

Algebraic Methods from Substructural Logics and Formal Languages

Rostislav Horčík

Institute of Computer Science
Academy of Sciences of the Czech Republic

1st Annual Scientific Meeting of CE-ITI
13–14 December 2012

A warm introduction



Syntactic monoid

Definition

Given an alphabet Σ and a language $L \subseteq \Sigma^*$, we define

Syntactic monoid

Definition

Given an alphabet Σ and a language $L \subseteq \Sigma^*$, we define

① **syntactic congruence**:

$$x \sim_L y \quad \text{iff} \quad (\forall u, v \in \Sigma^*)(uxv \in L \Leftrightarrow uyv \in L),$$

Syntactic monoid

Definition

Given an alphabet Σ and a language $L \subseteq \Sigma^*$, we define

- 1 syntactic congruence:

$$x \sim_L y \quad \text{iff} \quad (\forall u, v \in \Sigma^*)(uxv \in L \Leftrightarrow uyv \in L),$$

- 2 syntactic monoid: $\mathbf{M}(L) = \Sigma^*/\sim_L$.

Syntactic monoid

Definition

Given an alphabet Σ and a language $L \subseteq \Sigma^*$, we define

- 1 syntactic congruence:

$$x \sim_L y \quad \text{iff} \quad (\forall u, v \in \Sigma^*)(uxv \in L \Leftrightarrow uyv \in L),$$

- 2 syntactic monoid: $\mathbf{M}(L) = \Sigma^* / \sim_L$.

Theorem

Syntactic monoid

Definition

Given an alphabet Σ and a language $L \subseteq \Sigma^*$, we define

- 1 syntactic congruence:

$$x \sim_L y \quad \text{iff} \quad (\forall u, v \in \Sigma^*)(uxv \in L \Leftrightarrow uyv \in L),$$

- 2 syntactic monoid: $\mathbf{M}(L) = \Sigma^*/\sim_L$.

Theorem

- 1 \sim_L is the *largest* congruence such that $L = \bigcup_{w \in L} w/\sim_L$.

Syntactic monoid

Definition

Given an alphabet Σ and a language $L \subseteq \Sigma^*$, we define

- 1 syntactic congruence:

$$x \sim_L y \quad \text{iff} \quad (\forall u, v \in \Sigma^*)(uxv \in L \Leftrightarrow uyv \in L),$$

- 2 syntactic monoid: $\mathbf{M}(L) = \Sigma^*/\sim_L$.

Theorem

- 1 \sim_L is the *largest* congruence such that $L = \bigcup_{w \in L} w/\sim_L$.
- 2 $\mathbf{M}(L)$ is *finite* iff L is *regular* (Myhill-Nerode Theorem).

Remarks

- Syntactic monoids were mainly applied in the realm of regular languages.

Remarks

- Syntactic monoids were mainly applied in the realm of regular languages.
- Eilenberg variety theorem – there is a bijection between varieties of regular languages and varieties of finite monoids.

Remarks

- Syntactic monoids were mainly applied in the realm of regular languages.
- Eilenberg variety theorem – there is a bijection between varieties of regular languages and varieties of finite monoids.
- Beyond regular languages – they do not contain sufficiently enough information to distinguish very different languages, e.g.

$$L_1 = \{ww^R \mid w \in \{0,1\}^*\},$$

$$L_2 = \{w \in \{0,1\}^* \mid w \text{ is prime}\}.$$

Remarks

- Syntactic monoids were mainly applied in the realm of regular languages.
- Eilenberg variety theorem – there is a bijection between varieties of regular languages and varieties of finite monoids.
- Beyond regular languages – they do not contain sufficiently enough information to distinguish very different languages, e.g.

$$L_1 = \{ww^R \mid w \in \{0,1\}^*\},$$

$$L_2 = \{w \in \{0,1\}^* \mid w \text{ is prime}\}.$$

- The syntactic congruence is known in AAL as **Leibniz congruence** which is used in the construction of **Lindenbaum-Tarski algebra** for a given theory.

Remarks

- Syntactic monoids were mainly applied in the realm of regular languages.
- Eilenberg variety theorem – there is a bijection between varieties of regular languages and varieties of finite monoids.
- Beyond regular languages – they do not contain sufficiently enough information to distinguish very different languages, e.g.

$$L_1 = \{ww^R \mid w \in \{0, 1\}^*\},$$

$$L_2 = \{w \in \{0, 1\}^* \mid w \text{ is prime}\}.$$

- The syntactic congruence is known in AAL as **Leibniz congruence** which is used in the construction of **Lindenbaum-Tarski algebra** for a given theory.
- Can other constructions/ideas from (substructural) logics be used in the language theory?

Residuated lattices

Definition

Let $\mathbf{M} = \langle M, \cdot, 1 \rangle$ be a monoid. A quasi-order \leq on M is called **compatible** if for all $x, y, u, v \in M$:

$$x \leq y \implies uxv \leq uyv .$$

Residuated lattices

Definition

Let $\mathbf{M} = \langle M, \cdot, 1 \rangle$ be a monoid. A quasi-order \leq on M is called **compatible** if for all $x, y, u, v \in M$:

$$x \leq y \implies uxv \leq uyv.$$

Definition

A **residuated lattice** $\mathbf{A} = \langle A, \wedge, \vee, \cdot, \backslash, /, 1 \rangle$ is a monoid such that $\langle A, \wedge, \vee \rangle$ is a lattice and for all $a, b, c \in A$:

$$a \cdot b \leq c \quad \text{iff} \quad b \leq a \backslash c \quad \text{iff} \quad a \leq c / b.$$

Powerset monoid

Example

Let $\mathbf{M} = \langle M, \cdot, 1 \rangle$ be a monoid. Then

$$\mathcal{P}(\mathbf{M}) = \langle \mathcal{P}(M), \cap, \cup, \cdot, \setminus, /, \{1\} \rangle$$

is a residuated lattice, where

$$X \cdot Y = \{xy \in M \mid x \in X, y \in Y\},$$

$$X \setminus Z = \{y \in M \mid X \cdot \{y\} \subseteq Z\},$$

$$Z/Y = \{x \in M \mid \{x\} \cdot Y \subseteq Z\}.$$

Powerset monoid

Example

Let $\mathbf{M} = \langle M, \cdot, 1 \rangle$ be a monoid. Then

$$\mathcal{P}(\mathbf{M}) = \langle \mathcal{P}(M), \cap, \cup, \cdot, \setminus, /, \{1\} \rangle$$

is a residuated lattice, where

$$X \cdot Y = \{xy \in M \mid x \in X, y \in Y\},$$

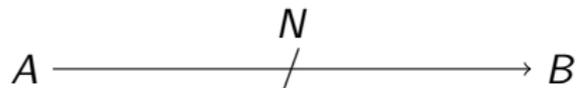
$$X \setminus Z = \{y \in M \mid X \cdot \{y\} \subseteq Z\},$$

$$Z/Y = \{x \in M \mid \{x\} \cdot Y \subseteq Z\}.$$

Other examples can be obtained by introducing a **suitable closure operator** on $\mathcal{P}(M)$.

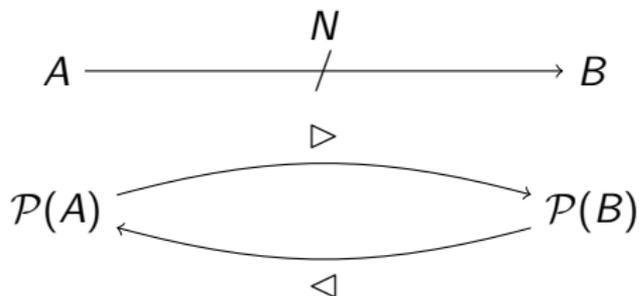
Closure operators

A **frame** $\mathbf{W} = \langle A, B, N \rangle$:



Closure operators

A frame $\mathbf{W} = \langle A, B, N \rangle$:

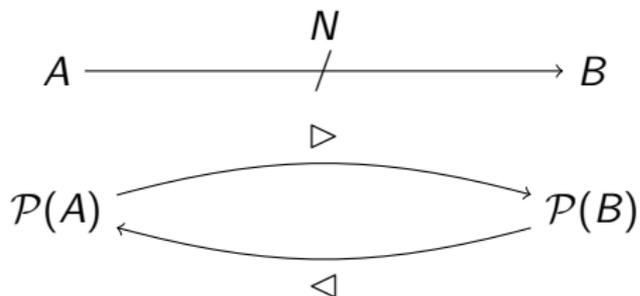


$$X^{\triangleright} = \{b \in B \mid (\forall a \in X)(a N b)\},$$

$$Y^{\triangleleft} = \{a \in A \mid (\forall b \in Y)(a N b)\}.$$

Closure operators

A **frame** $\mathbf{W} = \langle A, B, N \rangle$:



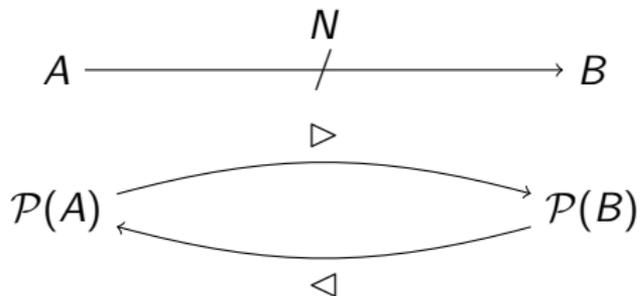
$$X^{\triangleright} = \{b \in B \mid (\forall a \in X)(a N b)\},$$

$$Y^{\triangleleft} = \{a \in A \mid (\forall b \in Y)(a N b)\}.$$

- $\gamma(X) = X^{\triangleright\triangleleft}$ is a closure operator on $\mathcal{P}(A)$.

Closure operators

A **frame** $\mathbf{W} = \langle A, B, N \rangle$:



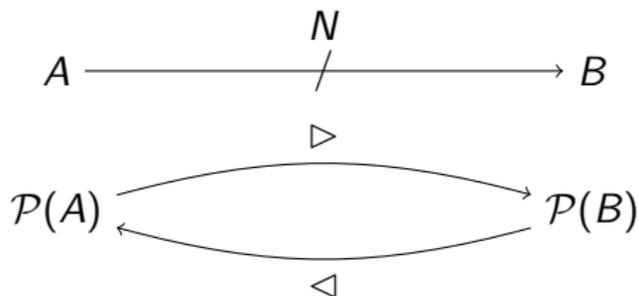
$$X^{\triangleright} = \{b \in B \mid (\forall a \in X)(a N b)\},$$

$$Y^{\triangleleft} = \{a \in A \mid (\forall b \in Y)(a N b)\}.$$

- $\gamma(X) = X^{\triangleright\triangleleft}$ is a closure operator on $\mathcal{P}(A)$.
- $\{\{b\}^{\triangleleft} \mid b \in B\}$ is its **basis**.

Closure operators

A **frame** $\mathbf{W} = \langle A, B, N \rangle$:



$$X^\triangleright = \{b \in B \mid (\forall a \in X)(a N b)\},$$

$$Y^\triangleleft = \{a \in A \mid (\forall b \in Y)(a N b)\}.$$

- $\gamma(X) = X^{\triangleright\triangleleft}$ is a closure operator on $\mathcal{P}(A)$.
- $\{\{b\}^\triangleleft \mid b \in B\}$ is its **basis**.
- The collection of closed sets forms a **complete lattice** $\mathbf{W}^+ = \langle \gamma[\mathcal{P}(A)], \cap, \cup_\gamma \rangle$, where

$$X \cup_\gamma Y = \gamma(X \cup Y).$$

Residuated frames

- Given a monoid \mathbf{A} and an frame $\mathbf{W} = \langle A, B, N \rangle$, define an extended frame $\widehat{\mathbf{W}} = \langle A, A^2 \times B, \widehat{N} \rangle$, where

$$x \widehat{N} \langle u, v, b \rangle \quad \text{iff} \quad uxv N b.$$

Residuated frames

- Given a monoid \mathbf{A} and an frame $\mathbf{W} = \langle A, B, N \rangle$, define an extended frame $\widehat{\mathbf{W}} = \langle A, A^2 \times B, \widehat{N} \rangle$, where

$$x \widehat{N} \langle u, v, b \rangle \quad \text{iff} \quad uxv N b.$$

- The closure operator γ induced by \widehat{N} is a **nucleus** (i.e., $\gamma(X)\gamma(Y) \subseteq \gamma(XY)$).

Residuated frames

- Given a monoid \mathbf{A} and an frame $\mathbf{W} = \langle A, B, N \rangle$, define an extended frame $\widehat{\mathbf{W}} = \langle A, A^2 \times B, \widehat{N} \rangle$, where

$$x \widehat{N} \langle u, v, b \rangle \quad \text{iff} \quad uxv N b.$$

- The closure operator γ induced by \widehat{N} is a **nucleus** (i.e., $\gamma(X)\gamma(Y) \subseteq \gamma(XY)$).
- Then $\widehat{\mathbf{W}}^+ = \langle \mathcal{P}(A)_\gamma, \cap, \cup, \circ, \backslash, /, \gamma\{1\} \rangle$ forms a **complete residuated lattice**, where $X \bullet_\gamma Y = \gamma(X \bullet Y)$ for $\bullet \in \{\circ, \backslash, /, \cup\}$.

Residuated frames

- Given a monoid \mathbf{A} and an frame $\mathbf{W} = \langle A, B, N \rangle$, define an extended frame $\widehat{\mathbf{W}} = \langle A, A^2 \times B, \widehat{N} \rangle$, where

$$x \widehat{N} \langle u, v, b \rangle \quad \text{iff} \quad uxv N b.$$

- The closure operator γ induced by \widehat{N} is a **nucleus** (i.e., $\gamma(X)\gamma(Y) \subseteq \gamma(XY)$).
- Then $\widehat{\mathbf{W}}^+ = \langle \mathcal{P}(A)_\gamma, \cap, \cup_\gamma, \circ_\gamma, \backslash_\gamma, /_\gamma, \gamma\{1\} \rangle$ forms a **complete residuated lattice**, where $X \bullet_\gamma Y = \gamma(X \bullet Y)$ for $\bullet \in \{\circ, \backslash, /, \cup\}$.
- The binary relation on A defined by

$$x \sqsubseteq y \quad \text{iff} \quad \gamma\{x\} \subseteq \gamma\{y\}$$

is a compatible quasi-order on \mathbf{A} .

Syntactic residuated lattice

Definition

Let $L \subseteq \Sigma^*$ be a language. Define frame $\mathbf{W} = \langle \Sigma^*, \{\star\}, N \rangle$, where $N \subseteq \Sigma^* \times \{\star\}$ is defined by

$$x N \star \quad \text{iff} \quad x \in L.$$

Then $\mathbf{R}(L) = \widehat{\mathbf{W}}^+$ is called the **syntactic residuated lattice** of L .

Syntactic residuated lattice

Definition

Let $L \subseteq \Sigma^*$ be a language. Define frame $\mathbf{W} = \langle \Sigma^*, \{\star\}, N \rangle$, where $N \subseteq \Sigma^* \times \{\star\}$ is defined by

$$x N \star \quad \text{iff} \quad x \in L.$$

Then $\mathbf{R}(L) = \widehat{\mathbf{W}}^+$ is called the **syntactic residuated lattice** of L .

Theorem

Syntactic residuated lattice

Definition

Let $L \subseteq \Sigma^*$ be a language. Define frame $\mathbf{W} = \langle \Sigma^*, \{\star\}, N \rangle$, where $N \subseteq \Sigma^* \times \{\star\}$ is defined by

$$x N \star \quad \text{iff} \quad x \in L.$$

Then $\mathbf{R}(L) = \widehat{\mathbf{W}}^+$ is called the **syntactic residuated lattice** of L .

Theorem

- 1 The nucleus γ is the **point-wise largest nucleus** making L a closed set.

Syntactic residuated lattice

Definition

Let $L \subseteq \Sigma^*$ be a language. Define frame $\mathbf{W} = \langle \Sigma^*, \{\star\}, N \rangle$, where $N \subseteq \Sigma^* \times \{\star\}$ is defined by

$$x N \star \quad \text{iff} \quad x \in L.$$

Then $\mathbf{R}(L) = \widehat{\mathbf{W}}^+$ is called the **syntactic residuated lattice** of L .

Theorem

- 1 The nucleus γ is the **point-wise largest nucleus** making L a closed set.
- 2 $\{\gamma\{x\} \mid x \in \Sigma^*\}$ forms a submonoid isomorphic to $\mathbf{M}(L)$.

Syntactic residuated lattice

Definition

Let $L \subseteq \Sigma^*$ be a language. Define frame $\mathbf{W} = \langle \Sigma^*, \{\star\}, N \rangle$, where $N \subseteq \Sigma^* \times \{\star\}$ is defined by

$$x N \star \quad \text{iff} \quad x \in L.$$

Then $\mathbf{R}(L) = \widehat{\mathbf{W}}^+$ is called the **syntactic residuated lattice** of L .

Theorem

- 1 The nucleus γ is the **point-wise largest nucleus** making L a closed set.
- 2 $\{\gamma\{x\} \mid x \in \Sigma^*\}$ forms a submonoid isomorphic to $\mathbf{M}(L)$.
- 3 $\mathbf{R}(L)$ is **finite** iff L is **regular**.

Generalized Myhill Theorem

The following theorem is the core of most decidability proofs we have for substructural logics.

Theorem

Let \mathbf{A} be a monoid and $\mathbf{W} = \langle A, B, N \rangle$ a frame where B is finite. Then $\widehat{\mathbf{W}}^+$ is *finite* iff there is a *compatible dual well quasi-order* \leq on \mathbf{A} such that

$$x \leq y, y N b \implies x N b.$$

Generalized Myhill Theorem

The following theorem is the core of most decidability proofs we have for substructural logics.

Theorem

Let \mathbf{A} be a monoid and $\mathbf{W} = \langle A, B, N \rangle$ a frame where B is finite. Then $\widehat{\mathbf{W}}^+$ is *finite* iff there is a *compatible dual well quasi-order* \leq on \mathbf{A} such that

$$x \leq y, y N b \implies x N b.$$

Corollary (Generalized Myhill Theorem – Ehrenfeucht, Rozenberg)

A language $L \subseteq \Sigma^*$ is regular iff L is downward closed w.r.t. a compatible dual well quasi-order on Σ^* .

Application

- Our decidability proof for the universal theory of residuated lattices satisfying $x^2 \leq x$ can be translated into the language theory.

Application

- Our decidability proof for the universal theory of residuated lattices satisfying $x^2 \leq x$ can be translated into the language theory.
- The variety of residuated lattices satisfying $x^2 \leq x$ can be equivalently axiomatized by

$$uxv \leq z \ \& \ uyv \leq z \implies uxyv \leq z.$$

Application

- Our decidability proof for the universal theory of residuated lattices satisfying $x^2 \leq x$ can be translated into the language theory.
- The variety of residuated lattices satisfying $x^2 \leq x$ can be equivalently axiomatized by

$$uxv \leq z \ \& \ uyv \leq z \implies uxyv \leq z.$$

Theorem

Every language $L \subseteq \Sigma^*$ closed under the following rule is *regular*:

$$uxv, uyv \in L \implies uxyv \in L. \quad (r)$$

Application

- Our decidability proof for the universal theory of residuated lattices satisfying $x^2 \leq x$ can be translated into the language theory.
- The variety of residuated lattices satisfying $x^2 \leq x$ can be equivalently axiomatized by

$$uxv \leq z \ \& \ uyv \leq z \implies uxyv \leq z.$$

Theorem

Every language $L \subseteq \Sigma^*$ closed under the following rule is **regular**:

$$uxv, uyv \in L \implies uxyv \in L. \quad (r)$$

Example

The language $a^+(b(a+b+c)^*b+b)c^+$ is closed under (r).

Application (cont.)

- Consider a closure operator $\gamma: \mathcal{P}(\Sigma^*) \rightarrow \mathcal{P}(\Sigma^*)$ s.t. its closed sets are closed under the rule:

$$uxv, uyv \in L \implies uxyv \in L.$$

Application (cont.)

- Consider a closure operator $\gamma: \mathcal{P}(\Sigma^*) \rightarrow \mathcal{P}(\Sigma^*)$ s.t. its closed sets are closed under the rule:

$$uxv, uyv \in L \implies uxyv \in L.$$

- Then γ is nucleus on $\mathcal{P}(\Sigma^*)$ and the following relation is a compatible quasi-order on Σ^* :

$$x \sqsubseteq y \quad \text{iff} \quad \gamma\{x\} \subseteq \gamma\{y\}.$$

Application (cont.)

- Consider a closure operator $\gamma: \mathcal{P}(\Sigma^*) \rightarrow \mathcal{P}(\Sigma^*)$ s.t. its closed sets are closed under the rule:

$$uxv, uyv \in L \implies uxyv \in L.$$

- Then γ is nucleus on $\mathcal{P}(\Sigma^*)$ and the following relation is a compatible quasi-order on Σ^* :

$$x \sqsubseteq y \quad \text{iff} \quad \gamma\{x\} \subseteq \gamma\{y\}.$$

- In order to show that L has to be regular, it suffices to show that \sqsubseteq is a dual well quasi-order using the generalized Myhill theorem.

Higman's lemma

Definition

Let $\langle Q, \leq \rangle$ be a quasi-ordered set. Define a binary relation \leq^* on Q^* by

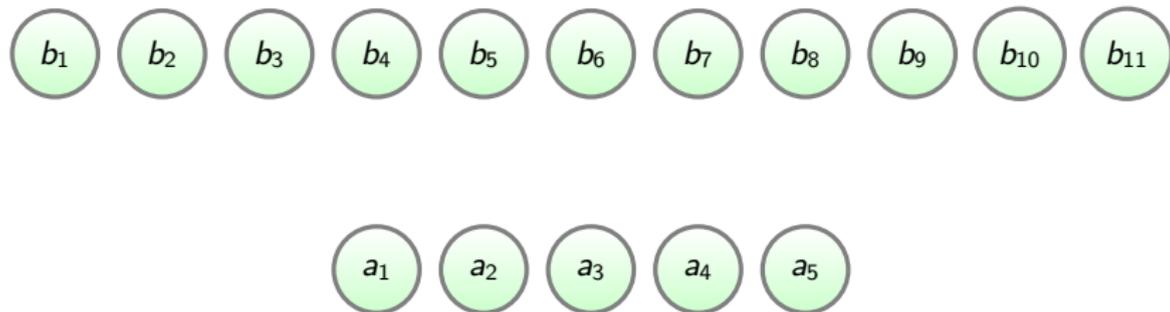
$a_1 \dots a_n \leq^* b_1 \dots b_m$ iff there is a strictly increasing map $f: [1, n] \rightarrow [1, m]$ s.t. $a_i \leq b_{f(i)}$ for all $i \in [1, n]$.

Higman's lemma

Definition

Let $\langle Q, \leq \rangle$ be a quasi-ordered set. Define a binary relation \leq^* on Q^* by

$a_1 \dots a_n \leq^* b_1 \dots b_m$ iff there is a strictly increasing map $f: [1, n] \rightarrow [1, m]$ s.t. $a_i \leq b_{f(i)}$ for all $i \in [1, n]$.

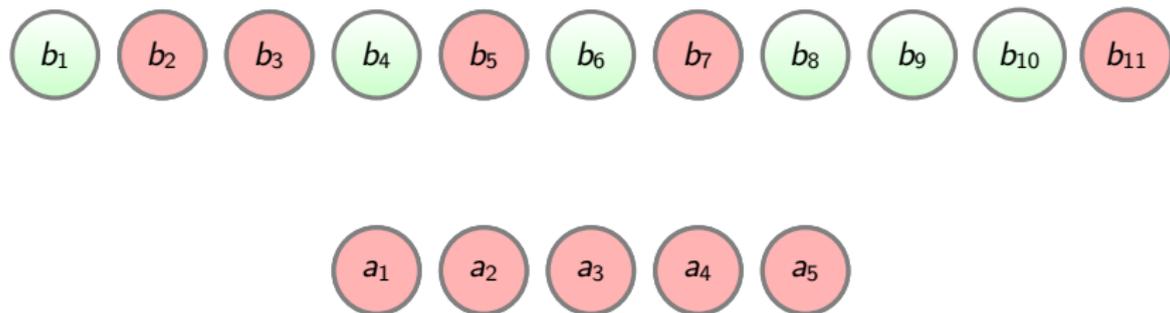


Higman's lemma

Definition

Let $\langle Q, \leq \rangle$ be a quasi-ordered set. Define a binary relation \leq^* on Q^* by

$a_1 \dots a_n \leq^* b_1 \dots b_m$ iff there is a strictly increasing map $f: [1, n] \rightarrow [1, m]$ s.t. $a_i \leq b_{f(i)}$ for all $i \in [1, n]$.

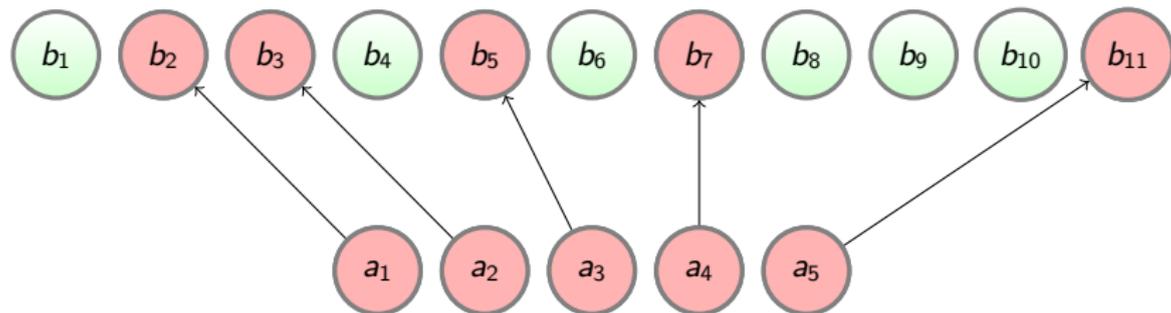


Higman's lemma

Definition

Let $\langle Q, \leq \rangle$ be a quasi-ordered set. Define a binary relation \leq^* on Q^* by

$a_1 \dots a_n \leq^* b_1 \dots b_m$ iff there is a strictly increasing map $f: [1, n] \rightarrow [1, m]$ s.t. $a_i \leq b_{f(i)}$ for all $i \in [1, n]$.

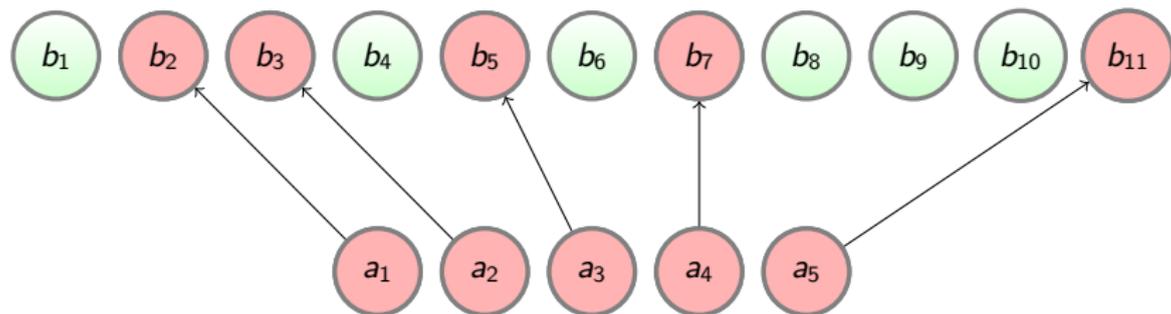


Higman's lemma

Definition

Let $\langle Q, \leq \rangle$ be a quasi-ordered set. Define a binary relation \leq^* on Q^* by

$a_1 \dots a_n \leq^* b_1 \dots b_m$ iff there is a strictly increasing map $f: [1, n] \rightarrow [1, m]$ s.t. $a_i \leq b_{f(i)}$ for all $i \in [1, n]$.



Lemma (Higman's lemma)

If $\langle Q, \leq \rangle$ is a well quasi-ordered set then so is $\langle Q^*, \leq^* \rangle$.

Modified Higman's lemma

Definition

Let $\langle Q, \leq \rangle$ be a quasi-ordered set. Define a binary relation \leq^+ on Q^+ by

$a_1 \dots a_n \leq^+ b_1 \dots b_m$ iff there is a strictly increasing map

$f: [1, n+1] \rightarrow [1, m+1]$ such that

- $f(1) = 1$ and $f(n+1) = m+1$,
- $a_i \leq b_{f(i)}$ and $a_i \leq b_{f(i+1)-1}$ for all $i \in [1, n]$.

Modified Higman's lemma

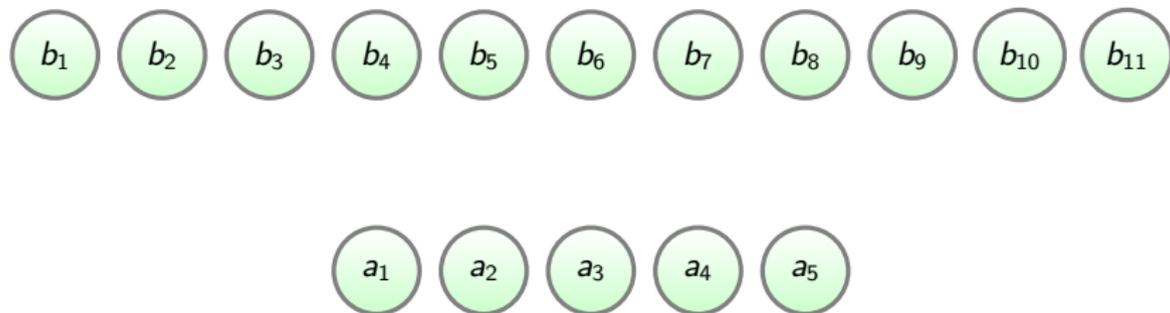
Definition

Let $\langle Q, \leq \rangle$ be a quasi-ordered set. Define a binary relation \leq^+ on Q^+ by

$a_1 \dots a_n \leq^+ b_1 \dots b_m$ iff there is a strictly increasing map

$f: [1, n+1] \rightarrow [1, m+1]$ such that

- $f(1) = 1$ and $f(n+1) = m+1$,
- $a_i \leq b_{f(i)}$ and $a_i \leq b_{f(i+1)-1}$ for all $i \in [1, n]$.



Modified Higman's lemma

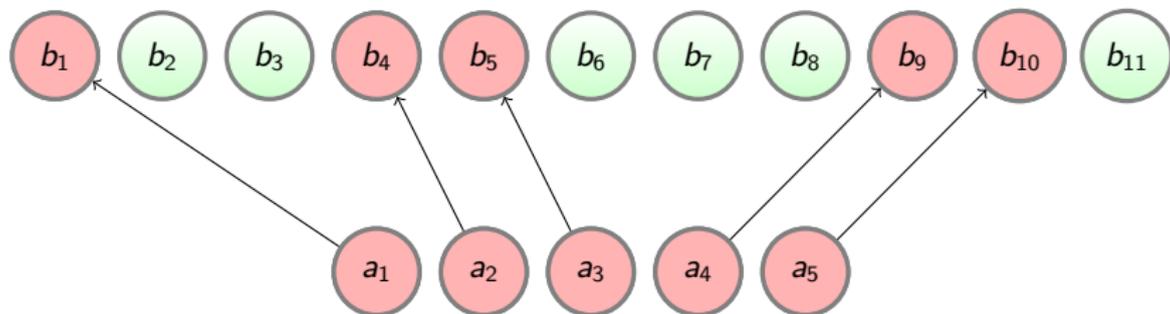
Definition

Let $\langle Q, \leq \rangle$ be a quasi-ordered set. Define a binary relation \leq^+ on Q^+ by

$a_1 \dots a_n \leq^+ b_1 \dots b_m$ iff there is a strictly increasing map

$f: [1, n+1] \rightarrow [1, m+1]$ such that

- $f(1) = 1$ and $f(n+1) = m+1$,
- $a_i \leq b_{f(i)}$ and $a_i \leq b_{f(i+1)-1}$ for all $i \in [1, n]$.



Modified Higman's lemma

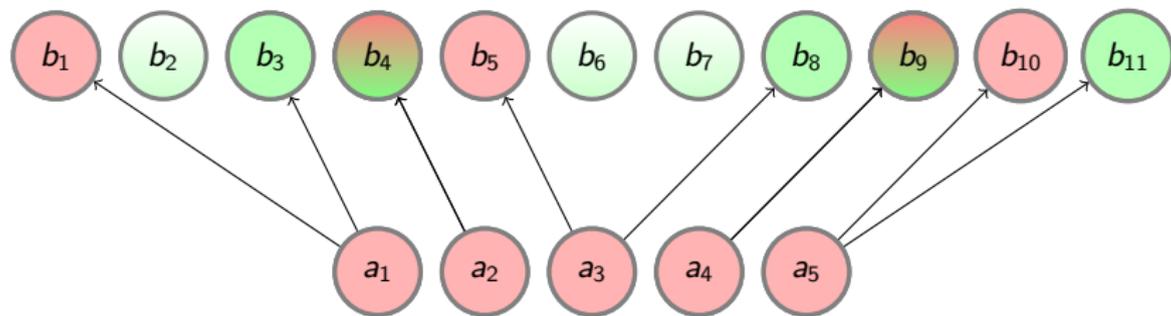
Definition

Let $\langle Q, \leq \rangle$ be a quasi-ordered set. Define a binary relation \leq^+ on Q^+ by

$a_1 \dots a_n \leq^+ b_1 \dots b_m$ iff there is a strictly increasing map

$f: [1, n+1] \rightarrow [1, m+1]$ such that

- $f(1) = 1$ and $f(n+1) = m+1$,
- $a_i \leq b_{f(i)}$ and $a_i \leq b_{f(i+1)-1}$ for all $i \in [1, n]$.



Modified Higman's lemma (cont.)

Lemma

If $\langle Q, \leq \rangle$ is a well quasi-ordered set then $\langle Q^+, \leq^+ \rangle$ forms a well quasi-ordered set as well.

Modified Higman's lemma (cont.)

Lemma

If $\langle Q, \leq \rangle$ is a well quasi-ordered set then $\langle Q^+, \leq^+ \rangle$ forms a well quasi-ordered set as well.

Lemma

Let $w \in \Sigma^$ and $\text{Alph}(w) = \Gamma$. Then $wuw \sqsubseteq w$ for every $u \in \Gamma^*$.*

Beyond regular languages?

Let $\Sigma = \{0, 1\}$.

$$L_1 = \{ww^R \mid w \in \Sigma^*\},$$

$$L_2 = \{w \in \Sigma^* \mid w \text{ is prime}\}.$$

Beyond regular languages?

Let $\Sigma = \{0, 1\}$.

$$L_1 = \{ww^R \mid w \in \Sigma^*\},$$

$$L_2 = \{w \in \Sigma^* \mid w \text{ is prime}\}.$$

Consider the following rule:

$$uxv, ux^2v \in L \implies uv \in L. \quad (r)$$

Then L_1 is closed under (r) and L_2 not.

Beyond regular languages?

Let $\Sigma = \{0, 1\}$.

$$L_1 = \{ww^R \mid w \in \Sigma^*\},$$

$$L_2 = \{w \in \Sigma^* \mid w \text{ is prime}\}.$$

Consider the following rule:

$$uxv, ux^2v \in L \implies uv \in L. \quad (r)$$

Then L_1 is closed under (r) and L_2 not.

The rule (r) is equivalent to

$$1 \leq x \vee x^2 \vee x \setminus y.$$

Thus the languages L_1, L_2 can be separated by a variety of residuated lattices.

Thank you!