	$x \wedge (y \wedge z) = y \wedge (z \wedge x)$	[8607 :8842]
8854	$\Box$	[8853,5741]

7.4.1 Uniqueness of $\wedge$ in WAL

The following new result generalizes the previously known result for lattice theory.

Theorem #WAL-2. If $(\vee, \wedge)$ and $(\vee, \cdot)$ are both weakly associative lattices, then $x \wedge y = x \cdot y$.

Proof (found by Otter 3.0.3l on gyro at 14.24 seconds).

1	$A \wedge B \neq A \cdot B$
3	$x \wedge x = x$
5	$x \wedge y = y \wedge x$
6	$((x \vee y) \wedge (z \vee y)) \wedge y = y$
8	$x \vee x = x$
10	$x \vee y = y \vee x$
11	$((x \wedge y) \vee (z \wedge y)) \vee y = y$

13	$x \cdot x = x$	
15	$x \cdot y = y \cdot x$	
16	$((x \vee y) \cdot (z \vee y)) \cdot y = y$	
18	$((x \cdot y) \vee (z \cdot y)) \vee y = y$	
28	$(x \vee y) \wedge y = y$	$[3 \rightarrow 6]$
32	$(x \vee y) \wedge x = x$	$[10 \rightarrow 28]$
34	$x \wedge (y \vee x) = x$	$[5 \rightarrow 28]$
36	$x \wedge (x \vee y) = x$	$[5 \rightarrow 32]$
50	$(x \wedge y) \vee y = y$	$[8 \rightarrow 11]$
66	$(x \wedge y) \vee x = x$	$[5 \rightarrow 50]$
68	$x \vee (y \wedge x) = x$	$[10 \rightarrow 50]$
76	$x \vee (x \wedge y) = x$	$[10 \rightarrow 66]$
83,82	$(x \vee y) \vee x = x \vee y$	$[36 \rightarrow 68]$
96	$((x \vee (y \wedge z)) \cdot z) \cdot (y \wedge z) = y \wedge z$	$[68 \rightarrow 16]$
102	$(x \vee y) \cdot y = y$	$[13 \rightarrow 16]$
120	$(x \vee y) \cdot x = x$	$[10 \rightarrow 102]$
134	$x \vee (y \cdot x) = x$	$[120 \rightarrow 18 : 83]$
160	$x \vee (x \cdot y) = x$	$[15 \rightarrow 134]$
168	$((x \vee (y \cdot z)) \wedge z) \wedge (y \cdot z) = y \cdot z$	$[134 \rightarrow 6]$
184	$(x \cdot y) \wedge x = x \cdot y$	$[160 \rightarrow 34]$
843,842	$(x \cdot y) \cdot (x \wedge y) = x \wedge y$	$[76 \rightarrow 96]$
1155,1154	$(x \wedge y) \wedge (x \cdot y) = x \wedge y$	$[842 \rightarrow 184 : 843]$
1470	$x \wedge y = x \cdot y$	$[160 \rightarrow 168 : 1155]$
1472	$\Box$	[1470,1]

The following theorem is a corollary of the preceding one, but we present here a complete proof. Note that although this theorem is weaker, OTTER with the same strategy, takes more time to find a proof; this situation occurs frequently, and part of the reason here is OTTER's difficulty in handling associative-commutative operations.

Theorem #LT-5. Uniqueness of the meet operation in a lattice. If $\wedge$, $\vee$, and $\cdot$ are binary operations such that both $(\mathrm{L}; \vee, \wedge)$ and $(\mathrm{L}; \vee, \cdot)$ are lattices, then $x \wedge y = x \cdot y$.

Proof (found by Otter 3.0.3l on gyro at 80.24 seconds).

1	$A \wedge B \neq A \cdot B$
5	$x \wedge y = y \wedge x$
6	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$
10	$x \vee y = y \vee x$
13	$x \wedge (x \vee y) = x$
15	$x \vee (x \wedge y) = x$
19	$x \cdot y = y \cdot x$
20	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$
22	$x \cdot (x \vee y) = x$

24	$x \vee (x \cdot y) = x$	
33	$x \wedge (y \vee x) = x$	$[10 \rightarrow 13]$
37	$(x \vee y) \wedge x = x$	$[5 \rightarrow 13]$
41	$(x \wedge y) \vee (x \wedge (y \wedge z)) = x \wedge y$	$[6 \rightarrow 15]$
43	$x \vee (y \wedge x) = x$	$[5 \rightarrow 15]$
45	$(x \wedge y) \vee x = x$	$[10 \rightarrow 15]$
47	$x \cdot (y \vee x) = x$	$[10 \rightarrow 22]$
49	$(x \vee y) \cdot x = x$	$[19 \rightarrow 22]$
66	$x \vee (y \cdot x) = x$	$[19 \rightarrow 24]$
70	$(x \cdot y) \vee x = x$	$[10 \rightarrow 24]$
82	$(x \vee y) \wedge y = y$	$[5 \rightarrow 33]$
96	$(x \wedge y) \vee y = y$	$[10 \rightarrow 43]$
125	$x \cdot (y \cdot (z \vee (x \cdot y))) = x \cdot y$	$[20 \rightarrow 47]$
132,131	$x \cdot (x \wedge y) = x \wedge y$	$[45 \rightarrow 49]$
166	$x \wedge (x \cdot y) = x \cdot y$	$[70 \rightarrow 37]$
170	$x \wedge (y \cdot x) = y \cdot x$	$[66 \rightarrow 82]$
185,184	$x \cdot (y \wedge x) = y \wedge x$	$[96 \rightarrow 49]$
485	$(x \wedge y) \vee (x \wedge (z \cdot y)) = x \wedge y$	$[170 \rightarrow 41]$
8074	$(x \wedge y) \vee (x \cdot y) = x \wedge y$	$[166 \rightarrow 485]$
8201	$x \wedge y = x \cdot y$	$[8074 \rightarrow 125 : 185,132]$
8203	$\Box$	[8201,1]

7.4.2 A Single Axiom for WAL

The results in this section are also reported in [20].

The term

$$p(x, y, z) = (x \wedge z) \vee (y \wedge (x \vee z))$$

is a majority polynomial for WAL as well as for LT, so if we can find an absorption basis for WAL, we can construct a single identity in the same way as for LT in Thm. #LT-4 above. In particular, we wish to find absorption identities that can be added to the three identites (B) to give WAL.

Theorem #WAL-3. An absorption basis for WAL.

$$\left\{ \begin{array}{l} (x \wedge y) \vee (x \wedge (x \vee y)) = x \\ (x \wedge x) \vee (y \wedge (x \vee x)) = x \\ (x \wedge y) \vee (y \wedge (x \vee y)) = y \\ ((x \vee y) \wedge (z \vee x)) \wedge x = x \\ ((x \wedge y) \vee (z \wedge x)) \vee x = x \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} x \wedge x = x \\ x \wedge y = y \wedge x \\ x \vee x = x \\ x \vee y = y \vee x \end{array} \right\}.$$

Because the two additional identites are commuted variants of (W3) and (W3′), it is sufficient to derive commutativity and idempotence of the two operations.

Proof (found by Otter 3.0.3l on gyro at 2.91 seconds).

1	$x = x$	
2	$A \wedge A = A,\ B \wedge A = A \wedge B,\ A \vee A = A,\ B \vee A = A \vee B\ \rightarrow\ \square$	
3	$(x \wedge y) \vee (x \wedge (x \vee y)) = x$	
5	$(x \wedge x) \vee (y \wedge (x \vee x)) = x$	
7	$(x \wedge y) \vee (y \wedge (x \vee y)) = y$	
9	$((x \vee y) \wedge (z \vee x)) \wedge x = x$	
11	$((x \wedge y) \vee (z \wedge x)) \vee x = x$	
13	$(x \wedge (y \vee (z \wedge x))) \wedge (z \wedge x) = z \wedge x$	$[7 \rightarrow 9]$
15	$(x \wedge (y \vee (x \wedge z))) \wedge (x \wedge z) = x \wedge z$	$[3 \rightarrow 9]$
20,19	$x \vee (x \wedge (((x \vee y) \wedge (z \vee x)) \vee x)) = x$	$[9 \rightarrow 7]$
23	$((x \wedge y) \vee x) \vee x = x$	$[9 \rightarrow 11]$
26,25	$((x \vee y) \wedge x) \wedge x = x$	$[11 \rightarrow 9]$
29	$(((x \wedge y) \vee x) \wedge x) \vee (x \wedge x) = x$	$[23 \rightarrow 7]$
33	$(x \wedge (y \wedge x)) \wedge (y \wedge x) = y \wedge x$	$[7 \rightarrow 25]$
44,43	$(x \wedge x) \wedge x = x$	$[25 \rightarrow 33 : 26,26]$
46,45	$(x \wedge (y \vee x)) \wedge x = x$	$[25 \rightarrow 13 : 26,26]$
47	$(x \wedge x) \wedge (x \wedge x) = x \wedge x$	$[29 \rightarrow 13]$
62,61	$x \wedge (x \wedge (y \vee x)) = x \wedge (y \vee x)$	$[7 \rightarrow 45 : 46]$
63	$x \vee (x \wedge ((x \wedge (y \vee x)) \vee x)) = x$	$[45 \rightarrow 7]$
69	$((x \wedge x) \vee (x \wedge x)) \vee (x \wedge x) = x \wedge x$	$[47 \rightarrow 23]$
73	$((x \wedge x) \wedge (y \vee x)) \wedge x = x$	$[43 \rightarrow 15 : 44,44]$
88,87	$x \wedge x = x$	$[23 \rightarrow 73 : 44]$
94,93	$(x \vee x) \vee x = x$	$[69 : 88,88,88,88]$
105	$x \vee (y \wedge (x \vee x)) = x$	$[5 : 88]$
107	$B \wedge A = A \wedge B,\ A \vee A = A,\ B \vee A = A \vee B\ \rightarrow\ \square$	$[2 : 88 : 1]$
113,112	$x \vee x = x$	$[87 \rightarrow 19 : 94,88]$
114	$B \wedge A = A \wedge B,\ B \vee A = A \vee B\ \rightarrow\ \square$	$[107 : 113 : 1]$
115	$x \vee (y \wedge x) = x$	$[105 : 113]$
118,117	$(x \wedge (((x \vee y) \wedge (z \vee x)) \vee x)) \vee x = x$	$[19 \rightarrow 3 : 62,88]$
122,121	$x \wedge (y \wedge x) = y \wedge x$	$[115 \rightarrow 13 : 88]$
127	$(x \wedge y) \vee y = y$	$[115 \rightarrow 3 : 122,88]$
130,129	$(x \wedge y) \wedge y = x \wedge y$	$[127 \rightarrow 3 : 113]$
133	$(x \vee y) \wedge x = x$	$[25 : 130]$
135	$x \wedge (((x \vee y) \wedge (z \vee x)) \vee x) = x$	$[19 \rightarrow 63 : 46,20,46,118, \text{flip}]$
140,139	$x \wedge ((x \wedge y) \vee x) = (x \wedge y) \vee x$	$[23 \rightarrow 133]$
141	$x \vee ((x \wedge (y \vee x)) \vee x) = x$	$[63 : 140]$
143	$(x \vee (x \vee y)) \vee (x \vee y) = x \vee y$	$[133 \rightarrow 23]$
151	$((x \wedge y) \vee (z \wedge y)) \vee y = y$	$[121 \rightarrow 11]$
171	$(x \wedge (y \vee x)) \vee x = x$	$[141 \rightarrow 135 : 140]$
178,177	$x \wedge (y \vee x) = x$	$[171 \rightarrow 3 : 46,46,113, \text{flip}]$
179	$(x \wedge y) \vee x = x$	$[139 : 178, \text{flip}]$
188,187	$(x \vee y) \vee y = x \vee y$	$[177 \rightarrow 115]$
193	$(x \vee (y \wedge (z \vee x))) \vee (z \vee x) = z \vee x$	$[177 \rightarrow 151]$
197	$x \vee (x \vee y) = x \vee y$	$[143 : 188]$
199	$(x \wedge y) \wedge x = x \wedge y$	$[179 \rightarrow 3 : 113]$

211	$x \wedge (x \vee y) = x$	[197 → 3 :113]
215	$(x \vee y) \vee x = x \vee y$	[211 → 115]
235	$x \vee (x \wedge y) = x$	[199 → 115]
242,241	$(x \wedge y) \wedge (y \wedge x) = y \wedge x$	[235 → 13]
285	$x \wedge y = y \wedge x$	[241 → 199 :242,242]
287,286	$(x \vee y) \vee (y \vee x) = y \vee x$	[211 → 193]
348	$x \vee y = y \vee x$	[286 → 215 :287,287]
351	$\Box$	[114,285,348]

Theorem #WAL-4. A short single axiom for WAL.

We use the same majority polynomial and axiom schema as in Prob. #LT-4, and we use the two additional absorption laws of Prob. #WAL-3. When the axiom is written in terms of $\wedge$ and $\vee$, it has length 75, with 6 variables:

$$(((x \wedge y) \vee (y \wedge (x \vee y))) \wedge z) \vee (((x \wedge (((y \wedge x_1) \vee (x_2 \wedge y)) \vee y)) \vee (((y \wedge (((y \vee x_1) \wedge (x_2 \vee y)) \wedge y)) \vee (u \wedge (y \vee (((y \vee x_1) \wedge (x_2 \vee y)) \wedge y)))) \wedge (x \vee (((y \wedge x_1) \vee (x_2 \wedge y)) \vee y)))) \wedge (((x \wedge y) \vee (y \wedge (x \vee y))) \vee z)) = y.$$

7.5 Quasilattices

One obtains a basis for quasilattice theory (QLT) if the absorption laws of LT are replaced a pair of link laws. The following set is a basis for QLT.

$$x \wedge y = y \wedge x, \qquad x \vee y = y \vee x,$$
$$(x \wedge y) \wedge z = x \wedge (y \wedge z), \qquad (x \vee y) \vee z = x \vee (y \vee z),$$
$$x \wedge x = x, \qquad x \vee x = x,$$
$$(x \wedge (y \vee z)) \vee (x \wedge y) = x \wedge (y \vee z), \qquad (x \vee (y \wedge z)) \wedge (x \vee y) = x \vee (y \wedge z).$$

The following theorem was previously known by a second-order proof. This is the first equational proof known to us.

Theorem #QLT-1. Distributivity in quasilattices.

$$\{\mathrm{QLT}, x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)\} \Rightarrow \{x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)\}$$

Proof (found by Otter 3.0.3l on gyro at 7.19 seconds).

2	$x \wedge x = x$
4	$x \wedge y = y \wedge x$
5	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$
8,7	$x \vee x = x$
9	$x \vee y = y \vee x$
11,10	$(x \vee y) \vee z = x \vee (y \vee z)$
14	$(x \vee (y \wedge z)) \wedge (x \vee y) = x \vee (y \wedge z)$

16	$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$	
18,17	$(x \wedge y) \vee (x \wedge z) = x \wedge (y \vee z)$	[flip 16]
19	$A \vee (B \wedge C) \neq (A \vee B) \wedge (A \vee C)$	
23	$x \wedge (x \wedge y) = x \wedge y$	[2 → 5, flip]
30	$x \vee (x \vee y) = x \vee y$	[7 → 10, flip]
43,42	$x \vee (y \vee x) = x \vee y$	[9 → 30]
51,50	$x \vee (y \vee (x \vee z)) = x \vee (y \vee z)$	[42 → 10 :11,11, flip]
58	$(x \vee ((x \vee y) \wedge z)) \wedge (x \vee y) = x \vee ((x \vee y) \wedge z)$	[30 → 14]
108	$x \vee (x \wedge y) = x \wedge (x \vee y)$	[2 → 17]
116	$x \wedge (y \vee (x \wedge z)) = x \wedge (y \vee z)$	[23 → 17 :18, flip]
122,121	$(x \wedge y) \vee x = x \wedge (y \vee x)$	[2 → 17]
123	$x \wedge (y \vee z) = x \wedge (z \vee y)$	[9 → 17 :18]
163	$A \vee (C \wedge B) \neq (A \vee B) \wedge (A \vee C)$	[4 → 19]
181,180	$(x \vee (y \wedge z)) \wedge (x \vee (y \wedge (z \vee y))) = x \vee (y \wedge z)$	[14 → 108 :8,11,51,122, flip]
183	$x \vee (y \wedge x) = x \wedge (x \vee y)$	[4 → 108]
226	$(x \vee y) \wedge z = z \wedge (y \vee x)$	[4 → 123]
230	$x \wedge (y \vee z) = (z \vee y) \wedge x$	[flip 226]
916,915	$(x \vee (y \wedge z)) \wedge y = y \wedge (x \vee z)$	[4 → 116]
918,917	$x \vee ((x \vee y) \wedge z) = (x \vee y) \wedge (x \vee z)$	[58 :916, flip]
919	$x \vee (y \wedge (z \vee x)) = x \vee (y \wedge z)$	[116 → 183 :11,18,43,11,122,181]
1440	$x \vee (y \wedge z) = (x \vee z) \wedge (x \vee y)$	[230 → 919 :918, flip]
1442	$\Box$	[1440,163]

The next theorem generalizes a previously known result in LT to QLT.

Theorem #QLT-2. Bowden's inequality, $x \vee (y \wedge z) \geq (x \vee y) \wedge z$, implies distributivity in quasilattices.

Proof (found by Otter 3.0.3l on gyro at 8.42 seconds).

3,2	$x \wedge x = x$	
4	$x \wedge y = y \wedge x$	
6,5	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$	
8,7	$x \vee x = x$	
9	$x \vee y = y \vee x$	
11,10	$(x \vee y) \vee z = x \vee (y \vee z)$	
12	$(x \wedge (y \vee z)) \vee (x \wedge y) = x \wedge (y \vee z)$	
14	$(x \vee (y \wedge z)) \wedge (x \vee y) = x \vee (y \wedge z)$	
16	$(x \vee (y \wedge z)) \vee ((x \vee y) \wedge z) = x \vee (y \wedge z)$	
17	$x \vee ((y \wedge z) \vee ((x \vee y) \wedge z)) = x \vee (y \wedge z)$	[copy,16 :11]
21	$A \vee (B \wedge C) \neq (A \vee B) \wedge (A \vee C)$	
23	$x \wedge (x \wedge y) = x \wedge y$	[2 → 5, flip]
25	$x \wedge (y \wedge z) = y \wedge (z \wedge x)$	[4 → 5]
28	$x \wedge (y \wedge z) = z \wedge (x \wedge y)$	[flip 25]
29	$x \vee (y \vee z) = y \vee (x \vee z)$	[9 → 10 :11]
30	$x \vee (x \vee y) = x \vee y$	[7 → 10, flip]

32	$x \vee (y \vee z) = y \vee (z \vee x)$	[9 → 10]
39,38	$x \wedge (y \wedge x) = x \wedge y$	[4 → 23]
43,42	$x \vee (y \vee x) = x \vee y$	[9 → 30]
46	$x \wedge (y \wedge (x \wedge z)) = x \wedge (y \wedge z)$	[38 → 5 :6,6, flip]
48	$x \vee (y \vee (z \vee x)) = x \vee (y \vee z)$	[10 → 42]
52	$(x \wedge (y \vee z)) \vee (x \wedge z) = x \wedge (z \vee y)$	[9 → 12]
54	$((x \vee y) \wedge z) \vee (z \wedge x) = z \wedge (x \vee y)$	[4 → 12]
56	$x \vee (y \vee ((x \vee y) \wedge x)) = x \vee y$	[2 → 12 :11,3]
60	$(x \wedge ((x \wedge y) \vee z)) \vee (x \wedge y) = x \wedge ((x \wedge y) \vee z)$	[23 → 12]
63,62	$(x \wedge (y \vee z)) \vee (y \wedge x) = x \wedge (y \vee z)$	[4 → 12]
68	$(x \wedge (y \vee z)) \vee ((x \wedge y) \vee u) = (x \wedge (y \vee z)) \vee u$	[12 → 10, flip]
125	$x \vee (y \vee z) = z \vee (y \vee x)$	[9 → 32]
160,159	$x \vee (y \vee ((x \vee y) \wedge y)) = x \vee y$	[2 → 17 :3]
161	$x \vee ((y \wedge z) \vee ((y \vee x) \wedge z)) = x \vee (y \wedge z)$	[9 → 17]
230	$x \vee (((y \vee x) \wedge y) \vee y) = y \vee x$	[32 → 56]
249	$(x \vee y) \wedge (y \vee x) = x \vee y$	[2 → 52 :11,160, flip]
255	$(x \wedge (y \vee z)) \vee (z \wedge x) = x \wedge (z \vee y)$	[4 → 52]
290,289	$(x \vee y) \wedge (z \wedge (y \vee x)) = (x \vee y) \wedge z$	[249 → 46 :39, flip]
293	$x \wedge (y \vee z) = (z \vee y) \wedge x$	[249 → 28 :290]
322,321	$(x \vee y) \wedge (y \vee (x \wedge z)) = y \vee (x \wedge z)$	[14 → 293, flip]
350	$(x \wedge y) \vee (y \wedge x) = y \wedge x$	[7 → 54 :8]
365,364	$((x \vee y) \wedge x) \vee x = x \wedge (x \vee y)$	[2 → 54]
368	$x \vee (y \wedge (y \vee x)) = y \vee x$	[230 :365]
405,404	$(x \wedge y) \vee (z \vee (y \wedge x)) = (x \wedge y) \vee z$	[350 → 48 :43, flip]
408	$x \vee (y \wedge z) = (y \wedge z) \vee ((z \wedge y) \vee x)$	[350 → 125]
411	$x \vee (y \wedge z) = (z \wedge y) \vee x$	[350 → 29 :405]
413,412	$(x \wedge y) \vee ((y \wedge x) \vee z) = (y \wedge x) \vee z$	[350 → 10, flip]
414	$(x \wedge y) \vee z = z \vee (y \wedge x)$	[flip 408 :413]
430	$x \vee (y \wedge (x \vee y)) = y \vee x$	[9 → 368]
521,520	$(x \wedge y) \vee ((x \vee z) \wedge y) = y \wedge (x \vee z)$	[54 → 411, flip]
536	$x \vee (y \wedge (z \vee x)) = x \vee (z \wedge y)$	[161 :521]
590	$(x \wedge (y \vee x)) \vee y = x \vee y$	[9 → 430]
675	$(x \wedge y) \vee (((x \wedge y) \vee z) \wedge x) = x \wedge ((x \wedge y) \vee z)$	[414 → 60]
1481	$((x \vee y) \wedge (x \vee z)) \vee x = (x \vee y) \wedge (x \vee z)$	[364 → 68 :63, flip]
1510	$x \vee (y \wedge (x \vee z)) = x \vee (z \wedge y)$	[9 → 536]
1522,1521	$x \vee ((x \vee y) \wedge z) = x \vee (y \wedge z)$	[293 → 536]
1535,1534	$(x \wedge (y \vee z)) \vee z = z \vee (y \wedge x)$	[9 → 536]
1550	$x \vee (y \wedge z) = x \vee (z \wedge (x \vee y))$	[flip 1510]
1559,1558	$(x \wedge y) \vee (z \wedge x) = x \wedge ((x \wedge y) \vee z)$	[675 :1522]
1617,1616	$x \wedge (y \vee (z \wedge x)) = x \wedge (y \vee z)$	[255 :1559,1535]
1634,1633	$(x \wedge (y \vee z)) \vee y = y \vee (z \wedge x)$	[536 → 590 :6,322,1617,1535]
1645,1644	$x \vee (y \wedge (x \vee z)) = (x \vee z) \wedge (x \vee y)$	[1481 :1634]
1653	$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$	[1550 :1645]
1655	$\square$	[1653,21]

Corollary #LT-7. A lattice satifying Bowden's inequality is distributive [2, p.??].

The next theorem was previously known by a model-theoretic argument. This is the first equational proof known to us.

Problem #QLT-3. Modularity in quasilattices.

$$\{\mathrm{QLT}, (x\wedge y)\vee(z\wedge(x\vee y)) = (x\vee y)\wedge(z\vee(x\wedge y))\} \Rightarrow \{x\wedge(y\vee(x\wedge z)) = (x\wedge y)\vee(x\wedge z)\}.$$

Proof (found by Otter 3.0.3l on gyro at 905.71 seconds).

1	$x = x$	
3,2	$x \wedge x = x$	
4	$x \wedge y = y \wedge x$	
6,5	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$	
8,7	$x \vee x = x$	
9	$x \vee y = y \vee x$	
11,10	$(x \vee y) \vee z = x \vee (y \vee z)$	
12	$(x \wedge (y \vee z)) \vee (x \wedge y) = x \wedge (y \vee z)$	
14	$(x \vee (y \wedge z)) \wedge (x \vee y) = x \vee (y \wedge z)$	
16	$(x \wedge y) \vee (z \wedge (x \vee y)) = (x \vee y) \wedge (z \vee (x \wedge y))$	
17	$A \wedge (B \vee (A \wedge C)) \neq (A \wedge B) \vee (A \wedge C)$	
18	$(A \wedge B) \vee (A \wedge C) \neq A \wedge (B \vee (A \wedge C))$	[flip 17]
20	$x \wedge (y \wedge z) = y \wedge (x \wedge z)$	[4 → 5 :6]
22,21	$x \wedge (x \wedge y) = x \wedge y$	[2 → 5, flip]
23	$x \wedge (y \wedge z) = y \wedge (z \wedge x)$	[4 → 5]
27	$x \vee (y \vee z) = y \vee (x \vee z)$	[9 → 10 :11]
29,28	$x \vee (x \vee y) = x \vee y$	[7 → 10, flip]
30	$x \vee (y \vee z) = y \vee (z \vee x)$	[9 → 10]
33	$x \vee (y \vee z) = z \vee (x \vee y)$	[flip 30]
37,36	$x \wedge (y \wedge x) = x \wedge y$	[4 → 21]
41,40	$x \vee (y \vee x) = x \vee y$	[9 → 28]
43,42	$x \wedge (y \wedge (z \wedge x)) = x \wedge (y \wedge z)$	[5 → 36]
45,44	$x \wedge (y \wedge (x \wedge z)) = x \wedge (y \wedge z)$	[36 → 5 :6,6, flip]
47,46	$x \vee (y \vee (z \vee x)) = x \vee (y \vee z)$	[10 → 40]
49,48	$x \vee (y \vee (x \vee z)) = x \vee (y \vee z)$	[40 → 10 :11,11, flip]
52	$(x \wedge (y \vee z)) \vee (x \wedge z) = x \wedge (z \vee y)$	[9 → 12]
60	$(x \wedge ((y \wedge x) \vee z)) \vee (x \wedge y) = x \wedge ((y \wedge x) \vee z)$	[36 → 12]
64	$(x \wedge (y \vee z)) \vee (y \wedge x) = x \wedge (y \vee z)$	[4 → 12]
69,68	$(x \wedge y) \vee (x \wedge (y \vee z)) = x \wedge (y \vee z)$	[9 → 12]
70	$(x \wedge (y \vee z)) \vee ((x \wedge y) \vee u) = (x \wedge (y \vee z)) \vee u$	[12 → 10, flip]
80	$x \wedge (y \wedge z) = z \wedge (y \wedge x)$	[4 → 23]
110	$x \wedge (y \wedge ((x \wedge y) \vee x)) = x \wedge y$	[7 → 14 :6,8]
116	$(x \vee ((y \vee z) \wedge u)) \wedge (y \vee (x \vee z)) = x \vee ((y \vee z) \wedge u)$	[27 → 14]
118	$(x \vee (y \wedge z)) \wedge (y \vee x) = x \vee (y \wedge z)$	[9 → 14]
123,122	$(x \vee y) \wedge (x \vee (y \wedge z)) = x \vee (y \wedge z)$	[4 → 14]

139	$x \vee (y \vee z) = z \vee (y \vee x)$	[9 → 30]
178	$x \vee (y \wedge x) = x \wedge (y \vee x)$	[2 → 16 :8,8,3]
182	$(x \wedge y) \vee (x \vee (y \wedge z)) = (x \vee y) \wedge (x \vee ((y \wedge z) \vee (x \wedge y)))$	[14 → 16 :11]
192	$x \wedge (y \vee x) = x \vee (y \wedge x)$	[flip 178]
196	$(x \vee y) \wedge (x \vee ((y \wedge z) \vee (x \wedge y))) = (x \wedge y) \vee (x \vee (y \wedge z))$	[flip 182]
230,229	$(x \wedge y) \vee (y \wedge x) = x \wedge (y \wedge (y \vee (x \wedge y)))$	[36 → 178 :6]
239	$x \vee (x \wedge y) = x \wedge (y \vee x)$	[4 → 178]
242,241	$(x \wedge y) \vee y = y \wedge (x \vee y)$	[9 → 178]
253	$x \wedge ((y \vee x) \wedge (x \vee y)) = x \vee (y \wedge x)$	[178 → 14 :6]
254	$x \vee (y \wedge (z \vee y)) = (z \wedge y) \vee (y \vee x)$	[178 → 139]
255	$x \vee (y \wedge (z \vee y)) = (z \wedge y) \vee (x \vee y)$	[178 → 33]
261,260	$x \vee (x \wedge (y \vee x)) = x \vee (y \wedge x)$	[178 → 28]
262	$(x \wedge y) \vee (z \wedge (x \wedge (y \vee x))) = (x \vee (y \wedge x)) \wedge (z \vee (x \wedge y))$	[178 → 16 :37,37]
266,265	$(x \wedge (y \vee x)) \vee z = x \vee ((y \wedge x) \vee z)$	[178 → 10]
267	$x \vee (y \wedge x) = x \wedge ((y \vee x) \wedge (x \vee y))$	[flip 253]
269	$(x \wedge y) \vee (z \vee y) = z \vee (y \wedge (x \vee y))$	[flip 255]
272	$(x \vee (y \wedge x)) \wedge (z \vee (x \wedge y)) = (x \wedge y) \vee (z \wedge (x \wedge (y \vee x)))$	[flip 262]
275	$x \wedge (y \wedge (x \vee y)) = x \wedge (y \wedge (y \vee (x \wedge y)))$	[178 → 192 :6,22,37,230]
278	$x \vee (y \vee (x \wedge y)) = (x \vee y) \wedge (y \vee x)$	[40 → 192 :11,261, flip]
287,286	$x \vee (y \wedge x) = x \wedge (x \vee y)$	[9 → 192, flip]
289	$(x \vee y) \wedge y = y \wedge (y \vee x)$	[4 → 192 :287]
304,303	$x \vee (y \wedge (y \vee x)) = (x \vee y) \wedge (y \vee x)$	[278 :287]
305	$x \wedge (y \wedge (x \vee y)) = x \wedge (y \wedge (y \vee x))$	[275 :287,22]
306	$x \wedge ((x \vee y) \wedge (z \vee (x \wedge y))) = (x \wedge y) \vee (z \wedge (x \wedge (y \vee x)))$	[272 :287,6]
308,307	$x \wedge ((y \vee x) \wedge (x \vee y)) = x \wedge (x \vee y)$	[267 :287, flip]
311,310	$x \vee (x \wedge (y \vee x)) = x \wedge (x \vee y)$	[260 :287]
314	$(x \wedge y) \vee (y \wedge x) = x \wedge (y \wedge (y \vee x))$	[229 :287,22]
318	$x \wedge (x \vee y) = x \wedge (y \vee x)$	[178 :287]
321	$x \wedge (x \vee y) = (y \vee x) \wedge x$	[flip 289]
335	$(x \vee y) \wedge (x \wedge y) = x \wedge (y \wedge (y \vee x))$	[16 → 239 :8,11,287,304,6,308]
338,337	$(x \wedge y) \vee x = x \wedge (y \vee x)$	[9 → 239]
343	$x \wedge (y \wedge (y \vee x)) = (x \vee y) \wedge (x \wedge y)$	[flip 335]
347,346	$x \wedge (y \wedge (y \vee x)) = x \wedge y$	[110 :338,45]
349,348	$(x \vee y) \wedge (x \wedge y) = x \wedge y$	[flip 343 :347]
351	$(x \wedge y) \vee (y \wedge x) = x \wedge y$	[314 :347]
354,353	$x \wedge (y \wedge (x \vee y)) = x \wedge y$	[305 :347]
361	$x \vee (x \wedge y) = x \wedge (x \vee y)$	[239 → 28 :311, flip]
381	$(x \wedge (y \wedge z)) \vee (x \wedge y) = x \wedge (y \wedge (z \vee (x \wedge y)))$	[23 → 241 :6]
399	$(x \wedge y) \vee (z \wedge (y \wedge (x \vee y))) = y \wedge ((x \vee y) \wedge (z \vee (x \wedge y)))$	[241 → 16 :6,3,242,6,3,6]
402	$x \wedge ((y \vee x) \wedge (z \vee (y \wedge x))) = (y \wedge x) \vee (z \wedge (x \wedge (y \vee x)))$	[flip 399]
410,409	$(x \wedge y) \vee (x \wedge (y \wedge z)) = x \wedge (y \wedge ((x \wedge y) \vee z))$	[23 → 286 :6]
419	$x \vee (y \wedge (y \vee z)) = (z \wedge y) \vee (y \vee x)$	[286 → 139]
428,427	$(x \wedge (x \vee y)) \vee z = x \vee ((y \wedge x) \vee z)$	[286 → 10]
429	$(x \wedge y) \vee (y \vee z) = z \vee (y \wedge (y \vee x))$	[flip 419]
436,435	$x \wedge ((x \vee y) \wedge y) = y \wedge x$	[286 → 289 :6,43,242,6,22,354]

439	$(x \vee y) \wedge (y \vee x) = y \vee x$	[40 → 289 :11,8,3]
530	$x \vee (y \wedge (x \vee y)) = x \vee y$	[318 → 241 :266,49,338,29,3]
545	$(x \vee y) \wedge x = (y \vee x) \wedge x$	[4 → 321]
699	$x \vee (y \wedge z) = (z \wedge y) \vee ((y \wedge z) \vee x)$	[351 → 139]
705,704	$(x \wedge y) \vee ((y \wedge x) \vee z) = (x \wedge y) \vee z$	[351 → 10, flip]
706	$(x \wedge y) \vee z = z \vee (y \wedge x)$	[flip 699 :705]
707	$x \vee (y \wedge z) = (z \wedge y) \vee x$	[699 :705]
814,813	$(x \vee y) \wedge (z \wedge (y \vee x)) = (x \vee y) \wedge z$	[439 → 42 :37, flip]
818	$x \wedge (y \vee z) = (z \vee y) \wedge x$	[439 → 20 :814]
929	$x \vee (y \wedge (z \wedge (x \vee (y \wedge z)))) = x \vee (y \wedge z)$	[5 → 530]
931	$x \vee ((x \vee y) \wedge y) = x \vee y$	[4 → 530]
1003,1002	$x \vee (y \vee (x \wedge (x \vee z))) = x \vee (y \vee (x \wedge z))$	[361 → 48]
1137	$(x \wedge (y \wedge z)) \vee u = u \vee (y \wedge (x \wedge z))$	[80 → 706 :6]
1141	$(x \wedge (y \wedge z)) \vee u = u \vee (x \wedge (z \wedge y))$	[20 → 706 :6]
1144	$(x \wedge y) \vee ((y \vee z) \wedge x) = x \wedge (y \vee z)$	[12 → 706, flip]
1148	$x \vee (y \wedge (z \wedge u)) = (z \wedge (y \wedge u)) \vee x$	[flip 1137]
1152	$x \vee (y \wedge (z \wedge u)) = (y \wedge (u \wedge z)) \vee x$	[flip 1141]
1201	$x \vee ((y \vee z) \wedge z) = z \vee ((y \wedge z) \vee x)$	[545 → 707 :428]
1208	$x \vee ((y \wedge x) \vee z) = z \vee ((y \vee x) \wedge x)$	[flip 1201]
1228	$x \vee (y \wedge (z \wedge ((z \wedge y) \vee x))) = x \vee (y \wedge z)$	[707 → 530 :6]
1311	$x \vee ((y \vee z) \wedge u) = ((z \vee y) \wedge u) \vee x$	[818 → 707]
1379	$(x \wedge (y \vee (x \wedge z))) \vee (x \wedge z) = x \wedge ((x \wedge z) \vee y)$	[21 → 52]
1813,1812	$(x \wedge y) \vee (x \wedge ((x \wedge y) \vee z)) = x \wedge ((x \wedge y) \vee z)$	[21 → 68]
1832	$x \wedge ((y \vee z) \wedge (y \vee x)) = x \wedge (y \vee z)$	[68 → 14 :338,6,45,69]
3385,3384	$(x \vee (y \wedge z)) \wedge ((y \vee x) \wedge u) = (x \vee (y \wedge z)) \wedge u$	[118 → 5, flip]
3500,3499	$x \vee ((y \wedge z) \vee (x \wedge y)) = x \vee (y \wedge z)$	[122 → 64 :11,1003,123]
3505	$(x \wedge y) \vee (x \vee (y \wedge z)) = x \vee (y \wedge z)$	[196 :3500,123, flip]
6639	$x \vee ((y \vee z) \wedge z) = (z \wedge y) \vee (((y \vee z) \wedge z) \vee x)$	[931 → 254 :6,37,436]
6666,6665	$(x \vee y) \wedge y) \vee z = (x \wedge y) \vee (y \vee z)$	[707 → 254]
6700	$x \vee ((y \vee z) \wedge z) = (z \wedge y) \vee (z \vee x)$	[6639 :6666,705]
6799	$x \vee ((y \vee z) \wedge y) = (z \wedge y) \vee (x \vee y)$	[818 → 255]
7057,7056	$(x \vee (y \wedge z)) \wedge (y \vee (x \vee z)) = x \vee (y \wedge z)$	[348 → 116 :349]
7442	$(x \wedge y) \vee ((y \vee z) \wedge (x \vee (y \vee z))) = (y \vee z) \wedge (x \vee (y \vee z))$	[70 → 269 :242, flip]
9037	$x \vee (y \vee ((z \vee x) \wedge x)) = x \vee (y \vee (x \wedge z))$	[429 → 1208 :1003,11, flip]
9109,9108	$x \wedge (y \wedge (z \vee (x \wedge y))) = x \wedge (y \wedge (z \vee x))$	[122 → 1832 :6,6]
9130	$x \vee (y \wedge (z \wedge (x \vee y))) = x \vee (y \wedge z)$	[929 :9109]
9135,9134	$(x \wedge (y \wedge z)) \vee (x \wedge y) = x \wedge (y \wedge (z \vee x))$	[381 :9109]
9226,9225	$x \vee (y \vee (z \wedge x)) = (x \vee y) \wedge (x \vee (y \vee z))$	[1144 → 3499 :287,11,11, flip]
9255,9254	$x \vee (y \vee (x \wedge z)) = (x \vee y) \wedge (x \vee (y \vee z))$	[9037 :9226,47, flip]
9272,9271	$(x \wedge y) \vee (z \wedge (x \vee z)) = (x \wedge y) \vee z$	[3505 → 46 :41,338, flip]
9275,9274	$(x \wedge y) \vee (y \vee z) = (y \vee z) \wedge (x \vee (y \vee z))$	[7442 :9272]
9283,9282	$(x \vee y) \wedge y) \vee z = (y \vee z) \wedge (x \vee (y \vee z))$	[6665 :9275]
9349,9348	$(x \wedge y) \vee (x \vee z) = (x \vee z) \wedge (y \vee (x \vee z))$	[9 → 6700 :9283, flip]
9351,9350	$(x \wedge y) \vee (z \vee y) = (y \vee z) \wedge (x \vee (y \vee z))$	[1311 → 6799 :9283, flip]
9365,9364	$x \wedge (y \wedge ((y \wedge x) \vee z)) = x \wedge (y \wedge (x \vee z))$	[409 → 60 :45,9135,11,9351,354,410,45, flip]

9366	$x \vee (y \wedge (z \wedge (y \vee x))) = x \vee (y \wedge z)$	[1228 :9365]
9510	$(x \wedge ((y \vee x) \wedge z)) \vee y = y \vee (x \wedge z)$	[1152 → 9130]
9519,9518	$(x \wedge (y \wedge (z \vee y))) \vee z = z \vee (y \wedge x)$	[1148 → 9130]
9662	$(x \wedge ((x \vee y) \wedge z)) \vee y = y \vee (x \wedge z)$	[1152 → 9366]
9977	$x \vee (y \wedge (z \vee (x \wedge y))) = x \vee (y \wedge z)$	[402 → 9510 :11,9519,9349,9255,3385,7057, flip]
10015	$x \vee (y \wedge (z \vee (y \wedge x))) = x \vee (y \wedge z)$	[306 → 9662 :11,9519,9275,9255,3385,7057, flip]
10048	$x \vee (y \wedge ((y \wedge x) \vee z)) = x \vee (y \wedge z)$	[707 → 9977]
10082,10081	$(x \wedge (y \vee (x \wedge z))) \vee z = z \vee (x \wedge y)$	[9 → 10015]
10129,10128	$(x \wedge y) \vee (x \wedge z) = x \wedge ((x \wedge y) \vee z)$	[21 → 10048 :1813, flip]
10141,10140	$(x \wedge y) \vee z = x \wedge (y \vee (x \wedge z))$	[1379 :10129,10082, flip]
10145	$A \wedge (B \vee (A \wedge C)) \neq A \wedge (B \vee (A \wedge C))$	[18 :10129,10141]
10146	$\Box$	[10145,1]

The following theorem was previously known using N_5 and Plonks-Sum argument [ref?]. This is the first equational proof.

Theorem #QLT-3a. Another modularity axiom for quasilattices.

$$\{\text{QLT}, ((x \vee y) \wedge z) \vee y = ((z \vee y) \wedge x) \vee y\} \Rightarrow \{x \wedge (y \vee (x \wedge z)) = (x \wedge y) \vee (x \wedge z)\}.$$

Proof (found by Otter 3.0.3l on gyro at 474.20 seconds).

2	$x \wedge x = x$	
4	$x \wedge y = y \wedge x$	
6,5	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$	
8,7	$x \vee x = x$	
9	$x \vee y = y \vee x$	
11,10	$(x \vee y) \vee z = x \vee (y \vee z)$	
12	$(x \wedge (y \vee z)) \vee (x \wedge y) = x \wedge (y \vee z)$	
14	$(x \vee (y \wedge z)) \wedge (x \vee y) = x \vee (y \wedge z)$	
16	$((x \vee y) \wedge z) \vee y = ((z \vee y) \wedge x) \vee y$	
17	$A \wedge (B \vee (A \wedge C)) \neq (A \wedge B) \vee (A \wedge C)$	
18	$(A \wedge B) \vee (A \wedge C) \neq A \wedge (B \vee (A \wedge C))$	[flip 17]
19	$x \wedge (y \wedge z) = y \wedge (x \wedge z)$	[4 → 5 :6]
21,20	$x \wedge (x \wedge y) = x \wedge y$	[2 → 5, flip]
22	$x \wedge (y \wedge z) = y \wedge (z \wedge x)$	[4 → 5]
26	$x \vee (y \vee z) = y \vee (x \vee z)$	[9 → 10 :11]
28,27	$x \vee (x \vee y) = x \vee y$	[7 → 10, flip]
29	$x \vee (y \vee z) = y \vee (z \vee x)$	[9 → 10]
32	$x \vee (y \vee z) = z \vee (x \vee y)$	[flip 29]
35	$x \wedge (y \wedge x) = x \wedge y$	[4 → 20]
40,39	$x \vee (y \vee x) = x \vee y$	[9 → 27]
44,43	$x \wedge (y \wedge (x \wedge z)) = x \wedge (y \wedge z)$	[35 → 5 :6,6, flip]
47	$x \vee (y \vee (x \vee z)) = x \vee (y \vee z)$	[39 → 10 :11,11, flip]
52,51	$(x \wedge (y \vee z)) \vee (x \wedge z) = x \wedge (z \vee y)$	[9 → 12]

59	$(x \wedge ((y \wedge x) \vee z)) \vee (x \wedge y) = x \wedge ((y \wedge x) \vee z)$	[35 → 12]
65	$(x \wedge (x \vee y)) \vee x = x \wedge (x \vee y)$	[2 → 12]
73	$x \wedge (y \wedge z) = x \wedge (z \wedge y)$	[4 → 19 :6]
79	$x \wedge (y \wedge z) = z \wedge (y \wedge x)$	[4 → 22]
94	$x \vee (y \vee z) = x \vee (z \vee y)$	[9 → 26 :11]
99	$(x \vee (y \wedge (z \wedge u))) \wedge (x \vee u) = x \vee (u \wedge (y \wedge z))$	[22 → 14]
101	$(x \vee (y \wedge (z \wedge u))) \wedge (x \vee (y \wedge z)) = x \vee (y \wedge (z \wedge u))$	[5 → 14 :6]
108	$((x \wedge y) \vee z) \wedge (z \vee x) = z \vee (x \wedge y)$	[9 → 14]
109	$x \wedge (y \wedge ((x \wedge y) \vee x)) = x \wedge y$	[7 → 14 :6,8]
121	$(x \vee y) \wedge (x \vee (y \wedge z)) = x \vee (y \wedge z)$	[4 → 14]
186	$((x \vee y) \wedge (z \wedge u)) \vee y = (((u \wedge z) \vee y) \wedge x) \vee y$	[73 → 16]
197	$((x \vee y) \wedge x) \vee y = x \vee y$	[2 → 16 :11,8,11,8, flip]
203,202	$((x \vee y) \wedge z) \vee y = y \vee ((z \vee y) \wedge x)$	[9 → 16, flip]
222,221	$x \vee ((y \vee x) \wedge y) = y \vee x$	[197 :203]
226	$x \vee (((y \wedge z) \vee x) \wedge u) = x \vee ((u \vee x) \wedge (z \wedge y))$	[186 :203,203]
258	$x \vee ((x \vee y) \wedge y) = y \vee x$	[9 → 221]
282,281	$(x \vee y) \wedge (y \vee x) = x \vee y$	[221 → 14 :40,222]
288	$x \wedge (y \vee z) = x \wedge (z \vee y)$	[221 → 12 :52,222]
330,329	$x \vee ((x \vee y) \wedge y) = x \vee y$	[258 → 27 :40, flip]
392	$x \wedge (y \vee z) = (z \vee y) \wedge ((y \vee z) \wedge x)$	[281 → 79]
399,398	$(x \vee y) \wedge ((y \vee x) \wedge z) = (x \vee y) \wedge z$	[281 → 5, flip]
400	$(x \vee y) \wedge z = z \wedge (y \vee x)$	[flip 392 :399]
401	$x \wedge (y \vee z) = (z \vee y) \wedge x$	[392 :399]
641	$x \vee (x \wedge y) = x \wedge (x \vee y)$	[401 → 65 :203,8]
695,694	$x \vee (y \wedge x) = x \wedge (x \vee y)$	[4 → 641]
699,698	$(x \wedge y) \vee x = x \wedge (x \vee y)$	[9 → 641]
705	$x \wedge (y \wedge (x \vee y)) = x \wedge y$	[109 :699,44]
735	$(x \wedge y) \vee (y \wedge x) = x \wedge (y \wedge ((x \wedge y) \vee y))$	[35 → 694 :6]
744,743	$(x \wedge y) \vee y = y \wedge (y \vee x)$	[9 → 694]
745	$(x \wedge y) \vee (y \wedge x) = x \wedge (y \wedge (y \vee x))$	[735 :744,21]
854,853	$x \wedge (y \wedge (y \vee x)) = x \wedge y$	[9 → 705]
872,871	$(x \wedge y) \vee (y \wedge x) = x \wedge y$	[745 :854]
1269,1268	$(x \wedge y) \vee (z \vee (y \wedge x)) = (x \wedge y) \vee z$	[871 → 47 :40, flip]
1271	$x \vee (y \wedge z) = x \vee (z \wedge y)$	[871 → 94 :872]
1272	$x \vee (y \wedge z) = (z \wedge y) \vee x$	[871 → 32 :1269]
1341	$x \wedge (y \vee (z \wedge u)) = x \wedge ((u \wedge z) \vee y)$	[1271 → 288]
1358	$x \wedge ((y \wedge z) \vee u) = x \wedge (u \vee (z \wedge y))$	[flip 1341]
1408	$(C \wedge A) \vee (A \wedge B) \neq A \wedge (B \vee (A \wedge C))$	[1272 → 18]
1431	$(x \wedge ((y \wedge x) \vee z)) \vee (y \wedge x) = x \wedge ((y \wedge x) \vee z)$	[4 → 59]
3062	$((x \wedge y) \vee z) \wedge (z \vee x) = (x \wedge y) \vee z$	[108 → 20 :282, flip]
3234,3233	$(x \vee y) \wedge (x \vee ((x \vee y) \wedge z)) = x \vee ((x \vee y) \wedge z)$	[27 → 121]
5031	$x \vee ((x \vee (y \wedge z)) \wedge y) = x \vee (y \wedge z)$	[329 → 101 :3234,330]
5341,5340	$(x \wedge (y \vee z)) \vee y = y \vee ((x \vee y) \wedge z)$	[400 → 202]
5400,5399	$(x \wedge y) \vee (y \wedge ((y \vee x) \wedge z)) = y \wedge ((x \wedge y) \vee z)$	[1431 :5341,695,6]
7284,7283	$x \vee ((x \vee y) \wedge (z \wedge y)) = x \vee (y \wedge z)$	[3062 → 226 :40,11,40, flip]

7333 $x \vee (y \wedge ((x \vee y) \wedge z)) = x \vee (y \wedge z)$ [99 → 5031 :28,7284]
7550,7549 $(x \wedge y) \vee (y \wedge z) = y \wedge ((x \wedge y) \vee z)$ [743 → 7333 :6,21,5400, flip]
7555 $A \wedge ((C \wedge A) \vee B) \neq A \wedge (B \vee (A \wedge C))$ [1408 :7550]
7556 $\Box$ [7555,1358]

Because the meet operation is unique for lattices and for weakly associative lattices, the analogous conjecture arose for quasilattices. MACE easily provided a counterexample.

Example #QLT-4. Uniqueness of the meet operation in a quasilattice. If $\wedge$, $\vee$, and $\cdot$ are binary operations such that both (QL; $\vee, \wedge$) and (QL; $\vee, \cdot$) are quasilattices, then $x \wedge y = x \cdot y$.

Counterexample. The clauses

$x \vee x = x$
$x \wedge x = x$
$x \cdot x = x$
$x \vee y = y \vee x$
$x \wedge y = y \wedge x$
$x \cdot y = y \cdot x$
$(x \vee y) \vee z = x \vee (y \vee z)$
$(x \wedge y) \wedge z = x \wedge (y \wedge z)$
$(x \cdot y) \cdot z = x \cdot (y \cdot z)$
$(x \wedge (y \vee z)) \vee (x \wedge y) = x \wedge (y \vee z)$
$(x \vee (y \wedge z)) \wedge (x \vee y) = x \vee (y \wedge z)$
$(x \cdot (y \vee z)) \vee (x \cdot y) = x \cdot (y \vee z)$
$(x \vee (y \cdot z)) \cdot (x \vee y) = x \vee (y \cdot z)$
$A \cdot B \neq A \wedge B$

have the following model (found by MACE 1.1.0 on gyro at 0.36 seconds).

```
v :
    | 0 1 2
  --+------
  0 | 0 0 0
  1 | 0 1 0
  2 | 0 0 2
^ :
    | 0 1 2
  --+------
  0 | 0 0 0
  1 | 0 1 0
  2 | 0 0 2
* :
    | 0 1 2
  --+------
```

```
      0 | 0 1 0
      1 | 1 1 1
      2 | 0 1 2
   A: 0
   B: 1
end_of_model
```

Theorem #QLT-4a. A self-dual form of distributivity for quasilattice theory.

$$\{\mathrm{QLT}, (((x\wedge y)\vee z)\wedge y)\vee(z\wedge x) = (((x\vee y)\wedge z)\vee y)\wedge(z\vee x)\} \Rightarrow \{x\vee(y\wedge z) = (x\vee y)\wedge(x\vee z)\}$$

Proof (found by Otter 3.0.3l on gyro at 948.75 seconds).

1	$x = x$	
3,2	$x \wedge x = x$	
4	$x \wedge y = y \wedge x$	
6,5	$(x \wedge y) \wedge z = x \wedge (y \wedge z)$	
8,7	$x \vee x = x$	
9	$x \vee y = y \vee x$	
11,10	$(x \vee y) \vee z = x \vee (y \vee z)$	
12	$(x \wedge (y \vee z)) \vee (x \wedge y) = x \wedge (y \vee z)$	
14	$(x \vee (y \wedge z)) \wedge (x \vee y) = x \vee (y \wedge z)$	
16	$(((x \wedge y) \vee z) \wedge y) \vee (z \wedge x) = (((x \vee y) \wedge z) \vee y) \wedge (z \vee x)$	
18	$A \wedge (B \vee C) \neq (A \wedge B) \vee (A \wedge C)$	
19	$(A \wedge B) \vee (A \wedge C) \neq A \wedge (B \vee C)$	[flip 18]
20	$x \wedge (y \wedge z) = y \wedge (x \wedge z)$	[4 → 5 :6]
22,21	$x \wedge (x \wedge y) = x \wedge y$	[2 → 5, flip]
23	$x \wedge (y \wedge z) = y \wedge (z \wedge x)$	[4 → 5]
26	$x \wedge (y \wedge z) = z \wedge (x \wedge y)$	[flip 23]
27	$x \vee (y \vee z) = y \vee (x \vee z)$	[9 → 10 :11]
29,28	$x \vee (x \vee y) = x \vee y$	[7 → 10, flip]
30	$x \vee (y \vee z) = y \vee (z \vee x)$	[9 → 10]
33	$x \vee (y \vee z) = z \vee (x \vee y)$	[flip 30]
37,36	$x \wedge (y \wedge x) = x \wedge y$	[4 → 21]
41,40	$x \vee (y \vee x) = x \vee y$	[9 → 28]
43,42	$x \wedge (y \wedge (z \wedge x)) = x \wedge (y \wedge z)$	[5 → 36]
44	$x \wedge (y \wedge (x \wedge z)) = x \wedge (y \wedge z)$	[36 → 5 :6,6, flip]
47,46	$x \vee (y \vee (z \vee x)) = x \vee (y \vee z)$	[10 → 40]
49,48	$x \vee (y \vee (x \vee z)) = x \vee (y \vee z)$	[40 → 10 :11,11, flip]
53,52	$(x \wedge (y \vee z)) \vee (x \wedge z) = x \wedge (z \vee y)$	[9 → 12]
56	$((x \vee y) \wedge z) \vee (z \wedge x) = z \wedge (x \vee y)$	[4 → 12]
58	$x \vee (y \vee ((x \vee y) \wedge x)) = x \vee y$	[2 → 12 :11,3]
60	$(x \wedge ((y \wedge x) \vee z)) \vee (x \wedge y) = x \wedge ((y \wedge x) \vee z)$	[36 → 12]
62	$(x \wedge ((x \wedge y) \vee z)) \vee (x \wedge y) = x \wedge ((x \wedge y) \vee z)$	[21 → 12]
66	$(x \wedge (x \vee y)) \vee x = x \wedge (x \vee y)$	[2 → 12]

69,68	$(x \wedge y) \vee (x \wedge (y \vee z)) = x \wedge (y \vee z)$	[9 → 12]
80	$x \wedge (y \wedge z) = z \wedge (y \wedge x)$	[4 → 23]
100	$(x \vee (y \wedge (z \wedge u))) \wedge (x \vee u) = x \vee (u \wedge (y \wedge z))$	[23 → 14]
109	$((x \wedge y) \vee z) \wedge (z \vee x) = z \vee (x \wedge y)$	[9 → 14]
110	$x \wedge (y \wedge ((x \wedge y) \vee x)) = x \wedge y$	[7 → 14 :6,8]
119,118	$(x \vee (y \wedge z)) \wedge (y \vee x) = x \vee (y \wedge z)$	[9 → 14]
123,122	$(x \vee y) \wedge (x \vee (y \wedge z)) = x \vee (y \wedge z)$	[4 → 14]
129	$(x \vee y) \wedge (z \wedge (x \vee (y \wedge u))) = z \wedge (x \vee (y \wedge u))$	[14 → 26, flip]
139	$x \vee (y \vee z) = z \vee (y \vee x)$	[9 → 30]
175	$(((x \wedge y) \vee z) \wedge x) \vee (z \wedge y) = (((y \vee x) \wedge z) \vee x) \wedge (z \vee y)$	[4 → 16]
186	$(((x \wedge y) \vee x) \wedge y) \vee x = (((x \vee y) \wedge x) \vee y) \wedge x$	[2 → 16 :8]
188	$(x \wedge y) \vee (((y \wedge z) \vee x) \wedge z) = (((y \vee z) \wedge x) \vee z) \wedge (x \vee y)$	[9 → 16]
190	$(((x \vee y) \wedge z) \vee y) \wedge (z \vee x) = (z \wedge x) \vee (((x \wedge y) \vee z) \wedge y)$	[flip 188]
256	$x \vee (((y \vee x) \wedge y) \vee y) = y \vee x$	[30 → 58]
280,279	$((x \vee y) \wedge x) \vee x = x \wedge (x \vee y)$	[4 → 66]
294,293	$x \vee (y \wedge (y \vee x)) = y \vee x$	[256 :280]
337	$x \vee (y \wedge (x \vee y)) = y \vee x$	[9 → 293]
341,340	$x \vee ((y \vee x) \wedge y) = y \vee x$	[4 → 293]
342	$(x \wedge (x \vee y)) \vee y = x \vee y$	[9 → 293]
355,354	$(x \vee y) \wedge (y \vee x) = x \vee y$	[293 → 14 :294]
359	$x \wedge (y \vee z) = x \wedge (z \vee y)$	[293 → 12 :53,294]
375	$x \vee ((x \vee y) \wedge y) = y \vee x$	[4 → 337]
376	$(x \wedge (y \vee x)) \vee y = x \vee y$	[9 → 337]
399	$x \vee (y \wedge (x \vee y)) = x \vee y$	[337 → 28 :41, flip]
427,426	$x \vee (y \wedge (((z \wedge y) \vee x) \wedge z)) = (z \wedge y) \vee x$	[26 → 340]
433,432	$((x \vee y) \wedge x) \vee y = x \vee y$	[9 → 340]
439	$(((x \wedge y) \vee x) \wedge y) \vee x = (x \vee y) \wedge x$	[186 :433]
476	$(x \wedge (y \wedge ((x \wedge y) \vee z))) \vee z = (x \wedge y) \vee z$	[5 → 342]
504	$x \vee ((y \wedge z) \vee ((x \vee (y \wedge z)) \wedge y)) = x \vee (y \wedge z)$	[14 → 52 :11,119]
509,508	$((x \vee y) \wedge z) \vee (z \wedge y) = z \wedge (y \vee x)$	[4 → 52]
522	$(x \wedge (y \vee (x \wedge z))) \vee (x \wedge z) = x \wedge ((x \wedge z) \vee y)$	[21 → 52]
563,562	$(x \vee y) \wedge (z \wedge (y \vee x)) = (x \vee y) \wedge z$	[354 → 44 :37, flip]
566	$x \wedge (y \vee z) = (z \vee y) \wedge ((y \vee z) \wedge x)$	[354 → 80]
567	$x \wedge (y \vee z) = (z \vee y) \wedge x$	[354 → 26 :563]
570,569	$(x \vee y) \wedge ((y \vee x) \wedge z) = (x \vee y) \wedge z$	[354 → 5, flip]
571	$(x \vee y) \wedge z = z \wedge (y \vee x)$	[flip 566 :570]
582	$x \wedge (y \wedge (z \vee u)) = (u \vee z) \wedge (x \wedge y)$	[359 → 26]
584	$x \wedge (y \wedge (z \vee u)) = y \wedge (x \wedge (u \vee z))$	[359 → 20]
592,591	$((x \vee y) \wedge y) \vee x = y \vee x$	[375 → 375 :570,341, flip]
618,617	$((x \vee y) \wedge y) \vee (y \vee x) = y \vee x$	[375 → 40 :592]
620,619	$x \vee (y \vee ((x \vee z) \wedge z)) = x \vee (y \vee z)$	[375 → 48 :47, flip]
632	$x \vee ((x \vee y) \wedge y) = x \vee y$	[375 → 28 :41, flip]
666	$x \vee (y \vee (y \wedge x)) = y \vee x$	[376 → 16 :355,11,41,618,3]
717	$x \vee (y \wedge (z \wedge (x \vee (y \wedge z)))) = x \vee (y \wedge z)$	[5 → 399]
767	$x \wedge (y \vee (z \vee u)) = (z \vee (y \vee u)) \wedge x$	[139 → 567 :11]

774	$(x \vee y) \wedge z = (y \vee x) \wedge z$	[4 → 567]
839	$(x \wedge y) \vee (y \wedge x) = y \wedge x$	[7 → 56 :8]
843	$x \vee ((y \wedge z) \vee ((x \vee y) \wedge x)) = x \vee (y \wedge z)$	[14 → 56 :11,123]
864,863	$(((x \wedge y) \vee z) \wedge x) \vee (x \wedge y) = x \wedge ((x \wedge y) \vee z)$	[21 → 56]
869	$(x \wedge y) \vee ((y \vee z) \wedge x) = x \wedge (y \vee z)$	[9 → 56]
966	$(x \wedge y) \vee (y \vee x) = x \vee y$	[33 → 666]
969,968	$x \vee ((x \wedge y) \vee y) = x \vee y$	[30 → 666]
1030,1029	$(x \wedge y) \vee (z \vee (y \wedge x)) = (x \wedge y) \vee z$	[839 → 46 :41, flip]
1033	$x \vee (y \wedge z) = (y \wedge z) \vee ((z \wedge y) \vee x)$	[839 → 139]
1036	$x \vee (y \wedge z) = (z \wedge y) \vee x$	[839 → 27 :1030]
1038,1037	$(x \wedge y) \vee ((y \wedge x) \vee z) = (y \wedge x) \vee z$	[839 → 10, flip]
1039	$(x \wedge y) \vee z = z \vee (y \wedge x)$	[flip 1033 :1038]
1161,1160	$x \wedge ((x \wedge y) \vee x) = x \vee (x \wedge y)$	[376 → 62, flip]
1285	$x \vee ((y \vee z) \wedge u) = (u \wedge (z \vee y)) \vee x$	[774 → 1036]
1286	$x \vee (y \wedge (z \vee u)) = (y \wedge (u \vee z)) \vee x$	[571 → 1036]
1287	$x \vee ((y \vee z) \wedge u) = ((z \vee y) \wedge u) \vee x$	[567 → 1036]
1291	$x \vee (y \wedge (z \wedge u)) = (z \wedge (u \wedge y)) \vee x$	[42 → 1036 :6,6,3]
1300	$(x \wedge y) \vee ((x \vee z) \wedge y) = y \wedge (x \vee z)$	[56 → 1036, flip]
1303,1302	$(x \wedge y) \vee (y \wedge (z \vee x)) = y \wedge (x \vee z)$	[52 → 1036, flip]
1304	$(x \wedge y) \vee (y \wedge (x \vee z)) = y \wedge (x \vee z)$	[12 → 1036, flip]
1323	$x \wedge ((y \wedge z) \vee u) = ((z \wedge y) \vee u) \wedge x$	[1036 → 567]
1344	$(x \wedge y) \vee ((z \vee y) \wedge x) = x \wedge (y \vee z)$	[52 → 1039, flip]
1349	$x \wedge (y \vee (z \wedge u)) = (y \vee (u \wedge z)) \wedge x$	[1039 → 567]
1389	$x \wedge (y \vee (y \wedge x)) = y \wedge x$	[20 → 110 :1161]
1408	$x \wedge (y \vee (z \vee (x \wedge (z \vee y)))) = (y \vee z) \wedge x$	[571 → 1389 :11]
1418	$x \wedge (y \wedge (y \vee (y \wedge x))) = y \wedge x$	[36 → 1389 :6,37]
1429,1428	$x \wedge (y \vee (x \wedge y)) = y \wedge x$	[4 → 1389]
1434	$x \wedge ((x \wedge y) \vee y) = y \wedge x$	[1036 → 1389]
1443,1442	$(x \wedge y) \vee x) \wedge y = x \wedge y$	[567 → 1389]
1446	$(x \vee (x \wedge y)) \wedge y = x \wedge y$	[4 → 1389]
1450,1449	$(x \wedge y) \vee x = (x \vee y) \wedge x$	[439 :1443]
1451	$(x \vee y) \wedge (x \wedge y) = x \wedge y$	[1442 :1450,6]
1460,1459	$x \vee (x \wedge y) = x \wedge (x \vee y)$	[1160 :1450,37, flip]
1464,1463	$x \wedge ((x \vee y) \wedge y) = x \wedge y$	[1446 :1460,6]
1472,1471	$x \wedge (y \wedge (y \vee x)) = y \wedge x$	[1418 :1460,22]
1477	$x \wedge ((y \vee z) \wedge (x \vee y)) = x \wedge (y \vee z)$	[68 → 14 :1450,6,43,69]
1496,1495	$(x \wedge y) \vee y) \wedge x = y \wedge x$	[567 → 1428]
1504	$(x \vee (y \wedge z)) \wedge (x \vee z) = x \vee (y \wedge z)$	[1428 → 14 :1429]
1531	$(((x \vee y) \wedge z) \vee z) \wedge (y \vee x) = z \wedge (x \vee y)$	[571 → 1434]
1542,1541	$x \wedge (y \wedge (x \vee y)) = y \wedge x$	[1434 → 1428 :11,1460,1303,1496]
1550,1549	$(x \wedge y) \vee y = (y \vee x) \wedge y$	[1434 → 1449 :969]
1562,1561	$x \vee (y \wedge x) = (x \vee y) \wedge x$	[1039 → 1449]
1572,1571	$(x \vee (y \vee z)) \wedge (x \wedge (z \vee y)) = x \wedge (y \vee z)$	[1531 :1550,6]
1582,1581	$x \vee (y \vee ((x \vee z) \wedge x)) = x \vee (y \vee (x \wedge z))$	[1449 → 46]
1583	$x \vee ((y \vee z) \wedge y) = y \vee ((y \wedge z) \vee x)$	[1449 → 139]

1585	$x \vee ((y \vee z) \wedge y) = (y \wedge z) \vee (y \vee x)$	[1449 → 30]
1588,1587	$((x \vee y) \wedge x) \vee z = (x \wedge y) \vee (x \vee z)$	[1449 → 10]
1589	$x \vee ((y \wedge z) \vee (x \wedge y)) = x \vee (y \wedge z)$	[843 :1582]
1595	$(x \wedge y) \vee (x \vee z) = z \vee ((x \vee y) \wedge x)$	[flip 1585]
1609	$(x \vee y) \wedge (y \wedge x) = y \wedge x$	[966 → 1451 :6,1472,6,1472]
1688,1687	$(x \wedge (x \vee y)) \vee z = x \vee ((x \wedge y) \vee z)$	[1459 → 10]
1844	$(x \vee y) \wedge ((x \wedge z) \vee y) = y \vee (x \wedge z)$	[567 → 109]
1867,1866	$(x \vee y) \wedge (x \vee (z \wedge y)) = x \vee (z \wedge y)$	[1541 → 122 :1542]
1894	$((x \wedge y) \vee z) \wedge (z \vee y) = (x \wedge y) \vee z$	[340 → 100 :427]
1931,1930	$((x \wedge y) \vee z) \wedge (x \vee z) = (x \wedge y) \vee z$	[118 → 569 :355, flip]
1932	$(x \vee y) \wedge ((y \wedge z) \vee x) = (y \wedge z) \vee x$	[354 → 129 :355]
2044	$x \wedge ((y \vee z) \wedge (x \vee z)) = x \wedge (y \vee z)$	[340 → 1477 :341]
2047,2046	$x \wedge ((y \vee z) \wedge (y \vee x)) = x \wedge (y \vee z)$	[9 → 1477]
2062,2061	$(x \vee y) \wedge (y \wedge (x \vee z)) = y \wedge (x \vee z)$	[582 → 1477]
2090	$x \vee ((x \wedge y) \vee (z \wedge y)) = x \vee (z \wedge y)$	[1504 → 1300 :1688,49,1867]
2092	$(x \wedge y) \vee (x \vee (z \wedge y)) = x \vee (z \wedge y)$	[1504 → 869 :1588,29,1867]
2104	$x \vee ((y \vee z) \wedge z) = z \vee ((z \wedge y) \vee x)$	[9 → 1583]
2105	$x \vee (y \wedge (z \vee y)) = y \vee ((y \wedge z) \vee x)$	[571 → 1583]
2107,2106	$((x \vee y) \wedge y) \vee z = y \vee ((y \wedge x) \vee z)$	[1287 → 1583]
2109,2108	$(x \wedge (y \vee x)) \vee z = x \vee ((x \wedge y) \vee z)$	[1285 → 1583]
2111	$x \vee ((x \wedge y) \vee z) = z \vee ((y \vee x) \wedge x)$	[flip 2104]
2112	$x \vee ((x \wedge y) \vee z) = z \vee (x \wedge (y \vee x))$	[flip 2105]
2121	$x \vee (y \wedge (z \vee y)) = (y \wedge z) \vee (y \vee x)$	[571 → 1585]
2124	$(x \wedge y) \vee (x \vee z) = z \vee (x \wedge (y \vee x))$	[flip 2121]
2136,2135	$x \vee (y \vee (z \wedge (y \vee x))) = x \vee ((y \vee z) \wedge y)$	[1344 → 1589 :11,11,1562]
2144,2143	$x \vee (y \vee (z \wedge x)) = (x \vee (y \vee z)) \wedge (x \vee y)$	[869 → 1589 :1562,11,11, flip]
2159,2158	$x \wedge (y \vee ((z \vee x) \wedge z)) = (y \vee z) \wedge x$	[1408 :2136]
2177	$x \wedge ((y \wedge x) \vee (y \vee z)) = x \wedge (y \vee z)$	[1595 → 60 :2159,509, flip]
2219	$(x \vee y) \wedge ((x \wedge z) \vee y) = (x \wedge z) \vee y$	[1844 → 839 :1931,11,29,41, flip]
2251	$(x \vee y) \wedge ((z \wedge x) \vee y) = (z \wedge x) \vee y$	[567 → 1894]
2308,2307	$x \wedge (y \wedge (z \vee (x \wedge y))) = x \wedge (y \wedge (z \vee y))$	[1866 → 2046 :6,6]
2309	$x \wedge (y \wedge (z \vee y)) = x \wedge (y \wedge (z \vee x))$	[122 → 2046 :6,2308,6]
2312	$x \vee (y \wedge (z \wedge (x \vee z))) = x \vee (y \wedge z)$	[717 :2308]
2322,2321	$(x \vee y) \wedge ((x \vee z) \wedge z) = (x \vee y) \wedge z$	[2046 → 36 :6,2062,37,6, flip]
2375	$x \vee (y \wedge z) = (y \wedge z) \vee ((z \vee x) \wedge x)$	[2090 → 2111]
2377	$x \vee (y \wedge z) = (y \wedge z) \vee (x \wedge (z \vee x))$	[2090 → 2112]
2427	$x \wedge ((x \wedge y) \vee (y \vee z)) = x \wedge (y \vee z)$	[4 → 2177]
2431	$x \wedge (y \vee (z \wedge (x \vee z))) = x \wedge (z \vee y)$	[2124 → 2177]
2448,2447	$(x \vee ((x \wedge y) \vee z)) \wedge y = y \wedge (x \vee z)$	[767 → 2177]
2466,2465	$x \wedge (y \wedge ((x \wedge y) \vee z)) = x \wedge (y \wedge (x \vee z))$	[2219 → 2044 :6,6]
2469	$(x \wedge (y \wedge (x \vee z))) \vee z = (x \wedge y) \vee z$	[476 :2466]
2479	$x \wedge (y \wedge (x \vee z)) = x \wedge (y \wedge (y \vee z))$	[2251 → 2044 :6,2466,6]
2506	$x \wedge ((y \vee z) \wedge z) = x \wedge (z \wedge (y \vee x))$	[632 → 2309 :6,37,6,2062]
2541	$x \vee (y \wedge (z \wedge (y \vee x))) = x \vee (z \wedge y)$	[584 → 2312]
2554	$(x \wedge ((y \vee x) \wedge z)) \vee y = y \vee (z \wedge x)$	[1291 → 2312]

2608	$(x \wedge y) \vee ((y \vee z) \wedge z) = (x \wedge y) \vee z$	[9 → 2375, flip]
2612,2611	$(x \wedge y) \vee (z \wedge (y \vee z)) = (x \wedge y) \vee z$	[9 → 2377, flip]
2643	$(x \vee ((y \wedge x) \vee z)) \wedge y = y \wedge (x \vee z)$	[767 → 2427]
2660	$(x \vee ((y \vee z) \wedge z)) \wedge y = y \wedge (z \vee x)$	[1349 → 2431]
2661	$(x \vee (y \wedge (z \vee y))) \wedge z = z \wedge (y \vee x)$	[4 → 2431]
2670,2669	$x \wedge (y \vee (z \wedge (x \vee z))) = x \wedge (y \vee z)$	[2431 → 1304 :1303, flip]
2761,2760	$(x \wedge ((x \vee y) \wedge z)) \vee y = (x \wedge z) \vee y$	[4 → 2469]
2802,2801	$x \vee (y \wedge ((y \wedge z) \vee x)) = x \vee (y \wedge z)$	[1287 → 504 :864]
2804,2803	$x \wedge (y \vee (x \vee z)) = x \wedge ((x \vee z) \wedge (y \vee x))$	[2479 → 2506 :11,11,8,3]
3000,2999	$x \vee (((y \wedge z) \vee x) \wedge y) = x \vee (y \wedge z)$	[1930 → 2541 :2802, flip]
3009	$(x \wedge ((x \wedge y) \vee z)) \vee z = z \vee (x \wedge y)$	[1932 → 2554 :3000]
3073	$x \vee ((x \wedge y) \vee z) = z \vee ((z \wedge y) \vee x)$	[2608 → 2112 :2107,2612]
3086,3085	$(x \vee (y \vee z)) \wedge y = y \wedge ((y \vee z) \wedge (x \vee y))$	[2092 → 2643 :2144,6,2322,2144,2047,2804]
3095	$(x \vee ((y \vee z) \wedge z)) \wedge y = y \wedge (x \vee z)$	[2660 → 1609 :620,1572, flip]
3099	$x \wedge (y \vee (z \wedge (x \vee y))) = x \wedge (y \vee z)$	[175 → 2661 :11,3086,2761,2109,41,6,2322,2448,3000, flip]
3232,3231	$((x \wedge y) \vee z) \wedge y) \vee z = z \vee (y \wedge x)$	[1323 → 3009]
3235	$x \wedge ((x \wedge y) \vee (x \wedge z)) = (x \wedge y) \vee (x \wedge z)$	[522 → 3009]
3241,3240	$x \vee ((x \wedge y) \vee z) = x \vee (z \wedge (y \vee z))$	[2112 → 3073, flip]
3261,3260	$(x \wedge (x \vee y)) \vee z = x \vee (z \wedge (y \vee z))$	[1687 :3241]
3265,3264	$(x \wedge y) \vee (x \vee z) = x \vee (z \wedge (y \vee z))$	[3095 → 1587 :3261,1464, flip]
3282	$x \wedge ((y \wedge (z \vee x)) \vee z) = x \wedge (z \vee y)$	[1286 → 3099]
3331,3330	$x \vee ((y \wedge x) \vee z) = x \vee (z \wedge (y \vee z))$	[4 → 3240]
3362,3361	$x \wedge (y \vee (x \wedge z)) = x \wedge (y \vee z)$	[190 → 3282 :11,3232,3265,1562,6,37,1472,3331,11,8,2670]
3371,3370	$(x \wedge y) \vee (x \wedge z) = x \wedge ((x \wedge y) \vee z)$	[3235 :3362, flip]
3377,3376	$x \wedge ((x \wedge (y \vee z)) \vee z) = x \wedge ((x \wedge z) \vee y)$	[522 :3362,3371]
3388,3387	$x \wedge ((x \wedge y) \vee z) = x \wedge (y \vee z)$	[52 :3371,3377]
3389	$A \wedge (B \vee C) \neq A \wedge (B \vee C)$	[19 :3371,3388]
3390	$\Box$	[3389,1]

7.6 Near Lattices (NL) and Transitive Near Lattices (TNL)

The following set is a basis for the variety of near lattices (NL).

$$x \wedge x = x, \qquad x \vee x = x,$$
$$x \wedge y = y \wedge x, \qquad x \vee y = y \vee x,$$
$$x \wedge (x \vee y) = x, \qquad x \vee (x \wedge y) = x.$$

To obtain a basis for the variety of Transitive Near Lattices (TNL), we can adjoin the following pair of axioms to NL.

$$x \wedge (y \vee (x \vee z)) = x, \qquad x \vee (y \wedge (x \wedge z)) = x.$$

Here also, MACE answers the question on the uniqueness of the meet operation.

Example #TNL-2. If $(\vee, \wedge)$ and $(\vee, \cdot)$ are both transitive near lattices, then $x \wedge y = x \cdot y$.

Counterexample. The clauses

$$x \wedge x = x$$
$$x \wedge y = y \wedge x$$
$$x \wedge (x \vee y) = x$$
$$x \wedge (y \vee (x \vee z)) = x$$
$$x \vee x = x$$
$$x \vee y = y \vee x$$
$$x \vee (x \wedge y) = x$$
$$x \vee (y \wedge (x \wedge z)) = x$$
$$x \cdot x = x$$
$$x \cdot y = y \cdot x$$
$$x \cdot (x \vee y) = x$$
$$x \cdot (y \vee (x \vee z)) = x$$
$$x \vee x = x$$
$$x \vee y = y \vee x$$
$$x \vee (x \cdot y) = x$$
$$x \vee (y \cdot (x \cdot z)) = x$$
$$0 \wedge 1 \neq 0 \cdot 1$$

have the following model (found by MACE 1.1.0 on gyro at 0.40 seconds).

```
^ :
    | 0 1 2 3 4
  --+----------
  0 | 0 2 2 0 4
  1 | 2 1 2 1 4
  2 | 2 2 2 2 2
  3 | 0 1 2 3 4
  4 | 4 4 2 4 4
v :
    | 0 1 2 3 4
  --+----------
  0 | 0 3 0 3 0
  1 | 3 1 1 3 1
  2 | 0 1 2 3 4
  3 | 3 3 3 3 3
  4 | 0 1 4 3 4
* :
    | 0 1 2 3 4
  --+----------
  0 | 0 4 2 0 4
  1 | 4 1 2 1 4
  2 | 2 2 2 2 2
```

```
      3 | 0 1 2 3 4
      4 | 4 4 2 4 4
end_of_model
```

7.7 Boolean Algebras

7.7.1 Frink's Theorem

The following theorem is on Frink's implicational basis for Boolean algebra. Padmanabhan found the first first-order proof that the system is a basis for Boolean algebra [27] (previous proofs were model theoretic), and we include OTTER's proof here.

Theorem #BA-1. A theorem of Frink.

$$\left\{ \begin{array}{l} x + x = x \\ ((x + y) + z) + u = (y + z) + x \ \rightarrow \ ((x + y) + z) + n(u) = 0 \\ ((x + y) + z) + n(u) = 0 \ \rightarrow \ ((x + y) + z) + u = (y + z) + x \end{array} \right\} \Rightarrow$$

$$\left\{ \begin{array}{l} n(x + n(y)) + n(n(x) + n(y)) = y \\ (x + y) + z = x + (y + z) \\ y + x = x + y \end{array} \right\}.$$

The conclusion is Huntington's axiom system for Boolean algebra.

Proof (found by Otter 3.0.3l on gyro at 7.69 seconds).

1	$x = x$	
2	$((x + y) + z) + u = (y + z) + x \ \rightarrow \ ((x + y) + z) + n(u) = 0$	
3	$((x + y) + z) + n(u) = 0 \ \rightarrow \ ((x + y) + z) + u = (y + z) + x$	
4	$n(A + n(B)) + n(n(A) + n(B)) = B, \ (A + B) + C = A + (B + C), \ B + A = A + B \ \rightarrow \ \square$	
6,5	$x + x = x$	
8,7	$x + n(x) = 0$	[2,5 :6,6,6,6]
9	$(x + y) + z = (y + z) + x$	[5 → 3 :8 :1]
12	$(x + y) + n(z) = 0 \ \rightarrow \ (x + y) + z = (x + y) + x$	[5 → 3 :6]
14	$(x + y) + z = (z + x) + y$	[flip 9]
22	$(n(x) + y) + x = 0 + y$	[7 → 9, flip]
25,24	$(x + y) + x = x + y$	[5 → 9, flip]
26	$(x + n(y + x)) + y = 0$	[7 → 9, flip]
34	$(x + y) + n(z) = 0 \ \rightarrow \ (x + y) + z = x + y$	[12 :25]
47,46	$0 + x = 0$	[7 → 24 :8]
49,48	$(x + y) + y = y + x$	[9 → 24]
51	$(n(x) + y) + x = 0$	[22 :47]
71	$x + y = y + x$	[5 → 14 :25,49]
74	$n(A + n(B)) + n(n(A) + n(B)) = B, \ (C + A) + B = A + (B + C) \ \rightarrow \ \square$	[14 → 4 :71]
92,91	$x + (x + y) = x + y$	[24 → 71, flip]
94,93	$(x + y) + z = x + (y + z)$	[14 → 71]

95	$x+(y+z)=y+(z+x)$	[9 → 71 :94]
96	$n(x)+x=0$	[7 → 71, flip]
98	$n(A+n(B))+n(n(A)+n(B))=B \ \rightarrow \ \Box$	[74 :94 :95]
99	$n(x)+(y+x)=0$	[51 :94]
101	$x+(y+n(z))=0 \ \rightarrow \ x+(y+z)=x+y$	[34 :94,94]
103	$x+(n(y+x)+y)=0$	[26 :94]
106,105	$x+(y+x)=x+y$	[24 :94]
107	$x+(y+z)=z+(x+y)$	[14 :94,94]
108	$n(x)+(x+y)=0$	[71 → 99]
110	$x+(y+n(x))=0$	[71 → 108 :94]
131	$x+(y+n(y+x))=0$	[105 → 103 :94,106]
137	$x+(n(x+y)+y)=0$	[71 → 103]
167	$n(A+n(B))+n(n(B)+n(A))=B \ \rightarrow \ \Box$	[71 → 98]
234	$x+n(y)=0 \ \rightarrow \ x+y=x$	[91 → 101 :92,6]
287	$n(n(x))+x=n(n(x))$	[234,96]
289	$n(x)+y=0 \ \rightarrow \ y+x=y$	[71 → 234]
368,367	$x+n(n(x))=n(n(x))$	[71 → 287]
386	$x+n(n(n(x)))=0$	[287 → 110]
422,421	$n(n(x))=x$	[234,386 :368]
424	$x+y=0 \ \rightarrow \ x+n(y)=x$	[421 → 234]
440	$x+y=0 \ \rightarrow \ y+n(x)=y$	[421 → 289]
544	$x+n(y+n(x))=x$	[424,110]
546	$n(x)+n(x+y)=n(x)$	[424,108]
587	$n(x+n(y))+y=y$	[71 → 544]
663,662	$n(x+y)+n(y)=n(y)$	[421 → 587]
700,699	$n(x+y)+(z+n(x))=z+n(x)$	[546 → 107, flip]
797	$n(x+y)+y=y+n(x)$	[440,137 :94,700, flip]
801	$x+n(x+y)=x+n(y)$	[440,131 :94,663, flip]
1090,1089	$n(x+y)+n(y+n(x))=n(y)$	[797 → 801 :663]
1099	$B=B \ \rightarrow \ \Box$	[167 :1090,422]
1100	$\Box$	[1099,1]

7.7.2 Padmanabhan's Self-Dual Basis

This section is on self-dual bases for Boolean algebras of type $<2,2,1,0,0>$, with corresponding operations $<+,\cdot,',0,1>$. Here, the dual of an identity is obtained by swapping $+$ with $\cdot$ and 0 with 1. A basis B is self-dual if for each identity E in B, the dual of E is also in B.

The next theorem is on Padmanabhan's previously known 6-basis [29].

Theorem #DUAL-BA-1. The following set is an independent self-dual basis for Boolean algebra.

$$\left\{ \begin{array}{ll} (x+y)\cdot y = y & (x\cdot y)+y = y \\ x\cdot(y+z) = (y\cdot x)+(z\cdot x) & x+(y\cdot z) = (y+x)\cdot(z+x) \\ x+x' = 1 & x\cdot x' = 0 \end{array} \right\}.$$

Independence is easily proved with three MACE runs showing that each identity of the left column is independent of the remaining five identities; a model of size three is quickly found in each case. To show that the set is a basis for Boolean algebra, it is sufficient to derive commutativity and associativity of one of the operations.

Proof (found by Otter 3.0.3l on gyro at 29.42 seconds).

1	$x = x$	
2	$B\cdot A = A\cdot B,\ (A\cdot B)\cdot C = A\cdot(B\cdot C)\ \rightarrow\ \Box$	
4,3	$(x+y)\cdot y = y$	
5	$x\cdot(y+z) = (y\cdot x)+(z\cdot x)$	
6	$(x\cdot y)+(z\cdot y) = y\cdot(x+z)$	[flip 5]
9,8	$x+x' = 1$	
11,10	$(x\cdot y)+y = y$	
12	$x+(y\cdot z) = (y+x)\cdot(z+x)$	
13	$x\cdot x' = 0$	
15	$(x+y)\cdot(z+y) = y+(x\cdot z)$	[flip 12]
18	$0+x' = x'$	[13 → 10]
21,20	$x+x = x$	[3 → 10]
23,22	$x\cdot x = x$	[10 → 3]
29	$x\cdot(y+(z+x)) = x$	[3 → 6 :11, flip]
31	$x\cdot y = y\cdot x$	[20 → 6 :21]
36,35	$x\cdot(y+x) = x$	[22 → 6 :11, flip]
38,37	$x+(y\cdot x) = x\cdot(x+y)$	[22 → 6]
56	$x+y = y+x$	[22 → 12 :23]
72	$0' = 1$	[8 → 18, flip]
76	$0\cdot 1 = 0$	[72 → 13]
94,93	$x\cdot(x+y) = x$	[20 → 15 :4,38, flip]
98	$x+(y\cdot(z\cdot x)) = x$	[10 → 15 :4, flip]
115	$x+(y\cdot x) = x$	[37 :94]
130	$x+0 = (0+x)\cdot(1+x)$	[76 → 12]
135	$(0+x)\cdot(1+x) = x+0$	[flip 130]
141	$x'\cdot x = 0$	[13 → 31, flip]
150	$x+0 = (y'+x)\cdot(y+x)$	[141 → 12]
153,152	$0+x = x$	[141 → 10]
155,154	$x\cdot(x'+y) = y\cdot x$	[141 → 6 :153, flip]
156	$(x'+y)\cdot(x+y) = y+0$	[flip 150]
161,160	$x+0 = x$	[135 :153,36, flip]
164	$(x'+y)\cdot(x+y) = y$	[flip 156 :161, flip]

235,234	$(x \cdot y) + z = (x + z) \cdot (y + z)$	[12 → 56, flip]
236	$x' + x = 1$	[8 → 56, flip]
276,275	$x \cdot 1 = x$	[236 → 29]
366	$(x + y) + x = x + y$	[93 → 115]
1269	$x + (x + y) = x + y$	[56 → 366]
1623	$(x' + y) \cdot x = y \cdot x$	[1269 → 154 :155, flip]
1922	$(x + y') \cdot (y + x) = x$	[56 → 164]
4171,4170	$((x + y') \cdot (z + y')) \cdot y = (x \cdot z) \cdot y$	[12 → 1623]
5275,5274	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$	[98 → 1922 :235,235,9,276,4171]
6098	□	[2 :5275 :31,1]

7.7.3 Algebras of Set Difference

The theorems in this section are related to Kalman's work on set difference [11, 7], where he shows that the identites

$$\begin{aligned} x - (y - x) &= x \\ x - (x - y) &= y - (y - x) \\ (x - y) - z &= (x - z) - (y - z) \end{aligned}$$

form a basis for families of sets closed under set difference.

Thm. #LT-1a is a check that intersection, when defined in terms of set difference, is associative and commutative. Thm. #LT-1b shows that the third identity of Kalman's basis can be replaced with a simpler one [12].

Theorem #LT-1a.

$$\left\{ \begin{array}{l} x - (y - x) = x \\ x - (x - y) = y - (y - x) \\ (x - y) - z = (x - z) - (y - z) \\ x \cdot y = x - (x - y) \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} (x \cdot y) \cdot z = x \cdot (y \cdot z) \\ x \cdot y = y \cdot x \end{array} \right\}.$$

Proof (found by Otter 3.0.3l on gyro at 4.68 seconds).

3,2	$x - (y - x) = x$	
4	$x - (x - y) = y - (y - x)$	
5	$(x - y) - z = (x - z) - (y - z)$	
7,6	$x \cdot y = x - (x - y)$	
8	$(A \cdot B) \cdot C = A \cdot (B \cdot C),\ A \cdot B = B \cdot A \ \rightarrow$ □	
9	$(A - (A - B)) - ((A - (A - B)) - C) = A - (A - (B - (B - C))) \ \rightarrow$ □	[copy,8 :7,7,7,7,7
10	$(x - y) - (z - y) = (x - z) - y$	[flip 5]
11	$(x - y) - y = x - y$	[2 → 2]
14,13	$(x - y) - (x - y) = y - y$	[11 → 4 :3]
15	$(x - y) - ((x - y) - x) = x - (y - (y - x))$	[4 → 4, flip]
22,21	$(x - (x - y)) - (y - (y - x)) = x - x$	[4 → 13 :14]
23	$x - x = y - y$	[4 → 13 :22,14]

24	$((x-y)-z)-(y-z)=(x-y)-z$	[11 → 5, flip]
28	$(x-y)-((z-x)-y)=x-y$	[2 → 5, flip]
44	$(x-(x-y))-y=z-z$	[5 → 23 :3]
48,47	$x-(y-y)=x$	[23 → 4 :3]
56,55	$(x-x)-y=x-x$	[47 → 2]
76	$(A-(A-B))-((B-(B-A))-C)=A-(A-(B-(B-C)))$ → □	[4 → 9]
103	$x-x=((y-(y-z))-u)-z$	[44 → 10 :56]
107,106	$((x-y)-z)-y=(x-y)-(z-y)$	[11 → 10, flip]
112,111	$(x-y)-(z-x)=x-(y-(z-x))$	[2 → 10, flip]
126,125	$(x-y)-x=x-x$	[55 → 10, flip]
128	$((x-(x-y))-z)-y=u-u$	[flip 103]
132	$x-(y-(y-x))=x-y$	[15 :126,48, flip]
148	$(x-(y-z))-y=x-y$	[125 → 10 :48, flip]
153,152	$x-(x-(x-y))=x-y$	[125 → 4 :48, flip]
178	$(x-y)-(x-(y-z))=z-z$	[148 → 125 :14,14]
227,226	$((x-(x-y))-z)-((y-x)-z)=(x-(x-y))-z$	[132 → 28]
294	$(x-(x-y))-z=(y-(y-x))-z$	[4 → 24 :227]
313	$x-(x-((y-(y-x))-z))=(y-(y-x))-z$	[128 → 4 :48, flip]
403	$x-(x-((y-x)-z))=z-z$	[2 → 178]
521	$x-(x-((y-x)-z))=x-x$	[132 → 403 :14,14,14]
615,614	$(x-y)-(z-y)=(x-y)-z$	[521 → 132 :48,107, flip]
770	$x-(y-(z-x))=x-y$	[28 :615,112]
774	$(x-y)-z=(x-z)-y$	[10 :615]
842,841	$x-((y-(z-x))-u)=x-(y-u)$	[774 → 770]
847,846	$(x-(x-y))-z=y-(y-(x-z))$	[313 :842, flip]
861	$x-(x-(y-z))=y-(y-(x-z))$	[294 :847,847]
862	$B-(B-(A-(B-C)))=A-(A-(B-(B-C)))$ → □	[76 :847,847,153]
863	□	[862,861]

Theorem #LT-1b.

$$\left\{\begin{array}{l} x-(y-x)=x \\ x-(x-y)=y-(y-x) \end{array}\right\} \Rightarrow \{(x-y)-z=(x-z)-(y-z) \Leftrightarrow (x-y)-z=(x-z)-y\}.$$

Proof (⇒) found by Otter 3.0.3l on gyro at 2.69 seconds.

3,2	$x-(y-x)=x$	
4	$x-(x-y)=y-(y-x)$	
5	$(x-y)-z=(x-z)-(y-z)$	
6	$(A-C)-B\neq(A-B)-C$	
7	$(x-y)-(z-y)=(x-z)-y$	[flip 5]
8	$(x-y)-y=x-y$	[2 → 2]
11,10	$(x-y)-(x-y)=y-y$	[8 → 4 :3]
12	$(x-y)-((x-y)-x)=x-(y-(y-x))$	[4 → 4, flip]
19,18	$(x-(x-y))-(y-(y-x))=x-x$	[4 → 10 :11]

20	$x - x = y - y$	[4 → 10 :19,11]
35	$(A - B) - (C - B) \neq (A - B) - C$	[5 → 6]
46,45	$x - (y - y) = x$	[20 → 4 :3]
53	$(x - x) - y = x - x$	[45 → 2]
83,82	$((x - y) - z) - y = (x - y) - (z - y)$	[8 → 7, flip]
98,97	$(x - y) - x = x - x$	[53 → 7, flip]
104	$x - (y - (y - x)) = x - y$	[12 :98,46, flip]
120	$(x - (y - z)) - y = x - y$	[97 → 7 :46, flip]
154	$(x - y) - (x - (y - z)) = z - z$	[120 → 97 :11,11]
359	$x - (x - ((y - x) - z)) = z - z$	[2 → 154]
569	$x - (x - ((y - x) - z)) = x - x$	[104 → 359 :11,11,11]
627	$(x - y) - (z - y) = (x - y) - z$	[569 → 104 :46,83, flip]
629	□	[627,35]

Proof (⇐) found by Otter 3.0.3l on gyro at 20.04 seconds.

3,2	$x - (y - x) = x$	
4	$x - (x - y) = y - (y - x)$	
5	$(x - y) - z = (x - z) - y$	
6	$(A - B) - C \neq (A - C) - (B - C)$	
7	$(A - C) - (B - C) \neq (A - B) - C$	[flip 6]
8	$(x - y) - y = x - y$	[2 → 2]
11,10	$(x - y) - (x - y) = y - y$	[8 → 4 :3]
19,18	$((x - y) - z) - y = (x - y) - z$	[8 → 5, flip]
21	$(x - (x - y)) - z = (y - z) - (y - x)$	[4 → 5]
22	$(x - y) - (z - x) = x - y$	[2 → 5, flip]
29	$(x - y) - (x - z) = (z - (z - x)) - y$	[flip 21]
33,32	$(x - y) - ((x - z) - y) = z - (z - (x - y))$	[5 → 4]
34	$x - ((y - x) - z) = x$	[5 → 2]
50	$x - x = y - y$	[34 → 4 :19,11]
55,54	$x - (y - y) = x$	[50 → 34]
57	$(x - x) - y = (z - y) - z$	[50 → 5]
61	$(x - y) - x = (z - z) - y$	[flip 57]
67,66	$(x - x) - y = x - x$	[54 → 2]
68	$(x - y) - x = z - z$	[61 :67]
75	$x - (x - (x - y)) = x - y$	[68 → 4 :55, flip]
103,102	$((x - y) - z) - (u - (x - z)) = (x - z) - y$	[5 → 22]
767	$(x - y) - ((z - (z - x)) - y) = (x - z) - ((x - z) - (x - y))$	[29 → 4]
841	$(x - (x - y)) - ((x - (x - y)) - (x - z)) = y - (y - (x - z))$	[75 → 32 :33, flip]
2094,2093	$(x - y) - (x - (x - z)) = (x - y) - z$	[75 → 102 :103, flip]
2125,2124	$(x - y) - ((x - y) - (x - z)) = (x - y) - z$	[29 → 102 :19]
2130,2129	$(x - (x - y)) - z = y - (y - (x - z))$	[841 :2125]
2132	$(x - y) - (z - y) = (x - z) - y$	[767 :2130,2094,2125]
2133	□	[2132,7]

7.7.4 Robbins Algebra

This section is on the celebrated Robbins problem, whether a Robbins algebra is necessarily a Boolean algebra. Consider the identities

$$n(x + n(y)) + n(n(x) + n(y)) = y, \qquad \text{(Huntington-axiom)}$$
$$n(n(x + y) + n(x + n(y))) = x. \qquad \text{(Robbins-axiom)}$$

It is known that the Huntington axiom, along with commutativity and associativity of $+$, is a basis for Boolean algebra, but it is unknown whether the Huntington axiom can be replaced with the Robbins axiom.

Problem #RBA-1. The Robbins conjecture.

$$\left\{ \begin{array}{l} x + y = y + x \\ (x + y) + z = x + (y + z) \\ \text{Robbins-axiom} \end{array} \right\} \Rightarrow \{\text{Huntington-axiom}\}.$$

Winker and Wos attacked the problem by finding weaker and weaker conditions that force a Robbins algebra to be Boolean [41]. We present two examples; the condition in the second is so week that it is hard for us to imagine a Robbins algebra that is not Boolean.

Theorem #RBA-2. If a Robbins algebra has an element c such that $c+c = c$, then it is a Boolean algebra.

$$\left\{ \begin{array}{l} x + y = y + x \\ (x + y) + z = x + (y + z) \\ n(n(x + y) + n(x + n(y))) = x \\ c + c = c \end{array} \right\} \Rightarrow \{n(x + n(y)) + n(n(x) + n(y)) = y\}.$$

Proof (found by Otter 3.0.3l on gyro at 21.87 seconds).

1	$x = x$	
2	$x + y = y + x$	
4,3	$(x + y) + z = x + (y + z)$	
6,5	$n(n(x + y) + n(x + n(y))) = x$	
7	$c + c = c$	
9	$n(A + n(B)) + n(n(A) + n(B)) \neq B$	
10	$c + (c + x) = c + x$	[7 → 3, flip]
13	$x + (y + z) = y + (z + x)$	[2 → 3]
14	$x + (y + z) = z + (x + y)$	[flip 13]
16,15	$c + (x + c) = c + x$	[2 → 10]
25	$n(n(c) + n(c + n(c))) = c$	[7 → 5]
27	$n(n(x + (y + z)) + n(x + (y + n(z)))) = x + y$	[3 → 5 :4]
29	$n(n(x + y) + n(y + n(x))) = y$	[2 → 5]
33	$n(n(x + (n(y + z) + n(y + n(z)))) + n(x + y)) = x$	[5 → 5]

35	$n(n(x+y)+n(n(y)+x))=x$	[2 → 5]
39	$n(n(x+n(y))+n(x+y))=x$	[2 → 5]
49	$x+(y+z)=z+(y+x)$	[2 → 13]
63	$n(n(c+n(c))+n(c))=c$	[2 → 25]
65	$n(n(n(c)+(c+n(c)))+c)=n(c)$	[25 → 5]
73	$n(n(A)+n(B))+n(A+n(B))\neq B$	[2 → 9]
98	$n(n(x+(n(c+n(c))+n(c)))+n(x+c))=x$	[63 → 5]
117	$n(n(x+(y+z))+n(y+(x+n(z))))=y+x$	[49 → 29 :4]
147	$n(n(x+y)+n(n(x)+y))=y$	[2 → 29]
159	$n(n(x+n(y))+n(y+x))=x$	[2 → 29]
227	$n(n(n(x)+y)+n(y+x))=y$	[2 → 35]
289	$n(c+n(n(c)+(c+n(c))))=n(c)$	[25 → 39]
303	$n(n(x+n(y+z))+n(z+(x+y)))=x$	[14 → 39]
381	$n(n(n(x)+y)+n(x+y))=y$	[2 → 147]
459	$n(n(c+(x+n(c)))+n(c+x))=c+x$	[10 → 159 :4]
646,645	$n(n(c)+n(n(c)+(c+n(c))))=c$	[65 → 381 :4,4,16]
652,651	$n(n(c)+(c+n(c)))=n(c+n(c))$	[65 → 227 :646, flip]
681	$n(c+n(c+n(c)))=n(c)$	[289 :652]
1451,1450	$n(n(c+(n(c+n(c))+n(c)))+n(c))=c$	[7 → 98]
1583,1582	$n(n(x+c)+n(n(c+n(c))+(x+n(c))))=x$	[25 → 303]
1644	$c+n(c+n(c))=c$	[681 → 459 :1451, flip]
1646	$n(c+n(c))+c=c$	[2 → 1644]
1719,1718	$n(c+n(c))+x=x$	[1646 → 117 :1583, flip]
1725,1724	$x+n(c+n(c))=x$	[1646 → 27 :1719,6, flip]
1770	$n(x+n(x))=n(c+n(c))$	[1718 → 33 :6,1719]
1957,1956	$n(n(n(n(x))+x))=n(n(x))$	[1770 → 227 :1719]
1959,1958	$n(n(x))=x$	[1770 → 227 :1725,1957]
2091,2090	$n(n(x)+y)+n(x+y)=n(y)$	[381 → 1958, flip]
2177	$B\neq B$	[73 :2091,1959]
2178	$\Box$	[2177,1]

Theorem #RBA-3. If a Robbins algebra has elements c and d such that $c+d=c$, then it is a Boolean algebra.

$$\left\{\begin{array}{l} x+y=y+x \\ (x+y)+z=x+(y+z) \\ n(n(x+y)+n(x+n(y)))=x \\ c+d=c \end{array}\right\} \Rightarrow \{n(x+n(y))+n(n(x)+n(y))=y\}.$$

By Thm. #RBA-2, it is sufficient to show $\exists e, e+e=e$.

Proof (found by Otter 3.0.3l on gyro at 1506.24 seconds).

1	$x+x\neq x$
4,3	$x+y=y+x$
6,5	$(x+y)+z=x+(y+z)$

8,7	$x + (y + z) = y + (x + z)$	
9	$n(n(x + y) + n(x + n(y))) = x$	
12,11	$c + d = c$	
14	$n(n(x + (y + z)) + n(y + n(x + z))) = y$	$[7 \to 9]$
18	$n(n(x + y) + n(y + n(x))) = y$	$[3 \to 9]$
20	$n(n(x + y) + n(x + (n(y + z) + n(y + n(z))))) = x$	$[9 \to 9 :4]$
22	$n(n(x + y) + n(n(y) + x)) = x$	$[3 \to 9]$
26	$c + (x + d) = x + c$	$[11 \to 7, \text{flip}]$
31,30	$c + (d + x) = c + x$	$[11 \to 5, \text{flip}]$
32	$n(n(x + c) + n(c + n(x + d))) = c$	$[26 \to 9]$
40	$n(n(c + x) + n(d + (n(c) + x))) = d + x$	$[30 \to 18 :4,8]$
44	$n(n(c) + n(d + n(c))) = d$	$[11 \to 18]$
58	$n(n(x + y) + n(n(x) + y)) = y$	$[3 \to 18]$
62	$n(n(x + n(y)) + n(y + x)) = x$	$[3 \to 18]$
67,66	$n(d + n(d + (n(c) + n(c)))) = n(c)$	$[44 \to 18 :4,8,4]$
77,76	$n(n(c + x) + n(d + n(c + x))) = d$	$[30 \to 14]$
80	$n(n(x + (y + z)) + n(y + n(z + x))) = y$	$[3 \to 14]$
102	$n(n(x + (n(y + z) + n(z + n(y)))) + n(z + x)) = x$	$[18 \to 22]$
108	$n(d + n(c + n(d + n(c)))) = n(d + n(c))$	$[44 \to 22 :4,4]$
112	$n(x + n(x + (y + n(n(y) + x)))) = n(n(y) + x)$	$[22 \to 22 :8,4,4]$
130	$n(n(x + (y + z)) + n(n(x + y) + z)) = z$	$[5 \to 58]$
146	$n(x + n(y + (x + n(n(y) + x)))) = n(n(y) + x)$	$[58 \to 58 :6,4]$
176	$n(n(x + n(y + z)) + n(y + (z + x))) = x$	$[5 \to 62]$
242	$n(n(x + c) + n(c + n(d + x))) = c$	$[3 \to 32]$
294	$n(n(x + n(y + n(z))) + n(x + (y + n(z + (y + n(y + n(z))))))) = x$	$[62 \to 20 :8,4,4]$
434	$n(n(c + n(d + x)) + n(x + c)) = c$	$[3 \to 242]$
529,528	$n(n(c) + n(d + (d + n(c)))) = d + d$	$[11 \to 40 :4]$
636	$n(n(n(d + (n(c) + x)) + (y + n(c + x))) + n(y + (d + x))) = y$	$[40 \to 80]$
814	$n(n(x + (y + z)) + n(n(y + x) + z)) = z$	$[7 \to 130]$
866	$n(n(x + n(y + z)) + n(z + (y + x))) = x$	$[3 \to 176]$
1140	$n(n(d + (x + n(c + y))) + n(y + (c + x))) = d + x$	$[30 \to 866 :6]$
1933,1932	$n(n(c) + n(d + (n(x + c) + n(c + n(x))))) = d$	$[11 \to 102 :4]$
2194	$n(n(c + n(d + n(c))) + n(c + n(c + n(d + n(c))))) = c$	$[108 \to 434 :4]$
2356	$n(n(d + n(c + x)) + n(c + (x + n(d + n(c + x))))) = d$	$[76 \to 112 :4,8,31,4,6,77]$
5429,5428	$n(d + n(d + (n(c + x) + n(c + (x + n(d + n(c + x))))))) = n(c + x)$	$[76 \to 294 :8,6,8,31,8]$
6608	$n(c + (x + n(d + n(c + x)))) = n(c + x)$	$[2356 \to 814 :8,4,5429, \text{flip}]$
6611,6610	$n(c + n(d + n(c))) = n(c)$	$[11 \to 6608 :31,12]$
6653,6652	$n(n(c) + n(c + n(c))) = c$	$[2194 :6611,6611]$
6721,6720	$n(c + n(c + (n(c) + n(c + (c + n(c + n(c))))))) = n(c)$	$[6652 \to 294 :8]$
6798	$n(n(c + n(c)) + n(c + (c + n(c + n(c))))) = c$	$[6652 \to 146 :4,6653]$
7832	$n(c + (c + n(c + n(c)))) = n(c)$	$[6798 \to 814 :8,4,6721, \text{flip}]$
7834	$d + n(c + n(c)) = d$	$[7832 \to 1140 :4,4,1933, \text{flip}]$
8090	$d + d = d$	$[7834 \to 636 :4,67,529]$
8092	$\square$	$[8090,1]$

The preceding theorem is very difficult for OTTER and the proof shown is the result of a very specialized search strategy. Our first automatic proof (without hints or special strategies) was found with a prototype theorem prover with associative-commutative (AC) unification and matching; that proof was the first known first-order proof. Wos and McCune then found an automatic proof with OTTER using the *tail strategy*, which penalizes equalities with complex right-hand sides, and a restriction strategy that discards equalities with more than 3 variables. Independently, R. Veroff found an OTTER proof with the *hints strategy* [40], using the AC proof as hints. The proof shown above was found with a strategy that discards equalities that match some simple patterns that do not appear in some of the other proofs; we have inlcluded this proof, because it is shorter than most of the other proofs we have found. We are applying the strategies we have developed for this theorem to searches for a proof of the main conjecture, #RBA-1.

7.7.5 Ternary Boolean Algebra

These results are also reported in [32]. Padmanabhan's reduction schema [26] gives us the following single axiom for ternary Boolean algebra (TBA).

$$f(f(x,g(x),y),g(f(f(z,g(f(f(u,v,w),v6,f(u,v,v7))),f(v,f(v7,v6,w),u)),g(v8),z)),z)=y$$

The following theorem gives us a simplier single axiom for TBA; it was found by running OTTER searches with many candidate axioms derived from the preceding axiom.

Theorem #TBA-1.

$$\left\{\begin{array}{l} f(f(v,w,x),y,f(v,w,z))=f(v,w,f(x,y,z)) \\ f(y,x,x)=x \\ f(x,y,g(y))=x \\ f(x,x,y)=x \\ f(g(y),y,x)=x \end{array}\right\} \Leftrightarrow \{f(f(x,g(x),y),g(f(f(z,u,v),w,f(z,u,v6))$$

Proof ($\Rightarrow$) found by Otter 3.0.3l on gyro at 3.94 seconds.

1	$x=x$	
3,2	$f(f(x,y,z),u,f(x,y,v))=f(x,y,f(z,u,v))$	
4	$f(x,y,y)=y$	
7,6	$f(x,y,g(y))=x$	
9,8	$f(x,x,y)=x$	
10	$f(g(x),x,y)=y$	
12	$f(f(A,g(A),B),g(f(f(C,D,E),F,f(C,D,G))),f(D,f(G,F,E),C))\neq B$	
13	$f(f(A,g(A),B),g(f(C,D,f(E,F,G))),f(D,f(G,F,E),C))\neq B$	[copy,12 :3]
14	$f(x,y,f(z,f(x,y,u),u))=f(x,y,u)$	$[2\rightarrow 4]$
17,16	$f(f(x,y,z),u,y)=f(x,y,f(z,u,y))$	$[4\rightarrow 2]$
18	$f(x,y,f(z,x,u))=f(z,x,f(x,y,u))$	$[4\rightarrow 2]$

19	$f(x,y,f(y,z,u)) = f(y,z,f(x,y,u))$	[flip 18]
20	$f(x,y,f(z,f(x,y,z),u)) = f(x,y,z)$	[2 → 8]
22	$f(x,y,x) = x$	[8 → 2 :9,9]
25,24	$f(f(x,y,z),u,x) = f(x,y,f(z,u,x))$	[22 → 2]
33	$f(x,y,f(z,x,g(y))) = x$	[6 → 14 :7]
46,45	$f(x,y,f(z,u,f(v,x,g(y)))) = f(x,y,f(z,u,x))$	[33 → 2 :25, flip]
57	$f(x,y,z) = f(x,z,f(g(z),y,z))$	[6 → 16]
60	$f(x,y,f(g(y),z,y)) = f(x,z,y)$	[flip 57]
61	$f(x,y,f(z,g(y),x)) = x$	[16 → 33 :46]
71	$f(g(g(x)),x,y) = g(g(x))$	[6 → 61]
80,79	$g(g(x)) = x$	[4 → 71, flip]
84,83	$f(x,g(x),y) = y$	[79 → 10]
85	$f(x,g(y),f(z,y,x)) = x$	[79 → 61]
90,89	$f(x,g(y),y) = x$	[79 → 6]
91	$f(B,g(f(C,D,f(E,F,G))),f(D,f(G,F,E),C)) \neq B$	[13 :84]
163,162	$f(x,y,f(z,x,y)) = f(z,x,y)$	[4 → 19, flip]
286	$f(x,g(y),f(y,x,z)) = x$	[89 → 20 :90]
374	$f(x,y,z) = f(y,z,x)$	[286 → 85 :80,17,163]
403,402	$f(g(x),y,x) = y$	[83 → 374, flip]
420	$f(x,y,z) = f(x,z,y)$	[60 :403]
444	$f(B,g(f(D,f(E,F,G),C)),f(D,f(G,F,E),C)) \neq B$	[374 → 91]
612	$f(x,y,z) = f(z,y,x)$	[374 → 420]
1085	$B \neq B$	[612 → 444 :90]
1086	□	[1085,1]

Proof (⇐) found by Otter 3.0.3l on gyro at 1.75 seconds.

1	$x = x$	
2	$f(f(D,E,A),B,f(D,E,C)) = f(D,E,f(A,B,C)),\ f(B,A,A) = A,\ f(A,B,g(B)) = A,\ f(A,A,B) = A,$	
4,3	$f(f(x,g(x),y),g(f(f(z,u,v),w,f(z,u,v_6))),f(u,f(v_6,w,v),z)) = y$	
5	$f(f(x,y,z),g(f(f(u,v,w),v_6,f(u,v,v_7))),f(v,f(v_7,v_6,w),u)) = f(y,f(z,g(f(x,y,v_8)),v_8),x)$ [3 → 3]	
6	$f(f(x,g(x),y),g(f(f(z,u,f(v,f(w,v_6,v_7),v_8)),g(f(f(v_8,v,v_7),v_6,f(v_8,v,w))),f(z,u,f(v_9,g(v_9),v_{10})))),$	
8	$f(x,f(y,g(f(z,x,u)),u),z) = f(f(z,x,y),g(f(f(v,w,v_6),v_7,f(v,w,v_8))),f(w,f(v_8,v_7,v_6),v))$ [flip 5]	
9	$f(x,f(y,g(f(z,x,u)),u),z) = f(x,f(y,g(f(z,x,v)),v),z)$ [5 → 5]	
10	$f(g(x),f(y,g(f(x,g(x),z)),z),x) = y$ [3 → 5, flip]	
13,12	$f(f(x,g(x),y),g(f(z,g(z),f(u,g(u),v))),f(g(z),v,z)) = y$ [6 → 6 :4]	
15,14	$f(g(x),y,x) = y$ [12 → 12 :13, flip]	
18	$f(f(x,g(x),y),g(f(z,g(z),g(g(u)))),u) = y$ [12 → 12 :15]	
20	$f(x,g(f(y,g(y),z)),z) = x$ [10 :15]	
27,26	$f(x,g(g(g(y))),y) = x$ [14 → 20]	
31,30	$g(f(x,g(x),y)) = g(y)$ [14 → 20]	
33,32	$f(x,g(y),y) = x$ [20 :31]	
35,34	$f(x,g(x),y) = y$ [18 :31,27]	
37,36	$f(x,g(f(f(y,z,u),v,f(y,z,w))),f(z,f(w,v,u),y)) = x$ [3 :35]	
38	$f(x,f(y,g(f(z,x,u)),u),z) = f(z,x,y)$ [8 :37]	
39	$f(x,y,z) = f(y,f(z,g(f(x,y,u)),u),x)$ [5 :37]	

43,42	$g(g(x)) = x$	[14 → 34]
47,46	$f(x, y, g(y)) = x$	[42 → 32]
49,48	$f(g(x), x, y) = y$	[42 → 34]
51,50	$f(x, y, g(x)) = y$	[42 → 14]
52	$f(f(D,E,A),B,f(D,E,C)) = f(D,E,f(A,B,C)),\ f(B,A,A) = A,\ f(A,A,B) = A\ \rightarrow$	
56,55	$f(x, f(y, g(f(z, x, u)), u), z) = f(x, f(y, g(z), g(x)), z)$	[46 → 9, flip]
59	$f(x, y, z) = f(y, f(z, g(x), g(y)), x)$	[39 :56]
60	$f(x, f(y, g(z), g(x)), z) = f(z, x, y)$	[38 :56]
67	$f(x, g(f(y, z, u)), f(u, z, y)) = x$	[48 → 36 :49,51]
107	$f(x, y, z) = f(z, y, x)$	[48 → 67 :43]
111	$f(f(x, y, z), g(f(z, y, x)), u) = u$	[67 → 107, flip]
132,131	$f(f(x, y, z), u, f(x, y, v)) = f(y, f(z, u, v), x)$	[36 → 111]
139	$f(E,f(A,B,C),D) = f(D,E,f(A,B,C)),\ f(B,A,A) = A,\ f(A,A,B) = A\ \rightarrow\ \Box$	[52 :13
144	$f(x, f(y, g(x), g(z)), z) = f(x, f(y, g(z), g(x)), z)$	[50 → 55]
149	$f(x, f(y, g(z), g(x)), z) = f(x, f(y, g(x), g(z)), z)$	[flip 144]
160	$f(x, y, z) = f(y, f(x, g(z), g(y)), z)$	[107 → 59]
171	$f(x, f(y, g(z), g(x)), z) = f(y, x, z)$	[flip 160]
290,289	$f(x, y, y) = y$	[50 → 60 :33, flip]
294,293	$f(x, f(y, g(x), g(z)), z) = f(x, z, y)$	[107 → 60]
301	$f(E,f(A,B,C),D) = f(D,E,f(A,B,C)),\ f(A,A,B) = A\ \rightarrow\ \Box$	[139 :290 :1]
310,309	$f(x, f(y, g(z), g(x)), z) = f(x, z, y)$	[149 :294]
340	$f(x, y, z) = f(z, x, y)$	[171 :310]
363,362	$f(x, x, y) = x$	[107 → 289]
364	$\Box$	[301 :363 :340,1]

Chapter 8

Miscellaneous Topics

8.1 Inverse Loops and Moufang Loops

The variety of quasigroups can be axiomatized equationally with the four identities

$$\begin{aligned} x \cdot (x\backslash y) &= y, & (x/y) \cdot y &= x, \\ x\backslash(x \cdot y) &= y, & (x \cdot y)/y &= x, \end{aligned}$$

in which '$\cdot$' is the quasigroup operation, $x\backslash y$ is the right solution of x and y, i.e., the unique element z such that $x \cdot z = y$, and x/y is the left solution of x and y. (In fact, the operations '$\backslash$' and '$/$' are quasigroups as well.)

A *loop* is a quasigroup containing an element, say 1, that is a left and right identity: $1 \cdot x = x \cdot 1 = x$. If we define $L(x)$ as $1/x$ and $R(x)$ as $x\backslash 1$, then it follows immediately the all elements (of loops) have unique left and right inverses, $L(x) \cdot x = x \cdot R(x) = 1$. We can therefore use the following set as an equational basis for the variety of loops,

$$\begin{aligned} x \cdot (x\backslash y) &= y, & (x/y) \cdot y &= x, \\ x\backslash(x \cdot y) &= y, & (x \cdot y)/y &= x, \\ 1 \cdot x &= x, & x \cdot 1 &= x, \\ L(x) \cdot x &= 1, & x \cdot R(x) &= 1, \end{aligned}$$

where the equations for left and right inverse are optional. An *inverse loop* is a loop in which $L(x) = R(x)$. A independent basis for inverse loops is the set

$$\begin{aligned} x' \cdot x &= 1, \\ x' \cdot (x \cdot y) &= y, \\ (x \cdot y) \cdot y' &= x, \end{aligned}$$

in which $'$ denotes inverse; the quasigroup properties follow, and the set is easily proved independent with three MACE runs.

8.1.1 Bases for Moufang Loops

A *Moufang loop* [5] is a loop that satisfies *any* of the so-called Moufang identities:

$$(x \cdot (y \cdot z)) \cdot x = (x \cdot y) \cdot (z \cdot x), \qquad \text{(Moufang-1)}$$
$$((x \cdot y) \cdot z) \cdot y = x \cdot (y \cdot (z \cdot y)), \qquad \text{(Moufang-2)}$$
$$((x \cdot y) \cdot x) \cdot z = x \cdot (y \cdot (x \cdot z)). \qquad \text{(Moufang-3)}$$

That is, given a loop, the three Moufang identities are equivalent. We show this in the following three problems as Moufang-1⇒Moufang-2⇒Moufang-3⇒Moufang-1.

Theorem #MFL-1.

$$\{\text{loop}, \text{Moufang-1}\} \Rightarrow \{\text{Moufang-2}\}$$

Proof (found by Otter 3.0.3l on gyro at 11.20 seconds).

3,2	$1 \cdot x = x$	
5,4	$x \cdot 1 = x$	
6	$x \cdot (x \backslash y) = y$	
8	$x \backslash (x \cdot y) = y$	
10	$(x / y) \cdot y = x$	
13,12	$(x \cdot y) / y = x$	
14	$x \cdot R(x) = 1$	
18	$(x \cdot (y \cdot z)) \cdot x = (x \cdot y) \cdot (z \cdot x)$	
20	$((A \cdot B) \cdot C) \cdot B \neq A \cdot (B \cdot (C \cdot B))$	
30,29	$x \backslash 1 = R(x)$	[14 → 8]
32,31	$x \backslash x = 1$	[4 → 8]
51	$(x \cdot (y / z)) \cdot (z \cdot x) = (x \cdot y) \cdot x$	[10 → 18, flip]
53	$(x \cdot y) \cdot x = (x \cdot z) \cdot ((z \backslash y) \cdot x)$	[6 → 18]
55,54	$(x \cdot y) \cdot x = x \cdot (y \cdot x)$	[2 → 18 :5]
56	$(x \cdot y) \cdot ((y \backslash z) \cdot x) = x \cdot (z \cdot x)$	[flip 53 :55]
58	$(x \cdot (y / z)) \cdot (z \cdot x) = x \cdot (y \cdot x)$	[51 :55]
60	$x \cdot ((y \cdot z) \cdot x) = (x \cdot y) \cdot (z \cdot x)$	[18 :55]
64	$x \cdot (R(x) \cdot x) = x$	[14 → 54 :3, flip]
68	$x \cdot ((x \backslash y) \cdot x) = y \cdot x$	[6 → 54, flip]
70	$(x \cdot (y \cdot x)) / x = x \cdot y$	[54 → 12]
78	$R(x) \cdot x = 1$	[64 → 8 :32, flip]
85,84	$R(R(x)) = x$	[78 → 8 :30]
104	$x \backslash (y \cdot x) = (x \backslash y) \cdot x$	[68 → 8]
106	$(x \backslash y) \cdot R(x) = R(x) \cdot (y \cdot R(x))$	[78 → 56 :3]
119,118	$(x \cdot y) / x = x \cdot (y / x)$	[10 → 70]
149,148	$R(x) \cdot (y / x) = R(x) \cdot (y \cdot R(x))$	[14 → 58 :5]
150	$(x \cdot (y / (z / x))) \cdot z = x \cdot (y \cdot x)$	[10 → 58]
188	$x \backslash ((x \cdot y) \cdot (z \cdot x)) = (y \cdot z) \cdot x$	[60 → 8]

236	$(x\backslash(y/x)) \cdot x = x\backslash y$	[10 → 104, flip]
255	$x \cdot ((x\backslash y)/x) = y/x$	[6 → 118, flip]
286	$x\backslash(y/x) = (x\backslash y)/x$	[236 → 12, flip]
493,492	$x\backslash y = R(x) \cdot y$	[106 → 12 :119,13, flip]
551,550	$(R(x) \cdot y)/x = R(x) \cdot (y \cdot R(x))$	[286 :493,149,493, flip]
559,558	$x/y = y \cdot (R(y) \cdot (x \cdot R(y)))$	[255 :493,551, flip]
566	$R(x) \cdot ((x \cdot y) \cdot (z \cdot x)) = (y \cdot z) \cdot x$	[188 :493]
585,584	$R(x) \cdot (x \cdot y) = y$	[8 :493]
587,586	$x \cdot (R(x) \cdot y) = y$	[6 :493]
630	$(x \cdot (y \cdot R(z \cdot R(x)))) \cdot z = x \cdot (y \cdot x)$	[150 :559,587,559,587]
634	$(x \cdot R(y)) \cdot y = x$	[10 :559,587]
658	$(x \cdot y) \cdot R(y) = x$	[84 → 634]
672	$x \cdot R(y \cdot x) = R(y)$	[584 → 658]
687,686	$R(x \cdot y) = R(y) \cdot R(x)$	[658 → 672, flip]
692	$(x \cdot (y \cdot (x \cdot R(z)))) \cdot z = x \cdot (y \cdot x)$	[630 :687,85]
946	$(x \cdot (y \cdot x)) \cdot z = x \cdot (y \cdot (x \cdot z))$	[692 → 634 :85]
954	$((x \cdot y) \cdot z) \cdot y = x \cdot (y \cdot (z \cdot y))$	[946 → 566 :585, flip]
956	□	[954,20]

Theorem #MFL-2.

$$\{\text{loop}, \text{Moufang-2}\} \Rightarrow \{\text{Moufang-3}\}$$

Proof (found by Otter 3.0.3l on gyro at 13.31 seconds).

3,2	$1 \cdot x = x$	
4	$x \cdot 1 = x$	
8	$x\backslash(x \cdot y) = y$	
11,10	$(x/y) \cdot y = x$	
12	$(x \cdot y)/y = x$	
14	$x \cdot R(x) = 1$	
18	$((x \cdot y) \cdot z) \cdot y = x \cdot (y \cdot (z \cdot y))$	
20	$((A \cdot B) \cdot A) \cdot C \neq A \cdot (B \cdot (A \cdot C))$	
30,29	$x\backslash 1 = R(x)$	[14 → 8]
32,31	$x\backslash x = 1$	[4 → 8]
37	$(x/y)\backslash x = y$	[10 → 8]
49	$x \cdot (R(x) \cdot (y \cdot R(x))) = y \cdot R(x)$	[14 → 18 :3, flip]
53,52	$(x \cdot y) \cdot x = x \cdot (y \cdot x)$	[2 → 18 :3]
54	$x \cdot (y \cdot (R(x \cdot y) \cdot y)) = y$	[14 → 18 :3, flip]
61	$(A \cdot (B \cdot A)) \cdot C \neq A \cdot (B \cdot (A \cdot C))$	[20 :53]
68	$x \cdot (R(x) \cdot x) = x$	[14 → 52 :3, flip]
77,76	$(x \cdot (y \cdot x))/x = x \cdot y$	[52 → 12]
84	$R(x) \cdot x = 1$	[68 → 8 :32, flip]
93,92	$R(R(x)) = x$	[84 → 8 :30]
96	$x \cdot (R(x) \cdot y) = y$	[10 → 49 :11]

98	$R(x) \cdot (x \cdot y) = y$	[92 → 96]
102	$x \cdot (y \cdot ((R(x \cdot y) \cdot z) \cdot y)) = z \cdot y$	[96 → 18, flip]
109,108	$x \backslash y = R(x) \cdot y$	[96 → 8]
114	$R(x/y) \cdot x = y$	[37 :109]
118	$x/(y \cdot x) = R(y)$	[98 → 12]
136	$(x \cdot y) \cdot z = R(z/x) \cdot (z \cdot (y \cdot z))$	[114 → 18]
138	$R(x/y) \cdot (x \cdot (z \cdot x)) = (y \cdot z) \cdot x$	[flip 136]
154	$x \cdot R(y \cdot x) = R(y)$	[54 → 118 :77]
165,164	$x/y = x \cdot R(y)$	[114 → 154 :93, flip]
172,171	$R(x \cdot R(y)) = y \cdot R(x)$	[10 → 154 :165, flip]
179	$(x \cdot R(y)) \cdot (y \cdot (z \cdot y)) = (x \cdot z) \cdot y$	[138 :165,172]
203,202	$R(x \cdot y) = R(y) \cdot R(x)$	[154 → 98, flip]
204	$x \cdot (y \cdot (((R(y) \cdot R(x)) \cdot z) \cdot y)) = z \cdot y$	[102 :203]
236	$(x \cdot y) \cdot ((R(y) \cdot R(x)) \cdot z) = z$	[202 → 96]
374	$(x \cdot y) \cdot ((R(y) \cdot z) \cdot x) = x \cdot (z \cdot x)$	[179 → 236]
463,462	$x \cdot (((R(x) \cdot y) \cdot z) \cdot x) = y \cdot (z \cdot x)$	[204 → 96 :93, flip]
506	$(x \cdot (y \cdot x)) \cdot z = x \cdot (y \cdot (x \cdot z))$	[374 → 18 :463]
508	□	[506,61]

Theorem #MFL-3.

$$\{\text{loop}, \text{Moufang-3}\} \Rightarrow \{\text{Moufang-1}\}$$

Proof (found by Otter 3.0.3l on gyro at 14.26 seconds).

3,2	$1 \cdot x = x$	
5,4	$x \cdot 1 = x$	
7,6	$x \cdot (x \backslash y) = y$	
12	$(x \cdot y)/y = x$	
14	$x \cdot R(x) = 1$	
16	$L(x) \cdot x = 1$	
18	$((x \cdot y) \cdot x) \cdot z = x \cdot (y \cdot (x \cdot z))$	
20	$(A \cdot (B \cdot C)) \cdot A \neq (A \cdot B) \cdot (C \cdot A)$	
40,39	$1/x = L(x)$	[16 → 12]
41	$L(R(x)) = x$	[14 → 12 :40]
47	$L(x) \cdot (x \cdot (L(x) \cdot y)) = L(x) \cdot y$	[16 → 18 :3, flip]
60,59	$(x \cdot y) \cdot x = x \cdot (y \cdot x)$	[4 → 18 :5]
65	$A \cdot ((B \cdot C) \cdot A) \neq (A \cdot B) \cdot (C \cdot A)$	[20 :60]
66	$(x \cdot (y \cdot x)) \cdot z = x \cdot (y \cdot (x \cdot z))$	[18 :60]
92	$L(x) \cdot (x \cdot y) = y$	[6 → 47 :7]
95,94	$x \cdot (R(x) \cdot y) = y$	[41 → 92]
102	$L(L(x)) = x$	[16 → 92 :5]
105,104	$L(x) = R(x)$	[14 → 92 :5]
111,110	$R(x) \cdot x = 1$	[4 → 92 :105]
115,114	$R(R(x)) = x$	[102 :105,105]

120	$R(x) \cdot (x \cdot y) = y$	[92 :105]
136	$x \cdot ((R(x) \cdot y) \cdot x) = y \cdot x$	[94 → 59, flip]
156	$x/(y \cdot x) = R(y)$	[120 → 12]
190	$(x \cdot (y \cdot (x \cdot z)))/z = x \cdot (y \cdot x)$	[66 → 12]
204	$(x \cdot R(y)) \cdot y = x$	[66 → 136 :111,5,95, flip]
222	$(x \cdot y) \cdot R(y) = x$	[114 → 204]
233,232	$x/y = R(y \cdot R(x))$	[204 → 156]
238,237	$R(x \cdot R(y)) = y \cdot R(x)$	[204 → 12 :233]
243	$(x \cdot (y \cdot (x \cdot z))) \cdot R(z) = x \cdot (y \cdot x)$	[190 :233,238]
256	$x \cdot R(y \cdot x) = R(y)$	[120 → 222]
267,266	$R(x \cdot y) = R(y) \cdot R(x)$	[222 → 256, flip]
440	$(x \cdot (y \cdot z)) \cdot (R(z) \cdot x) = x \cdot (y \cdot x)$	[94 → 243 :267,115]
552	$(x \cdot y) \cdot (z \cdot x) = x \cdot ((y \cdot z) \cdot x)$	[222 → 440 :115]
559	$x \cdot ((y \cdot z) \cdot x) = (x \cdot y) \cdot (z \cdot x)$	[flip 552]
560	$\Box$	[559,65]

In the preceding proof we see that Moufang loops are in fact inverse loops (i.e., $L(x) = R(x)$), and we henceforth write the inverse of x as x'.

It turns out that we can simplify our equational basis for Moufang loops, but Moufang-1, Moufang-2, and Moufang-3 are no longer "equivalent" in the simplified basis. In particular, the set

$$\begin{aligned} &1 \cdot x = x, \\ &x' \cdot x = 1, \\ &((x \cdot y) \cdot z) \cdot y = x \cdot (y \cdot (z \cdot y)), \end{aligned} \qquad \text{(Moufang-2)}$$

is a basis for Moufang loops, and and we can replace Moufang-2 with Moufang-3, but we cannot replace Moufang-2 with Moufang-1.

To prove that the preceding set is a basis, we show that '1' is also a right identity, that '$'$' is also a right inverse, and that '$\cdot$' is a quasigroup (by showing that left and right solutions exist and that the left and right cancellation laws hold). The following three theorems accomplish this.

Theorem #MFL-4.

$$\left\{ \begin{array}{l} 1 \cdot x = x \\ x' \cdot x = 1 \\ \text{Moufang-2} \end{array} \right\} \Rightarrow \left\{ \begin{array}{l} x \cdot 1 = x \\ x \cdot x' = 1 \\ \forall x \forall y \exists z \ (x \cdot z = y) \\ \forall x \forall y \exists z \ (z \cdot x = y) \end{array} \right\}$$

Proof (found by Otter 3.0.3l on gyro at 7.03 seconds).

1	$x = x$
3,2	$1 \cdot x = x$
5,4	$x' \cdot x = 1$

7,6	$((x \cdot y) \cdot z) \cdot y = x \cdot (y \cdot (z \cdot y))$	
8	$A \cdot 1 = A,\ B \cdot B' = 1,\ C \cdot x = D,\ y \cdot E = F\ \rightarrow\ \square$	
9	$x' \cdot (x \cdot (y \cdot x)) = y \cdot x$	[4 → 6 :3, flip]
12,11	$(x \cdot y) \cdot x = x \cdot (y \cdot x)$	[2 → 6 :3]
13	$(x \cdot (y \cdot (z \cdot y))) \cdot z = (x \cdot y) \cdot (z \cdot (y \cdot z))$	[6 → 6]
17	$x' \cdot (x \cdot x') = x'$	[4 → 11 :3, flip]
19	$(x \cdot (y \cdot x)) \cdot y = x \cdot (y \cdot (x \cdot y))$	[11 → 6]
33	$x' \cdot (x \cdot (x \cdot (y \cdot x))) = x \cdot (y \cdot x)$	[11 → 9 :12]
37	$x' \cdot (x \cdot (y \cdot (x \cdot (z \cdot x)))) = y \cdot (x \cdot (z \cdot x))$	[6 → 9 :7]
42,41	$x' \cdot (x \cdot x) = x$	[2 → 9 :3]
44,43	$x \cdot x' = 1$	[17 → 9 :5, flip]
47	$A \cdot 1 = A,\ C \cdot x = D,\ y \cdot E = F\ \rightarrow\ \square$	[8 :44 :1]
50	$x \cdot (y \cdot ((x \cdot y)' \cdot y)) = y$	[43 → 6 :3, flip]
53,52	$x \cdot 1 = x$	[43 → 11 :3,5, flip]
54	$x \cdot (x' \cdot (y \cdot x')) = y \cdot x'$	[43 → 6 :3, flip]
56	$C \cdot x = D,\ y \cdot E = F\ \rightarrow\ \square$	[47 :53 :1]
58,57	$(x \cdot y) \cdot y = x \cdot (y \cdot y)$	[2 → 13 :53,53,3, flip]
68,67	$x' \cdot ((x \cdot x) \cdot x') = 1$	[41 → 11 :44, flip]
73	$x \cdot (x' \cdot x') = x'$	[43 → 57 :3, flip]
95	$x \cdot ((x' \cdot x') \cdot x) = 1$	[73 → 11 :5, flip]
98,97	$x'' = (x \cdot x) \cdot x'$	[67 → 9 :53]
99	$(x \cdot y') \cdot (y \cdot (y \cdot y)) = x \cdot (y \cdot y)$	[67 → 13 :53,42,12, flip]
112,111	$(x \cdot x) \cdot (x' \cdot x') = 1$	[97 → 4 :58]
113	$(x' \cdot x') \cdot x = x'$	[95 → 9 :53, flip]
149	$x \cdot ((y \cdot ((x \cdot y)' \cdot y)) \cdot x) = y \cdot x$	[50 → 11, flip]
168,167	$(x \cdot x) \cdot x' = x$	[113 → 54 :98,68,53,98,98,7,58,112,53, flip]
176,175	$x'' = x$	[97 :168]
183	$x \cdot ((x \cdot x)' \cdot x) = 1$	[50 → 33 :5, flip]
192,191	$(x \cdot x)' \cdot x = x'$	[183 → 9 :53, flip]
206,205	$x' \cdot (x \cdot y) = y$	[191 → 37 :44,53,192,44,53]
208,207	$x \cdot (x' \cdot y) = y$	[167 → 37 :176,5,53,168,5,53]
220,219	$x \cdot ((y \cdot x)' \cdot x) = y' \cdot x$	[50 → 205, flip]
235	$x \cdot ((x' \cdot y) \cdot x) = y \cdot x$	[149 :220]
316,315	$(x \cdot y) \cdot x' = x \cdot (y \cdot x')$	[235 → 207 :176, flip]
317	$(x \cdot y) \cdot (y' \cdot x) = x \cdot x$	[235 → 19 :208,58,208]
321,320	$(x' \cdot y) \cdot x = x' \cdot (y \cdot x)$	[235 → 205, flip]
354,353	$(x \cdot x) \cdot y = x \cdot (x \cdot y)$	[317 → 6 :321,208]
887	$(x \cdot (y \cdot y)) \cdot y' = x \cdot y$	[99 → 6 :316,354,44,53,206]
909	$(x \cdot y') \cdot y = x$	[6 → 887 :354,44,53,5,53, flip]
995	$\square$	[56,207,909]

Theorem #MFL-5.

$$\left\{ \begin{array}{l} 1 \cdot x = x \\ x' \cdot x = 1 \\ \text{Moufang-2} \end{array} \right\} \Rightarrow \{\text{left cancellation}\}$$

Proof (found by Otter 3.0.3l on gyro at 1.48 seconds).

3,2	$1 \cdot x = x$	
5,4	$x' \cdot x = 1$	
7,6	$((x \cdot y) \cdot z) \cdot y = x \cdot (y \cdot (z \cdot y))$	
8	$A \cdot C = A \cdot B$	
10	$C \neq B$	
13	$x' \cdot (x \cdot (y \cdot x)) = y \cdot x$	[4 → 6 :3, flip]
16,15	$(x \cdot y) \cdot x = x \cdot (y \cdot x)$	[2 → 6 :3]
23	$x' \cdot (x \cdot x') = x'$	[4 → 15 :3, flip]
45	$x' \cdot (x \cdot (x \cdot (y \cdot x))) = x \cdot (y \cdot x)$	[15 → 13 :16]
53	$x' \cdot (x \cdot (y \cdot (x \cdot (z \cdot x)))) = y \cdot (x \cdot (z \cdot x))$	[6 → 13 :7]
60,59	$x \cdot x' = 1$	[23 → 13 :5, flip]
69	$x \cdot (y \cdot ((x \cdot y)' \cdot y)) = y$	[59 → 6 :3, flip]
72,71	$x \cdot 1 = x$	[59 → 15 :3,5, flip]
267	$x \cdot ((x \cdot x)' \cdot x) = 1$	[69 → 45 :5, flip]
276,275	$(x \cdot x)' \cdot x = x'$	[267 → 13 :72, flip]
294,293	$x' \cdot (x \cdot y) = y$	[275 → 53 :60,72,276,60,72]
333	$C = B$	[8 → 293 :294, flip]
335	$\Box$	[333,10]

Theorem #MFL-6.

$$\left\{ \begin{array}{l} 1 \cdot x = x \\ x' \cdot x = 1 \\ \text{Moufang-2} \end{array} \right\} \Rightarrow \{\text{right cancellation}\}$$

Proof (found by Otter 3.0.3l on gyro at 0.48 seconds).

3,2	$1 \cdot x = x$	
5,4	$x' \cdot x = 1$	
7,6	$((x \cdot y) \cdot z) \cdot y = x \cdot (y \cdot (z \cdot y))$	
8	$C \cdot A = B \cdot A$	
10	$C \neq B$	
11	$C \cdot (A \cdot (x \cdot A)) = B \cdot (A \cdot (x \cdot A))$	[8 → 6 :7, flip]
13	$x' \cdot (x \cdot (y \cdot x)) = y \cdot x$	[4 → 6 :3, flip]
15	$(x \cdot y) \cdot x = x \cdot (y \cdot x)$	[2 → 6 :3]
29	$x' \cdot (x \cdot x') = x'$	[4 → 15 :3, flip]
60,59	$x \cdot x' = 1$	[29 → 13 :5, flip]
68,67	$x \cdot 1 = x$	[59 → 15 :3,5, flip]

71	$(x \cdot y) \cdot y = x \cdot (y \cdot y)$	[67 → 6 :3]
95	$x \cdot (x' \cdot x') = x'$	[59 → 71 :3, flip]
121	$x \cdot ((x' \cdot x') \cdot x) = 1$	[95 → 15 :5, flip]
142,141	$(x' \cdot x') \cdot x = x'$	[121 → 13 :68, flip]
143	$C = B$	[121 → 11 :68,142,60,68]
145	$\Box$	[143,10]

That completes the proof that the simplified set is a basis for Moufang loops. The following problem shows that we can obtain an alternate basis by replacing Moufang-2 with Moufang-3.

Theorem #MFL-7.

$$\left\{ \begin{array}{l} 1 \cdot x = x \\ x' \cdot x = 1 \\ \text{Moufang-3} \end{array} \right\} \Rightarrow \{\text{Moufang-2}\}$$

Proof (found by Otter 3.0.3l on gyro at 33.90 seconds).

1	$x = x$	
3,2	$1 \cdot x = x$	
5,4	$x' \cdot x = 1$	
7,6	$((x \cdot y) \cdot x) \cdot z = x \cdot (y \cdot (x \cdot z))$	
8	$((A \cdot B) \cdot C) \cdot B \neq A \cdot (B \cdot (C \cdot B))$	
9	$x' \cdot (x \cdot (x' \cdot y)) = x' \cdot y$	[4 → 6 :3, flip]
12,11	$(x \cdot 1) \cdot y = x \cdot y$	[2 → 6 :3,3]
13	$(x \cdot (y \cdot (x \cdot 1))) \cdot z = x \cdot (y \cdot (x \cdot z))$	[6 → 11 :7]
17	$(x \cdot x) \cdot y = x \cdot (x \cdot y)$	[11 → 6 :3]
19	$((x \cdot y) \cdot (x \cdot 1)) \cdot z = x \cdot (y \cdot (x \cdot z))$	[11 → 6 :12,12]
34,33	$(x \cdot (x \cdot 1)) \cdot y = x \cdot (x \cdot y)$	[11 → 17 :12,12]
38,37	$x' \cdot (x \cdot 1) = 1$	[4 → 9 :5]
43	$((x \cdot y) \cdot x)' \cdot (x \cdot (y \cdot (x \cdot 1))) = 1$	[6 → 37]
51	$x \cdot (x' \cdot (x \cdot y)) = x \cdot y$	[37 → 13 :12, flip]
53	$(x \cdot (y \cdot (y \cdot (x \cdot 1)))) \cdot z = x \cdot (y \cdot (y \cdot (x \cdot z)))$	[33 → 13 :34]
61	$x' \cdot (x'' \cdot 1) = 1$	[37 → 51 :38]
128,127	$x'' \cdot (x' \cdot (x' \cdot (x'' \cdot y))) = y$	[61 → 53 :38,3, flip]
144,143	$x'' \cdot (x' \cdot (x' \cdot 1)) = x' \cdot 1$	[37 → 127]
146,145	$x' \cdot (x'' \cdot y) = y$	[9 → 127 :128, flip]
148,147	$x' \cdot 1 = x'$	[4 → 127 :144]
182,181	$x' \cdot (x \cdot y) = y$	[145 → 9 :146]
185	$(x \cdot y') \cdot z = y' \cdot ((y'' \cdot x) \cdot (y' \cdot z))$	[145 → 19 :148]
188	$x' \cdot ((x'' \cdot y) \cdot (x' \cdot z)) = (y \cdot x') \cdot z$	[flip 185]
205	$((x \cdot y) \cdot x)'' = x \cdot (y \cdot (x \cdot 1))$	[43 → 181 :148]
224,223	$x'' = x$	[4 → 181 :148]
225	$x' \cdot ((x \cdot y) \cdot (x' \cdot z)) = (y \cdot x') \cdot z$	[188 :224]
237	$(x \cdot y) \cdot x = x \cdot (y \cdot (x \cdot 1))$	[205 :224]

245	$x \cdot (x' \cdot y) = y$	[223 → 181]
248,247	$x \cdot 1 = x$	[223 → 147 :224]
249	$x \cdot x' = 1$	[223 → 4]
252,251	$(x \cdot y) \cdot x = x \cdot (y \cdot x)$	[237 :248]
261	$(x \cdot (y \cdot x)) \cdot z = x \cdot (y \cdot (x \cdot z))$	[13 :248]
285	$x \cdot ((x' \cdot y) \cdot (x \cdot z)) = (y \cdot x) \cdot z$	[223 → 225 :224,224]
286	$(x \cdot y') \cdot y = x$	[249 → 225 :248,182,224, flip]
291	$(x \cdot y) \cdot z = y \cdot ((y' \cdot x) \cdot (y \cdot z))$	[flip 285]
295	$(x \cdot y) \cdot y' = x$	[223 → 286]
307	$x \cdot (y \cdot x)' = y'$	[181 → 295]
314,313	$(x \cdot y)' = y' \cdot x'$	[295 → 307, flip]
562	$(x \cdot (y \cdot (x \cdot z))) \cdot z' = x \cdot (y \cdot x)$	[261 → 295]
843	$B \cdot (((B' \cdot A) \cdot (B \cdot C)) \cdot B) \neq A \cdot (B \cdot (C \cdot B))$	[291 → 8 :252]
1465	$(x \cdot (y \cdot z)) \cdot (z' \cdot x) = x \cdot (y \cdot x)$	[245 → 562 :314,224]
1791	$(x \cdot y) \cdot (z \cdot x) = x \cdot ((y \cdot z) \cdot x)$	[295 → 1465 :224]
1824,1823	$x \cdot (((x' \cdot y) \cdot z) \cdot x) = y \cdot (z \cdot x)$	[245 → 1791, flip]
1837	$A \cdot (B \cdot (C \cdot B)) \neq A \cdot (B \cdot (C \cdot B))$	[843 :1824,252]
1838	$\Box$	[1837,1]

To show that one does *not* obtain a basis for Moufang loops by replacing Moufang-2 with Moufang-1, we use MACE to find a counterexample.

Example #MFL-8.

$$\left\{ \begin{array}{l} 1 \cdot x = x \\ x' \cdot x = 1 \\ \text{Moufang-1} \end{array} \right\} \not\Rightarrow \{\text{Moufang-2}\}$$

The clauses

$1 \cdot x = x$
$x' \cdot x = 1$
$(x \cdot (y \cdot z)) \cdot x = (x \cdot y) \cdot (z \cdot x)$ % Moufang 1
$((A \cdot B) \cdot C) \cdot B \neq A \cdot (B \cdot (C \cdot B))$ % Moufang 2

have the following model (found by MACE 1.1.0 on gyro at 0.76 seconds).

```
* :
      | 0 1 2
   --+------
   0  | 1 0 1
   1  | 0 1 2
   2  | 1 2 1
@ :
      0 1 2
   ---------
```

```
        0 1 0
  A: 0
  B: 2
  C: 1
end_of_model
```

8.1.2 Single Axioms for Inverse Loops and Moufang Loops

In [25], Padmanabhan presents the single axiom, in terms of divsion ($x/y = x \cdot y'$), for inverse loops,

$$(u/u)/((x/y)/(z/(y/x))) = z,$$

and he derives from that the single axiom schema for subvarieties of inverse loops:

$$((u/u)/\mathcal{W})/((x/y)/(z/(y/x))) = z.$$

The term $\mathcal{W}$, containing fresh variables, comes from the equation $\mathcal{W} = 1$, which specifies the properties of the subvariety. For example, a single axiom for Moufang loops (in terms of division) can be easily built with Padmanabhan's schema.

Padmanabhan's results are a generalization of the important work of Higman and Neumann [9] for groups and subvarieties in terms of division. Neumann much later obtained similar results for groups in terms of product and inverse [24], but the schema is more complicated, with two meta-terms, because there is no single axiom for groups in terms of product, inverse, and identity.

Here, in a generalization of Neumann's results, we solve the problem of finding a single axiom and a schema for inverse loops in terms of product and inverse. To find the axioms, we used OTTER with methods similar to those presented in [16].

Theorem #IL-1. A single axiom for inverse loops.

$$\{x \cdot ((((x \cdot y') \cdot y)' \cdot z) \cdot (u' \cdot u)) = z\} \Leftrightarrow \left\{ \begin{array}{l} x' \cdot x = y' \cdot y \\ x' \cdot (x \cdot y) = y \\ (x \cdot y) \cdot y' = x \end{array} \right\}.$$

We prove ($\Rightarrow$) in two steps, first showing that $x' \cdot x$ is a constant, then including $x' \cdot x = 1$ to derive the right-hand side. The third OTTER proof is ($\Leftarrow$).

Proof (found by Otter 3.0.3l on gyro at 0.46 seconds).

1	$A' \cdot A = B' \cdot B \rightarrow \square$	
4,3	$x \cdot ((((x \cdot y') \cdot y)' \cdot z) \cdot (u' \cdot u)) = z$	
5	$x \cdot (y \cdot (z' \cdot z)) = (((((x \cdot u') \cdot u)' \cdot v') \cdot v)' \cdot y) \cdot (w' \cdot w)$	[3 → 3]
6	$(((((x \cdot y') \cdot y)' \cdot z') \cdot z)' \cdot u) \cdot (v' \cdot v) = x \cdot (u \cdot (w' \cdot w))$	[flip 5]
28	$x \cdot (y \cdot (z' \cdot z)) = x \cdot (y \cdot (u' \cdot u))$	[6 → 6]
64	$x \cdot (y' \cdot y) = x \cdot (z' \cdot z)$	[28 → 3 :4]
84	$x' \cdot x = y' \cdot y$	[64 → 3 :4]

85 $\square$ [84,1]

Proof ($\Rightarrow$) found by Otter 3.0.3l on gyro at 0.69 seconds.

1	$x = x$	
2	$B' \cdot B = A' \cdot A,\ A' \cdot (A \cdot B) = B,\ (A \cdot B) \cdot B' = A \ \rightarrow\ \square$	
3	$x \cdot ((((x \cdot y') \cdot y)' \cdot z) \cdot (u' \cdot u)) = z$	
6,5	$x' \cdot x = 1$	
7	$x \cdot ((((x \cdot y') \cdot y)' \cdot z) \cdot 1) = z$	[3 :6]
9	$A' \cdot (A \cdot B) = B,\ (A \cdot B) \cdot B' = A \ \rightarrow\ \square$	[2 :6,6 :1]
10	$x'' \cdot (((1 \cdot x)' \cdot y) \cdot 1) = y$	[5 $\rightarrow$ 7]
12	$(((((x \cdot y') \cdot y)' \cdot z') \cdot z)' \cdot u) \cdot 1 = x \cdot (u \cdot 1)$	[7 $\rightarrow$ 7, flip]
15,14	$(x \cdot y') \cdot y = x \cdot (1 \cdot 1)$	[5 $\rightarrow$ 7, flip]
17,16	$(((x \cdot (1 \cdot 1))' \cdot (1 \cdot 1))' \cdot y) \cdot 1 = x \cdot (y \cdot 1)$	[12 :15,15]
18	$x \cdot (((x \cdot (1 \cdot 1))' \cdot y) \cdot 1) = y$	[7 :15]
23,22	$x'' \cdot (1 \cdot 1) = 1 \cdot x$	[5 $\rightarrow$ 14, flip]
24	$x'' \cdot ((1 \cdot x)' \cdot (1 \cdot 1)) = 1'$	[14 $\rightarrow$ 10]
28	$(1 \cdot 1)' \cdot ((1' \cdot x) \cdot 1) = x$	[5 $\rightarrow$ 18]
36	$((1' \cdot (1 \cdot 1))' \cdot x) \cdot 1 = (1 \cdot 1)' \cdot (x \cdot 1)$	[18 $\rightarrow$ 28, flip]
39,38	$(1 \cdot 1)' \cdot (1' \cdot (1 \cdot 1)) = 1'$	[14 $\rightarrow$ 28]
40	$1'' \cdot (x \cdot 1) = (1' \cdot x) \cdot 1$	[28 $\rightarrow$ 10]
42	$1'' \cdot 1 = 1' \cdot (1 \cdot 1)$	[38 $\rightarrow$ 10 :6]
44	$(x \cdot (1 \cdot 1)') \cdot (y \cdot 1) = x \cdot (y \cdot 1)$	[14 $\rightarrow$ 16 :17, flip]
48	$(x \cdot (1 \cdot 1))' \cdot (x \cdot (y \cdot 1)) = y$	[16 $\rightarrow$ 18]
55	$(1' \cdot ((1 \cdot 1)' \cdot x)) \cdot 1 = x$	[18 $\rightarrow$ 40 :23, flip]
66	$1' \cdot ((1 \cdot 1)' \cdot (x \cdot 1)) = x$	[5 $\rightarrow$ 48]
69,68	$(x \cdot (1 \cdot 1))' \cdot (x \cdot y) = 1' \cdot ((1 \cdot 1)' \cdot y)$	[55 $\rightarrow$ 48]
71,70	$1'' = 1' \cdot 1'$	[42 $\rightarrow$ 48 :69,39, flip]
75	$1' \cdot ((1 \cdot 1)' \cdot (x \cdot (1 \cdot 1))) = x \cdot 1'$	[14 $\rightarrow$ 48 :69]
82	$((x \cdot 1)' \cdot (1 \cdot 1))' \cdot 1 = x$	[5 $\rightarrow$ 48]
104	$(1' \cdot 1') \cdot (1 \cdot 1) = 1 \cdot 1$	[70 $\rightarrow$ 22]
110	$(1' \cdot 1')' \cdot (((1 \cdot 1')' \cdot x) \cdot 1) = x$	[70 $\rightarrow$ 10]
121,120	$1' \cdot (1 \cdot 1) = 1'$	[70 $\rightarrow$ 24 :6,15]
124	$(1 \cdot 1)' \cdot 1' = 1'$	[38 :121]
126	$((1' \cdot 1') \cdot x) \cdot 1 = (1 \cdot 1)' \cdot (x \cdot 1)$	[36 :121,71]
127	$(1 \cdot 1)' \cdot (x \cdot 1) = ((1' \cdot 1') \cdot x) \cdot 1$	[flip 126]
128	$(1 \cdot 1)' \cdot 1 = 1 \cdot 1$	[120 $\rightarrow$ 28 :6]
137,136	$(1 \cdot 1)' = 1$	[128 $\rightarrow$ 66 :6,6, flip]
142,141	$((1' \cdot 1') \cdot x) \cdot 1 = 1 \cdot (x \cdot 1)$	[127 :137, flip]
144,143	$1 \cdot 1' = 1'$	[124 :137]
149	$1' \cdot (1 \cdot (x \cdot (1 \cdot 1))) = x \cdot 1'$	[75 :137]
151	$(x \cdot (1 \cdot 1))' \cdot (x \cdot y) = 1' \cdot (1 \cdot y)$	[68 :137]
158,157	$(x \cdot 1) \cdot (y \cdot 1) = x \cdot (y \cdot 1)$	[44 :137]
162	$(1' \cdot 1')' \cdot (1 \cdot (x \cdot 1)) = x$	[110 :144,71,142]
173,172	$1' = 1 \cdot (1 \cdot 1)$	[136 $\rightarrow$ 22 :121]

177,176	$1 \cdot (1 \cdot 1) = 1$	[136 → 5]
187,186	$1 \cdot (1 \cdot (x \cdot 1)) = x$	[162 :173,177,173,177,137]
195,194	$1 \cdot 1 = 1$	[104 :173,177,173,177,158,177, flip]
202	$(x \cdot 1)' \cdot (x \cdot y) = 1 \cdot (1 \cdot y)$	[151 :195,173,195,195]
206,205	$x \cdot 1 = x$	[149 :173,195,195,195,187,173,195,195, flip]
226,225	$x'' = x$	[82 :206,206,206,206]
232,231	$1 \cdot x = x$	[22 :226,206,206, flip]
235	$(x \cdot y') \cdot y = x$	[14 :206,206]
238,237	$x' \cdot (x \cdot y) = y$	[202 :206,232,232]
239	$(A \cdot B) \cdot B' = A \ \rightarrow \ \square$	[9 :238 :1]
244	$(x \cdot y) \cdot y' = x$	[225 → 235]
246	$\square$	[244,239]

Proof ($\Leftarrow$) found by Otter 3.0.3l on gyro at 0.09 seconds.

1	$x = x$	
2	$A \cdot ((((A \cdot B') \cdot B)' \cdot C) \cdot (D' \cdot D)) = C \ \rightarrow \ \square$	
3	$x' \cdot x = y' \cdot y$	
4	$x' \cdot (x \cdot y) = y$	
6	$(x \cdot y) \cdot y' = x$	
8	$A \cdot ((((A \cdot B') \cdot B)' \cdot C) \cdot (x' \cdot x)) = C \ \rightarrow \ \square$	[3 → 2]
10,9	$x'' \cdot y = x \cdot y$	[4 → 4]
12,11	$x \cdot (y' \cdot y) = x$	[3 → 4 :10]
13	$A \cdot (((A \cdot B') \cdot B)' \cdot C) = C \ \rightarrow \ \square$	[8 :12]
24	$x'' = x$	[4 → 11, flip]
31,30	$(x \cdot y') \cdot y = x$	[24 → 6]
33,32	$x \cdot (x' \cdot y) = y$	[24 → 4]
35	$C = C \ \rightarrow \ \square$	[13 :31,33]
36	$\square$	[35,1]

Lemma #IL-2.

$$\{\beta = \alpha\} \Rightarrow \left(\{x \cdot ((((x \cdot y') \cdot y)' \cdot z) \cdot ((\alpha \cdot u)' \cdot (\beta \cdot u))) = z\} \Leftrightarrow \left\{ \begin{array}{l} x' \cdot x = y' \cdot y \\ x' \cdot (x \cdot y) = y \\ (x \cdot y) \cdot y' = x \end{array} \right\} \right).$$

Like Thm. #IL-1, we prove ($\Rightarrow$) in two steps, first showing that $x' \cdot x$ is a constant, then including $x' \cdot x = 1$ to derive the right-hand side. The third OTTER proof is ($\Leftarrow$).

Proof (found by Otter 3.0.3l on gyro at 1.23 seconds).

1	$A' \cdot A = B' \cdot B \ \rightarrow \ \square$	
4,3	$\beta = \alpha$	
5	$x \cdot ((((x \cdot y') \cdot y)' \cdot z) \cdot ((\alpha \cdot u)' \cdot (\beta \cdot u))) = z$	
7,6	$x \cdot ((((x \cdot y') \cdot y)' \cdot z) \cdot ((\alpha \cdot u)' \cdot (\alpha \cdot u))) = z$	[copy,5 :4]

10,9	$x \cdot ((((x \cdot y') \cdot y)' \cdot z) \cdot (u' \cdot u)) = z$	[6 → 6 :7]
12	$x \cdot (y \cdot (z' \cdot z)) = (((((x \cdot u') \cdot u)' \cdot v') \cdot v)' \cdot y) \cdot (w' \cdot w)$	[9 → 9]
13	$(((((x \cdot y') \cdot y)' \cdot z') \cdot z)' \cdot u) \cdot (v' \cdot v) = x \cdot (u \cdot (w' \cdot w))$	[flip 12]
35	$x \cdot (y \cdot (z' \cdot z)) = x \cdot (y \cdot (u' \cdot u))$	[13 → 13]
141	$x \cdot (y' \cdot y) = x \cdot (z' \cdot z)$	[35 → 9 :10]
174	$x' \cdot x = y' \cdot y$	[141 → 9 :10]
175	$\Box$	[174,1]

Proof ($\Rightarrow$) found by Otter 3.0.3l on gyro at 0.70 seconds.

1	$x = x$	
2	$B' \cdot B = A' \cdot A,\ A' \cdot (A \cdot B) = B,\ (A \cdot B) \cdot B' = A\ \rightarrow\ \Box$	
4,3	$\beta = \alpha$	
6,5	$x' \cdot x = 1$	
7	$x \cdot ((((x \cdot y') \cdot y)' \cdot z) \cdot ((\alpha \cdot u)' \cdot (\beta \cdot u))) = z$	
8	$x \cdot ((((x \cdot y') \cdot y)' \cdot z) \cdot 1) = z$	[copy,7 :4,6]
10	$A' \cdot (A \cdot B) = B,\ (A \cdot B) \cdot B' = A\ \rightarrow\ \Box$	[2 :6,6 :1]
11	$x'' \cdot (((1 \cdot x)' \cdot y) \cdot 1) = y$	[5 → 8]
13	$(((((x \cdot y') \cdot y)' \cdot z') \cdot z)' \cdot u) \cdot 1 = x \cdot (u \cdot 1)$	[8 → 8, flip]
16,15	$(x \cdot y') \cdot y = x \cdot (1 \cdot 1)$	[5 → 8, flip]
18,17	$(((x \cdot (1 \cdot 1))' \cdot (1 \cdot 1))' \cdot y) \cdot 1 = x \cdot (y \cdot 1)$	[13 :16,16]
19	$x \cdot (((x \cdot (1 \cdot 1))' \cdot y) \cdot 1) = y$	[8 :16]
24,23	$x'' \cdot (1 \cdot 1) = 1 \cdot x$	[5 → 15, flip]
25	$x'' \cdot ((1 \cdot x)' \cdot (1 \cdot 1)) = 1'$	[15 → 11]
29	$(1 \cdot 1)' \cdot ((1' \cdot x) \cdot 1) = x$	[5 → 19]
37	$((1' \cdot (1 \cdot 1))' \cdot x) \cdot 1 = (1 \cdot 1)' \cdot (x \cdot 1)$	[19 → 29, flip]
40,39	$(1 \cdot 1)' \cdot (1' \cdot (1 \cdot 1)) = 1'$	[15 → 29]
41	$1'' \cdot (x \cdot 1) = (1' \cdot x) \cdot 1$	[29 → 11]
43	$1'' \cdot 1 = 1' \cdot (1 \cdot 1)$	[39 → 11 :6]
45	$(x \cdot (1 \cdot 1)') \cdot (y \cdot 1) = x \cdot (y \cdot 1)$	[15 → 17 :18, flip]
49	$(x \cdot (1 \cdot 1))' \cdot (x \cdot (y \cdot 1)) = y$	[17 → 19]
56	$(1' \cdot ((1 \cdot 1)' \cdot x)) \cdot 1 = x$	[19 → 41 :24, flip]
73	$1' \cdot ((1 \cdot 1)' \cdot (x \cdot 1)) = x$	[5 → 49]
76,75	$(x \cdot (1 \cdot 1))' \cdot (x \cdot y) = 1' \cdot ((1 \cdot 1)' \cdot y)$	[56 → 49]
78,77	$1'' = 1' \cdot 1'$	[43 → 49 :76,40, flip]
82	$1' \cdot ((1 \cdot 1)' \cdot (x \cdot (1 \cdot 1))) = x \cdot 1'$	[15 → 49 :76]
89	$((x \cdot 1)' \cdot (1 \cdot 1))' \cdot 1 = x$	[5 → 49]
104	$x \cdot 1' = 1' \cdot ((1 \cdot 1)' \cdot (x \cdot (1 \cdot 1)))$	[flip 82]
107	$(1' \cdot 1') \cdot (1 \cdot 1) = 1 \cdot 1$	[77 → 23]
117	$(1' \cdot 1')' \cdot (((1 \cdot 1')' \cdot x) \cdot 1) = x$	[77 → 11]
124,123	$1' \cdot (1 \cdot 1) = 1'$	[77 → 25 :6,16]
127	$(1 \cdot 1)' \cdot 1' = 1'$	[39 :124]
129	$((1' \cdot 1') \cdot x) \cdot 1 = (1 \cdot 1)' \cdot (x \cdot 1)$	[37 :124,78]
130	$(1 \cdot 1)' \cdot (x \cdot 1) = ((1' \cdot 1') \cdot x) \cdot 1$	[flip 129]
131	$(1 \cdot 1)' \cdot 1 = 1 \cdot 1$	[123 → 29 :6]

142,141	$(1 \cdot 1)' = 1$	[131 → 73 :6,6, flip]
149,148	$((1' \cdot 1') \cdot x) \cdot 1 = 1 \cdot (x \cdot 1)$	[130 :142, flip]
151,150	$1 \cdot 1' = 1'$	[127 :142]
152	$x \cdot 1' = 1' \cdot (1 \cdot (x \cdot (1 \cdot 1)))$	[104 :142]
156	$(x \cdot (1 \cdot 1))' \cdot (x \cdot y) = 1' \cdot (1 \cdot y)$	[75 :142]
163,162	$(x \cdot 1) \cdot (y \cdot 1) = x \cdot (y \cdot 1)$	[45 :142]
171	$(1' \cdot 1')' \cdot (1 \cdot (x \cdot 1)) = x$	[117 :151,78,149]
192,191	$1' = 1 \cdot (1 \cdot 1)$	[141 → 23 :124]
196,195	$1 \cdot (1 \cdot 1) = 1$	[141 → 5]
200,199	$1 \cdot 1 = 1$	[107 :192,196,192,196,163,196, flip]
204,203	$1 \cdot (1 \cdot (x \cdot 1)) = x$	[171 :192,200,200,192,200,200,200,192,200,200]
219	$(x \cdot 1)' \cdot (x \cdot y) = 1 \cdot (1 \cdot y)$	[156 :200,192,200,200]
223,222	$x \cdot 1 = x$	[152 :192,200,200,192,200,200,200,204]
237,236	$x'' = x$	[89 :223,223,223,223]
247,246	$1 \cdot x = x$	[23 :237,223,223, flip]
250	$(x \cdot y') \cdot y = x$	[15 :223,223]
253,252	$x' \cdot (x \cdot y) = y$	[219 :223,247,247]
254	$(A \cdot B) \cdot B' = A \ \rightarrow \ \square$	[10 :253 :1]
255	$(x \cdot y) \cdot y' = x$	[236 → 250]
257	$\square$	[255,254]

Proof ($\Leftarrow$) found by Otter 3.0.3l on gyro at 0.12 seconds.

2	$A \cdot ((((A \cdot B') \cdot B)' \cdot C) \cdot ((\alpha \cdot D)' \cdot (\beta \cdot D))) = C \ \rightarrow \ \square$	
4,3	$\beta = \alpha$	
5	$x' \cdot x = y' \cdot y$	
7,6	$x' \cdot (x \cdot y) = y$	
8	$(x \cdot y) \cdot y' = x$	
10	$A \cdot ((((A \cdot B') \cdot B)' \cdot C) \cdot ((\alpha \cdot D)' \cdot (\alpha \cdot D))) = C \ \rightarrow \ \square$	[2 :4]
12,11	$x'' \cdot y = x \cdot y$	[6 → 6]
15	$x \cdot (y \cdot x)' = y'$	[6 → 8]
22,21	$x \cdot (y' \cdot y) = x$	[5 → 6 :12]
23	$A \cdot (((A \cdot B') \cdot B)' \cdot C) = C \ \rightarrow \ \square$	[10 :22]
27,26	$x'' = x$	[6 → 21, flip]
31,30	$(x \cdot y)' = y' \cdot x'$	[8 → 15, flip]
32	$A \cdot (A' \cdot C) = C \ \rightarrow \ \square$	[23 :31,31,27,7]
41	$x \cdot (x' \cdot y) = y$	[26 → 6]
43	$\square$	[41,32]

Lemma #IL-3.

$$\left\{ \begin{array}{l} x \cdot ((((x \cdot y') \cdot y)' \cdot z) \cdot ((\alpha \cdot u)' \cdot (\beta \cdot u))) = z \\ x' \cdot x = y' \cdot y \\ x' \cdot (x \cdot y) = y \\ (x \cdot y) \cdot y' = x \end{array} \right\} \Rightarrow \{\beta = \alpha\}.$$

Proof (found by Otter 3.0.3k on gyro at 0.46 seconds).

1	$\beta = \alpha \ \rightarrow \ \Box$	
3	$x \cdot ((((x \cdot y') \cdot y)' \cdot z) \cdot ((\alpha \cdot u)' \cdot (\beta \cdot u))) = z$	
5	$x' \cdot x = y' \cdot y$	
6	$x' \cdot (x \cdot y) = y$	
8	$(x \cdot y) \cdot y' = x$	
11	$x \cdot ((((x \cdot y') \cdot y)' \cdot z) \cdot (u' \cdot (\beta \cdot ((((\alpha \cdot v') \cdot v)' \cdot u) \cdot ((\alpha \cdot w)' \cdot (\beta \cdot w)))))) = z$	[3 → 3]
19,18	$(((x \cdot y') \cdot y)' \cdot z) \cdot ((\alpha \cdot u)' \cdot (\beta \cdot u)) = x' \cdot z$	[3 → 6, flip]
23	$x \cdot ((((x \cdot y') \cdot y)' \cdot z) \cdot (u' \cdot (\beta \cdot (\alpha' \cdot u)))) = z$	[11 :19]
26	$x \cdot (x' \cdot y) = y$	[3 :19]
31,30	$x \cdot (y \cdot x)' = y'$	[6 → 8]
35,34	$x'' = x$	[26 → 8 :31]
37,36	$(x \cdot y') \cdot y = x$	[34 → 8]
40	$x \cdot ((x' \cdot y) \cdot (z' \cdot (\beta \cdot (\alpha' \cdot z)))) = y$	[23 :37]
48	$x \cdot (y' \cdot y) = x$	[5 → 26]
52	$(x' \cdot x) \cdot y = y$	[5 → 36 :35]
55,54	$x \cdot (y \cdot y') = x$	[34 → 48]
61,60	$(x \cdot x') \cdot y = y$	[34 → 52]
70	$x \cdot x' = y \cdot y'$	[54 → 26]
84	$x \cdot (y' \cdot (\beta \cdot (\alpha' \cdot y))) = x$	[70 → 40 :61,35]
126	$x \cdot (\alpha' \cdot \beta) = x$	[70 → 84 :35,55]
143	$\beta = \alpha$	[26 → 126]
145	$\Box$	[143,1]

Theorem #IL-4. The axiom schema

$$x \cdot ((((x \cdot y') \cdot y)' \cdot z) \cdot ((\alpha \cdot u)' \cdot (\beta \cdot u))) = z$$

can be used to construct a single axiom for any finitely defined equational subvariety of inverse loops.

Proof. First, the equations Σ that specify the subvariety can be bundled together into an equavalent (modulo inverse loops) single equation $\delta = \gamma$; see one of [9, 25, 24] for the method. Second, $\delta = \gamma$ is transformed to the equivalent (modulo inverse loops) formula $\delta_1 \gamma_1' = \delta_2 \gamma_2'$, in which the two sides share no variables and are unifiable; call this equation $\alpha = \beta$. Third, plug α and β into the axiom. The terms α and β are unifiable without affecting the rest of the axiom, so by Lemma #IL-2, we can derive a basis for inverse loops. Given the basis for inverse loops, by Lemma #IL-3, we can derive $\alpha = \beta$, so we have the theory of the subvariety and nothing more.

Corollary #MFL-9. The axiom schema of Thm. #IL-4 gives us a single axiom for the variety of Moufang loops, which is the subvariety of inverse loops satisfying one of the Moufang identities, for example, Moufang-3:

$$((x \cdot y) \cdot x) \cdot z = x \cdot (y \cdot (x \cdot z)).$$

We can transform Moufang-3, call it $\delta = \gamma$, into the appropriate form for the schema by writing it as $\delta_1\gamma_1' = \delta_2\gamma_2'$, in which the two sides of the equation have disjoint sets of variables. When we plug these terms into the schema, we get

$$x\cdot((((x\cdot y')\cdot y)'\cdot z)\cdot((((((x_1\cdot y_1)\cdot x_1)\cdot z_1)\cdot(x_1\cdot(y_1\cdot(x_1\cdot z_1)))')\cdot u)'\cdot(((((x_2\cdot y_2)\cdot x_2)\cdot z_2)\cdot(x_2\cdot(y_2\cdot(x_2\cdot z_2)))')\cdot u)))$$

which is a single identity, in terms of product and inverse, for the variety of Moufang loops.

8.2 Quasigroups

[[Note to RP: Mention Ross Hillard's result here??]]

Theorem #QGT-3.

$$\{x(y(yx)) = yx, \text{quasigroup}\} \Rightarrow \{x(xy) = yx\}.$$

This was known to be true.

Proof (found by Otter 3.0.3l on gyro at 0.51 seconds).

4	$x\backslash(x \cdot y) = y$	
7,6	$(x/y) \cdot y = x$	
8	$(x \cdot y)/y = x$	
10	$x \cdot (y \cdot (y \cdot x)) = y \cdot x$	
12	$A \cdot (A \cdot B) \neq B \cdot A$	
13	$B \cdot A \neq A \cdot (A \cdot B)$	[flip 12]
14	$(x/y)\backslash x = y$	[6 → 4]
21,20	$x \cdot ((y/x) \cdot y) = y$	[6 → 10 :7]
33,32	$((x/y) \cdot x) \cdot (y \cdot x) = x$	[20 → 10 :21]
34	$x/((x/y) \cdot x) = y$	[20 → 8]
37,36	$x\backslash y = (y/x) \cdot y$	[20 → 4]
38	$(x/(x/y)) \cdot x = y$	[14 :37]
49,48	$x/(y \cdot x) = (x/y) \cdot x$	[34 → 34]
54	$x/y = y/(y/x)$	[38 → 8]
55	$x/(x/y) = y/x$	[flip 54]
68	$(x \cdot y)/x = (y/x) \cdot y$	[8 → 55 :49]
74	$(x/y) \cdot (y/x) = y$	[55 → 6]
80	$((x/y) \cdot x) \cdot y = y \cdot x$	[8 → 74 :49]
132	$x \cdot y = y \cdot (y \cdot x)$	[68 → 80 :33]
133	$\Box$	[132,13]

Theorem #STN-6.

$$\{((xx)y)(z(xy)) = z\} \Leftrightarrow \left\{ \begin{array}{l} xx = x \\ (xy)x = y \end{array} \right\}.$$

Status: True. First proved by Padmanabhan.

Proof ($\Rightarrow$) found by Otter 3.0.3l on gyro at 0.55 seconds.

1	$x = x$	
3,2	$((x \cdot x) \cdot y) \cdot (z \cdot (x \cdot y)) = z$	
4	$A \cdot A = A,\ (A \cdot B) \cdot A = B \ \rightarrow\ \square$	
9	$((x \cdot x) \cdot (y \cdot z)) \cdot x = (y \cdot y) \cdot z$	[2 $\rightarrow$ 2]
15	$(x \cdot x) \cdot (y \cdot (y \cdot y)) = x \cdot (y \cdot y)$	[2 $\rightarrow$ 9, flip]
57,56	$(x \cdot (y \cdot y)) \cdot x = (y \cdot y) \cdot (y \cdot y)$	[15 $\rightarrow$ 9]
58	$((x \cdot x) \cdot (x \cdot x)) \cdot (y \cdot (x \cdot x)) = y \cdot y$	[15 $\rightarrow$ 2]
61	$x \cdot x = ((y \cdot y) \cdot (y \cdot y)) \cdot (x \cdot (y \cdot y))$	[flip 58]
119,118	$(x \cdot x) \cdot (x \cdot x) = (x \cdot x) \cdot x$	[56 $\rightarrow$ 9 :57]
138,137	$x \cdot x = x$	[61 :119,3]
142,141	$(x \cdot y) \cdot x = y$	[56 :138,138,138,138]
143	$\square$	[4 :138,142 :1,1]

Proof ($\Leftarrow$) found by Otter 3.0.3l on gyro at 0.06 seconds.

3,2	$x \cdot x = x$	
4	$(x \cdot y) \cdot x = y$	
6	$((A \cdot A) \cdot B) \cdot (C \cdot (A \cdot B)) \neq C$	
7	$(A \cdot B) \cdot (C \cdot (A \cdot B)) \neq C$	[copy,6 :3]
8	$x \cdot (y \cdot x) = y$	[4 $\rightarrow$ 4]
10	$\square$	[8,7]

Theorem #STN-7.

$$\{(((xx)y)x)(zy) = z\} \Leftrightarrow \left\{ \begin{array}{l} xx = x \\ (xy)x = y \end{array} \right\}.$$

Status: True. First proved by Barry Wolk.

Proof ($\Rightarrow$) found by Otter 3.0.3l on gyro at 0.38 seconds.

1	$x = x$	
3,2	$(((x \cdot x) \cdot y) \cdot x) \cdot (z \cdot y) = z$	
4	$A \cdot A = A,\ (A \cdot B) \cdot A = B \ \rightarrow\ \square$	
5	$((((x \cdot x) \cdot x) \cdot y) \cdot (((x \cdot x) \cdot x) \cdot x)) \cdot (z \cdot y) = z$	[2 $\rightarrow$ 2]
7	$(((x \cdot x) \cdot (y \cdot z)) \cdot x) \cdot y = ((u \cdot u) \cdot z) \cdot u$	[2 $\rightarrow$ 2]
11	$(((x \cdot x) \cdot y) \cdot x) \cdot (((z \cdot z) \cdot u) \cdot z) = ((v \cdot v) \cdot (y \cdot u)) \cdot v$	[2 $\rightarrow$ 7]
12	$((x \cdot x) \cdot y) \cdot x = ((z \cdot z) \cdot y) \cdot z$	[7 $\rightarrow$ 7]
15	$((x \cdot x) \cdot (y \cdot z)) \cdot x = (((u \cdot u) \cdot y) \cdot u) \cdot (((v \cdot v) \cdot z) \cdot v)$	[flip 11]
23,22	$(((x \cdot x) \cdot y) \cdot x) \cdot (((z \cdot z) \cdot u) \cdot z) = (y \cdot y) \cdot u$	[12 $\rightarrow$ 2]
28	$((x \cdot x) \cdot (y \cdot z)) \cdot x = (y \cdot y) \cdot z$	[15 :23]
36	$(((x \cdot y) \cdot (x \cdot y)) \cdot (x \cdot y)) \cdot ((x \cdot y) \cdot (x \cdot y)) = (x \cdot x) \cdot y$	[28 $\rightarrow$ 28]
44	$(((x \cdot x) \cdot ((y \cdot y) \cdot z)) \cdot x) \cdot ((u \cdot u) \cdot (y \cdot z)) = ((v \cdot v) \cdot u) \cdot v$	[28 $\rightarrow$ 7]

46,45	$(((x \cdot x) \cdot y) \cdot x) \cdot ((z \cdot z) \cdot u) = (y \cdot y) \cdot (z \cdot u)$	[28 → 2]
52	$(((x \cdot x) \cdot y) \cdot ((x \cdot x) \cdot y)) \cdot (z \cdot (x \cdot y)) = ((u \cdot u) \cdot z) \cdot u$	[44 :46]
62,61	$((x \cdot x) \cdot x) \cdot (y \cdot x) = y$	[12 → 5 :3]
79,78	$(x \cdot x) \cdot y = x \cdot y$	[36 :62, flip]
105,104	$x \cdot (y \cdot x) = y$	[61 :79,79]
107,106	$(x \cdot y) \cdot x = y$	[52 :79,79,79,105,79, flip]
112	$A \cdot A = A \ \rightarrow \ \square$	[4 :107 :1]
113	$x \cdot x = x$	[106 → 78, flip]
115	$\square$	[113,112]

Proof ($\Leftarrow$) found by Otter 3.0.3l on gyro at 0.05 seconds.

3,2	$x \cdot x = x$	
5,4	$(x \cdot y) \cdot x = y$	
6	$(((A \cdot A) \cdot B) \cdot A) \cdot (C \cdot B) \neq C$	
7	$B \cdot (C \cdot B) \neq C$	[copy,6 :3,5]
8	$x \cdot (y \cdot x) = y$	[4 → 4]
10	$\square$	[8,7]

Theorem #STN-8.

$$\{((xx)y)(z(yx)) = z\} \Leftrightarrow \left\{ \begin{array}{l} xy = yx \\ xx = x \\ (xy)x = y \end{array} \right\}.$$

Status: True.

Proof ($\Rightarrow$) found by Otter 3.0.3l on gyro at 0.27 seconds.

1	$x = x$	
2	$((x \cdot x) \cdot y) \cdot (z \cdot (y \cdot x)) = z$	
4	$B \cdot A = A \cdot B, \ A \cdot A = A, \ (A \cdot B) \cdot A = B \ \rightarrow \ \square$	
5	$x \cdot (y \cdot ((x \cdot ((z \cdot z) \cdot z)) \cdot (z \cdot z))) = y$	[2 → 2]
9	$(((x \cdot y) \cdot (x \cdot y)) \cdot z) \cdot z = (y \cdot y) \cdot x$	[2 → 2]
15	$x \cdot (x \cdot ((y \cdot y) \cdot y)) = (y \cdot y) \cdot y$	[2 → 5]
26,25	$(x \cdot x) \cdot (x \cdot x) = (x \cdot x) \cdot x$	[2 → 15]
29	$((((x \cdot x) \cdot x) \cdot ((x \cdot x) \cdot x)) \cdot y) \cdot ((x \cdot x) \cdot x) = y$	[15 → 2]
36,35	$((x \cdot x) \cdot x) \cdot ((x \cdot x) \cdot x) = ((x \cdot x) \cdot x) \cdot (x \cdot x)$	[25 → 25 :26,26]
37	$((((x \cdot x) \cdot x) \cdot (x \cdot x)) \cdot y) \cdot ((x \cdot x) \cdot x) = y$	[29 :36]
41	$x \cdot (x \cdot (((y \cdot y) \cdot y) \cdot (y \cdot y))) = ((y \cdot y) \cdot y) \cdot (y \cdot y)$	[25 → 15 :26]
46,45	$((x \cdot x) \cdot x) \cdot (x \cdot x) = x \cdot x$	[25 → 2 :36]
55	$x \cdot (x \cdot (y \cdot y)) = y \cdot y$	[41 :46,46]
58,57	$((x \cdot x) \cdot y) \cdot ((x \cdot x) \cdot x) = y$	[37 :46]
60,59	$x \cdot x = x$	[35 :58,46, flip]
62,61	$(x \cdot y) \cdot x = y$	[57 :60,60,60]
63	$x \cdot (x \cdot y) = y$	[55 :60,60]

75	$((x \cdot y) \cdot z) \cdot z = y \cdot x$	[9 :60,60]
79	$B \cdot A = A \cdot B \ \rightarrow \ \Box$	[4 :60,62 :1,1]
81,80	$(x \cdot y) \cdot y = x$	[61 → 63]
82	$x \cdot y = y \cdot x$	[75 :81]
83	$\Box$	[82,79]

Proof ($\Leftarrow$) found by Otter 3.0.3l on gyro at 0.06 seconds.

1	$x = x$	
3,2	$x \cdot x = x$	
4	$(x \cdot y) \cdot x = y$	
6	$x \cdot y = y \cdot x$	
7	$((A \cdot A) \cdot B) \cdot (C \cdot (B \cdot A)) \neq C$	
8	$(A \cdot B) \cdot (C \cdot (B \cdot A)) \neq C$	[copy,7 :3]
10,9	$x \cdot (y \cdot x) = y$	[4 → 4]
15	$C \neq C$	[6 → 8 :10]
16	$\Box$	[15,1]

Theorem #STN-9. Type (2,1) with one binary and one unary.

$$\{(g(x) \cdot y) \cdot (z \cdot (y \cdot x)) = z\} \Leftrightarrow \left\{ \begin{array}{l} x \cdot y = y \cdot x \\ g(x) = x \\ (x \cdot y) \cdot x = y \end{array} \right\}.$$

First proved by N.S. Mendelsohn, Padmanabhan, and Barry Wolk. This shows that the equational theory of any finitely based subvariety of Steiner quasigroups is one-based. The unary $g(x)$ packs all the remaining identities true in the subvariety in question. For example, if $g(x) = x \cdot x$, then we obtain Thm. #STN-8.

Proof ($\Rightarrow$) found by Otter 3.0.3l on gyro at 1.84 seconds.

1	$x = x$	
2	$(g(x) \cdot y) \cdot (z \cdot (y \cdot x)) = z$	
4	$B \cdot A = A \cdot B, \ g(A) = A, \ (A \cdot B) \cdot A = B \ \rightarrow \ \Box$	
5	$(g(x \cdot (y \cdot z)) \cdot (g(z) \cdot y)) \cdot (u \cdot x) = u$	[2 → 2]
8,7	$(g(x \cdot y) \cdot z) \cdot z = g(y) \cdot x$	[2 → 2]
10,9	$g(x) \cdot (g(y \cdot z) \cdot x) = g(y) \cdot g(z)$	[7 → 7 :8, flip]
13	$(g(x) \cdot y) \cdot (g(z) \cdot u) = g(u \cdot z) \cdot (y \cdot x)$	[7 → 2]
24	$(g(x) \cdot g(y \cdot z)) \cdot (g(y) \cdot g(z)) = g(x)$	[9 → 2]
59,58	$g(x \cdot y) \cdot x = g(y)$	[7 → 5]
69	$g(g(x)) \cdot g(y \cdot x) = g(y)$	[58 → 58]
77,76	$g(x \cdot (y \cdot z)) = g(x) \cdot (g(z) \cdot y)$	[2 → 58, flip]
121	$g(x) \cdot (y \cdot (z \cdot (z \cdot x))) = y$	[58 → 2]
131,130	$g(g(x \cdot y)) = g(g(x)) \cdot g(g(y))$	[58 → 69, flip]
148	$g(x) \cdot (g(x) \cdot g(y)) = g(g(y))$	[69 → 24]

155	$g(x) \cdot (y \cdot (g(x \cdot z) \cdot g(z))) = y$	[69 → 2]
174	$(g(x) \cdot y) \cdot y = (g(x) \cdot g(z)) \cdot g(z)$	[121 → 7 :77,59]
186	$(g(x) \cdot g(y)) \cdot g(y) = (g(x) \cdot z) \cdot z$	[flip 174]
197	$g(x) \cdot g(y) = g(y) \cdot x$	[148 → 7 :10]
233	$((g(g(x)) \cdot g(g(y))) \cdot (g(z) \cdot u)) \cdot (g(z) \cdot u) = g(g(y) \cdot x)$	[13 → 58 :77,131]
240	$g(g(x) \cdot y) = ((g(g(y)) \cdot g(g(x))) \cdot (g(z) \cdot u)) \cdot (g(z) \cdot u)$	[flip 233]
245,244	$g(x \cdot y) \cdot g(y) = g(x)$	[69 → 197, flip]
249	$g(x) \cdot (y \cdot g(x)) = y$	[155 :245]
276,275	$g(g(x) \cdot y) = g(x) \cdot g(y)$	[58 → 249, flip]
288	$((g(g(x)) \cdot g(g(y))) \cdot (g(z) \cdot u)) \cdot (g(z) \cdot u) = g(y) \cdot g(x)$	[240 :276, flip]
335,334	$g(g(x)) \cdot (y \cdot g(x)) = y$	[249 → 121]
340,339	$g(g(x)) \cdot g(g(y)) = g(x) \cdot g(y)$	[249 → 9 :59,131]
344,343	$g(x \cdot g(y)) = g(x) \cdot g(y)$	[249 → 58, flip]
346,345	$(g(x) \cdot g(y)) \cdot g(y) = g(x)$	[249 → 24 :344,335]
353,352	$g(x) \cdot (y \cdot x) = y$	[249 → 2 :344,346]
370	$((g(x) \cdot g(y)) \cdot (g(z) \cdot u)) \cdot (g(z) \cdot u) = g(y) \cdot g(x)$	[288 :340]
392	$(g(x) \cdot y) \cdot y = g(x)$	[186 :346, flip]
403,402	$g(x \cdot y) = g(x) \cdot g(y)$	[9 :353]
418,417	$((g(x) \cdot g(y)) \cdot z) \cdot z = g(y) \cdot x$	[7 :403]
472,471	$g(x) \cdot g(y) = g(x) \cdot y$	[370 :418, flip]
530,529	$g(x \cdot y) = g(x) \cdot y$	[402 :472]
570	$x \cdot (x \cdot y) = g(y)$	[352 → 392]
585,584	$g(x) = x$	[570 → 121 :530,353]
591,590	$(x \cdot y) \cdot x = y$	[570 → 2 :585,585]
594	$x \cdot y = y \cdot x$	[570 → 2 :585,585]
619	$\square$	[4 :585,591 :594,1,1]

Proof ($\Leftarrow$) found by Otter 3.0.3l on gyro at 0.08 seconds.

1	$x = x$	
2	$x \cdot y = y \cdot x$	
4,3	$g(x) = x$	
5	$(x \cdot y) \cdot x = y$	
7	$(g(A) \cdot B) \cdot (C \cdot (B \cdot A)) \neq C$	
8	$(A \cdot B) \cdot (C \cdot (B \cdot A)) \neq C$	[copy,7 :4]
10,9	$x \cdot (y \cdot x) = y$	[5 → 5]
15	$C \neq C$	[2 → 8 :10]
16	$\square$	[15,1]

Theorem #STN-10. The equational theory of any finitely based subvariety of Steiner quasigroups is one-based.

8.3 Other Algebras

The following theorem was first reported in [34]. It is used to show that every finitely based equational theory of algebras with distributive and permutable congruences is one based. In particular, if the theory admits a term $p(x,y,z)$ satifying the Pixley properties $p(y,y,x) = p(x,z,z) = p(x,u,x) = x$, then a single axiom for the theory can be constructed.

Theorem #PIX-2. The type is (5,2,0), with nullary e.

$$\{p(p(u,u,x),p(f(z),y,z),z) = x\} \Leftrightarrow \left\{ \begin{array}{l} p(x,x,y) = y \\ p(x,y,y) = x \\ p(x,y,x) = x \\ f(x) = x \end{array} \right\}.$$

The proof of ($\Leftarrow$) is obvious. The proof of ($\Rightarrow$) follows.

Proof (found by Otter 3.0.3l on gyro at 0.06 seconds).

1	$x = x$	
2	$p(A,A,B) = B,\ p(A,B,B) = A,\ p(A,B,A) = A \ \rightarrow\ \Box$	
3	$p(p(x,x,y),p(f(z),u,z),z) = y$	
6,5	$p(x,p(f(y),z,y),y) = x$	[3 $\rightarrow$ 3]
8,7	$p(x,x,y) = y$	[3 :6]
9	$p(A,B,B) = A,\ p(A,B,A) = A \ \rightarrow\ \Box$	[2 :8 :1]
11,10	$p(x,y,y) = x$	[7 $\rightarrow$ 5]
12	$p(x,f(y),y) = x$	[5 $\rightarrow$ 5]
14	$p(f(x),y,x) = x$	[7 $\rightarrow$ 5, flip]
16	$p(A,B,A) = A \ \rightarrow\ \Box$	[9 :11 :1]
18,17	$f(x) = x$	[7 $\rightarrow$ 12, flip]
19	$p(x,y,x) = x$	[14 :18]
21	$\Box$	[19,16]

Appendix A

Open Questions

A.1 Uniqueness of Algebraic Laws

A.2 $=\!(gL)\!\Rightarrow$ in Other Algebras

Problem #TBG-2. We have the following (gL)-basis for Boolean groups in terms of a ternary operation (Thm. #TBG-1).

$$\left\{ \begin{array}{l} p(x,x,x) = x \\ p(x,y,p(z,u,v)) = p(y,z,p(u,v,x)) \end{array} \right\}$$

Can the associative law be replaced with an identity with fewer variables?

Problem #CS-GL-7. The type is (2,0) with constant e.

$$\left\{ \begin{array}{l} \text{cancellation} \\ x(ey) = y(ex) \\ xe = x \end{array} \right\} =\!(gL)\!\Rightarrow \{x(y(zu)) = (x(yz))u\}.$$

Problem #CS-GL-8. The type is (2,0) with constant e.

$$\left\{ \begin{array}{l} x(ey) = y(ex) \\ xe = x \end{array} \right\} =\!(gL)\!\Rightarrow \{x(y(zu)) = (x(yz))u\}.$$

Problem #CS-GL-11. The type is (2).

$$\left\{ \begin{array}{l} \text{cancellation} \\ x((yz)u) = (x(yz))u \end{array} \right\} =\!(gL)\!\Rightarrow \{xy = yx\}.$$

Problem #TC-1.

$$\left\{ \begin{array}{l} \text{TC} \\ \text{cancellation} \end{array} \right\} \Rightarrow \text{RC}.$$

A.3 Semigroups

Problem #CS-6.

$$\{\mathrm{CS}, (xy)^n = (yx)^n\} \Rightarrow \{xy^n = y^n x\}.$$

A.4 Independent Self-Dual Bases

A.5 Lattice-like Algebras

Problem #NL-1. Is the variety of Near Lattices one based? See Sec. 7.6.

Problem #TNL-1. Is the variety of Transitive Near Lattices one based? See Sec. 7.6.

Problem #RBA-1. The Robbins conjecture.

$$\left\{ \begin{array}{l} x + y = y + x \\ (x + y) + z = x + (y + z) \\ \text{Robbins-axiom} \end{array} \right\} \Rightarrow \{\text{Huntington-axiom}\}.$$

Problem #SAX-4. Let T (for triangle) denote the 3-element algebra of type (2,2) with two binary operations of join and meet defined on the set $T = \{0, 1, 2\}$ with $0 < 1 < 2 < 0$. The binary relation $<$ is reflexive and antisymmetric but not transitive. Define $x \vee y = l.u.b.(x, y)$ and $x \wedge y = g.l.b.(x, y)$. Thus both $\vee$ and $\wedge$ are idmepotent and commutative but not associative. If you draw the Hasse diagram of the algebra, it will be a triangle with $0 \vee 1 = 1$, $1 \vee 2 = 2$, $2 \vee 0 = 0$, etc. It is known that T is not one-based. Find an elegant, short two-basis for the equational theory of T.

A.6 Miscellaneous Topics

Problem #SAX-1. Find the smallest possible equational basis for axiom set $A2$, of type (2,0) with constant e.

$$A1 = \{(xe)e = x, e(ex) = x, ee = e, e(xe) = (ex)e\}$$
$$A2 = A1 \cup \{((xx)e)(xx) = e\}$$

Problem #SAX-2. The type is (2,0), with constant e. Find an identity A containing a term $f(x)$ or $f(y)$ such that

$$\{A\} \; =(gL)\Rightarrow \; \left\{ \begin{array}{l} ((x|(((x|y)|z)|(y|e)))|(e|e)) = z \\ f(x) = x \end{array} \right\}.$$

Problem #SAX-3. The type is (3,1). Find a single identity for the equational theory specified by the following three identities.

$$\left\{ \begin{array}{l} g(x) = x \\ f(x,x,x) = x \\ f(x,y,f(z,x,y)) = z \end{array} \right\}.$$

Problem #HBCK. A Problem from Portugal. The type is (2,0) with constant 1. The quasivariety HBCK is defined by

$$\left\{ \begin{array}{ll} (M3) & x \cdot 1 = 1 \\ (M4) & 1 \cdot x = x \\ (M5) & (x \cdot y) \cdot ((z \cdot x) \cdot (z \cdot y)) = 1 \\ (M7) & x \cdot y = 1, y \cdot x = 1 \rightarrow x = y \\ (M8) & x \cdot x = 1 \\ (M9) & x \cdot (y \cdot z) = y \cdot (x \cdot z) \\ (H) & (x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z) \end{array} \right\}.$$

Theorem: (Blok and Ferreirim [?]) HBCK is an equational class of algerbas defined by the identities (M3-5,8-9), (H), and (J) $(((x \cdot y) \cdot y) \cdot x) \cdot x = (((y \cdot x) \cdot x) \cdot y) \cdot y$. Find a first order derivation of (J) from the axioms of HBCK:

$$\{\text{M3,M4,M5,M7,M8,M9,H}\} \rightarrow \{\text{J}\}.$$

(The known proof is model-theoretic—information from Stan Burris of Waterloo).

Appendix B

Theorems Proved

Bibliography

[1] Anonymous. The QED Manifesto. ftp://info.mcs.anl.gov/pub/qed/manifesto, 1993.

[2] G. Birkhoff. On the structure of abstract algebras. *Proc. of the Camb. Philos. Soc.*, 29:433–454, 1935.

[3] R. S. Boyer and J S. Moore. *A Computational Logic.* Academic Press, New York, 1979.

[4] R. S. Boyer and J S. Moore. *A Computational Logic Handbook.* Academic Press, New York, 1988.

[5] R. H. Bruck. *A Survey of Binary Systems.* Springer-Verlag, Berlin, 1958.

[6] I. M. S. Etherington. Quasigroups and cubic curves. *Proc. Edinburgh Math. Soc.*, 14:273–291, 1965.

[7] ?? Forder and J. Kalman. ?? *Math. Gazette*, 46:122–126, 1962.

[8] G. Grätzer and R. Padmanabhan. Symmetric difference in Abelian groups. *Pac. J. Math.*, 74(2):339–347, 1978.

[9] G. Higman and B. H. Neumann. Groups as groupoids with one law. *Publicationes Mathematicae Debrecen*, 2:215–227, 1952.

[10] B. Jónsson. Algebras whose congruence lattices are distributive. *Math. Scand.*, 21:110–121, 1967.

[11] J. Kalman. Equational completeness and families of sets closed under subtraction. *Indag. Math.*, 22:402–405, 1960.

[12] J. Kalman, Sept.–Oct. 1994. Correspondence by electronic mail.

[13] A. Knapp, editor. *Elliptic Curves.* Princeton University Press, 1993.

[14] D. Knuth and P. Bendix. Simple word problems in universal algebras. In J. Leech, editor, *Computational Problems in Abstract Algebras*, pages 263–297. Pergamon Press, Oxford, U.K., 1970.

[15] K. Kunen. Single axioms for groups. *J. Automated Reasoning*, 9(3):291–308, 1992.

[16] W. McCune. Single axioms for groups and Abelian groups with various operations. *J. Automated Reasoning*, 10(1):1–13, 1993.

[17] W. McCune. A Davis-Putnam program and its application to finite first-order model search: Quasigroup existence problems. Tech. Memo. ANL/MCS-TM-194, Argonne National Laboratory, Argonne, IL, 1994.

[18] W. McCune. Models And Counter-Examples (MACE). http://www.mcs.anl.gov/home/mccune/ar/mace/, 1994.

[19] W. McCune. OTTER 3.0 Reference Manual and Guide. Tech. Report ANL-94/6, Argonne National Laboratory, Argonne, IL, 1994.

[20] W. McCune and R. Padmanabhan. Single identities for lattice theory and for weakly associative lattices. Preprint MCS-P493-0395, Argonne National Laboratory, Argonne, IL, 1995.

[21] R. N. McKenzie. Equational bases for lattice theories. *Math. Scand.*, 27:24–38, 1970.

[22] N. S. Mendelsohn, R. Padmanabhan, and B. Wolk. Straight edge constructions on cubic curves. *C. R. Math. Rep. Acad. Sci. Canada*, 10:77–82, 1988.

[23] J. S. Milne. Abelian varieties. In *Arithmetic, Geometry*, pages 103–150. Springer-Verlag, New York, 1986.

[24] B. H. Neumann. Another single law for groups. *Bull. Australian Math. Soc.*, 23:81–102, 1981.

[25] R. Padmanabhan. Inverse loops as groupoids with one law. *J. London Math. Soc.*, 2(1 44):203–206, 1969.

[26] R. Padmanabhan. Equational theory of algebras with a majority polynomial. *Algebra Universalis*, 7(2):273–275, 1977.

[27] R. Padmanabhan. A first-order proof of a theorem of Frink. *Algebra Universalis*, 13(3):397–400, 1981.

[28] R. Padmanabhan. Logic of equality in geometry. *Discrete Mathematics*, 15:319–331, 1982.

[29] R. Padmanabhan. A self-dual equational basis for Boolean algebras. *Canad. Math. Bull.*, 26(1):9–12, 1983.

[30] R. Padmanabhan and W. McCune. Automated reasoning about cubic curves. *Computers and Math. Applic.*, 29(2):17–26, 1995.

[31] R. Padmanabhan and W. McCune. An equational characterization of the conic construction on cubic c urves. Preprint MCS-P517-0595, Argonne National Laboratory, Argonne, IL, 1995.

[32] R. Padmanabhan and W. McCune. Single identities for ternary boolean algebras. *Computers and Math. Applic.*, 29(2):13–16, 1995.

[33] R. Padmanabhan and W. McCune. Stiener-n, gt-dual document. In preparation, 1995.

[34] R. Padmanabhan and R. W. Quackenbush. Equational theories of algebras with distributive congruences. *Proc. of AMS*, 41(2):373–377, 1973.

[35] G. Pieper. The QED Workshop. Tech. memo., Argonne National Laboratory, Argonne, IL, May 1994.

[36] G. Robinson and L. Wos. Paramodulation and theorem-proving in first-order theories with equality. In D. Michie and R. Meltzer, editors, *Machine Intelligence, Vol. IV*, pages 135–150. Edinburg U. Press, 1969.

[37] I. R. Shafarevich. *Basic Algebraic Geometry.* Springer-Verlag, New York, 1977.

[38] T. A. Springer. *Linear Algebraic Groups.* Birkhauser, Boston, 1980.

[39] A. Tarski. Equational logic and equational theories of algebras. In K. Schütte, editor, *Contributions to Mathematical Logic*, pages 275–288. North-Holland, Amsterdam, 1968.

[40] R. Veroff. Using hints to increase the effectiveness of an automated reasoning program: Case studies. *J. Automated Reasoning*, 1995. To appear.

[41] S. Winker. Robbins algebra: Conditions that make a near-boolean algebra boolean. *J. Automated Reasoning*, 6(4):465–489, 1990.

[42] L. Wos, R. Overbeek, E. Lusk, and J. Boyle. *Automated Reasoning: Introduction and Applications,* revised edition. McGraw-Hill, New York, 1992.

[43] L. Wos, G. Robinson, and D. Carson. Efficiency and completeness of the set of support strategy in theorem proving. *J. ACM*, 12(4):536–541, 1965.

Index

#ABGT-1, theorem, 47
#ABGT-2, theorem, 48
#ABGT-3, theorem, 48
#ABGT-4, theorem, 34
#ABGT-5, theorem, 33
#ABGT-6, theorem, 33
#ABGT-7, theorem, 49
#ABGT-8, theorem, 51
#BA-1, theorem, 127
#CS-1, theorem, 76
#CS-11, theorem, 80
#CS-14, theorem, 80
#CS-15, theorem, 81
#CS-2, theorem, 76
#CS-3, theorem, 77
#CS-4, theorem, 78
#CS-5, theorem, 79
#CS-5a, theorem, 79
#CS-6, problem, 162
#CS-7, theorem, 79
#CS-8, theorem, 80
#CS-9, theorem, 80
#CS-GL-1, theorem, 70
#CS-GL-11, problem, 161
#CS-GL-2, theorem, 71
#CS-GL-3, theorem, 72
#CS-GL-4, theorem, 72
#CS-GL-5, example, 72
#CS-GL-6, theorem, 73
#CS-GL-7, problem, 161
#CS-GL-8, problem, 161
#CS-GL-9, theorem, 70
#DUAL-BA-1, theorem, 128
#DUAL-GT-1, theorem, 85
#DUAL-GT-10, theorem, 93
#DUAL-GT-11, theorem, 94
#DUAL-GT-2, example, 86
#DUAL-GT-3, theorem, 87
#DUAL-GT-4, example, 88
#DUAL-GT-5, theorem, 89
#DUAL-GT-6, theorem, 90
#DUAL-GT-7, theorem, 90
#DUAL-GT-8, theorem, 91
#DUAL-GT-9, theorem, 93
#GEO-1, theorem, 29
#GT-1, theorem, 81
#HBCK, problem, 163
#IL-1, theorem, 148
#IL-2, lemma, 150
#IL-3, lemma, 152
#IL-4, theorem, 153
#LT-1, theorem, 97
#LT-1a, theorem, 130
#LT-1b, theorem, 131
#LT-1c, theorem, 98
#LT-2, theorem, 102
#LT-3, theorem, 105
#LT-4, theorem, 106
#LT-5, theorem, 109
#LT-6, theorem, 58
#LT-6a, theorem, 58
#LT-7, corollary, 115
#LT-N5, theorem, 99
#MAJ-1, theorem, 103
#MAJ-2, theorem, 104
#MAJ-4, theorem, 57
#MCV-1, theorem, 36
#MED-0, theorem, 30
#MED-1, theorem, 5
#MED-2, theorem, 32
#MED-3, theorem, 31
#MED-4, theorem, 32

#MED-5, theorem, 32
#MFL-1, theorem, 140
#MFL-2, theorem, 141
#MFL-3, theorem, 142
#MFL-4, theorem, 143
#MFL-5, theorem, 144
#MFL-6, theorem, 145
#MFL-7, theorem, 146
#MFL-8, example, 147
#MFL-9, corollary, 153
#NL-1, problem, 162
#OC-GL-1, theorem, 59
#OC-GL-2, corollary, 59
#OC-GL-3, theorem, 59
#OC-GL-4, corollary, 60
#PIX-1, theorem, 57
#PIX-2, theorem, 159
#QGT-1, theorem, 54
#QGT-2, theorem, 54
#QGT-3, theorem, 154
#QLT-1, theorem, 112
#QLT-2, theorem, 113
#QLT-3, problem, 115
#QLT-3a, theorem, 118
#QLT-4, example, 120
#QLT-4a, theorem, 121
#QUART-1, theorem, 44
#QUART-2, theorem, 44
#RBA-1, problem, 133, 162
#RBA-2, theorem, 133
#RBA-3, theorem, 134
#RC-0, theorem, 69
#RC-1, theorem, 64
#RC-2, theorem, 65
#RC-3, theorem, 65
#RC-4, theorem, 66
#RC-5, theorem, 67
#SAX-1, problem, 162
#SAX-2, problem, 162
#SAX-3, problem, 163
#SAX-4, problem, 162
#STN-1, theorem, 52
#STN-10, theorem, 158
#STN-3, problem, 39
#STN-4, theorem, 39
#STN-5, theorem, 40
#STN-6, theorem, 154
#STN-7, theorem, 155
#STN-8, theorem, 156
#STN-9, theorem, 157
#TBA-1, theorem, 136
#TBG-1, theorem, 55
#TBG-2, problem, 161
#TC-0, theorem, 69
#TC-1, problem, 161
#TC-10, theorem, 66
#TC-11, theorem, 67
#TC-12, theorem, 67
#TC-13, theorem, 68
#TC-2, theorem, 60
#TC-3, theorem, 61
#TC-4, theorem, 61
#TC-5, theorem, 62
#TC-6, theorem, 63
#TC-7, theorem, 63
#TC-8, theorem, 64
#TC-9, theorem, 65
#TNL-1, problem, 162
#TNL-2, example, 126
#UAL-1, theorem, 38
#UAL-2, corollary, 43
#UAL-3, theorem, 34
#UAL-3a, corollary, 36
#UAL-4a, lemma, 40
#UAL-4b, theorem, 41
#UAL-5, theorem, 36
#UAL-6, theorem, 37
#UAL-7, corollary, 38
#WAL-1, theorem, 107
#WAL-2, theorem, 108
#WAL-3, theorem, 110
#WAL-4, theorem, 112

Abelian group theory, 47
ABGT, *see* Abelian group theory

BA, *see* Boolean algebra
Boolean algebra, 127
    Frink's theorem, 127
    Huntington's axiom, 133
    self-dual basis, 128

set difference, 130
ternary, 136
Bowden's law, 113

cancellative semigroup, 75
conic-cubic construction, 43
CS, *see* cancellative semigroup
cubic-conic construction, 43

distributivity
lattice theory, 97, 98
quasilattice, 112, 121
dual group theory, 85
DUAL-GT, *see* dual group theory

email addresses, vi

Frink's theorem, 127
FTP addresses, v

GT, *see* group theory

HTTP addresses, v

IL, *see* inverse loop
interpolation theorem, 85
inverse loop, 139
inverse loops
single axioms, 148

Jónsson polynomial, 103

lattice theory, 97
$M_5 - N_5$ argument, 97
N_5 theorem, 99
absorption basis, 102
distributivity, 97, 98
inconsistency with $=(gL)\Rightarrow$, 57
reduction schemata, 103
single axioms, 105, 106
LT, *see* lattice theory

MAJ, *see* majority polynomial
majority polynomial
definition, 103
inconsistency with $=(gL)\Rightarrow$, 57
MCV, *see* Mal'cev polynomial
MED, *see* median law
median law
$=(gL)\Rightarrow$ proofs, 30
sample proofs, 5
meta-Abelian CS, 81
MFL, *see* Moufang loop
modularity
quasilattice, 115
Moufang loop, 139
Moufang loops
single axioms, 153

near lattice, 125
network addresses, v, vi
NL, *see* near lattice

OC, *see* overlay condition
open questions, 161
overlay condition, 58

PIX, *see* Pixley polynomial
Pixley polynomial
inconsistency with $=(gL)\Rightarrow$, 57
single axiom, 159

QGT, *see* quasigroup theory
QLT, *see* quasilattice theory
QUART, *see* quartic curve
quartic curve, 44
quasigroup, 154
axioms, 139
consistency with $=(gL)\Rightarrow$, 52
overlay condition, 58
quasilattice
Bowden's law, 113
distributivity, 112, 121
modularity, 115
uniqueness of meet, 120
quasilattice theory, 112
quotient condition, 81

RBA, *see* Robbins algebra
RC, *see* Reidemeister closure
Reidemeister closure, 60
Robbins algebra, 133

semigroup, 75
    quotient condition, 81
single axioms
    inverse loops, 148
    lattice theory, 105
    Moufang loops, 153
    Steiner identity, 154
    ternary Boolean algebra, 136
    weakly associative lattice, 110
Steiner identity
    single axioms, 154
STN, *see* Steiner identity

TBA, *see* ternary Boolean Algebra
TBG, *see* ternary Boolean group
TC, *see* Thomsen closure
ternary Boolean algebra
    single axioms, 136
ternary Boolean group, 55
Thomsen closure, 60
TNL, *see* transitive near lattice
transitive near lattice, 125
    uniqueness of meet, 125

UAL, *see* unique algebraic law
unique algebraic law, 27
uniqueness under $=\!\!(gL)\!\!\Rightarrow$
    groups, 34
    Mal'cev polynomial, 36
    Steiner laws, 38

WAL, *see* weakly associative lattice
weakly associative lattice, 106
    absorption basis, 110
    single axioms, 110
    uniqueness of meet, 108