UNIVERSITÄT AUGSBURG

Deriving Tableau-Based Solutions to Lattice Word Problems

Georg Struth

Report 2003-12 August 2003

INSTITUT FÜR INFORMATIK
D-86135 AUGSBURG

Deriving Tableau-Based Solutions to Lattice Word Problems *

Georg Struth

Institut für Informatik, Universität Augsburg
Universitätsstr. 14, D-86135 Augsburg, Germany
{struth@informatik.uni-augsburg.de

Abstract We derive tableau calculi as solutions to the word problem for the free semilattice, the free distributive lattice and the free boolean lattice with a new method introduced in [13]. The method uses ordered resolution as a logical framework. The theory-specific and procedural information about the goal, the subformula property, is encoded via the ordering. Completeness of the calculi follows from correctness of their construction. Besides demonstrating the power of the derivation method, our formal reconstruction of tableaux also concerns the algebraic foundations of tableau and sequent calculi, in particular the connection of distributivity with the data-structure of sequents and with cut-elimination.
Keywords: automated deduction, lattice theory, ordered resolution, theory resolution, tableaux, sequent calculus.

1 Introduction

Applicability of logic in computer science often crucially depends on the integration of domain-specific knowledge into focused calculi. In [13], a new two-step method for deriving theory-specific inference rules for ordered resolution has been proposed. First, a theory specification is closed under the ordered resolution calculus, eliminating redundant expressions on the fly. This resolution basis satisfies an independence property: Inferences among its members are superfluous in all refutations. Thus part of the search complexity has been shifted from run time to compile time. Second, the patterns arising in refutations from inferences between non-theory clauses and members of the resolution basis are turned into derived inference rules. The calculi constructed this way are complete, if their construction is correct. This method is in contrast with previous approaches [7,1], where inference rules had to be guessed and justified a posteriori in model-theoretic completeness proofs. In [13], the method has been exemplified by an ordered chaining calculus for transitive relations. In [14], chaining calculi for various lattices have been developed, in particular, an ordered resolution calculus at the lattice level as a solution to the uniform word problem for distributive lattices, thus further formalizing a result from [12].

* This research was sponsored by DFG Project InopSys — Interoperability of Calculi for System Modelling

Here, we use this method for developing tableau-like calculi as solutions to the word problems for free semilattices, distributive lattices and boolean lattices. This is the problem to decide whether an equality $s \approx t$ between (semi)lattice terms holds for every member of the respective algebraic class, or in our context, whether the empty clause is derivable from the clause $(s \not\leq t) \vee (t \not\leq s)$ and the respective theory axioms. Our emphasis is however not mainly on the tableau calculi, but on the method behind them and the proof-theoretic insights of their formal reconstruction. Theory-specific information enters the development of the calculi mainly by refining the syntactic ordering of ordered resolution. In [13], to derive resolution-like rules, we built the ordering around multisets as the natural data-structures for clauses. Here, in order to derive tableau-like rules, we encode the subformula property.

Besides demonstrating the naturalness and power of the development method, several other features are also interesting. First, the correspondence between lattice-theoretic problems and logical calculi, such as sequent calculi and tableaux, are developed in a formal way, in particular that between specifications of least upper and greatest lower bounds and disjunction and conjunction rules of the sequent calculus[1]. Second, our algebraic treatment of distributivity explains the role of the data-structure of sequents and the cut rule in the sequent calculus. Third, our construction yields an algebraic completeness proof of propositional tableaux and shows that it is a decision procedure. Fourth we formally demonstrate that the rules of the sequent calculus are in fact independent.

In the present text, we can only sketch some proofs. A full formal treatment can be found in [11]. We also presuppose knowledge on tableau and sequent calculi (for our purposes, we identify tableaux with cut-free sequent calculi). See [9,5] for introductions.

The remaining text is organized as follows. Section 2 and section 3 introduce some basic facts about ordered resolution and lattices. Section 4 defines the syntactic orderings for our tableau calculi, section 5 the calculi themselves. Section 6 contains the first step of th derivation of tableau rules: the computation of the resolution basis. Section 7 contains the second step: the derivation of the inference rules. Section 8 discusses the proof-theoretic implications of our results; section 9 contains a conclusion.

2 Ordered Resolution

Let $T_\Sigma(X)$ be a set of terms with signature Σ and variables in X. Let P be a set of predicates. The set A of *atoms* consists of all expressions $p(t_1, \ldots, t_n)$, where p is an n-ary predicate and $t_1, \ldots, t_n$ are terms. A *clause* is an expression $\{\!|\phi_1, \ldots, \phi_m|\!\} \longrightarrow \{\!|\psi_1, \ldots, \psi_n|\!\}$. Its *antecedent* $\{\!|\phi_1, \ldots, \phi_m|\!\}$ and *succedent* $\{\!|\psi_1, \ldots, \psi_n|\!\}$ are finite multisets of atoms. Antecedents are schematically denoted by Γ, succedents by Δ. Brackets will usually be omitted. A *Horn clause* contains at most one atom in its succedent.

[1] This correspondence already appears in Whitman's solution to the word problem for the free lattice [15].

Definition 1 (Ordered Resolution Calculus). *Let $\prec$ be a well-founded ordering on atoms that is total on ground terms. The* ordered resolution calculus OR *consists of the deduction inference rules*

$$\frac{\Gamma \longrightarrow \Delta, \phi \qquad \Gamma', \psi \longrightarrow \Delta'}{\Gamma\sigma, \Gamma'\sigma \longrightarrow \Delta\sigma, \Delta'\sigma}, \quad \text{(Res)} \qquad \frac{\Gamma \longrightarrow \Delta, \phi, \psi}{\Gamma\sigma \longrightarrow \Delta\sigma, \phi\sigma}. \quad \text{(Fact)}$$

Thereby σ is a most general unifier of ϕ and ψ. In the ordered resolution rule (Res), $\phi\sigma$ is strictly maximal according to $\prec$ in the σ-instance of the first and maximal in that of the second premise. In the ordered factoring rule (Fact), $\phi\sigma$ is maximal in the σ-instance of the premise.

In all inference rules, *side formulas* are the parts of clauses denoted by capital Greek letters. Atoms occurring explicitly in the premises are called *minor formulas*, those in the conclusion *principal formulas*.

Let S be a clause set. Let $\mathsf{cl}_{\models}(S)$ and $\mathsf{cl}_{\mathsf{OR}}(S)$ denote the set of (semantic clausal) consequences of S and the set of clauses derivable in OR from S. A clause C is *$\prec$-redundant* or simply redundant in S, if $C \in \mathsf{cl}_{\models}(C_1, \ldots, C_k)$ for some $S \ni C_1, \ldots, C_k \prec C$. Elimination of redundant clauses from S during the iterative application of OR-rules changes $\mathsf{cl}_{\mathsf{OR}}(S)$, but preserves semantic consequences. We denote this operation of OR-*closure modulo* $\prec$-redundancy elimination by $\mathsf{cl}^{mod}_{\mathsf{OR}}$. It induces a basis transformation from S to a *resolution basis* $S' = \mathsf{cl}^{mod}_{\mathsf{OR}}(S)$. This transformation need not terminate, but all fair OR-strategies derive the empty clause within finitely many steps from an inconsistent S. The basis S' is special. By definition it satisfies the independence property that all conclusions of *primary S'-inferences*, that is OR-inferences with both premises from S', are redundant.

Proposition 1. *(i) If S is inconsistent, then S' contains the empty clause.*
(ii) Let S' be consistent and T a clause set such that $S' \cup T$ is inconsistent. There is a OR-refutation without primary S'-inferences.

By proposition 1 (ii), resolution bases allow set-of-support-like ordered resolution strategies[2]. The computation of a resolution basis will constitute the first step of our derivation of tableaux. For more information consider [11,13].

3 Lattices

Since we are investigating word problems for free lattices, we can restrict our signatures and predicates. $\Sigma = \{\vee, \wedge\}$ and $P = \{\leq\}$. $\vee$ and $\wedge$ are varyadic operation symbols for the lattice join and meet operations; $\leq$ is a binary predicate symbol denoting a *quasiordering*—a reflexive transitive relation. A *join semilattice* (*meet semilattice*) is a quasi-ordered set closed under least upper bounds or joins (greatest lower bounds or meets) for all pairs of elements. Join and meet

[2] According to the set of support strategy for unordered resolution, inferences among a consistent part of a clause set are superfluous in refutations [16].

semilattices are duals. *Lattice duality* means exchange of joins and meets and inversion of the ordering. A *lattice* is both a join and a meet semilattice. It is *distributive*, if (cut) holds (see below)[3]. A quasiordering is axiomatized by the set $Q = \{(\text{ref}), (\text{trans})\}$, the join and meet semilattice by $J = Q \cup \{(\text{lub}), (\text{ub})\}$ and $M = Q \cup \{(\text{glb}), (\text{lb})\}$, a lattice by $L = J \cup M$, a distributive lattice by $D = L \cup \{(\text{cut})\}$. Thereby

$$
\begin{array}{llll}
 & \longrightarrow x \leq x \quad (\text{ref}) & x \leq y, y \leq z \longrightarrow x \leq z & (\text{trans}) \\
\longrightarrow x \wedge y \leq x & \longrightarrow x \wedge y \leq y \quad (\text{lb}) & x \leq y, x \leq z \longrightarrow x \leq y \wedge z & (\text{glb}) \\
\longrightarrow x \leq x \vee y & \longrightarrow y \leq x \vee y \quad (\text{ub}) & x \leq z, y \leq z \longrightarrow x \vee y \leq z & (\text{lub})
\end{array}
$$

$$
x_1 \leq y_1 \vee z, x_2 \wedge z \leq y_2 \longrightarrow x_1 \wedge x_2 \leq y_1 \vee y_2 \qquad (\text{cut})
$$

For a quasiordering, joins and meets are unique up to the congruence $\sim\, = (\leq \cap \geq)$. Semantically, $\leq/\sim$ is a partial ordering, hence an antisymmetric quasiordering ($x \leq y, y \leq x \longrightarrow x = y$). Operationally, the only role of antisymmetry is splitting equalities into inequalities. We can therefore disregard it. Joins and meets are associative, commutative, idempotent ($x \wedge x = x = x \vee x$) and monotonic in the associated partial ordering. We will henceforth consider all inequalities modulo associativity and commutativity. See [3] for further information on lattices. The similarities between the rules in J, M, D and those of the sequent or tableau calculus are already quite apparent. (glb) and (lub) are similar to the right conjunction and left disjunction rule, (cut) is evident.

Let K be some variety of lattices. The *word problem* for K is the following: Determine, if some identity or *query* $s \approx t$ over some set of constants (or generators) in the language for K holds for every member of K. In particular, since K contains a free algebra A, it suffices to show $s \approx t$ in A, because if it holds there, it holds for every member in K automatically. Cum grano salis we use the notion *word problem* also for inequalites: in lattice theory, every inequality can be written as an equality: $s \leq t$ iff $s \vee t = t$ iff $s \wedge t = s$. Here, we want to use ordered resolution for solving lattice theoretic word problems. Then, the query Q is a ground clause $s \approx t \longrightarrow$ or $s \leq t, t \leq s \longrightarrow$ with empty succedent. But so far, proposition 1 only guarantees a semi-decision procedure: Whenever Q does not hold in the respective free algebra, there is a OR-refutation from Q and the respective theory axioms. But if Q holds, then the OR-closure can still be infinite.

Lemma 1. *All* OR*-proofs from queries* $Q = \Gamma \rightarrow$ *and* D *have the following properties.*

(i) The OR*-rule (Fact) is never applicable.*
(ii) All conclusions except of primary theory inferences are of the form $\Gamma' \rightarrow$ *(with* Γ' *possibly empty).*

[3] A non-standard axiomatization similar to this one has been used already in [8]. See [11] for a proof of equivalence with the standard one. See [12] for a discussion on its relevance to lattice-word problems and resolution.

(iii) The final resolution step in a refutation uses always (ref).

This is obvious from the structure of the query and the clauses in D. To obtain a decision procedure, is suffices that Q is maximal in $\mathsf{cl}^{mod}_{\mathsf{OR}}(\{Q\} \cup T)$, where T is one of J, M or D and the number of ground clauses smaller than Q is finite. Let G be a finite set of generators. The free semilattice, distributive lattice and boolean lattice generated by G are finite (c.f [3]). Thus for every term over G the number of smaller terms generated by G is finite. Therefore we obtain decidability, if we can specialize the ordered resolution inferences such that all conclusions are smaller than the maximal premises (which in our situation is always Q). As a consequence, no rule may introduce a fresh variable. These properties must be enforced by an appropriate syntactic ordering. This is the purpose of the following section.

4 Syntactic Orderings for Semilattices and Distributive Lattices

There is a natural syntactic ordering for the sequent calculus: any ordering enforcing the subformula property. In our lattice theoretic context this is any AC-compatible simplification ordering[4]. One can for instance choose an AC-compatible ordering with a precedence in which the join and meet operation are maximal and identical. Let $\prec$ be such an ordering. Let $\mathbb{B}$ be the two-element boolean algebra with ordering $<_{\mathbb{B}}$. Let $M = G \times \mathbb{B} \times \mathbb{B} \times G$, where G denotes a multiset of generators. Let A be a set of atoms occurring in some clause $C = \Gamma \longrightarrow \Delta$. The ordering $\prec_1 \subseteq M \times M$ is the lexicographic combination of $\prec$ for the first and last component of M and $<_{\mathbb{B}}$ for the others. A ground *atom measure* (for clause C) is the mapping $\mu_C : A \longrightarrow M$ defined by $\mu_C : \phi \mapsto (t_\nu(\phi), p(\phi), s(\phi), t_\mu(\phi))$ for each (ground) atom $\phi \in A$ occurring in C. Hereby $t_\nu(\phi)$ ($t_\mu(\phi)$) denotes the maximal (minimal) term with respect to $\prec$ in ϕ. $p(\phi) = 1$ ($p(\phi) = 0$), if ϕ occurs in Γ (in Δ). $s(\phi) = 1$ ($s(\phi) = 0$), if $\phi = s < t$ and $s \succeq t$ ($s \prec t$). The (ground) *atom ordering* $\prec_2 \subseteq A \times A$ is defined by $\phi \prec_2 \psi$ iff $\mu_C(\phi) \prec_1 \mu_C(\psi)$ for $\phi, \psi \in A$. Hence $\prec_2$ is embedded in $\prec_1$ via the atom measure. The ordering $\prec_1$ is total and well-founded by construction. Via the embedding, $\prec_2$ inherits these properties. See [13] for a motivation of the components arising in a similar ordering. Intuitively, the role of the syntactic ordering is precisely to enforce that all non-theory clauses are split into clauses containing only subterms by the clauses in D. This enforces the subformula property of the sequent calculus.

As free variables are implicitly universally quantified, the orderings $\prec$, $\prec_1$ and $\prec_2$ are lifted to the non-ground case, defining the ordering $\prec' \subseteq T_\Sigma(X) \times T_\Sigma(X)$ by $s \prec' t$ iff $s\sigma \prec t\sigma$ for all ground substitutions σ. Defining $\prec_1'$ and $\prec_2'$ is then

[4] Roughly, an ordering is AC-compatible, if it respects AC-equivalence classes. Orderings that are appropriate for our purposes exist [2,4]. A simplification ordering in particular contains the subterm ordering: Every term is greater than all of its subterms.

obvious. These orderings are still well-founded, but need no longer be total. In particular, $s \not\preceq t$ if $t\sigma \succ s\sigma$ for some ground terms $s\sigma$ and $t\sigma$. Atom measure and ordering are extended to clauses, measuring clauses as multisets of their atoms and using the multiset extension of the atom orderings. The clause ordering on ground clauses inherits totality and well-foundedness from the atom ordering. Again, the non-ground extension need not be total. In unambiguous situations we will denote all orderings by $\prec$.

Note that the definition of $\prec$ is still not sufficient to show that OR with D is a decision procedure. The problem are the primary theory inferences. Hence we still must transform D into a resolution basis. This is the subject of section 6. But first, we present our tableau calculi.

5 The Tableau Calculi

Definition 2 (Distributive Lattice Tableau). *Let $\prec$ be the atom and clause ordering of section 4. The* tableau calculus for (finite) distributive lattices DT *consists of the following inference rules.*

$$\frac{\Gamma, x \leq x \longrightarrow}{\Gamma \longrightarrow}, \qquad \text{(Ref)}$$

$$\frac{\Gamma, x \leq y \wedge z \longrightarrow}{\Gamma, x \leq y, x \leq z \longrightarrow}, \quad \text{(MR)} \qquad \frac{\Gamma, x \vee y \leq z \longrightarrow}{\Gamma, x \leq z, y \leq z \longrightarrow}, \quad \text{(JL)}$$

$$\frac{\Gamma, x \leq w \vee (y \wedge z) \longrightarrow}{\Gamma, x \leq w \vee y, x \leq w \vee z \longrightarrow}, \quad \text{(EMR)} \qquad \frac{\Gamma, w \wedge (x \vee y) \leq z \longrightarrow}{\Gamma, w \wedge x \leq z, w \wedge y \leq z \longrightarrow}, \quad \text{(EJL)}$$

$$\frac{\Gamma, x \wedge y \leq z \longrightarrow}{\Gamma, x \leq z \longrightarrow}, \quad \text{(ML)} \qquad \frac{\Gamma, x \leq y \vee z \longrightarrow}{\Gamma, x \leq z \longrightarrow}. \quad \text{(JR)}$$

In all rules, the minor formula is maximal in the premise. All rules are meant modulo associativity, commutativity and idempotence.

(Ref) stands for *reflexivity*, (MR) for *meet right*, (EMR) for *extended meet right*, (ML) for *meet left*, (JL) for *join left*, (EJL) for *extended join left*, (JR) for *join right*. The respective join and meet rules are completely dual. There is no variant of a cut rule (c.f. section 7 for an explanation). Note also the correspondence with tableau or sequent calculus rules. See finally section 8 for a discussion of the role of (EJL) and (EMR).

Definition 3 (Semilattice Tableaux). *Under the conditions of definition 2, the deduction inference rules of the* tableau calculi JT and MT for the join and meet semilattice *arise as restrictions of the* DT*-rules to join and meet semilattice terms (c.f. [11] for explicit rules).*

Thus in particular, JT consists solely of variants of the rules (JL) and (JR), MT of variants of (ML) and (MR). JT and MT are dual and of course one can use JT also for the meet semilattice, dualizing meet semilattice inequalities.

6 Construction of the Resolution Bases

We now perform the first step of the derivation of the tableau calculi. Our theories are J, M and D. With the orderings of section 4, we compute the respective resolution bases; the OR-closures modulo redundancy elimination. Use of duality prevents us from repetitions.

We first assign indices to clauses to determine their orientation with respect to $\prec$: i (increasing), if the antecedent is smaller than the succedent, d (decreasing), if the converse holds and ? if the clause can only be oriented instance wise. Note that all clauses in J, M and D are indexed by i, except (trans) and (cut), which are indexed by ?.

Consider now the Horn clauses

$$x \leq w \vee y, x \leq w \vee z \longrightarrow_i x \leq w \vee (y \wedge z), \qquad \text{(emr)}$$

$$x \leq y \wedge z \longrightarrow_d x \leq y, \qquad \text{(imr)}$$

$$x \leq w \vee (y \wedge z) \longrightarrow_d x \leq w \vee y, \qquad \text{(eimr)}$$

$$x \leq z \longrightarrow_i x \wedge y \leq z \qquad \text{(ml)}$$

and their duals (ejl), (ijl), (eijl) and (jr). Let

$$J' = \{(\text{ref}), (\text{lub}), (\text{imr}), (\text{ml}), (\text{cut})\}, \qquad M' = \{(\text{ref}), (\text{glb}), (ijl), (jr), (\text{cut})\},$$
$$D' = J' \cup M' \cup \{(\text{emr}), (\text{eimr}), (ejl), (eijl), (\text{cut})\ \}.$$

Thereby, restricted variants of (cut), for instance $x_1 \leq z, x_2 \wedge z \leq y_2 \longrightarrow x_1 \wedge x_2 \leq y_2$ occur in M' and J'. Moreover, (trans) is a restriction of these (cut) rules, forgetting the lattice term structure. Now—up to the extended rules (ejl), (eijl), (emr) and (eimr)—all rules are reminiscent to those in the sequent calculus. The inverse rules (imr) and (ijl) also hold in the sequent calculus by the inversion lemma (they are derivable with and admissible without the cut rule [9]). The extended rules are combinations of the non-extended rules and monotonicity of join and meet. They also encode the effect of distributivity. See section 8 for further discussion.

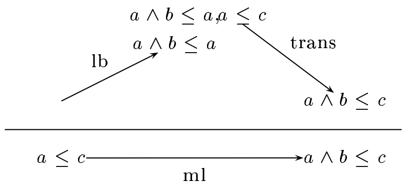
Lemma 2. *Let $\prec$ be the atom ordering defined in section 4.*

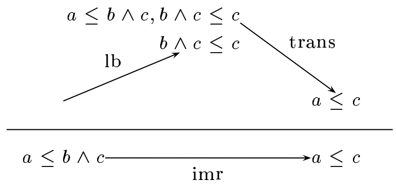
(i) M' is a resolution basis for the meet semilattice.
(ii) J' is a resolution basis for the join semilattice.
(iii) D' is a resolution basis for the distributive lattice.

We always implicitly normalize with respect to idempotence of join and meet and consider terms modulo associativity and commutativity.

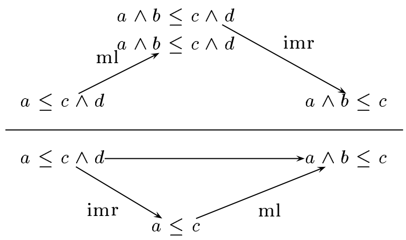
Proof. The proofs consist of three steps. First, we orient the rules in J, M and D with respect to $\prec$. Second, we derive the rules in J', M' and D' in OR. Third, we show that all conclusions of primary theory inferences in OR with respect to J', M' and D' are redundant. Here, we show only some inferences. The complete case analysis is beyond the scope of this paper. It can be found in [11].

(ad i). As an example we show the derivation of (ml) and (imr).





Having derived the clauses in M', it remains to show that their resolvents are redundant. An example, the inference between (ml) and (imr), is depicted in the following diagram.



The upper part of the diagram is the resolution step, the lower part shows a smaller proof using (imr) and (ml) also yielding the resolvent. In a similar way, most other resolvents can be shown to be redundant. There are however a few irredundant resolvents between members in M'. Consider, for instance, the inference

$$\frac{\longrightarrow_i a \wedge c \leq a \wedge c \quad a \leq b, c \wedge b \leq c \wedge b \longrightarrow_d a \wedge c \leq b \wedge c}{a \leq b \longrightarrow_i a \wedge c \leq b \leq c}$$

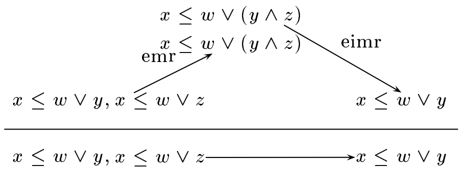
between (irr) and (cut), that yields monotonicity of meet. But (ml) yields $\rightarrow a \wedge c \leq b$ and $\rightarrow a \wedge c \leq c$ from $\rightarrow a \leq b$ and from $\rightarrow c \leq c$, that is (ref). Using (glb), we obtain $a \wedge c \leq b \wedge c$ from these rules. Thus we can prove the monotonicity clause already using (ml), (glb) and (ref). All these rules are indexed also with i. Therefore in every proof, an inference using the monotonicity rule can be replaced by a a monotonic subproof with members of M' and the monotonicity can be discarded. For further details see [11].

(ad ii) This follows from (i) by duality.

(ad iii) As in the example in (i), the rules of D' are derived from the interaction between the rules in M', J' and (cut). (eimr), for instance, is derived from (ml) and (cut) as follows.

$$\frac{\longrightarrow_i y \wedge z \leq y \qquad x \leq w \vee (y \wedge z), y \wedge z \leq y \longrightarrow_d x \leq w \vee y}{x \leq w \vee (y \wedge z) \longrightarrow x \leq w \vee y}.$$

Having derived the clauses in D', it again remains to show that their resolvents are redundant. The resolution step between (emr) and (eimr), for instance, is shown in the diagram



The resolvent is a tautology. The remaining steps are similar. □

Proposition 1 (ii) and lemma 2 immediately imply the following fact, which is essential for the arguments in the following section.

Corollary 1. *For every inconsistent clause set containing J', M' or D' there exists a refutation without primary theory inferences.*

Continuing our discussion at the end of section 3 and section 4, we still have no solution to the word problem for the free distributive lattice or join and meet semilattice, since resolution inferences with (cut) introduce new variables (remind that (cut) is indexed with ?) and leads to non-monotonic proofs. This is analogous to the sequent calculus, where propositional decidability depends on cut elimination. We will show an algebraic variant in the following section.

7 Deriving the Tableau Rules

We now derive the inference rules of DC from OR-derivations with D'. Our main assumptions are refutational completeness of OC (theorem 1) and the fact that our ordering constraints rule out primary theory inferences (corollary 1).

Theorem 1. *The tableau calculus* DT *solves the word problem for the free distributive lattice: For every query $s \leq t \rightarrow$, such that $s \leq t$ holds in the free distributive lattice, there exists a refutation in* DT.

Proof. We consider a refutation of a query $Q = s \leq t \rightarrow$, s and t lattice terms in presence of the members of D'. By corollary 1, there are no primary theory inferences. Moreover, by lemma 1 (ii), all non-theory clauses that may occur in $\mathsf{cl}_{\mathsf{OR}}^{mod}(Q \cup D')$ have empty succedent. We can therefore restrict our attention to non-theory clauses of this form. Since Q and all clauses in D' are Horn, it suffices to consider ordered resolution inferences between members of D' and non-theory clauses. Ordered factoring steps can be disregarded.

(case i) Resolution of a clause $\Gamma, a \leq a \longrightarrow$ and (ref) is

$$\frac{\longrightarrow a \leq a \qquad \Gamma, a \leq a \longrightarrow}{\Gamma \longrightarrow},$$

where, due to the constraints of ordered resolution, the inequality $a \leq a$ majorizes Γ. Internalizing (ref) immediately yields the rule (Ref).

(case ii) Resolution of a clause $\Gamma, a \leq b \wedge c \longrightarrow$ and (glb) is

$$\frac{a \leq b, a \leq c \longrightarrow a \leq b \wedge c \qquad \Gamma, a \leq b \wedge c \longrightarrow}{\Gamma, a \leq b, a \leq c \longrightarrow},$$

where $a \leq b \wedge c$ is maximal in the right-hand premise. Internalizing (glb) immediately yields (MR). The fact that in this rule the left-hand side of a sequent is split shows the necessity to consider a non-empty Γ.

(case iii) Resolution of a clause $\Gamma, a \leq b \vee (c \wedge d) \longrightarrow$ and (emr) is

$$\frac{a \leq b \vee c, a \leq b \vee d \longrightarrow a \leq b \vee (c \wedge d) \qquad \Gamma, a \leq b \vee (c \wedge d) \longrightarrow}{\Gamma, a \leq b \vee c, a \leq b \vee d \longrightarrow},$$

where $a \leq b \vee (c \wedge d)$ is maximal in the right-hand premise. This yields (EMR).

(case iv) The antecedent of (imr) is greater than the succedent according to $\prec$ and never satisfies the ordering constraints of ordered resolution with a clause with empty succedent. Therefore it does not contribute an inference rule.

(case v) For (eimr), the situation is analogous to (case iv).

(case vi) Resolution of a clause $\Gamma, a \wedge b \leq c \longrightarrow$ and (ml) is

$$\frac{a \leq c \longrightarrow_S a \wedge b \leq c \qquad \Gamma, a \wedge b \leq c \longrightarrow}{\Gamma, a \leq c \longrightarrow},$$

where $a \wedge b \leq c$ is maximal in the right-hand premise. This yields (ML).

(case vii) to (case xi), yielding the inference rules (JL), (EJL) and (JR) from the clauses (lub), (ejl), (ijl), (eijl) and (jr) are dual to (case ii) to (case vi).

(case xii) Resolution of a query $\Gamma, a \wedge b \leq c \vee d \longrightarrow$ with (cut) is

$$\frac{a \leq c \vee e, b \wedge e \leq d \longrightarrow a \wedge b \leq c \vee d \qquad \Gamma, a \wedge b \leq c \vee d \longrightarrow}{\Gamma, a \leq c \vee e, b \wedge e \leq d \longrightarrow}.$$

We show by induction on the distance from such an inference to the empty clause and the *cut rank* of the lattice term, that is the size of the minor term which is cut out, that this inference is not needed. In proof-theoretic terms we show a version of cut elimination. Since the proof is standard we give only a sketch and refer to [6,9] for details. In particular, for simplicity, we assume that $c = 0$.

(case α) Let e be a generator. Then $a \leq e$ must be of the form $a' \wedge e \leq e$ and in particular $b \wedge e \leq d$ must either be of the form $b' \wedge d \wedge e \leq d$ or $d = e$ such that $b \wedge d \leq d$ in order to eliminate both these inequalities from the conclusion. So also $a \wedge b \leq d$ either is of the form $a' \wedge b \wedge d \leq d$ or of the form $a \wedge b' \wedge d \leq d$ and already the minor formula of the right-hand premise can be eliminated using (ML) and (Ref).

(case β) Let $e = e_1 \wedge e_2$. Then we may assume that (MR) has been applied to the inequality $a \leq e_1 \wedge e_2$, which transforms the conclusion of the above inference into $\Gamma, a \leq e_1, a \leq e_2, b \wedge e_1 \wedge e_2 \leq c \longrightarrow$. Using the induction hypothesis we can then argue that this sequent has been obtained from the right-hand premise of the above inference by two smaller cuts, respecting the ordering constraints. Hence in any case the above inference is not needed.

Since we have considered all clauses from D' and all these clauses produce conclusions with empty succedent, we have computed a refutationally complete set of inference rules for a negative query Q. The inference rules yield a decision procedure, since the calculus has the sub-formula (or lattice sub-term) property. Only the constants in Q occur in the refutation. □

Corollary 2. *The tableau calculi* JT *and* MT *solve the word problem for the free join and meet semilattice.*

The following corollary expresses a simple refinement of our tableau calculus.

Corollary 3. *Under the assumptions of theorem 1, the rule (Ref) can be restricted to generators.*

This holds, since by structural induction, all inequalities $s \leq s \longrightarrow$ can be transformed to a clause $x_1 \leq x_1, \ldots, x_n \leq x_n \longrightarrow$ with $x_i \in X$ by the rules of theorem 1. A restriction of (Ref) to generator can then be used for the reduction to the empty clause.

The extension of theorem 1 from distributive to boolean lattices is also straightforward.

Corollary 4. *In a lattice with* 0 *and* 1*, let* x' *denote the complement of* x*, that is* $x' \vee x = 1$ *and* $x' \wedge x = 0$*. The rules of* DT *together with the rules*

$$\frac{\Gamma, x \wedge y' \leq z \longrightarrow}{\Gamma, x \leq y \vee z \longrightarrow}, \qquad \frac{\Gamma, x \leq y' \vee z \longrightarrow}{\Gamma, x \wedge y \leq z \longrightarrow},$$

for eliminating complements solve the reachability problem and the word problem for the free boolean lattice.

8 Discussion

Our solution to the word problem for the free distributive lattice used extended rules that do not occur in the sequent calculus or tableaux. These rules deal essentially with distributivity. The strategy of the sequent calculus, as opposed to this, is to introduce a layer of *sequents* between the layer of lattice terms and that of proofs. Consider, for instance, the following derivation in some variant of the cut-free sequent calculus. $\leq$ is now replaced by the sequent-arrow $\longrightarrow$ (both are quasi-orderings) and x, y and z are logical formulas.

$$\cfrac{\cfrac{x, y \vee z \longrightarrow x, z \qquad \cfrac{x, y \longrightarrow y, z \quad x, z \longrightarrow y, z}{x, y \vee z \longrightarrow y, z}}{x, y \vee z \longrightarrow x \wedge y, z}}{x \wedge (y \vee z) \longrightarrow (x \wedge y) \vee z}$$

Shifting formulas to sequents, the distributivity law is implicitly applied to multiply out terms and make the invertible conjunctive rules applicable, whereas the commata model the disjunctive ones. For a comparison, a proof in DT is

$$\cfrac{\cfrac{\cfrac{\cfrac{x \wedge (y \vee z) \leq (x \wedge y) \vee z \longrightarrow}{x \wedge (y \vee z) \leq x \vee z, x \wedge (y \vee z) \leq y \vee z \longrightarrow}\ \text{(EMR}}{x \wedge y \leq x \vee z, x \wedge z \leq x \vee z, x \wedge y \leq y \vee z, x \wedge z \leq y \vee z \longrightarrow}\ \text{(EJL)}}{x \leq x, x \leq x, y \leq y, z \leq z \longrightarrow}\ \text{(ML)(JR)}}{\longrightarrow}\ \text{(Ref)}$$

Algebraically, the cut rule of the sequent calculus is strongly connected with distributivity and transitivity, as we have seen. But in the sequent calculus, distributivity is already applied via the shift to the sequent level. In the free case, when there are no further relations between generators, it seems unnecessary to derive further consequences of relations (by analytic cut) or even invent completely fresh generators (by non-analytic cut). From the algebraic point of view, therefore, admissibility of cut in the sequent calculus seems quite natural. Our reconstruction supports this intuition with a formal argument. On the other hand, of course, in presence of relations between generators, further consequences of these relations must be computed, possibly using cut: In case of finitely presented distributive lattices, when further relations between generators exist, resolution steps using (cut) cannot in general be circumvented. On the contrary, it can be turned into the central ingredient of the calculus, as the chaining calculi for distributive lattices [14] show. This has a correspondence in the sequent calculus, where in presence of further axioms, cut is often unavoidable.

The tableau calculi given in this text are more focused than mere derivations with the axioms in J, M or D. For instance, a resolution inference with two instances of (trans) generates new variables, that might not be needed in a proof. In unordered resolution, strategies to avoid such kind of reasoning have already been given, for instance set of support or theory resolution [10]. But the transfer of these strategies to ordered resolution is non-trivial, as we have seen. Here, JT, MT or DT yields no advantage in efficiency over plain ordered resolution with the resolution bases J', M' and D', but without (cut), when primary theory inferences are forbidden by a priori (for instance by coloring clauses), instead of testing for redundancy a posteriori. However, the focused calculi encode the inferences in a more succinct way. In general, the specific inference rules can be much more effective than plain resolution with resolution bases (c.f. [13]).

9 Conclusion

We have used a new two-step method to synthesize propositional tableau calculi as solutions to lattice-theoretic word problems. In the first step, a resolution basis of the lattice axioms has been computed. The members of this basis are independent in the sense that resolution inferences among them are not needed in resolution proofs. In the second step, the interaction of the basis with queries of the word problem lead to tableau-like derived inference rules. In contrast to the standard tableau or sequent calculi, distributivity has not been included by introducing an additional data-structure of sequents, but by allowing certain splittings below contexts. We have seen that cut-rules naturally arise in lattice theory in presence of distributivity and that they can be eliminated in the free case, in absence of relations between generators to be propagated.

The synthesis of tableaux is only one of several applications of our method. We have already mentioned chaining calculi for for transitive relations, quasi-orderings, semilattices, distributive lattices and boolean lattices in [13,13]. A consideration of equational theories might be very interesting in the future.

References

1. L. Bachmair and H. Ganzinger. Rewrite-based equational theorem proving with selection and simplification. *J. Logic and Computation*, 4(3):217–247, 1994.
2. L. Bachmair and D. Plaisted. Termination orderings for associative-commutative rewriting systems. *J. Symbolic Computation*, 1(4):329–349, 1985.
3. G. Birkhoff. *Lattice Theory*, volume 25 of *Colloquium Publications*. American Mathematical Society, 1984. Reprint.
4. C. Delor and L. Puel. Extension of the associative path ordering to a chain of associative-commutative symbols. In C. Kirchner, editor, *5th Conference on Rewrite Techniques and Applications*, volume 690 of *LNCS*, pages 389–404. Springer-Verlag, 1993.
5. M. Fitting. *First-Order Logic and Automated Theorem Proving*. Springer-Verlag, second edition, 1996.
6. G. Gentzen. Untersuchungen über das logische Schließen. *Mathematische Zeitschrift*, 39:176–210, 405–431, 1935.
7. J. Hsiang and M. Rusinowitch. Proving refutational completeness of theorem proving strategies: The transfinite semantic tree method. *Journal of the ACM*, 38(3):559–587, 1991.
8. P. Lorenzen. Algebraische und logistische Untersuchungen über freie Verbände. *The Journal of Symbolic Logic*, 16(2):81–106, 1951.
9. H. Schwichtenberg. Proof theory: Some applications of cut-elimination. In J. Barwise, editor, *Handbook of Mathematical Logic*, pages 867–895. North-Holland, 1977.
10. M. Stickel. Automated deduction by theory resolution. In A. Joshi, editor, *9th International Joint Conference on Artificial Intelligence*, pages 1181–1186. Morgan Kaufmann, 1985.
11. G. Struth. *Canonical Transformations in Algebra, Universal Algebra and Logic*. PhD thesis, Institut für Informatik, Universität des Saarlandes, 1998.
12. G. Struth. An algebra of resolution. In L. Bachmair, editor, *Rewriting Techniques and Applications, 11th International Conference*, volume 1833 of *LNCS*, pages 214–228. Springer-Verlag, 2000.
13. G. Struth. Deriving focused calculi for transitive relations. In A. Middeldorp, editor, *Rewriting Techniques and Applications, 12th International Conference*, volume 2051 of *LNCS*, pages 291–305. Springer-Verlag, 2001.
14. G. Struth. Deriving focused lattice calculi. In S. Tison, editor, *Rewriting Techniques and Applicaions, 13th International Conference*, volume 2378 of *LNCS*, pages 83–97. Springer-Verlag, 2002.
15. Ph.M. Whitman. Free lattices. *Ann. of Math.*, 42(2):325–330, 1941.
16. L. Wos, G. Robinson, and D. Carson. Efficiency and completeness of the set of support strateg in theorem proving. *J. of the Association for Computing Machinery*, 12:536–541, 1965.