J. Symbolic Computation (1993) **16**, 279–288

Term Rewrite Systems for Lattice Theory

Ralph Freese, J. Ježek, and J. B. Nation

Department of Mathematics, University of Hawaii

November 20, 1997

It is shown that, even though there is a very well-behaved, natural normal form for lattice theory, there is no finite, convergent AC term rewrite system for the equational theory of all lattices.

The study of the equational theory of a class $\mathcal{K}$ of algebras and their free algebras $\mathbf{F}_{\mathcal{K}}(X)$ is greatly facilitated by a normal form for the terms over the language of $\mathcal{K}$. For terms u and v over some set of variables X, u is *equivalent to* v *modulo* $\mathcal{K}$ if the equation $u \approx v$ holds identically in $\mathcal{K}$ (i.e., for all substitutions of the variables into all algebras in $\mathcal{K}$). We write this $u \approx v \pmod{\mathcal{K}}$. By a *normal form* we mean an effective choice function from the equivalence classes of this relation. We will use the notation $\mathrm{nf}(w)$ for such a normal form function. Having a normal form is equivalent to the equational theory being decidable. Moreover, if this normal form can be computed efficiently, it is very helpful for computer implementations of the free algebras in $\mathcal{K}$.

A term rewrite system, abbreviated TRS, constitutes a very specific method for transforming terms. A normal form TRS transforms terms into a unique normal form and, as such, is computationally useful. (The definitions will be given below.) Not every decidable equational theory has a normal form TRS. For example, it is easy to see that commutative groupoids have no such TRS. An *associative and commutative* TRS, denoted AC TRS, is one in which we are allowed to apply the associative and commutative laws, as well as the rewrite rules.

The class of lattices, $\mathcal{L}$, has a very nice normal form, discovered by Whitman (1941) and (1942). Whitman showed each lattice term is equivalent to a term of shortest length which is unique up to associativity and commutativity. In this paper, we reserve the term *canonical form* for Whitman's normal form. The canonical form of a term is also lattice-theoretically the best way to write it: if $w = w_1 \vee \cdots \vee w_n$ canonically, then $w_1, \ldots, w_n$ are the lowest possible elements of the free lattice that irredundantly join to w, see Theorem 4.

Whitman (1942) gave a procedure to test if a term is in canonical form and using this it is not hard to see that there is a polynomial time algorithm to put an arbitrary term into canonical form. The details are presented in our monograph, *Free Lattices* (1993). Besides containing a detailed study of free lattices, this monograph also has a chapter on

This research was partially supported by NSF grants DMS–9204481 and DMS–9122011.

the computational aspects of lattice theory and includes a description of our computer implementations of various algorithms for lattices.

The purpose of this note is to prove that, despite having this very nice canonical form, there is no finite, convergent AC TRS for lattice theory. The existence of such an AC TRS is raised as Problem 32 in *Open problems in rewriting* (1991) by N. Dershowitz, J.-P. Jouannaud, and J. W. Klop. The next two sections contain the necessary lattice theoretic and TRS prerequisites.

The monograph on free lattice mentioned above will also contain some new results about term rewrite systems for equational classes of lattices other than the class of all lattices.

The authors would like to thank George McNulty for suggesting this problem to them and Stan Burris for several enlightening lectures on term rewrite systems. They also would like to thank the referees for several helpful suggestions.

Term Rewrite Systems

Term rewrite systems were pioneered by Trevor Evans (1951) who gave a convergent TRS for quasigroups. The subject was popularized with Knuth and Bendix (1970) who gave methods which could sometimes convert equational axioms into a convergent TRS. They were able to use these methods to find a convergent TRS for groups. Since that time the subject has become popular, especially with computer scientists. Equational TRS's were introduced by Lankford and Ballantyne (1977) and Peterson and Stickel (1981). A good general reference is Dershowitz and Jouannaud (1990); see also Jouannaud and Kirchner (1986). Ježek (1982) considers TRS–like systems for groupoids and Burris and Lawrence (1991) consider AC TRS's for certain finite rings.

A set R of ordered equations is called a *term rewrite system* and abbreviated TRS. The equations are written with an arrow: $p \to q$. A *substitution* is simply an endomorphism of the term algebra. If $(p \to q) \in R$ and r is a term which has a subterm of the form $\sigma(p)$ for some substitution σ, then we can rewrite r by replacing (one occurrence of) $\sigma(p)$ by $\sigma(q)$. If t is the resulting term, then we write $r \to_R t$ and call this a *one step rewrite.* A term rewrite system R is finite if R is; it is *terminating* if there is no infinite sequence of (one step) rewrites. This means that if we start with any term and apply the rewrite rules repeatedly in any order, we will eventually reach a term which cannot be further rewritten. A terminating TRS is *convergent* if, for every term s, every sequence of rewrites starting with s terminates with the same term, which is then called the *normal form* of s. If R is a convergent TRS, we denote the normal form of a term w by $\mathrm{nf}_R(w)$ or $\mathrm{nf}(w)$, when R is understood. We say that an equational theory E has a convergent TRS provided there is a convergent TRS such that $s \approx t$ is in E if and only if $\mathrm{nf}(s) = \mathrm{nf}(t)$.

Not every recursive equational theory has a finite, convergent TRS. It is easy to see that theories which contain the commutative law, $x \cdot y \approx y \cdot x$, do not have such a TRS. This defect can be corrected sometimes by an equational TRS. Let E_0 be a set of regular equations (an equation is *regular* if the set of variables occurring on the left side is the same as those on the right) and define $s \equiv t$ if $E_0 \vDash s \approx t$. An *equational* TRS is a pair $\langle E_0, R\rangle$ where R is a TRS. In such a system we allow sequences of rewrites of the form

$$s_0 \equiv s_1 \to_R s_2 \equiv s_3 \to_R \cdots . \qquad (1)$$

A term u is *terminal* for an equational TRS if no rewrite rule applies to it nor to any $u' \equiv u$. A *convergent equational* TRS is one in which, for every term s, every sequence in the above form, with $s_0 = s$, eventually terminates, that is, ends in a terminal element and the $\equiv$–class of this element is unique. We let $\mathrm{nf}(s)$ denote some representative of this $\equiv$–class. It would make more sense to define $\mathrm{nf}(x)$ to be the equivalence class, but our definition is notationally easier. In this paper we will be concerned with the case when E_0 consists of the associative and commutative laws for the lattice operations $\vee$ and $\wedge$. In this case the rewrite system is called an AC TRS. The theory of AC TRS's is developed by Peterson and Stickel (1981). Their paper shows, among other things, that the equational theory of distributive lattices (which is the same as the equational theory of the 2 element lattice) has an AC TRS.

The next lemma collects some basic facts about equational TRS's. We say that a term v is an E_0*–subterm* of u if v is a subterm of u' for some $u' \equiv u$. Since E_0 is regular, we can speak about the variables occurring in $\mathrm{nf}(u)$ because the set of variables which occur is independent of the choice of $\mathrm{nf}(u)$.

Lemma 1. *Suppose that $\langle E_0, R\rangle$ is a finite, convergent, equational TRS. Then the following hold.*

1. *If v is an E_0–subterm of u and $\mathrm{nf}(u) \equiv u$, then $\mathrm{nf}(v) \equiv v$.*
2. *If w is a term and σ is an automorphism of the term algebra, then $\mathrm{nf}(\sigma(w)) \equiv \sigma(\mathrm{nf}(w))$.*
3. *If $u = \sigma(v)$ for some endomorphism of the term algebra and $\mathrm{nf}(u) \equiv u$, then $\mathrm{nf}(v) \equiv v$.*
4. *The variables which occur in $\mathrm{nf}(w)$ all occur in w.*

Proof. (1) follows since none of the rewrite rules can apply to u. (2) is a direct consequence of the way rewrite rules are applied. For (3), first note that if v' is an E_0–subterm of v then $\sigma(v')$ is an E_0–subterm of u. So if $p \to q$ is a rewrite rule and $v' = \tau(p)$ for some substitution τ, then $p \to q$ would apply to u under the substitution $\sigma\tau$. But no rewrite rule can apply to u because it is in normal form.

If there was a variable occurring in $\mathrm{nf}(w)$ which did not occur in w, then there must be a rewrite rule of the form $u(x_1, \ldots, x_n) \to v(x_1, \ldots, x_n, y_1, \ldots, y_k)$ with $k \geq 1$. But then, applying this rule under the substitution which maps y_1 to $u(x_1, \ldots, x_n)$ and fixing the other variables, we obtain an infinite chain of rewrites:

$$u(\mathbf{x}) \to v(\mathbf{x}, u(\mathbf{x}), \mathbf{y}) \to v(\mathbf{x}, v(\mathbf{x}, u(\mathbf{x}), \mathbf{y}), \mathbf{y}) \to \cdots$$

where $\mathbf{x} = x_1, \ldots, x_n$ and $\mathbf{y} = y_2, \ldots, y_k$. □

Lattice Theory and Free Lattices

A lattice is a partially ordered set L such that every pair of elements x, $y \in L$ has a least upper bound, denoted $x \vee y$, and a greatest lower bound, $x \wedge y$. We use $\leq$ to denote the order relation of the lattice. A lattice can also be viewed as an algebraic system, $\mathbf{L} = \langle L, \vee, \wedge\rangle$ with two binary operations. Lattices have the following equational axiomization (actually the idempotency can be derived from the others):

$$\begin{array}{ccl} x \vee (y \vee z) \approx (x \vee y) \vee z & x \wedge (y \wedge z) \approx (x \wedge y) \wedge z & \text{(associative)} \\ x \vee y \approx y \vee x & x \wedge y \approx y \wedge x & \text{(commutative)} \\ x \approx x \vee x & x \approx x \wedge x & \text{(idempotent)} \\ x \approx x \vee (y \wedge x) & x \approx x \wedge (y \vee x) & \text{(absorptive)} \end{array}$$

It is easy to verify that these axioms hold in all lattices. Coversely if $\mathbf{L} = \langle L, \vee, \wedge \rangle$ is an algebra satisfying these equations, we can define $x \leq y$ if $x \vee y = y$. This partially orders L and under this order L is a lattice with least upper bounds agreeing with $x \vee y$ and greatest lower bounds agreeing with $x \wedge y$. The simple details can be found in any book on lattices.

By an AC TRS for lattices we mean an equational TRS, where E_0 consists of both commutative and associative laws above.

The *dual* of a statement about lattices is the statement obtained by interchanging the roles of $\vee$ and $\wedge$, and those of $\leq$ and $\geq$. Notice that the above axioms are self dual. Thus, if a statement is true about lattices, its dual is also true.

Since the class of all lattices, $\mathcal{L}$, is equationally defined, it has free algebras over any set X. Naturally these are called *free lattices*; the free lattice over X is denoted $\mathbf{FL}(X)$. This lattice can be constructed in the usual way: if s and t are terms in the operations $\vee$ and $\wedge$ with variables from X, $s \approx t$ will mean that this equation follows from the lattice axioms; that is, it holds in all lattices under all substitutions of the variables. $\mathbf{FL}(X)$ consists of the equivalence classes of $\approx$. It is convenient (although not absolutely correct) to view s as an element of $\mathbf{FL}(X)$. We define an order relation $\leq$ on terms by $s \leq t$ if this holds in $\mathbf{FL}(X)$ when we view s and t as elements of $\mathbf{FL}(X)$. This is only a quasi-order on the set of terms; in fact, $s \approx t$ if and only if $s \leq t$ and $t \leq s$.

Since both lattice operations are associative, we include in our definition of terms expressions which omit unnecessary parentheses. Thus

$$x \vee (y \vee z) \qquad x \vee y \vee z \qquad (x \vee y) \vee z \tag{2}$$

are all terms. In this paper the word 'term' will refer to terms over the two binary operation symbols $\vee$ and $\wedge$. Whitman gave a recursive algorithm for determining if $s \leq t$.

Theorem 2. *Let s and t be terms with variables in X. Then $s \leq t$ holds if and only if one of the following holds.*

(1) *$s = s_1 \vee \cdots \vee s_k$ is a formal join and $s_i \leq t$ holds for all i.*
(2) *$t = t_1 \wedge \cdots \wedge t_k$ is a formal meet and $s \leq t_i$ holds for all i.*
(3) *s and $t \in X$ and $s = t$.*
(4) *$s \in X$ and $t = t_1 \vee \cdots \vee t_k$ is a formal join and $s \leq t_j$ for some j.*
(5) *$s = s_1 \wedge \cdots \wedge s_k$ is a formal meet and $t \in X$ and $s_j \leq t$ for some j.*
(6) *$s = s_1 \wedge \cdots \wedge s_k$ is a formal meet and $t = t_1 \vee \cdots \vee t_m$ is a formal join and $s_i \leq t$ holds for some i or $s \leq t_j$ holds for some j.*

A term s is *formally a meet* if it has the form $s = s_1 \wedge s_2$. For example, the term $(x \vee y) \wedge (x \vee y \vee z)$ is formally a meet, even though when it is thought of as an element of the free lattice, it is equal to $x \vee y$, which is meet irreducible in the free lattice. Of course, a term is *formally a join* if the dual condition holds.

Item (6) is known as Whitman's condition and is denoted (W). Notice it implies that every element of a free lattice is either meet irreducible or join irreducible. (An element a of a lattice is *meet irreducible* if $a = b \wedge c$ implies $a = b$ or $a = c$; join irreducibility is defined dually.) Using Theorem 2, Whitman showed that *for each term u there is a shortest term w, unique up to* AC*, such that $u \approx w$ holds in lattice theory*. This element w is the *canonical form* of u. He proved the following criterion for deciding if a term is in canonical form. This criterion provides a way to reduce a term to canonical form. Notice that each step of this process reduces the length of the term.

THEOREM 3. *A term $t = t_1 \vee \cdots \vee t_n$, with $n > 1$, is in canonical form if and only if*

1. *each t_i is either in X or formally a meet,*
2. *each t_i is in canonical form,*
3. *$t_i \not\leq t_j$ for all $i \neq j$ (the t_i's form an antichain),*
4. *if $t_i = \bigwedge t_{ij}$ then $t_{ij} \not\leq t$ for all j.*

A term $t = t_1 \wedge \cdots \wedge t_n$, with $n > 1$, is in canonical form if and only if the duals of the above conditions hold. A term $x \in X$ is always in canonical form.

For subsets A and B of a lattice, we say that A *join refines* B, written $A \ll B$, if for each $a \in A$ there is a $b \in B$ such that $a \leq b$.

THEOREM 4. *Let $w = w_1 \vee \cdots \vee w_n$ be a term in canonical form, where each w_i is either a variable or a formal meet. If $u = u_1 \vee \cdots \vee u_m$ and $w \approx u \pmod{\mathfrak{L}}$, then*

$$\{w_1, \ldots, w_n\} \ll \{u_1, \ldots, u_m\}.$$

This theorem, which is due to Whitman, shows that the canonical form (of a join reducible element) is the best representation of the element as a join, in that its joinands are as far down in the lattice as possible. Moreover this representation is unique. The uniqueness of this representation has important consequences for free lattices. For example, it implies the following semidistributive law:

$$a \vee b = a \vee c \qquad \text{implies} \qquad a \vee b = a \vee (b \wedge c).$$

If $u = u_1 \vee \cdots \vee u_n$ is in canonical form, we say that each u_i is a *canonical joinand* of u. The next lemma, which appears in Tschantz (1990), can be proved easily using Theorem 2.

LEMMA 5. *Let u_1 be a canonical joinand of u. Then*

1. *if $u_1 \leq s \wedge t \leq u$ then either $s \leq u$ or $t \leq u$ or $u_1 = s \wedge t$;*
2. *if $u_1 \leq s \vee t \leq u$ then either $u_1 \leq s$ or $u_1 \leq t$;*
3. *if $u_1 \leq x \leq u$, where $x \in X$, then $u_1 = x$.*

If a and b are elements of a lattice we say that b *covers* a, denoted $a \prec b$, if $a < b$ and there is no c such that $a < c < b$. In the free lattice generated by $X = \{x_1, \ldots, x_n\}$, $\mathbf{FL}(X)$, let $\underline{x}_i = \bigwedge_{j \neq i} x_j$. Using the argument given below, it is not hard to see that $0 = \bigwedge X \prec \underline{x}_i \prec \underline{x}_i \vee \underline{x}_j$, for $i \neq j$, but we only require the following easy fact.

LEMMA 6. *If $u > \underline{x}_i$ in $\mathbf{FL}(x_1, \ldots, x_n)$, then $u \geq \underline{x}_j$ for some $j \neq i$.*

PROOF. If we look at the homomorphism from $\mathbf{FL}(x_1, \ldots, x_n)$ onto the two element lattice, $\mathbf{2} = \{0, 1\}$, which maps a fixed x_k to 0 and all other x_j's to 1, we see that every element of $\mathbf{FL}(x_1, \ldots, x_n)$ is either below x_k or above $\underline{x}_k$. Suppose $u > \underline{x}_i$. If $u \leq x_k$ for all $k \neq i$, then $u \leq \underline{x}_i$, a contradiction. Hence, $u \not\leq x_j$ for some $j \neq i$, and thus $u \geq \underline{x}_j$. □

The Result

In this section we prove that there is no finite, convergent AC TRS for the equational theory of lattices. From now on we use $u \equiv v$ to mean that the lattice terms u and v are equivalent modulo AC. We use $u \approx v$ to mean that u is equivalent to v in lattice theory, i.e., u and v evaluate to the same element under every substitution of the variables into every lattice. This, of course, is equivalent to the fact that u and v represent the same element in $\mathbf{FL}(X)$, for any set X which contains the variables occurring in u and v. Of course, $u = v$ means that u and v are the same term.

Suppose we have a finite, convergent AC TRS for lattice theory. For w a term, let $\mathrm{nf}(w)$ denote the normal form of w associated with this TRS. This normal form is really only defined up to equivalence modulo AC. We will assume that $\mathrm{nf}(w)$ chooses some element of this AC class which does not have any unnecessary parentheses. For example, the three terms in (2) are AC–equivalent and, if they are in normal form (we will see that they are), then the value of $\mathrm{nf}(w)$ for any of them, must be $x \vee y \vee z$. This means that if $\mathrm{nf}(w) = u_1 \vee \cdots \vee u_k$ then each u_i is assumed to be either a formal meet or a variable. The expression 'w is in normal form' means $\mathrm{nf}(w) \equiv w$. Recall that the term *canonical form* refers to Whitman's canonical form. Also, as above, we say that v is an AC–*subterm* of u if v is a subterm of u' for some $u' \equiv u$.

Lemma 7. *Let $t = t_1 \vee \cdots \vee t_n$ be in canonical form with $n > 1$. Then $\mathrm{nf}(t)$ is a formal join, say $\mathrm{nf}(t) = u = u_1 \vee \cdots \vee u_m$, and there is a map σ from $\{1, \ldots, n\}$ onto $\{1, \ldots, m\}$ such that $t_i \le u_{\sigma(i)}$ for all i. In particular, $1 < m \le n$. Moreover, $u_1, \ldots, u_m$ is an antichain.*

Proof. Since $n > 1$, $t \not\approx x$ for all variables and hence u cannot be a variable. If u is a formal meet $u = u_1 \wedge \cdots \wedge u_m$, then $u_i \approx u$ for some i since $u \approx t$ is meet irreducible. But then by Lemma 1, $u_i \equiv \mathrm{nf}(u_i) = \mathrm{nf}(u) \equiv u$, which is clearly false.

So suppose $u = u_1 \vee \cdots \vee u_m$. Then, by the refinement property of the Whitman canonical form (Theorem 4), for each i, there is a $\sigma(i)$ such that $t_i \le u_{\sigma(i)}$. Clearly

$$u' = \bigvee_{j \in \operatorname{range} \sigma} u_j$$

is an AC–subterm of u and so is in normal form. It is also clear that $u' \approx u$ and hence they have the same normal form. Thus $u' \equiv \mathrm{nf}(u') = \mathrm{nf}(u) \equiv u$, which is not possible if u' is a proper subterm of u. This implies that σ must be onto.

A similar argument shows that the u_i's form an antichain. □

Lemma 8. *Suppose that w is a term in normal form, w is a formal meet, and x is a variable such that $x \vee w$ is in canonical form. Then $x \vee w$ is in normal form.*

Proof. By Lemma 7,

$$\mathrm{nf}(x \vee w) = s \vee t \tag{3}$$

for some s and t with $x \le s < x \vee w$ and $w \le t < x \vee w$. Moreover, each of s and t is either a generator or a formal meet. Also, (3) implies that $\mathrm{nf}(t) = t$. We claim that $w \equiv t$. If $w \approx t$ then $w \equiv t$ since both are in normal form. In the other case, $w < t$. By a repeated application of parts (1) and (2) of Lemma 5, t has a subterm $v \vee r$ with $r \approx w$ (and v possibly a join). Since r is a subterm of t, it is in normal form. Hence $r \equiv w$.

For any term u, let u' denote the image of u under the endomorphism which maps every variable to x. Of course, $u' \approx x$ for all u. Now the chain of rewrites that transforms $x \vee w$ to $s \vee t$ can be applied in the same way to $x \vee w'$, yielding $s' \vee t'$. But t' has $v' \vee r' \equiv v' \vee w'$ as a subterm. Since $\mathrm{nf}(v') = x$, some additional rewrites transform $v' \vee w'$ into $x \vee w'$. Thus the concatenation of these rewritings transforms $x \vee w'$ into a term having $x \vee w'$ as a subterm, and this clearly leads to an infinite chain of rewrites, a contradiction. Hence $t \equiv w$.

Thus $\mathrm{nf}(x \vee w) \equiv s \vee w$. Unless $x \equiv s$, there is a chain of rewrites (of positive length) which transforms $x \vee w$ to $s \vee w$. When these rewrites are applied to $x \vee w'$, they yield $s' \vee w'$. Since $\mathrm{nf}(s') = x$, a further chain of rewrites transforms $s' \vee w'$ to $x \vee w'$. This again leads to an infinite chain of rewrites, and thus we must have $x \equiv s$. □

The next lemma shows that, if a term $t = t_1 \vee \cdots \vee t_n$ has the property that the t_i's are the same except for a change of variables, then Lemma 7 can be strengthened.

Lemma 9. *Suppose that $t = t_1 \vee \cdots \vee t_n$ canonically with $n > 1$ and that there is a subgroup $\mathbf{G} \cong \mathbf{S}_n$ of the automorphism group of the term algebra which acts faithfully on $\{t_1, \ldots, t_n\}$. Let $\mathrm{nf}(t) = r = r_1 \vee \cdots \vee r_m$. Then $m = n$ and, after reordering, $r_i \geq t_i$, for $i = 1, \ldots, n$, and $r_i \not\geq t_j$ for $i \neq j$.*

Proof. By part (2) of Lemma 1, $\sigma(r) \equiv r$ for each $\sigma \in G$. Thus

$$\sigma(r_1) \vee \cdots \vee \sigma(r_m) = \sigma(r) \equiv r = r_1 \vee \cdots \vee r_m$$

from which it follows that, for each i, $\sigma(r_i) \equiv r_j$, for some j. Suppose r_i is above exactly k of the t_j's. Since $\mathbf{S}_n$ acts transitively on the k element subsets of $\{t_1, \ldots, t_n\}$, each k–element subset has some r_i above it. By Lemma 7, $k < n$. Suppose $k > 1$. Then $n \geq 3$, and there are at least $\binom{n}{k}$ different r_i's. Since $\binom{n}{k} > n$ for $1 < k < n - 1$, this contradicts Lemma 7 unless $k = n - 1$. But in this case the join of the r_i's is clearly redundant, since $n > 2$. □

Lemma 10. *Let x, y, $z_1, \ldots, z_n$, and $e_1, \ldots, e_s$ be distinct variables, and let $\underline{z}_i = \bigwedge_{j \neq i} z_j$. If n, $s \geq 1$, and $k \geq 0$, then the following terms are all in normal form.*

$$z_1 \wedge \cdots \wedge z_n \tag{4}$$

$$\bigvee_{i=1}^{n} (x \wedge \underline{z}_i) \tag{5}$$

$$\bigvee_{i=1}^{n} (x \wedge z_i) \tag{6}$$

$$x \wedge \left[\bigvee_{i=1}^{k} (x \wedge z_i) \vee \bigvee_{j=1}^{s} e_j \right] \tag{7}$$

Proof. Straightforward applications of Theorem 3 show that each of these elements is in canonical form. By Lemma 9, $\mathrm{nf}(z_1 \wedge \cdots \wedge z_n) = r_1 \wedge \cdots \wedge r_n$. There is an obvious term algebra endomorphism mapping $z_1 \wedge \cdots \wedge z_n$ onto $r_1 \wedge \cdots \wedge r_n$ so, by part (3) of Lemma 1, $z_1 \wedge \cdots \wedge z_n$ is in normal form.

Let w be the element of (5), let $\mathrm{nf}(w) = r = r_1 \vee \cdots \vee r_m$, and let $a_i = x \wedge \underline{z}_i$. By part (4) of Lemma 1, the only variables that can occur in r are x, $z_1, \ldots, z_n$, and hence, r can be viewed as an element of $\mathbf{FL}(x, z_1, \ldots, z_n)$. By Lemma 9, $n = m$ and we may assume that $r_i \geq a_i$ and $r_i \not\geq a_j$ for all distinct i and j. But if $r_i > a_i$, then, by Lemma 6, $r_i \geq a_j$ for some $j \neq i$, a contradiction. Thus $a_i \approx r_i$. Since r_i is a subterm of r, $\mathrm{nf}(r_i) \equiv r_i$, and $\mathrm{nf}(a_i) \equiv a_i$ by the previous example. Thus $a_i \equiv r_i$ and so $\mathrm{nf}(w) = r_1 \vee \cdots \vee r_n \equiv a_1 \vee \cdots \vee a_n$, proving w is in normal form.

Since there is an obvious term algebra endomorphism mapping the element of (6) to the element of (5), the former element is in normal form by part (3) of Lemma 1.

Choose $n \geq k + s$. Then there is an endomorphism mapping the element

$$\bigvee_{i=1}^{k} (x \wedge z_i) \vee \bigvee_{j=1}^{s} e_j$$

to the element of (6), and hence the former is in normal form by Lemma 1 again. It now follows from the dual of Lemma 8 that the element of (7) is in normal form. □

Theorem 11. *There is no finite, convergent AC term rewrite system for the equational theory of lattices.*

Proof. Let w be the term given in (6), where n is large enough so that the length of w is greater than the length of the left hand side of all of the rewrite rules. Clearly $w \leq x$ and thus $x \wedge w \approx w$, so some rewrite rule must apply to $x \wedge w$. Since $\mathrm{nf}(w) \equiv w$, every proper AC–subterm of $x \wedge w$ is in normal form. Since the left hand side of a rewrite rule can never match a term in normal form, the left hand side of some rewrite rule must match $x \wedge w$.

What terms with length less than the length of $x \wedge w$ match $x \wedge w$? That is, for which terms t is there a term algebra endomorphism mapping t onto $x \wedge w$? (To avoid confusion, we will use letters at the beginning of the alphabet to denote variables.) Besides a and $a \wedge b$, the term

$$a \wedge [(c_1 \wedge d_1) \vee \cdots \vee (c_k \wedge d_k) \vee e_1 \vee \cdots \vee e_s]$$

matches $x \wedge w$ under an obvious substitution. (This term with $k = n$ and no e_j's also matches $x \wedge w$, but has the same length.) Some or all of the c_i's can be equal to each other or to a, but the other variables must be distinct. All of these terms have endomorphisms onto the term

$$a \wedge [(a \wedge d_1) \vee \cdots \vee (a \wedge d_k) \vee e_1 \vee \cdots \vee e_s]$$

which is in normal form by Lemma 10. Hence any term shorter than $x \wedge w$, which has an endomorphism onto $x \wedge w$, is in normal form and so cannot be the left hand side of a rewrite rule. Thus no rewrite rule applies to $x \wedge w$. □

An Extension

By a terminating AC TRS, we mean one in which every sequence of rewritings ends in a *terminal* element in a finite number of steps. Recall that a term u is terminal if no rewrite rule applies to it nor to any $u' \equiv u$. Suppose we weaken this notion by defining u to be terminal if, for all $u' \equiv u$, if u' rewrites to v, then $v \equiv u$. (We would also have to modify the requirement on sequences as in (1) by insisting that, when $s_i \rightarrow_R s_{i+1}$, we have $s_i \not\equiv s_{i+1}$.) Does Theorem 11 still hold for such a system? In most parts of the proof we produced an infinite chain of rewrites with terms of increasing length. For example, the proof of the first part of Lemma 8 constructed certain subterms. A closer look at the proof shows that these are proper subterms and this implies that rewriting will produce longer and longer terms. Since AC equivalence classes are finite, such sequences cannot exist even with our modified definition of a terminal element. The proof that $x \equiv s$ showed that if this failed, we could rewrite $x \vee w'$ to $s' \vee w'$ and then rewrite the latter back to $x \vee w'$. Since x is only AC equivalent to itself, this also leads to an infinite chain of rewrites even under our modified definition of a terminal element. However, part (3) of Lemma 1 is no longer valid. The only places where it is not obvious that the use of this cannot be avoided are in the proof that the terms given in (6) and (7) of Lemma 10 are in normal form. To see that they are, note by Lemma 9,

$$\mathrm{nf}((x \wedge z_1) \vee \cdots \vee (x \wedge z_n)) = r_1(x, z_1, \ldots, z_n) \vee \cdots \vee r_n(x, z_1, \ldots, z_n),$$

for some $r_1, \ldots, r_n$. This rewrite rule applies to the element of (5) to yield

$$(x \wedge \underline{z}_1) \vee \cdots \vee (x \wedge \underline{z}_n) \to r_1(x, \underline{z}_1, \ldots, \underline{z}_n) \vee \cdots \vee r_n(x, \underline{z}_1, \ldots, \underline{z}_n).$$

Since the left side is in normal form, this implies that (by our new rule for rewriting) these terms are AC equivalent, and so, after renumbering, $x \wedge \underline{z}_i \equiv r_i(x, \underline{z}_1, \ldots, \underline{z}_n)$. But it is easy to see that this implies that $r_i(x, z_1, \ldots, z_n) = x \wedge z_i$ or $z_i \wedge x$, which implies the element (6) is in normal form.

To see that the element of (7) is in normal form, it suffices, by the dual of Lemma 8, to show that $w = \bigvee_{i=1}^{k}(x \wedge z_i) \vee \bigvee_{j=1}^{s} e_j$ is in normal form. By Lemma 7, we may assume the normal form of this element is $r_1 \vee \cdots \vee r_m$, where each r_i is either a meet or a variable and $m \leq k + s$. Choose $n > k + s$. Then there is an endomorphism σ mapping w to $\bigvee_{i=1}^{n}(x \wedge z_i)$ and this induces the rewrite:

$$\bigvee_{i=1}^{n}(x \wedge z_i) \to \sigma(r_1) \vee \cdots \vee \sigma(r_m).$$

Since the left side is in normal form, these two elements must be AC equivalent. If r_i is a meet then $\sigma(r_i)$ is also. Thus, since $n > m$, some of the r_i's must be variables. But, by Lemma 7, each r_i must satisfy either $x \wedge z_j \leq r_i < w$ or $e_j \leq r_i < w$, for some j. This implies that if r_i is a variable, it must be some e_j. If r_i is not a variable, then, since $\sigma(r_i) = x \wedge z_j$, for some j, $r_i = x \wedge z_j$. It is not hard to see that implies that w is in normal form.

Thus, even under this weaker set of rules for rewriting, there is no finite, convergent AC TRS for lattices.

Final Remarks

As we mentioned earlier, Peterson and Stickel have shown that the equational theory of distributive lattices does have a convergent AC TRS. However deciding if an equation is true in all distributive lattices is harder than deciding if it is true in all lattices. To make this more precise, we define the *term equivalence problem*, denoted TEP, for a class $\mathcal{K}$ of lattices. An instance of this problem is given two terms u and v (in the language of lattices) and asks if the equation $u \approx v$ holds in every lattice in $\mathcal{K}$. As we indicated earlier, when $\mathcal{K}$ is the class of all lattices, the TEP is polynomial time.[1] On the other hand, P. Bloniarz, H. B. Hunt, and D. Rosenkrantz have shown that the TEP for the class of distributive lattices is co–NP complete. In fact, they show that the TEP for $\mathcal{K} = \{\mathbf{L}\}$ is co–NP complete for any finite, nontrivial lattice $\mathbf{L}$. (This includes the result on distributive lattices, since the equational theory of distributive lattices is the same as that of the two element lattice.) The class of modular lattices lies properly between the class of distributive lattices and the class of all lattices. Modular lattices are usually defined by an implication, but can be defined by (the lattice axioms and) the equation

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

[1] It is interesting that the first polynomial time algorithm for this goes back to Thoralf Skolem (1920).

The equational theory of the class of modular lattices was shown to be undecidable by Freese (1980).

Using more involved lattice theory, we have been able to show that certain varieties of lattices generated by a finite lattice have AC TRS's. These results will appear in our monograph *Free Lattices* (1993).

References

P. Bloniarz, H. B. Hunt III, and D. Rosenkrantz (1987), *On the computational complexity of algebra on lattices*, Siam J. Computing **16**, 129–148.

S. Burris and J. Lawrence (1991), *Term rewrite rules for finite fields*, International J. of Algebra and Computation **1**, 353–369.

N. Dershowitz and J.-P. Jouannaud (1990), *Rewrite systems*, Handbook of Theoretical Computer Science, Vol B: Formal Models and Semantics (J. van Leeuwen, ed.), Elsevier, Amsterdam–New York, pp. 245–320.

N. Dershowitz, J.-P. Jouannaud, and J. W. Klop (1991), *Open problems in rewriting*, Rewriting Techniques and Applications (R. V. Book, ed.), Lecture Notes in Computer Science, **488**, Springer-Verlag, Berlin, pp. 443–456.

T. Evans (1951), *On multiplicative systems defined by generators and relations,* I, Proc. Cambridge Philos. Soc. **47**, 637–649.

R. Freese (1980), *Free modular lattices*, Trans. Amer. Math. Soc. **261**, 81–91.

R. Freese (1987), *Free lattice algorithms*, Order **3**, 331–344.

R. Freese, J. Ježek, and J. B. Nation (1993), *Free Lattices.*

R. Freese and J. B. Nation (1985), *Covers in free lattices*, Trans. Amer. Math. Soc. **288**, 1–42.

J. Ježek (1982), *Free groupoids in varieties determined by a short equation*, Acta Univ. Carolin.-Math. Phys. **23**, 3–24.

J.-P. Jouannaud and H. Kirchner (1986), *Completion of a set of rules modulo a set of equations*, Siam J. Comput. **15**, 1155–1194.

D. E. Knuth and P. B. Bendix (1970), *Simple word problems in universal algebra*, Computational Problems in Abstract Algebra, Pergamon, Oxford, pp. 263–297.

D. S. Lankford and A. M. Ballantyne (1977), *Decision procedures for simple equational theories with commutative-associative axioms: Complete sets of commutative-associative reductions*, Research Report Memo ATP-39, Department of Mathematics and Computer Science, University of Texas, Austin, Texas.

G. E. Peterson and M. E. Stickel (1981), *Complete sets of reductions for some equational theories*, J. Assoc. Comput. Mach. **28**, 233–264.

T. Skolem (1920), *Logisch-kombinatorische Untersuchungen über die Erfüllbarkeit und Beweisbarkeit mathematischen Sätze nebst einem Theoreme über dichte Mengen*, Videnskapsselskapets skrifter I, Matematisk-naturvidenskabelig klasse, Videnskabsakademiet i Kristiania **4**, 1–36.

S. T. Tschantz (1990), *Infinite intervals in free lattices*, Order **6**, 367–388.

Ph. M. Whitman (1941), *Free lattices*, Ann. of Math. (2) **42**, 325–330.

Ph. M. Whitman (1942), *Free lattices* II, Ann. of Math. (2) **43**, 104–115.

E-mail addresses: ralph@math.hawaii.edu, jarda@math.hawaii.edu, jb@math.hawaii.edu