Undecidability of $\{\cdot, 1, \vee\}$-equations in subvarieties of commutative residuated lattices.

Gavin St. John

Under the advisement of Nikolaos Galatos
University of Denver
Department of Mathematics

Topology, Algebra, and Categories in Logic 2017
Institute of Computer Science, Czech Academy of Sciences

27 June 2017

Residuated Lattices

Definition

A (commutative) **residuated lattice** is a structure
$\mathbf{R} = (R, \cdot, \vee, \wedge, \backslash, /, 1)$, such that

- $(R, \vee, \wedge)$ is a lattice
- $(R, \cdot, 1)$ is a (commutative) monoid
- For all $x, y, z \in R$

$$x \cdot y \leq z \iff y \leq x \backslash z \iff x \leq z / y,$$

  where $\leq$ is the lattice order.

We denote the variety of (commutative) residuated lattices by ($\mathcal{CRL}$) $\mathcal{RL}$.
If (r) is a rule (axiom), then $(\mathcal{C})\mathcal{RL}_{\mathrm{r}} := (\mathcal{C})\mathcal{RL} + (\mathrm{r})$.

Known results for Quasi-Equational Theory

(k_n^m) represents the knotted rule $x^n \leq x^m$

Undecidable Q.Eq. Theory	Decidable Q.Eq. Theory

Known results for Quasi-Equational Theory

(k_n^m) represents the knotted rule $x^n \leq x^m$

Undecidable Q.Eq. Theory	Decidable Q.Eq. Theory
$\mathcal{RL}$	
$\mathcal{CRL}$	

Known results for Quasi-Equational Theory

(k_n^m) represents the knotted rule $x^n \leq x^m$

Undecidable Q.Eq. Theory	Decidable Q.Eq. Theory
$\mathcal{RL}$	
$\mathcal{CRL}$	
$\mathcal{RL} + (\mathrm{k}_n^m), 1 \leq n < m$	

Known results for Quasi-Equational Theory

(k_n^m) represents the knotted rule $x^n \leq x^m$

Undecidable Q.Eq. Theory	Decidable Q.Eq. Theory
$\mathcal{RL}$	
$\mathcal{CRL}$	
$\mathcal{RL} + (\mathrm{k}_n^m), 1 \leq n < m$	
	$\mathcal{CRL} + (\mathrm{k}_n^m)$

Known results for Quasi-Equational Theory

(k_n^m) represents the knotted rule $x^n \le x^m$

Undecidable Q.Eq. Theory	Decidable Q.Eq. Theory
$\mathcal{RL}$	
$\mathcal{CRL}$	
$\mathcal{RL} + (\mathrm{k}_n^m), 1 \le n < m$	
	$\mathcal{CRL} + (\mathrm{k}_n^m)$
$\mathcal{CRL} + (?)$	

- Van Alten (2005) showed $\mathcal{CRL}$ in the presence of any knotted rule has the FEP.

- Van Alten (2005) showed $\mathcal{CRL}$ in the presence of any knotted rule has the FEP.
  ○ Consequently, extensions of $\mathcal{CRL}$ in the signatures $\{\leq, \cdot, 1\}$ have been fully characterized.

- Van Alten (2005) showed $\mathcal{CRL}$ in the presence of any knotted rule has the FEP.
  ◦ Consequently, extensions of $\mathcal{CRL}$ in the signatures $\{\leq, \cdot, 1\}$ have been fully characterized.
- We inspect (in)equations in the signature $\{\cdot, 1, \vee\}$.

- Van Alten (2005) showed $\mathcal{CRL}$ in the presence of any knotted rule has the FEP.
  ○ Consequently, extensions of $\mathcal{CRL}$ in the signatures $\{\leq, \cdot, 1\}$ have been fully characterized.
- We inspect (in)equations in the signature $\{\cdot, 1, \vee\}$.
  ○ Proof theoretically, such axioms correspond to inference rules, e.g.,

$$x \leq x^2 \vee 1 \iff \frac{X, Y, Y, Z \vdash C \quad X, Z \vdash C}{X, Y, Z \vdash C}$$

- Van Alten (2005) showed $\mathcal{CRL}$ in the presence of any knotted rule has the FEP.
  ◦ Consequently, extensions of $\mathcal{CRL}$ in the signatures $\{\leq, \cdot, 1\}$ have been fully characterized.
- We inspect (in)equations in the signature $\{\cdot, 1, \vee\}$.
  ◦ Proof theoretically, such axioms correspond to inference rules, e.g.,

$$x \leq x^2 \vee 1 \iff \frac{X, Y, Y, Z \vdash C \quad X, Z \vdash C}{X, Y, Z \vdash C}$$

  ◦ The work of Chvalovský & Horčík (2016) implies the undecidability for many such extensions in $\mathcal{RL}$.

- Van Alten (2005) showed $\mathcal{CRL}$ in the presence of any knotted rule has the FEP.
  ∘ Consequently, extensions of $\mathcal{CRL}$ in the signatures $\{\leq, \cdot, 1\}$ have been fully characterized.
- We inspect (in)equations in the signature $\{\cdot, 1, \vee\}$.
  ∘ Proof theoretically, such axioms correspond to inference rules, e.g.,

$$x \leq x^2 \vee 1 \iff \frac{X, Y, Y, Z \vdash C \quad X, Z \vdash C}{X, Y, Z \vdash C}$$

  ∘ The work of Chvalovský & Horčík (2016) implies the undecidability for many such extensions in $\mathcal{RL}$.
  ∘ So we restrict our investigation to the commutative case.

Linearization

Any equation $s = t$ in the signature $\{\cdot, 1, \vee\}$ is equivalent to some conjunction of linear inequations we call "d-**rules**" of the form:

$$(\mathrm{d}) \quad x_1 \cdots x_n \leq \bigvee_{j=1}^{m} x_1^{d_j(1)} \cdots x_n^{d_j(n)},$$

where $\mathrm{d} := \{d_1, ..., d_m\} \subset \mathbb{N}^n$.

Linearization

Any equation $s = t$ in the signature $\{\cdot, 1, \vee\}$ is equivalent to some conjunction of linear inequations we call "d-**rules**" of the form:

$$\text{(d)} \quad x_1 \cdots x_n \leq \bigvee_{j=1}^{m} x_1^{d_j(1)} \cdots x_n^{d_j(n)},$$

where $\mathrm{d} := \{d_1, ..., d_m\} \subset \mathbb{N}^n$. Such conjoins can be determined by the properties of $\mathcal{CRL}$:

- $x \leq y \iff x \vee y = y$
- $x \vee y \leq z \iff x \leq z$ and $y \leq z$
- **linearization**

Linearization

Any equation $s = t$ in the signature $\{\cdot, 1, \vee\}$ is equivalent to some conjunction of linear inequations we call "d-**rules**" of the form:

$$(\mathrm{d}) \quad x_1 \cdots x_n \leq \bigvee_{j=1}^{m} x_1^{d_j(1)} \cdots x_n^{d_j(n)},$$

where $\mathrm{d} := \{d_1, ..., d_m\} \subset \mathbb{N}^n$. Such conjoins can be determined by the properties of $\mathcal{CRL}$:

- $x \leq y \iff x \vee y = y$
- $x \vee y \leq z \iff x \leq z$ and $y \leq z$
- **linearization**
  E.g., the rule
  $$(\forall u)(\forall v)\ u^2 v \leq u^3 \vee uv$$
  is equivalent to, via the substitutions $u = x \vee y$ and $v = z$,
  $$(\forall x)(\forall y)(\forall z)\ xyz \leq x^3 \vee x^2 y \vee xy^2 \vee y^3 \vee xz \vee yz$$

Conditions on $\mathrm{d} \subset \mathbb{N}^n$

- If (d) implies a knotted rule, then $\mathcal{CRL} + (\mathrm{d})$ is decidable.

Conditions on $\mathrm{d} \subset \mathbb{N}^n$

- If (d) implies a knotted rule, then $\mathcal{CRL} + (\mathrm{d})$ is decidable.
  E.g., if (d) is $xy \leq xy^2 \vee x^2y$, then

$$\mathcal{CRL} + (\mathrm{d}) \models x^2 \leq x^3.$$

Conditions on $\mathrm{d} \subset \mathbb{N}^n$

- If (d) implies a knotted rule, then $\mathcal{CRL} + (\mathrm{d})$ is decidable.
  E.g., if (d) is $xy \leq xy^2 \vee x^2y$, then
  $$\mathcal{CRL} + (\mathrm{d}) \models x^2 \leq x^3.$$
- If $\mathcal{CRL} + (\mathrm{d})$ is to be undecidable, $\mathrm{d} \subset \mathbb{N}^n$ must refute certain conditions with respect to the set of vectors representing the exponents of the variables.

Conditions on $\mathrm{d} \subset \mathbb{N}^n$

- If (d) implies a knotted rule, then $\mathcal{CRL} + (\mathrm{d})$ is decidable. E.g., if (d) is $xy \leq xy^2 \vee x^2y$, then
$$\mathcal{CRL} + (\mathrm{d}) \models x^2 \leq x^3.$$
- If $\mathcal{CRL} + (\mathrm{d})$ is to be undecidable, $\mathrm{d} \subset \mathbb{N}^n$ must refute certain conditions with respect to the set of vectors representing the exponents of the variables.
- We view $\mathrm{d} = \{d_j\}_{j=1}^m$ as a set of linear subspaces of $\mathbf{R}^n$.

Conditions on $\mathrm{d} \subset \mathbb{N}^n$

- If (d) implies a knotted rule, then $\mathcal{CRL} + (\mathrm{d})$ is decidable. E.g., if (d) is $xy \leq xy^2 \vee x^2y$, then
$$\mathcal{CRL} + (\mathrm{d}) \models x^2 \leq x^3.$$
- If $\mathcal{CRL} + (\mathrm{d})$ is to be undecidable, $\mathrm{d} \subset \mathbb{N}^n$ must refute certain conditions with respect to the set of vectors representing the exponents of the variables.
- We view $\mathrm{d} = \{d_j\}_{j=1}^m$ as a set of linear subspaces of $\mathbf{R}^n$. $(\star)$ Given any nonempty $A \subseteq \{1, ..., n\}$, and any nontrivial valuation of variables $x_1, ..., x_n$ in $\mathbb{N}$, there exists $j \neq j' \leq m$ such that the supports of d_j and $d_{j'}$ intersect A, and
$$\sum_{i=1}^{n} d_j(i)x_i \neq \sum_{i=1}^{n} d_{j'}(i)x_i$$

Conditions on $\mathrm{d} \subset \mathbb{N}^n$

- If (d) implies a knotted rule, then $\mathcal{CRL} + (\mathrm{d})$ is decidable. E.g., if (d) is $xy \leq xy^2 \vee x^2y$, then
$$\mathcal{CRL} + (\mathrm{d}) \models x^2 \leq x^3.$$
- If $\mathcal{CRL} + (\mathrm{d})$ is to be undecidable, $\mathrm{d} \subset \mathbb{N}^n$ must refute certain conditions with respect to the set of vectors representing the exponents of the variables.
- We view $\mathrm{d} = \{d_j\}_{j=1}^m$ as a set of linear subspaces of $\mathbf{R}^n$.
$(\star)$ Given any nonempty $A \subseteq \{1, \ldots, n\}$, and any nontrivial valuation of variables $x_1, \ldots, x_n$ in $\mathbb{N}$, there exists $j \neq j' \leq m$ such that the supports of d_j and $d_{j'}$ intersect A, and
$$\sum_{i=1}^{n} d_j(i)x_i \neq \sum_{i=1}^{n} d_{j'}(i)x_i$$
$(\star\star)$ For any valuation of the x_i's, there exists $j \leq m$ such that
$$\sum_{i=1}^{n} x_i < \sum_{i=1}^{n} d_j(i)x_i$$

Examples and Non-examples of $(\star)$ & $(\star\star)$

Rule	$(\star)$	$(\star\star)$
$x \leq x^2$		✓
$x \leq x^2 \vee 1$		✓
$x \leq x^2 \vee x^3$	✓	✓
$xy \leq x^2 \vee y^2$		
$xy \leq x \vee x^2 y$		
$xy \leq x \vee x^2 y \vee y^2$	✓	✓
$xyz \leq x^3 \vee x^2 y \vee y^3 \vee y^2 z \vee z^3 \vee z^2 x$	✓	
$xyzw \leq x^2 yzw \vee x^3 y^2 z^2 w^2$	✓	✓

Examples and Non-examples of $(\star)$ & $(\star\star)$

Rule	$(\star)$	$(\star\star)$
$x \leq x^2$		✓
$x \leq x^2 \vee 1$		✓
$x \leq x^2 \vee x^3$	✓	✓
$xy \leq x^2 \vee y^2$		
$xy \leq x \vee x^2 y$		
$xy \leq x \vee x^2 y \vee y^2$	✓	✓
$xyz \leq x^3 \vee x^2 y \vee y^3 \vee y^2 z \vee z^3 \vee z^2 x$	✓	
$xyzw \leq x^2 yzw \vee x^3 y^2 z^2 w^2$	✓	✓

Determining whether a given (d)-rule satisfies these conditions amounts to showing certain systems of equations do not have "non-trivial " solutions in $\mathbb{N}^n$. This can be simplified by asking if there are positive solutions in $\mathbb{R}^n$.

An **And-branching k-Counter Machine** (k-ACM), (Linclon et. al. 1992) $M = (R_k, Q, P)$ is a type of non-deterministic parallel-computing counter machine that has

And-branching Counter Machines

An **And-branching k-Counter Machine** (k-ACM), (Linclon et. al. 1992) $M = (R_k, Q, P)$ is a type of non-deterministic parallel-computing counter machine that has

- a set $R_k := \{r_1, ..., r_k\}$ of k **registers** (bins) that can each store a non-negative integer (tokens),

And-branching Counter Machines

An **And-branching k-Counter Machine** (k-ACM), (Linclon et. al. 1992) $M = (R_k, Q, P)$ is a type of non-deterministic parallel-computing counter machine that has

- a set $R_k := \{r_1, ..., r_k\}$ of k **registers** (bins) that can each store a non-negative integer (tokens),
- a finite set Q of **states** with designated **initial state** q_I and **final state** q_f,

And-branching Counter Machines

An **And-branching k-Counter Machine** (k-ACM), (Linclon et. al. 1992) $M = (R_k, Q, P)$ is a type of non-deterministic parallel-computing counter machine that has

- a set $R_k := \{r_1, ..., r_k\}$ of k **registers** (bins) that can each store a non-negative integer (tokens),
- a finite set Q of **states** with designated **initial state** q_I and **final state** q_f,
- and a finite set P of **instructions** p of the form:

  - **Increment:** $q \leq^p q'r$
  - **Decrement:** $qr \leq^p q'$
  - **Fork:** $q \leq^p q' \vee q''$,

  where $q, q', q'' \in Q$ and $r \in R_k$.

ACM's continued

- Instructions of an ACM act on **configurations**, which consist of a single state and a number register tokens
$$C = q r_1^{n_1} r_2^{n_2} \cdots r_k^{n_k}.$$

ACM's continued

- Instructions of an ACM act on **configurations**, which consist of a single state and a number register tokens

$$C = q r_1^{n_1} r_2^{n_2} \cdots r_k^{n_k}.$$

- Forking instructions allow parallel computation. The status of a machine at a given time in a computation is called an **instantaneous description** (ID),

$$u = C_1 \vee C_2 \vee \cdots \vee C_n,$$

where $C_1, ..., C_n$ are configurations.

ACM's continued

- Instructions of an ACM act on **configurations**, which consist of a single state and a number register tokens
$$C = q r_1^{n_1} r_2^{n_2} \cdots r_k^{n_k}.$$
- Forking instructions allow parallel computation. The status of a machine at a given time in a computation is called an **instantaneous description** (ID),
$$u = C_1 \vee C_2 \vee \cdots \vee C_n,$$
where $C_1, ..., C_n$ are configurations.
- An instruction p acts on a single configuration of an ID u to create a new configuration u'.

Computations

We view computations as order relations on the free commutative idempotent semiring $\mathbf{A}_M = (A_M, \vee, \cdot, \perp, 1)$ generated by $Q \cup R_k$, where $M = (R_k, Q, P)$ is a k-ACM and

Computations

We view computations as order relations on the free commutative idempotent semiring $\mathbf{A}_M = (A_M, \vee, \cdot, \bot, 1)$ generated by $Q \cup R_k$, where $M = (R_k, Q, P)$ is a k-ACM and

- $(A_M, \vee, \bot)$ is a $\vee$-semilattice with bottom element $\bot := \bigvee \emptyset$, and

Computations

We view computations as order relations on the free commutative idempotent semiring $\mathbf{A}_M = (A_M, \vee, \cdot, \bot, 1)$ generated by $Q \cup R_k$, where $M = (R_k, Q, P)$ is a k-ACM and

- $(A_M, \vee, \bot)$ is a $\vee$-semilattice with bottom element $\bot := \bigvee \emptyset$, and
- $(A_M, \cdot, 1)$ is a commutative monoid with identity 1, and multiplication distributes over join.

Computations

We view computations as order relations on the free commutative idempotent semiring $\mathbf{A}_M = (A_M, \vee, \cdot, \bot, 1)$ generated by $Q \cup R_k$, where $M = (R_k, Q, P)$ is a k-ACM and

- $(A_M, \vee, \bot)$ is a $\vee$-semilattice with bottom element $\bot := \bigvee \emptyset$, and
- $(A_M, \cdot, 1)$ is a commutative monoid with identity 1, and multiplication distributes over join.

Each instruction $p \in P$ defines a relation $\leq^p$ closed under

$$\frac{u \leq^p v}{ux \leq^p vx}\ [\cdot] \qquad \text{and} \qquad \frac{u \leq^p v}{u \vee w \leq^p v \vee w}\ [\vee],$$

for $u, v, w \in \mathrm{ID}(M)$ and $x \in R_k^*$, where R_k^* is the free commutative monoid generated by R_k.

Computations

We view computations as order relations on the free commutative idempotent semiring $\mathbf{A}_M = (A_M, \vee, \cdot, \bot, 1)$ generated by $Q \cup R_k$, where $M = (R_k, Q, P)$ is a k-ACM and

- $(A_M, \vee, \bot)$ is a $\vee$-semilattice with bottom element $\bot := \bigvee \emptyset$, and
- $(A_M, \cdot, 1)$ is a commutative monoid with identity 1, and multiplication distributes over join.

Each instruction $p \in P$ defines a relation $\leq^p$ closed under

$$\frac{u \leq^p v}{ux \leq^p vx}\ [\cdot] \qquad \text{and} \qquad \frac{u \leq^p v}{u \vee w \leq^p v \vee w}\ [\vee],$$

for $u, v, w \in \mathrm{ID}(M)$ and $x \in R_k^*$, where R_k^* is the free commutative monoid generated by R_k.

We define the **computation relation** $\leq_M$ to be the smallest preorder containing $\bigcup_{p \in P} \leq^p$.

Computations cont.

We say a machine M **terminates on an ID** u if $u \leq_M q_f$.

Computations cont.

We say a machine M **terminates on an ID** u if $u \leq_M q_f$.

- If $u = C_1 \vee \cdots \vee C_n$, then $u \leq_M q_f$ iff $C_i \leq_M q_f, \forall i \leq n$.

Computations cont.

We say a machine M **terminates on an ID** u if $u \leq_M q_f$.

- If $u = C_1 \vee \cdots \vee C_n$, then $u \leq_M q_f$ iff $C_i \leq_M q_f, \forall i \leq n$.
- If $u \leq_M q_f$, then there exists $p_1, ..., p_n \in P$ and $u_0, ..., u_n \in \mathrm{ID}(M)$, such that
$$u = u_0 \leq^{p_1} u_1 \leq^{p_2} \cdots \leq^{p_n} u_n = q_f.$$

Computations cont.

We say a machine M **terminates on an ID** u if $u \leq_M q_f$.

- If $u = C_1 \vee \cdots \vee C_n$, then $u \leq_M q_f$ iff $C_i \leq_M q_f, \forall i \leq n$.
- If $u \leq_M q_f$, then there exists $p_1, ..., p_n \in P$ and $u_0, ..., u_n \in \mathrm{ID}(M)$, such that
$$u = u_0 \leq^{p_1} u_1 \leq^{p_2} \cdots \leq^{p_n} u_n = q_f.$$

Example Machine

Let $M = M_{\text{even}} := (\{r\}, \{q_0, q_1, q_f\}, \{p_1, p_2, p_3\})$, with instructions

$$q_0 r \leq^{p_1} q_1; \quad q_1 r \leq^{p_2} q_0; \quad q_0 \leq^{p_3} q_f.$$

Computations cont.

We say a machine M **terminates on an ID** u if $u \leq_M q_f$.

- If $u = C_1 \vee \cdots \vee C_n$, then $u \leq_M q_f$ iff $C_i \leq_M q_f, \forall i \leq n$.
- If $u \leq_M q_f$, then there exists $p_1, ..., p_n \in P$ and $u_0, ..., u_n \in \mathrm{ID}(M)$, such that
$$u = u_0 \leq^{p_1} u_1 \leq^{p_2} \cdots \leq^{p_n} u_n = q_f.$$

Example Machine

Let $M = M_{\text{even}} := (\{r\}, \{q_0, q_1, q_f\}, \{p_1, p_2, p_3\})$, with instructions

$$q_0 r \leq^{p_1} q_1; \quad q_1 r \leq^{p_2} q_0; \quad q_0 \leq^{p_3} q_f.$$

- Note that $q_0 r^n \leq_M q_f$ iff n is even.

Computations cont.

We say a machine M **terminates on an ID** u if $u \leq_M q_f$.

- If $u = C_1 \vee \cdots \vee C_n$, then $u \leq_M q_f$ iff $C_i \leq_M q_f, \forall i \leq n$.
- If $u \leq_M q_f$, then there exists $p_1, ..., p_n \in P$ and $u_0, ..., u_n \in \mathrm{ID}(M)$, such that
$$u = u_0 \leq^{p_1} u_1 \leq^{p_2} \cdots \leq^{p_n} u_n = q_f.$$

Example Machine

Let $M = M_{\text{even}} := (\{r\}, \{q_0, q_1, q_f\}, \{p_1, p_2, p_3\})$, with instructions

$$q_0 r \leq^{p_1} q_1; \quad q_1 r \leq^{p_2} q_0; \quad q_0 \leq^{p_3} q_f.$$

- Note that $q_0 r^n \leq_M q_f$ iff n is even.

$$q_0 r^4 \leq^{p_1} q_1 r^3 \leq^{p_2} q_0 r^2 \leq^{p_1} q_1 r \leq^{p_2} q_0 \leq^{p_3} q_f$$

Computations cont.

We say a machine M **terminates on an ID** u if $u \leq_M q_f$.

- If $u = C_1 \vee \cdots \vee C_n$, then $u \leq_M q_f$ iff $C_i \leq_M q_f, \forall i \leq n$.
- If $u \leq_M q_f$, then there exists $p_1, ..., p_n \in P$ and $u_0, ..., u_n \in \mathrm{ID}(M)$, such that

$$u = u_0 \leq^{p_1} u_1 \leq^{p_2} \cdots \leq^{p_n} u_n = q_f.$$

Example Machine

Let $M = M_{\text{even}} := (\{r\}, \{q_0, q_1, q_f\}, \{p_1, p_2, p_3\})$, with instructions

$$q_0 r \leq^{p_1} q_1; \quad q_1 r \leq^{p_2} q_0; \quad q_0 \leq^{p_3} q_f.$$

- Note that $q_0 r^n \leq_M q_f$ iff n is even.

$$q_0 r^4 \leq^{p_1} q_1 r^3 \leq^{p_2} q_0 r^2 \leq^{p_1} q_1 r \leq^{p_2} q_0 \leq^{p_3} q_f$$

$$q_0 r^3 \leq^{p_1} q_1 r^2 \leq^{p_2} q_0 r \leq^{p_3} q_f r$$

Undecidable Problem

Theorem [Lincoln *et. al.*, 1992]

There exists a 2-ACM $\widetilde{M}$ such that membership of the set $\{u \in \mathrm{ID}(\widetilde{M}) : u \leq_{\widetilde{M}} q_f\}$ is undecidable. Furthermore, it is undecidable whether $q_I \leq_{\widetilde{M}} q_f$.

Undecidable Problem

Theorem [Lincoln *et. al.*, 1992]

There exists a 2-ACM $\widetilde{M}$ such that membership of the set $\{u \in \mathrm{ID}(\widetilde{M}) : u \leq_{\widetilde{M}} q_f\}$ is undecidable. Furthermore, it is undecidable whether $q_I \leq_{\widetilde{M}} q_f$.

- Given an ACM M we define the **theory of** M $\mathrm{Th}(M)$ to be the conjunction of all syntactic instructions in P, i.e.,

$$\mathrm{Th}(M) := \&\{C \leq u : (C \leq^p u) \in P\}.$$

Undecidable Problem

Theorem [Lincoln *et. al.*, 1992]

There exists a 2-ACM $\widetilde{M}$ such that membership of the set $\{u \in \mathrm{ID}(\widetilde{M}) : u \leq_{\widetilde{M}} q_f\}$ is undecidable. Furthermore, it is undecidable whether $q_I \leq_{\widetilde{M}} q_f$.

- Given an ACM M we define the **theory of** M $\mathrm{Th}(M)$ to be the conjunction of all syntactic instructions in P, i.e.,
$$\mathrm{Th}(M) := \bigwith\{C \leq u : (C \leq^p u) \in P\}.$$
- Given an ID u, we define the quasi-equation $\mathrm{Halt}_M(u)$ to be
$$\mathrm{Th}(M) \implies u \leq q_f.$$

d-rules and the relation $\leq_{\mathrm{d}(M)}$

Given a d-rule, e.g. $[\mathrm{d}]$ is given by $x \leq x^2 \vee x^4$, we add "ambient" instructions of the form

$$qxy \leq^{\mathrm{d}} qxy^2 \vee qxy^4,$$

for each $q \in Q$ and any $x, y \in R_k^*$.

d-rules and the relation $\leq_{\mathrm{d}(M)}$

Given a d-rule, e.g. $[\mathrm{d}]$ is given by $x \leq x^2 \vee x^4$, we add “ambient” instructions of the form

$$qxy \leq^{\mathrm{d}} qxy^2 \vee qxy^4,$$

for each $q \in Q$ and any $x, y \in R_k^*$.
As with the instructions in P, we close $\leq^{\mathrm{d}}$ under the inference rules $[\cdot]$ and $[\vee]$, and we define the relation $\leq_{\mathrm{d}(M)}$ to be the smallest preorder generated by $\leq^{\mathrm{d}} \cup \leq_M$.

- Clearly, if $u \leq_M q_f$ then $u \leq_{\mathrm{d}(M)} q_f$ since $\leq_M \subset \leq_{\mathrm{d}(M)}$.

- Clearly, if $u \leq_M q_f$ then $u \leq_{\mathrm{d}(M)} q_f$ since $\leq_M \subset \leq_{\mathrm{d}(M)}$.
- However, for some ACM's M, it's possible that $u \leq_{\mathrm{d}(M)} q_f$ but $u \not\leq_M q_f$.

- Clearly, if $u \leq_M q_f$ then $u \leq_{\mathrm{d}(M)} q_f$ since $\leq_M \subset \leq_{\mathrm{d}(M)}$.
- However, for some ACM's M, it's possible that $u \leq_{\mathrm{d}(M)} q_f$ but $u \not\leq_M q_f$.

Example

Consider $M = M_{\mathrm{even}}$ and (d) given by $x \leq x^2 \vee x^4$.

- Clearly, if $u \leq_M q_f$ then $u \leq_{\mathrm{d}(M)} q_f$ since $\leq_M \subset \leq_{\mathrm{d}(M)}$.
- However, for some ACM's M, it's possible that $u \leq_{\mathrm{d}(M)} q_f$ but $u \not\leq_M q_f$.

Example

Consider $M = M_{\mathrm{even}}$ and (d) given by $x \leq x^2 \vee x^4$.

- $q_0 r^3 \not\leq_M q_f$ since 3 is odd.

- Clearly, if $u \leq_M q_f$ then $u \leq_{\mathrm{d}(M)} q_f$ since $\leq_M \subset \leq_{\mathrm{d}(M)}$.
- However, for some ACM's M, it's possible that $u \leq_{\mathrm{d}(M)} q_f$ but $u \not\leq_M q_f$.

Example

Consider $M = M_{\text{even}}$ and (d) given by $x \leq x^2 \vee x^4$.

- $q_0 r^3 \not\leq_M q_f$ since 3 is odd.
- However, $q_0 r^3 \leq_{\mathrm{d}(M)} q_f$, witnessed by

$$q_0 r^3 = q_0 r^2 r \leq^{\mathrm{d}} q_0 r^2 r^2 \vee q_0 r^2 r^4 = q_0 r^4 \vee q_0 r^6 \leq_{\mathrm{d}(M)} q_f,$$

since $q_0 r^4 \leq_M q_f$ and $q_0 r^6 \leq_M q_f$.

Goal

Given an ACM M and a d-rule, is it possible to construct a new ACM M' such that

$$u \leq_M q_f \text{ if and only if } \theta(u) \leq_{\mathrm{d}(M')} q_F,$$

(where $\theta : \mathrm{ID}(M) \to \mathrm{ID}(M')$ is computable and q_F is the final state of M') and if so, under what conditions?

Then M_K machine

Let $M = (R_2, Q, P)$ be a 2-ACM and let $K > 1$ be given. We define the 3-ACM $M_K = (R_3, Q_K, P_K)$ such that

Then M_K machine

Let $M = (R_2, Q, P)$ be a 2-ACM and let $K > 1$ be given. We define the 3-ACM $M_K = (R_3, Q_K, P_K)$ such that

- $Q \subset Q_K$ with q_F the final state of M_K and instruction $(q_f r_1 r_2 \leq^F q_F) \in P_K$,

Then M_K machine

Let $M = (R_2, Q, P)$ be a 2-ACM and let $K > 1$ be given. We define the 3-ACM $M_K = (R_3, Q_K, P_K)$ such that

- $Q \subset Q_K$ with q_F the final state of M_K and instruction $(q_f r_1 r_2 \leq^F q_F) \in P_K$,
- each forking instruction in P is contained in P_K,

Then M_K machine

Let $M = (R_2, Q, P)$ be a 2-ACM and let $K > 1$ be given. We define the 3-ACM $M_K = (R_3, Q_K, P_K)$ such that

- $Q \subset Q_K$ with q_F the final state of M_K and instruction $(q_f r_1 r_2 \leq^F q_F) \in P_K$,
- each forking instruction in P is contained in P_K,
- each increment and decrement instruction of P is replaced by multiply and divide by K **programs**, i.e.

$$\begin{array}{llllll} q & \leq^p & q'r & \in P & \Longrightarrow & qr^{\forall} \sqsubseteq^p q'r^{K\cdot\forall} & \subset P_K \\ qr & \leq^p & q' & \in P & \Longrightarrow & qr^{\forall} \sqsubseteq^p q'r^{K\backslash\forall} & \subset P_K \end{array}.$$

Then M_K machine

Let $M = (R_2, Q, P)$ be a 2-ACM and let $K > 1$ be given. We define the 3-ACM $M_K = (R_3, Q_K, P_K)$ such that

- $Q \subset Q_K$ with q_F the final state of M_K and instruction $(q_f r_1 r_2 \leq^F q_F) \in P_K$,
- each forking instruction in P is contained in P_K,
- each increment and decrement instruction of P is replaced by multiply and divide by K **programs**, i.e.

$$\begin{array}{lllllll} q & \leq^p & q'r & \in P & \Longrightarrow & qr^\forall \sqsubseteq^p q'r^{K\cdot\forall} & \subset P_K \\ qr & \leq^p & q' & \in P & \Longrightarrow & qr^\forall \sqsubseteq^p q'r^{K\backslash\forall} & \subset P_K \end{array}.$$

- We obtain, for each $q \in Q$,

$$qr_1^{n_1} r_2^{n_2} \leq_M q_f \iff qr_1^{K^{n_1}} r_2^{K^{n_2}} \leq_{M_K} q_F.$$

Detecting applications of $\leq^{\mathrm{d}}$

Observation

Consider a configuration where the contents of some register r is $n = s + t$, whereafter $\leq^{\mathrm{d}}$ is applied to t-many tokens, i.e.,

$$qr^n = qr^s r^t \leq^{\mathrm{d}} qr^s(r^{2t} \vee r^{4t}) = qr^{s+2t} \vee qr^{s+4t}$$

Detecting applications of $\leq^{\mathrm{d}}$

Observation

Consider a configuration where the contents of some register r is $n = s + t$, whereafter $\leq^{\mathrm{d}}$ is applied to t-many tokens, i.e.,

$$qr^n = qr^s r^t \leq^{\mathrm{d}} qr^s(r^{2t} \vee r^{4t}) = qr^{s+2t} \vee qr^{s+4t}$$

Fact

For $\mathrm{d}: \; x \leq x^2 \vee x^4$, if $K \geq (4-2)+1 = 3$, it is **impossible** for $s + 2t$ and $s + 4t$ to **both be powers of** K.

Detecting applications of $\leq^{\mathrm{d}}$

Observation

Consider a configuration where the contents of some register r is $n = s + t$, whereafter $\leq^{\mathrm{d}}$ is applied to t-many tokens, i.e.,

$$qr^n = qr^s r^t \leq^{\mathrm{d}} qr^s(r^{2t} \vee r^{4t}) = qr^{s+2t} \vee qr^{s+4t}$$

Fact

For $\mathrm{d} :\ x \leq x^2 \vee x^4$, if $K \geq (4-2)+1 = 3$, it is **impossible** for $s + 2t$ and $s + 4t$ to **both be powers of** K.

- Such a K will exist for any rule satisfying $(\star)$.
- Consequently, $qr^n \leq_{\mathrm{d}(M_K)} q_f$ iff $qr^n \leq_{M_K} q_F$.
- For rules in more than one variable, satisfying $(\star\star)$ is sufficient to guarantee “detection.”

Let $M = \widetilde{M} = (R_2, Q, P)$ be the 2-ACM such that it is undecidable whether $q_I \leq_M q_f$. Consider the rule (d) be given by $x \leq x^2 \vee x^4$. We construct $M_K = (R_3, Q_K, P_K)$ for $K = 3$.

Let $M = \widetilde{M} = (R_2, Q, P)$ be the 2-ACM such that it is undecidable whether $q_I \leq_M q_f$. Consider the rule (d) be given by $x \leq x^2 \vee x^4$.
We construct $M_K = (R_3, Q_K, P_K)$ for $K = 3$.
By the observation, for any $q' \in Q_3$,

$$q' r_1^{n_1} r_2^{n_2} r_3^{n_3} \leq_{M_3} q_F \iff q' r_1^{n_1} r_2^{n_2} r_3^{n_3} \leq_{\mathrm{d}(M_3)} q_F.$$

$\leq_{\mathrm{d}(M_K)}$

Let $M = \widetilde{M} = (R_2, Q, P)$ be the 2-ACM such that it is undecidable whether $q_I \leq_M q_f$. Consider the rule (d) be given by $x \leq x^2 \vee x^4$.
We construct $M_K = (R_3, Q_K, P_K)$ for $K = 3$.
By the observation, for any $q' \in Q_3$,

$$q' r_1^{n_1} r_2^{n_2} r_3^{n_3} \leq_{M_3} q_F \iff q' r_1^{n_1} r_2^{n_2} r_3^{n_3} \leq_{\mathrm{d}(M_3)} q_F.$$

Hence, for any $q \in Q$,

$$q r_1^{n_1} r_2^{n_2} \leq_M q_f \iff q r_1^{3^{n_1}} r_2^{3^{n_2}} \leq_{\mathrm{d}(M_3)} q_F,$$

so it is undecidable whether $q_I r_1 r_2 \leq_{\mathrm{d}(M_3)} q_F$.

Undecidable word problem

Let $\mathcal{V} \subseteq \mathcal{CRL}$ be a variety. We can show $\mathcal{V}$ has an undecidable word problem (and hence quasi-equational theory) if we can demonstrate

$$\mathcal{V} \models \mathrm{Halt}_{\mathrm{d}(M_K)}(q_I r_1 r_2) \iff q_I r_1 r_2 \leq_M q_f.$$

- If $\mathcal{V} \subseteq \mathcal{CRL}$ then $(\Leftarrow)$ is immediate.
- We use the theory of **Residuated Frames** (Galatos & Jipsen 2013) for a completeness of encoding to provide a model and valuation proving the contrapositive of $(\Rightarrow)$, for varieties $\mathcal{V}$ satisfying certain conditions.

Residuated frames

Definition [Galatos & Jipsen 2013]

A **residuated frame** is a structure $\mathbf{W} = (W, W', N, \circ, \mathbin{\backslash\!\!\backslash}, /\!\!/, 1)$, s.t.

- $(W, \circ, 1)$ is a monoid and W' is a set.
- $N \subseteq W \times W'$, called the *Galois relation*, and
- $\mathbin{\backslash\!\!\backslash} : W \times W' \to W'$ and $/\!\!/ : W' \times W \to W'$ such that
- N is a **nuclear**, i.e. for all $u, v \in W$ and $w \in W'$,
  $(u \circ v) \; N \; w$ iff $u \; N \; (w \mathbin{/\!\!/} v)$ iff $v \; N \; (u \mathbin{\backslash\!\!\backslash} w)$.

Residuated frames

Definition [Galatos & Jipsen 2013]

A **residuated frame** is a structure $\mathbf{W} = (W, W', N, \circ, \backslash\!\!\backslash, /\!\!/, 1)$, s.t.

- $(W, \circ, 1)$ is a monoid and W' is a set.
- $N \subseteq W \times W'$, called the *Galois relation,* and
- $\backslash\!\!\backslash : W \times W' \to W'$ and $/\!\!/ : W' \times W \to W'$ such that
- N is a **nuclear**, i.e. for all $u, v \in W$ and $w \in W'$,
  $(u \circ v)\ N\ w$ iff $u\ N\ (w /\!\!/ v)$ iff $v\ N\ (u \backslash\!\!\backslash w)$.

Define $^{\triangleright} : \mathcal{P}(W) \to \mathcal{P}(W')$ and $^{\triangleleft} : \mathcal{P}(W') \to \mathcal{P}(W)$ via
$X^{\triangleright} = \{y \in W' : \forall x \in X,\ xNy\}$ and
$Y^{\triangleleft} = \{x \in W : \forall y \in Y,\ xNy\}$, for each $X \subseteq W$ and $Y \subseteq W'$.
Then $(^{\triangleright}, ^{\triangleleft})$ is a Galois connection.
So $X \xmapsto{\gamma_N} X^{\triangleright\triangleleft}$ is a closure operator on $\mathcal{P}(W)$.

Residuated frames cont.

Theorem [Galatos & Jipsen 2013]

$\mathbf{W}^+ := (\gamma_N[\mathcal{P}(W)], \cup_{\gamma_N}, \cap, \circ_{\gamma_N}, \backslash\!\!\backslash, /\!\!/, \gamma_N(\{1\}))$,

$$X \cup_{\gamma_N} Y = \gamma_N(X \cup Y) \text{ and } X \circ_{\gamma_N} Y = \gamma_N(X \circ Y),$$

is a residuated lattice.

Proposition [Galatos & Jipsen 2013]

All simple rules are preserved by $(-)^+$.

Termination as a nuclear relation

Let $M = (R_k, Q, P)$ be a k-ACM and $W := (Q \cup R_k)^*$ be the free commutative monoid generated by $Q \cup R_k$.

Termination as a nuclear relation

Let $M = (R_k, Q, P)$ be a k-ACM and $W := (Q \cup R_k)^*$ be the free commutative monoid generated by $Q \cup R_k$.

The frame $\mathbf{W_M}$

Similar to Chvalovský & Horčík (2016) , we let $W' := W$ and define the relation $N_M \subseteq W \times W'$ via

$$x \, N_M \, z \quad \text{iff} \quad xz \leq_M q_f,$$

for all $x, z \in W$. Observe that, for any $x, y, z \in W$,

$$xy \, N_M \, z \iff xyz \leq_M q_f \iff x \, N_M \, yz.$$

Since W is commutive it follows that N_M is nuclear.

Termination as a nuclear relation

Let $M = (R_k, Q, P)$ be a k-ACM and $W := (Q \cup R_k)^*$ be the free commutative monoid generated by $Q \cup R_k$.

The frame $\mathbf{W_M}$

Similar to Chvalovský & Horčík (2016) , we let $W' := W$ and define the relation $N_M \subseteq W \times W'$ via

$$x \; N_M \; z \quad \text{iff} \quad xz \leq_M q_f,$$

for all $x, z \in W$. Observe that, for any $x, y, z \in W$,

$$xy \; N_M \; z \iff xyz \leq_M q_f \iff x \; N_M \; yz.$$

Since W is commutive it follows that N_M is nuclear.

Lemma

$\mathbf{W_M} := (W, W', N_M)$ *is a residuated frame,* $\mathbf{W}^+ \in \mathcal{CRL}$*, and there exists a valuation* $\nu : \mathrm{Fm} \to W^+$ *such that* $\mathbf{W}^+, \nu \models \mathrm{Th}(M)$.

Lemma

Let (d) *be any rule satisfying* $(\star)$*. Define* $\mathbf{W}_{\mathrm{d}(\mathbf{M})} := (W, W', N_{\mathrm{d}(M)})$*. Then* $\mathbf{W}^+_{\mathrm{d}(M)} \in \mathcal{CRL}_{\mathrm{d}}$*.*

Lemma

Let (d) *be any rule satisfying* $(\star)$*. Define* $\mathbf{W}_{\mathrm{d}(\mathbf{M})} := (W, W', N_{\mathrm{d}(M)})$*. Then* $\mathbf{W}^{+}_{\mathrm{d}(M)} \in \mathcal{CRL}_{\mathrm{d}}$*.*

Fix $M = \widetilde{M}$ be the 2-ACM such that it is undecidable whether $q_I \leq_M q_f$.

Theorem

Let (d) *be a rule satisfying* $(\star)$ *and* $(\star\star)$*, and let* $K \geq 2$ *be sufficiently large. Then it is undecidable whether* $\mathbf{W}^{+}_{\mathrm{d}(M_K)} \models \mathrm{Halt}_{\widetilde{M_K}}(q_I r_1 r_2)$*.*

Lemma

Let (d) *be any rule satisfying* $(\star)$*. Define* $\mathbf{W}_{\mathrm{d}(\mathbf{M})} := (W, W', N_{\mathrm{d}(M)})$*. Then* $\mathbf{W}^{+}_{\mathrm{d}(M)} \in \mathcal{CRL}_{\mathrm{d}}$*.*

Fix $M = \widetilde{M}$ be the 2-ACM such that it is undecidable whether $q_I \leq_M q_f$.

Theorem

Let (d) *be a rule satisfying* $(\star)$ *and* $(\star\star)$*, and let* $K \geq 2$ *be sufficiently large. Then it is undecidable whether* $\mathbf{W}^{+}_{\mathrm{d}(M_K)} \models \mathrm{Halt}_{\widetilde{M}_K}(q_I r_1 r_2)$*.*

Corollary

For any variety $\mathcal{V} \subseteq \mathcal{CRL}$*, if*

$$\mathbf{W}^{+}_{\mathrm{d}(M_K)} \in \mathcal{V},$$

then $\mathcal{V}$ *has an undecidable word problem, and hence an undecidable quasi-equational theory.*

Known results for Equational Theory

(k_n^m) represents the knotted rule $x^n \leq x^m$

Undecidable Eq. Theory	Decidable Eq. Theory
	$\mathcal{RL}$
	$\mathcal{CRL}$
$\mathcal{RL} + (\mathrm{k}_n^m), 1 \leq n < m$	
	$\mathcal{CRL} + (\mathrm{k}_n^m)$
$\mathcal{CRL} + (?)$	

We can encode the instructions of an ACM $M = (R_k, Q, P)$ as a single term θ_M using the full signature of of $\mathcal{CRL}$ via

$$\theta_M := 1 \wedge \bigwedge_{(C \leq_M u) \in P} C \to u.$$

Let (d) be given such that there exists $n \geq 1$ and $k, c_1, ..., c_n \geq 1$ such that

$$\mathbf{CRL}_{\mathrm{d}} \models x^k \leq \bigvee_{i=1}^{n} x^{k+c_i}, \qquad (\star\star\star)$$

then (d) can be used to "bootstrap" the undeciablity of the quasi-equation theory of $\mathcal{CRL}_{\mathrm{d}}$ to the equational theory.

Undecidable equational theory

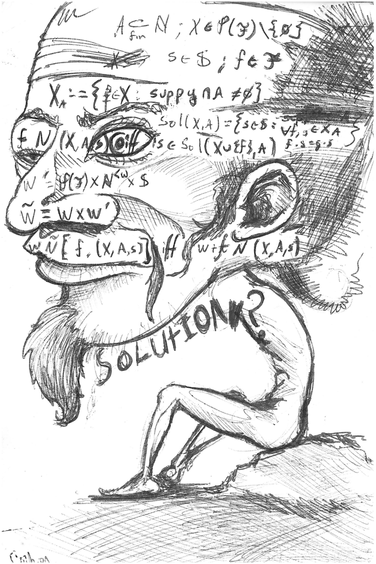
Corollary

Let (d) *be a rule satisfying* $(\star)$, $(\star\star)$, $(\star\star\star)$ *and let* $K \geq 2$ *be sufficiently large. Then it is undecidable whether*

$$\mathcal{CRL}_{\mathrm{d}} \models \theta_{M_K} \to (q_I r_1 r_2 \to q_F),$$

and therefore $\mathcal{CRL}_{\mathrm{d}}$ *has an undecidable equational theory.*

Thank You!



References

- C.J. van Alten, *The finite model property for knotted extensions of propositional linear logic.* J. Symbolic Logic 70 (2005), no. 1, 84-98.
- K. Chvalovský, R. Horčík, *Full Lambek calculus with contraction is undecidable.* J. Symbolic Logic 81 (2016), no. 2, 524-540.
- P. Lincoln, J. Mitchell, A. Scedrov, N. Shankar, *Decision problems for proposition linear logic.* Annals of Pure and Applied Logic 56 (1992), 239-311
- A. Urquhart, *The complexity of decision procedures in relevance logic. II,* J. Symbolic Logic 64 (1999), no. 4, 1774-1802.
- N. Galatos, P. Jipsen, *Residuated frames with applications to decidability.* Trans. Amer. Math. Soc. 365 (2013), no. 3, 1219-1249.