A GENTZEN SYSTEM AND DECIDABILITY FOR RESIDUATED LATTICES

PETER JIPSEN

Abstract. This note presents details of a result of Okada and Terui[2] which shows that the equational theory of residuated lattices is decidable and gives an effective algorithm based on a Gentzen system for propositional intuitionistic linear logic.

The variety of residuated lattices is denoted by $\mathcal{RL}$. An algebra $(L, \vee, \wedge, *, \backslash, /, 1)$ is a member of this variety if $(L, \vee, \wedge)$ is a lattice, $(L, *, 1)$ is a monoid, and $x * y \leq z$ iff $y \leq x\backslash z$ iff $x \leq z/y$ for all $x, y, z \in L$ (these equivalences can be expressed by equations). We use s, t, u for terms in the language of $\mathcal{RL}$, and $\gamma, \delta, \rho, \sigma$ for (finite) sequences of terms. Concatenation of sequences γ and δ is denoted by $\gamma\delta$, and terms are considered as sequences of length 1. (In this note, multiplication in $\mathcal{RL}$ is written explicitly as $s * t$.) A pair (σ, t) is called a *sequent* and is written $\sigma \vdash t$. The symbol $\vdash$ is read as *yields*, and the semantic interpretation of $s_1 s_2 \dots s_n \vdash t$ is that the inclusion $s_1 * s_2 * \cdots * s_n \leq t$ holds in $\mathcal{RL}$. The empty sequence ε is interpreted as the multiplicative unit 1. Using this notation, we list below some quasi-inclusions $s_1 \leq t_1 \,\&\, \cdots \,\&\, s_n \leq t_n \Rightarrow s \leq t$ in the style of Gentzen rules:

$$\frac{s_1 \vdash t_1 \;\; \dots \;\; s_n \vdash t_n}{s \vdash t} \text{ name of rule.}$$

With the given semantic interpretation it is straight forward to check that all these quasi-inclusions hold in $\mathcal{RL}$. The details in the proof of the completeness lemma (Lemma 3 below) justify the specific form of these rules.

$$\frac{}{t \vdash t}\ \text{Id} \qquad \frac{\gamma\delta \vdash u}{\gamma 1 \delta \vdash u}\ 1\text{-left} \qquad \frac{}{\varepsilon \vdash 1}\ 1\text{-right}$$

$$\frac{\gamma s t \delta \vdash u}{\gamma s * t \delta \vdash u}\ *\text{left} \qquad \frac{\gamma \vdash s \quad \delta \vdash t}{\gamma\delta \vdash s * t}\ *\text{right}$$

$$\frac{\sigma \vdash s \quad \gamma t \delta \vdash u}{\gamma \sigma s\backslash t \delta \vdash u}\ \backslash\text{left} \qquad \frac{s\gamma \vdash t}{\gamma \vdash s\backslash t}\ \backslash\text{right}$$

Date: April 3, 2000.

$$\frac{\sigma \vdash s \quad \gamma t \delta \vdash u}{\gamma \sigma t/s\delta \vdash u}\ /\text{left} \qquad \frac{\gamma s \vdash t}{\gamma \vdash t/s}\ /\text{right}$$

$$\frac{\gamma s\delta \vdash u \quad \gamma t\delta \vdash u}{\gamma s \vee t\delta \vdash u} \vee \text{left} \qquad \frac{\gamma \vdash s}{\gamma \vdash s \vee t} \vee \text{right}_1 \qquad \frac{\gamma \vdash t}{\gamma \vdash s \vee t} \vee \text{right}_2$$

$$\frac{\gamma s\delta \vdash u}{\gamma s \wedge t\delta \vdash u} \wedge \text{left}_1 \qquad \frac{\gamma t\delta \vdash u}{\gamma s \wedge t\delta \vdash u} \wedge \text{left}_2 \qquad \frac{\gamma \vdash s \quad \gamma \vdash t}{\gamma \vdash s \wedge t} \wedge \text{right}$$

A *proof-tree* is a tree in which each node is a sequent, and if $\sigma_1 \vdash t_1, \ldots, \sigma_n \vdash t_n$ are all the child nodes of node $\sigma \vdash t$, then $n \in \{0, 1, 2\}$ and the rule $\frac{\sigma_1 \vdash t_1 \ \ldots \ \sigma_n \vdash t_n}{\sigma \vdash t}$ matches one of the above rules. Hence each node has at most 2 child nodes, and a sequent can appear at a leaf iff it matches one of the rules Id or 1-right. A sequent is said to be *provable*[1] if there exists a proof-tree with this sequent as the root. A subtree of a proof-tree is again a proof-tree, hence all the nodes in a proof-tree are provable.

Note that for each of the rules, there are only a finite number of ways a given sequent can match the denominator of a rule, and this determines exactly what sequents must appear in the numerator of the rule. In each case the sequents in the numerator are structurally simpler than the sequent in the denominator, so the depth of a proof-tree is bounded by the size (defined in a suitable way) of the sequent at the root. Hence it is decidable whether a given sequent is provable.

As an exercise it is instructive to show that sequents such as

$$x*(y \vee z) \vdash x*y \vee x*z \text{ and } x\backslash(y \wedge z) \vdash x\backslash y \wedge x\backslash z$$

are provable, whereas $x \wedge (y \vee z) \vdash (x \wedge y) \vee (x \wedge z)$ is not. For lattice theorists it is also interesting to note that the 6 rules for $\vee$ and $\wedge$ are essentially equivalent to Whitman's method for deciding if $s \leq t$ holds in all lattices, where s, t are lattice terms, and γ, δ in the rules are taken to be empty sequences. A different method for deciding lattice inclusions, due to Skolem, is described by Burris in [1].

We now prove the result of Okada and Terui[2] which shows that for terms s, t, the sequent $s \vdash t$ is provable iff the inclusion $s \leq t$ holds in $\mathcal{RL}$. The forward implication is the soundness of the proof procedure, and follows from the observation that all the rules are vaild (as quasi-inclusions) in $\mathcal{RL}$. The reverse implication is completeness, which is proved by defining a semantics for residuated lattices, based on a non-commutative version of the phase spaces of linear logic. In the theory

[1]In the literature on Gentzen systems this corresponds to *cut-free provable* since the Gentzen system presented here does not mention the so-called *cut-rule* $\frac{\sigma \vdash t \quad \gamma t \delta \vdash u}{\gamma \sigma \delta \vdash u}$.

of quantales, such phase spaces can also be viewed as quantic nuclei of powerset quantales. However the argument below does not require any knowledge of linear logic or quantales.

A *non-commutative phase space* is of the form $(M, \mathcal{L})$, where M is a monoid (with unit e and $x \cdot y$ written as xy), and $\mathcal{L} \subseteq \mathcal{P}(M)$ such that

(P1) $\mathcal{L}$ is closed under arbitrary intersections and
(P2) for all $X \subseteq M$, $Y \in \mathcal{L}$ we have $X\backslash Y$ and $Y/X \in \mathcal{L}$,

where $X\backslash Y = \{z \in M : X\{z\} \subseteq Y\}$, $Y/X = \{z \in M : \{z\}X \subseteq Y\}$ and $XY = \{xy : x \in X,\ y \in Y\}$. We also define

$$X^C = \bigcap\{Z \in \mathcal{L} : X \subseteq Z\} \quad \text{the closure of } X$$

$$X \vee Y = (X \cup Y)^C \qquad X \wedge Y = X \cap Y \qquad X{*}Y = (XY)^C \quad 1 = \{e\}^C$$

Lemma 1. *For any non-commutative phase space $(M, \mathcal{L})$, the algebra $(\mathcal{L}, \vee, \wedge, *, \backslash, /, 1)$ is a residuated lattice.*

Proof. It is a lattice (in fact a complete lattice) since it is the collection of closed sets of a closure operation. By definition of $\backslash$ we have $Z \subseteq X\backslash Y$ iff $XZ \subseteq Y$, and for $Y \in \mathcal{L}$ this is equivalent to $X{*}Y = (XY)^C \subseteq Y$. Similarly, $Z \subseteq Y/X$ is equivalent to $Z{*}X \subseteq Y$. It remains to show that $*$ is associative and 1 is an identity.

For all $X, Y \subseteq M$, $XY \subseteq (XY)^C$ implies $Y \subseteq X\backslash(XY)^C$, hence

$$XY^C \subseteq X(X\backslash(XY)^C)^C = X(X\backslash(X * Y)) \subseteq X * Y$$

where the middle equality makes use of the fact that $X\backslash(XY)^C$ is closed by (P2). Similarly $X^CY \subseteq X * Y$, hence $X^CY^C \subseteq X^C * Y = (X^CY)^C \subseteq (X * Y)^C = X * Y$. Since we also have $XY \subseteq X^CY^C$, it follows that $(XY)^C = (X^CY^C)^C$. Now

$$\begin{aligned}(X * Y) * Z &= ((XY)^CZ)^C = ((XY)^{CC}Z^C)^C = ((XY)Z)^C \\ &= (X(YZ))^C = (X^C(YZ)^C)^C = X * (Y * Z),\end{aligned}$$

and $1 * X = (\{e\}^CX)^C = (\{e\}^{CC}X^C)^C = (\{e\}X)^C = X^C = X$ for $X \in \mathcal{L}$. □

In logic it is common to refer to a structure with an assignment as a model. Let $\mathcal{X}$ be a set of variables. A *non-commutative phase model* $\mathbf{M} = (M, \mathcal{L}, h)$ is a non-commutative phase space $(M, \mathcal{L})$ together with an assignment $h : \mathcal{X} \to \mathcal{L}$. As usual, h extends to a homomorphism from the absolutely free term algebra $T(\mathcal{X})$ to $\mathcal{L}$, with $h(1)$ defined as 1. A term p is *satisfied* in $\mathbf{M}$ if $e \in h(p)$. This is equivalent to $h(1) \subseteq h(p)$, which agrees with the usual algebraic notion of satisfaction for the inclusion $1 \leq p$ under the assignment h. Since $s \leq t$ is equivalent

to $1 \leq s\backslash t$, the satisfaction of arbitrary inclusions is captured by this notion.

Given a term p, let $S(p)$ be the set of subterms of p. We now define a syntactical model $\mathbf{M}(p) = (M(p), \mathcal{L}(p), h)$. The universe $M(p)$ is the free monoid generated by $S(p)$, i.e. the set of all finite sequences of subterms of p. The empty sequence is again denoted by ε. For $\gamma, \delta \in M(p)$, $u \in S(p)$, define

$$[\gamma\_\delta \vdash u] = \{\sigma \in M(p) : \gamma\sigma\delta \vdash u \text{ is provable}\}.$$

The notation $[u]$ is shorthand for $[\varepsilon\_\varepsilon \vdash u]$, called the *value* of u. Further let

$$\begin{aligned}
\mathcal{L}_0 &= \{[\gamma_\delta \vdash u] : \gamma, \delta \in M(p),\ u \in S(p)\} \\
\mathcal{L}(p) &= \{\bigcap \mathcal{K} : \mathcal{K} \subseteq \mathcal{L}_0\} \\
h(x) &= [x] \ \text{ for any variable } x \text{ in } p.
\end{aligned}$$

In the subsequent proofs we will frequently make use of the following observation:

($*$) For any $X \subseteq M(p)$, $t \in S(p)$,

$$t \in X^C \text{ if and only if}$$

for all $\gamma, \delta \in M(p)$ and $u \in S(p)$, $X \subseteq [\gamma\_\delta \vdash u]$ implies $t \in [\gamma\_\delta \vdash u]$.

Lemma 2. $\mathbf{M}(p)$ *is a non-commutative phase model.*

Proof. (P1) holds by construction. To prove (P2), let $X \subseteq M(p)$ and $Y \in \mathcal{L}(p)$. Now $\sigma \in X\backslash Y$ iff $X\{\sigma\} \subseteq Y$ iff for all $\rho \in X$, $\rho\sigma \in Y = Y^C$. By (*) this is equivalent to showing that $Y \subseteq [\gamma\_\delta \vdash u]$ implies $\rho\sigma \in [\gamma\_\delta \vdash u]$. This last containment holds iff $\gamma\rho\sigma\delta \vdash u$ is proveable iff $\sigma \in [\gamma\rho\_\delta \vdash u]$. Hence

$$\sigma \in X\backslash Y \text{ iff } \sigma \in \bigcap\{[\gamma\rho\_\delta \vdash u] : \rho \in X \text{ and } Y \subseteq [\gamma\_\delta \vdash u]\},$$

which implies that $X\backslash Y \in \mathcal{L}$, and Y/X is similar. □

The following result is the central part of the completeness argument.

Lemma 3. *Let* $\mathbf{M}(p)$ *be defined as above. For any subterm* t *of* p *we have* $t \in h(t) \subseteq [t]$. *In particular, if* $\varepsilon \in h(t)$ *then the sequent* $\varepsilon \vdash t$ *is provable.*

Proof. By induction on the structure of the subterm. If it is a variable of p, say x, then $h(x) = [x]$ by definition, and $x \in [x]$ since $x \vdash x$ is provable (using Id). Suppose s, t are subterms of p, and $s \in h(s) \subseteq [s]$, $t \in h(t) \subseteq [t]$.

$s \vee t \in h(s \vee t) \subseteq [s \vee t]$: Note that $h(s \vee t) = (h(s) \cup h(t))^C$. Let $\gamma \in h(s) \cup h(t)$. If $\gamma \in h(s)$, then $\gamma \in [s]$, so $\gamma \vdash s$ is provable. By the $\vee\text{right}_1$ rule it follows that $\gamma \vdash s \vee t$ is provable, hence $\gamma \in [s \vee t]$ and therefore $h(s) \subseteq [s \vee t]$. Similarly $h(t) \subseteq [s \vee t]$, and since $[s \vee t]$ is closed, $h(s \vee t) \subseteq [s \vee t]$.

To see that $s \vee t \in h(s \vee t)$, we use observation $(*)$: Suppose $h(s) \cup h(t) \subseteq [\gamma\_\delta \vdash u]$ where $\gamma, \delta \in M(p)$, $u \in S(p)$. Then $\gamma s \delta \vdash u$ and $\gamma t \delta \vdash u$ are provable (since $s \in h(s)$ and $t \in h(t)$). Therefore $\gamma s \vee t \delta \vdash u$ is provable by $\vee$left and so $s \vee t \in [\gamma\_\delta \vdash u]$. By $(*)$ we conclude that $s \vee t \in (h(s) \cup h(t))^C = h(s \vee t)$.

$s \wedge t \in h(s \wedge t) \subseteq [s \wedge t]$: Let $\gamma \in h(s \wedge t) = h(s) \cap h(t)$. Then $\gamma \in [s] \cap [t]$, hence $\gamma \vdash s$ and $\gamma \vdash t$ are provable. So now $\gamma \vdash s \wedge t$ is provable by the $\wedge$right rule, which shows that $\gamma \in [s \wedge t]$.

Suppose $h(s) \subseteq [\gamma\_\delta \vdash u]$. Then $\gamma s \delta \vdash u$ is provable, and by the $\wedge\text{left}_1$ rule, $\gamma s \wedge t \delta \vdash u$ is provable. Therefore $s \wedge t \in [\gamma\_\delta \vdash u]$, and it follows from $(*)$ that $s \wedge t \in h(s)^C = h(s)$. Similarly $s \wedge t \in h(t)$, hence $s \wedge t \in h(s \wedge t)$.

$s * t \in h(s * t) \subseteq [s * t]$: Note that $h(s * t) = (h(s)h(t))^C$, and let $\sigma \in h(s)h(t)$. Then $\sigma = \gamma\delta$, where $\gamma \in h(s) \subseteq [s]$ and $\delta \in h(t) \subseteq [t]$. Therefore $\gamma \vdash s$ and $\delta \vdash t$ are provable, hence by $*$right $\gamma\delta \vdash s * t$ is provable, and so $\sigma \in [s * t]$. It follows that $h(s)h(t) \subseteq [s * t]$, and since $[s * t]$ is closed, $h(s * t) \subseteq [s * t]$.

Suppose $h(s)h(t) \subseteq [\gamma\_\delta \vdash u]$. Then $st \in [\gamma\_\delta \vdash u]$ since $s \in h(s)$ and $t \in h(t)$. Thus $\gamma s t \delta \vdash u$ is provable, and by $*$left, $\gamma s * t \delta \vdash u$ is provable. This implies $s * t \in [\gamma\_\delta \vdash u]$, so by $(*)$, it follows that $s * t \in h(s * t)$.

$s \backslash t \in h(s \backslash t) \subseteq [s \backslash t]$: Here $h(s \backslash t) = h(s) \backslash h(t) = \{\gamma \in M(p) : h(s)\{\gamma\} \subseteq h(t)\}$. Thus $\gamma \in h(s \backslash t)$ implies $s\gamma \in h(t) \subseteq [t]$, since we are assuming $s \in h(s)$. This means $s\gamma \vdash t$ is provable, so by $\backslash$right $\gamma \in [s \backslash t]$.

Suppose $h(t) \subseteq [\gamma\_\delta \vdash u]$, then $t \in h(t)$ implies $\gamma t \delta \vdash u$ is provable. For any $\sigma \in h(s) \subseteq [s]$ we have that $\sigma \vdash s$ is provable, so from $\backslash$left we get that $\sigma s \backslash t \in [\gamma\_\delta \vdash u]$. By $(*)$ it follows that $\sigma s \backslash t \in h(t)$ whenever $\sigma \in h(s)$, hence $h(s)\{s \backslash t\} \subseteq h(t)$. This implies $s \backslash t \in h(s) \backslash h(t) = h(s \backslash t)$.

The case for $s/t \in h(s/t) \subseteq [s/t]$ is similar. Since we are assuming that h has been extended to a homomorphism from the term algebra to $\mathcal{L}$, we have $h(1) = 1 = \{\varepsilon\}^C$. Suppose $\{\varepsilon\} \subseteq [\gamma\_\delta \vdash u]$, then $\gamma\delta \vdash u$ is provable, and by the 1-left rule $1 \in [\gamma\_\delta \vdash u]$. Hence $(*)$ implies $1 \in h(1)$. Finally, $h(1) \subseteq [1]$ holds since $\{\varepsilon\} \subseteq [1]$ follows from 1-right.

The second statement is a simple consequence: if $\varepsilon \in h(t)$ then $\varepsilon \in [t]$ which means $\varepsilon \vdash t$ is provable. $\square$

Theorem 4. *For any term p the following statements are equivalent:*

(i) $\mathcal{RL} \models 1 \leq p$
(ii) $\varepsilon \in h(p)$ *in* $\mathbf{M}(p)$
(iii) $\varepsilon \vdash p$ *is provable.*

Proof. (i) implies (ii) by Lemma 2, (ii) implies (iii) by Lemma 3, and (iii) implies (i) by a standard soundness argument using the observation that all the (quasi-inclusions corresponding to) sequent rules are valid in $\mathcal{RL}$. □

Since it was observed earlier that condition (iii) is decidable, and since any equation can be reduced to this form, the equational theory of $\mathcal{RL}$ is decidable. Okada and Terui[2] go on to prove that $\mathcal{RL}$ is generated by its finite members, and they also consider several subvarieties and expansions of $\mathcal{RL}$. For example, to decide inclusions for bounded residuated lattices, one simply adds the two rules $\frac{}{\gamma 0 \delta \vdash u}$ and $\frac{}{\gamma \vdash \top}$. In fact their results are formulated for what amounts to bounded commutative residuated lattices, and the non-commutative case is only mentioned briefly at the end. However their method of proving decidability and the finite model property is very versatile and can perhaps be adapted to cover other subvarieties of $\mathcal{RL}$, such as the varieties of distributive or of cancellative residuated lattices, or the variety generated by residuated chains.

References

[1] S. Burris, *Polynomial time uniform word problems* Math. Logic Quarterly **41** (1995), 173–182.

[2] M. Okada and K. Terui, *The finite model property for various fragments of intuitionistic linear logic*, Journal of Symbolic Logic, **64**(2) (1999) 790–802.