Layer Systems for Confluence — Formalized

Bertram Felgenhauer

Computational Logic

Master Seminar 1 2018-01-17

Context

Automating Confluence

- CSI – tool for proving (non-)confluence of term rewrite systems

Certification

- CeTA – certifier for termination, confluence and more

Formalization

- IsaFoR – formalization of rewriting

Term Rewriting

$$+(x, 0) \to x \qquad +(x, \mathsf{S}(y)) \to \mathsf{S}(+(x, y))$$

$$+(0, \underline{+(0, \mathsf{S}(\mathsf{S}(0)))})$$

Term Rewriting

$$+(x, 0) \to x \qquad +(x, \mathsf{S}(y)) \to \mathsf{S}(+(x, y))$$

$$+(0, \underline{+(0, \mathsf{S}(\mathsf{S}(0)))}) \downarrow \underline{+(0, \mathsf{S}(\underline{+(0, \mathsf{S}(0))}))}$$

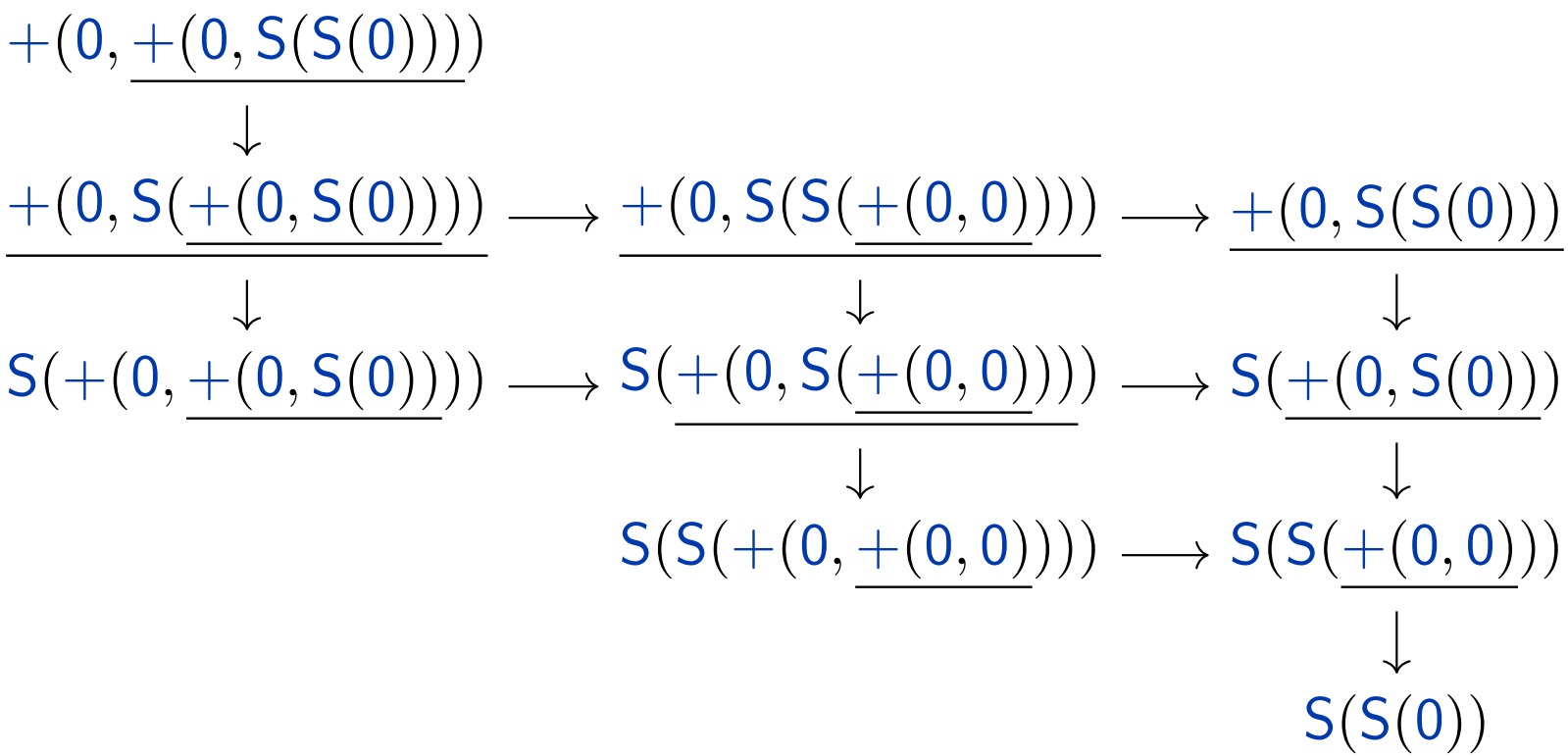
Term Rewriting

$$+(x, 0) \to x \qquad +(x, \mathsf{S}(y)) \to \mathsf{S}(+(x, y))$$

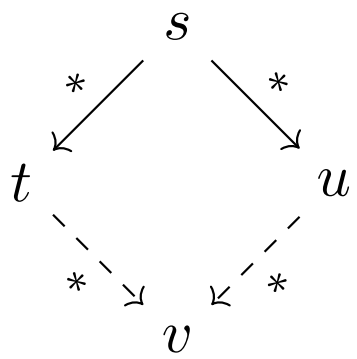
$$\begin{array}{c} +(0, \underline{+(0, \mathsf{S}(\mathsf{S}(0)))}) \\ \downarrow \\ \underline{+(0, \mathsf{S}(\underline{+(0, \mathsf{S}(0))}))} \\ \downarrow \\ \mathsf{S}(+(0, \underline{+(0, \mathsf{S}(0))})) \end{array} \longrightarrow \underline{+(0, \mathsf{S}(\mathsf{S}(\underline{+(0, 0)})))}$$

Term Rewriting

$$+(x, 0) \to x \qquad +(x, \mathsf{S}(y)) \to \mathsf{S}(+(x, y))$$



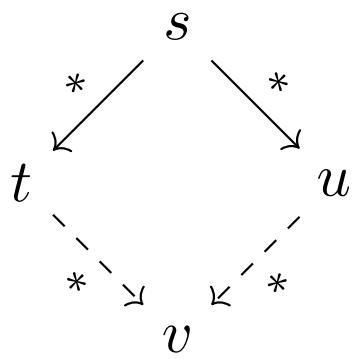
Confluence



Definition

- $s \to^* t \wedge s \to^* u \implies \exists v.\, t \to^* v \wedge u \to^* v$

Confluence



Definition

- $s \to^* t \wedge s \to^* u \implies \exists v.\, t \to^* v \wedge u \to^* v$

Criteria

- Orthogonality: left-linear, no critical pairs
- Knuth-Bendix: terminating, joinable critical pairs
- ...

Example

$$@(@(\mathsf{K}, x), y) \to x \qquad @(@(@(\mathsf{S}, x), y), z) \to @(@(x, z), @(y, z))$$
$$\mathsf{e}(x, x) \to \top$$

Orthogonal?

Example

$$\mathsf{@}(\mathsf{@}(\mathsf{K}, x), y) \to x \qquad \mathsf{@}(\mathsf{@}(\mathsf{@}(\mathsf{S}, x), y), z) \to \mathsf{@}(\mathsf{@}(x, z), \mathsf{@}(y, z))$$
$$\mathsf{e}(x, x) \to \top$$

Orthogonal?

- not left-linear ☹
- no critical pairs ☺

Example

$$\mathsf{@}(\mathsf{@}(\mathsf{K}, x), y) \to x \qquad \mathsf{@}(\mathsf{@}(\mathsf{@}(\mathsf{S}, x), y), z) \to \mathsf{@}(\mathsf{@}(x, z), \mathsf{@}(y, z))$$
$$\mathsf{e}(x, x) \to \top$$

Orthogonal?

- not left-linear ☹
- no critical pairs ☺

Knuth-Bendix?

Example

$$\mathsf{@}(\mathsf{@}(\mathsf{K}, x), y) \to x \qquad \mathsf{@}(\mathsf{@}(\mathsf{@}(\mathsf{S}, x), y), z) \to \mathsf{@}(\mathsf{@}(x, z), \mathsf{@}(y, z))$$
$$\mathsf{e}(x, x) \to \top$$

Orthogonal?

- not left-linear ☹
- no critical pairs ☺

Knuth-Bendix?

- non-terminating ☹

$$\mathsf{@}(\mathsf{@}(\mathsf{@}(\mathsf{S}, \mathsf{I}), \mathsf{I}), \mathsf{@}(\mathsf{@}(\mathsf{S}, \mathsf{I}), \mathsf{I})) \to^+ \mathsf{@}(\mathsf{@}(\mathsf{@}(\mathsf{S}, \mathsf{I}), \mathsf{I}), \mathsf{@}(\mathsf{@}(\mathsf{S}, \mathsf{I}), \mathsf{I}))$$

  where $\mathsf{I} = \mathsf{@}(\mathsf{@}(\mathsf{S}, \mathsf{K}), \mathsf{K})$

- joinable critical pairs ☺

Modularity

Theorem

Let $\mathcal{R}_1$, $\mathcal{R}_2$ be TRSs over disjoint signatures. Then

$$\mathsf{CR}(\mathcal{R}_1 \cup \mathcal{R}_2) \iff \mathsf{CR}(\mathcal{R}_1) \wedge \mathsf{CR}(\mathcal{R}_2)$$

Modularity

Theorem

Let $\mathcal{R}_1$, $\mathcal{R}_2$ be TRSs over disjoint signatures. Then

$$\mathsf{CR}(\mathcal{R}_1 \cup \mathcal{R}_2) \iff \mathsf{CR}(\mathcal{R}_1) \wedge \mathsf{CR}(\mathcal{R}_2)$$

Example

$$\mathsf{@}(\mathsf{@}(\mathsf{K}, x), y) \to x \qquad \mathsf{@}(\mathsf{@}(\mathsf{@}(\mathsf{S}, x), y), z) \to \mathsf{@}(\mathsf{@}(x, z), \mathsf{@}(y, z))$$
$$\mathsf{e}(x, x) \to \top$$

Modularity

Theorem

Let $\mathcal{R}_1$, $\mathcal{R}_2$ be TRSs over disjoint signatures. Then

$$\mathsf{CR}(\mathcal{R}_1 \cup \mathcal{R}_2) \iff \mathsf{CR}(\mathcal{R}_1) \wedge \mathsf{CR}(\mathcal{R}_2)$$

Example

$$\mathsf{@}(\mathsf{@}(\mathsf{K}, x), y) \to x \qquad \mathsf{@}(\mathsf{@}(\mathsf{@}(\mathsf{S}, x), y), z) \to \mathsf{@}(\mathsf{@}(x, z), \mathsf{@}(y, z))$$
$$\mathsf{e}(x, x) \to \top$$

- first two rules are orthogonal ☺

Modularity

Theorem

Let $\mathcal{R}_1$, $\mathcal{R}_2$ be TRSs over disjoint signatures. Then

$$\mathsf{CR}(\mathcal{R}_1 \cup \mathcal{R}_2) \iff \mathsf{CR}(\mathcal{R}_1) \wedge \mathsf{CR}(\mathcal{R}_2)$$

Example

$$\mathsf{@}(\mathsf{@}(\mathsf{K}, x), y) \to x \qquad \mathsf{@}(\mathsf{@}(\mathsf{@}(\mathsf{S}, x), y), z) \to \mathsf{@}(\mathsf{@}(x, z), \mathsf{@}(y, z))$$
$$\mathsf{e}(x, x) \to \top$$

- first two rules are orthogonal ☺
- last rule is terminating, and has no critical pairs ☺

Modularity

Theorem

Let $\mathcal{R}_1$, $\mathcal{R}_2$ be TRSs over disjoint signatures. Then

$$\mathsf{CR}(\mathcal{R}_1 \cup \mathcal{R}_2) \iff \mathsf{CR}(\mathcal{R}_1) \wedge \mathsf{CR}(\mathcal{R}_2)$$

Example

$$\mathsf{@}(\mathsf{@}(\mathsf{K}, x), y) \to x \qquad \mathsf{@}(\mathsf{@}(\mathsf{@}(\mathsf{S}, x), y), z) \to \mathsf{@}(\mathsf{@}(x, z), \mathsf{@}(y, z))$$
$$\mathsf{e}(x, x) \to \top$$

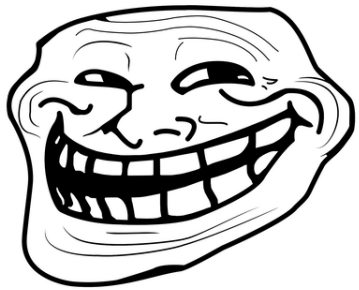
- first two rules are orthogonal ☺
- last rule is terminating, and has no critical pairs ☺
- disjoint signatures $\implies$ confluent by modularity ☺ ■

So...

- modularity looks useful
- let's prove it...

So...

- modularity looks useful
- let's prove it...



How hard could it be?

Proving Modularity

History

- Toyama 1987
- Klop *et al.* 1994
- van Oostrom 2008
- ...

Proving Modularity

History

- Toyama 1987
- Klop *et al.* 1994
- van Oostrom 2008
- ...

Proof idea

Proving Modularity

History

- Toyama 1987
- Klop *et al.* 1994
- van Oostrom 2008
- ...

Proof idea

- $\Longrightarrow$ is easy (homogeneous terms are closed under rewriting)

Proving Modularity

History

- Toyama 1987
- Klop *et al.* 1994
- van Oostrom 2008
- ...

Proof idea

- $\Longrightarrow$ is easy (homogeneous terms are closed under rewriting)
- recursively decompose terms into maximal homogeneous top and aliens

Proving Modularity

History

- Toyama 1987
- Klop *et al.* 1994
- van Oostrom 2008
- ...

Proof idea

- $\Longrightarrow$ is easy (homogeneous terms are closed under rewriting)
- recursively decompose terms into maximal homogeneous top and aliens
- use induction on rank

Proving Modularity

History

- Toyama 1987
- Klop *et al.* 1994
- van Oostrom 2008
- ...

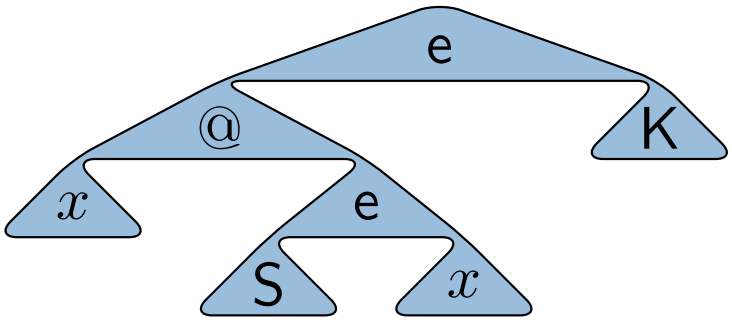
Proof idea

- $\Longrightarrow$ is easy (homogeneous terms are closed under rewriting)
- recursively decompose terms into maximal homogeneous top and aliens
- use induction on rank
- ...details are complicated

Example

$$\mathsf{@}(\mathsf{@}(\mathsf{K}, x), y) \to x \qquad \mathsf{@}(\mathsf{@}(\mathsf{@}(\mathsf{S}, x), y), z) \to \mathsf{@}(\mathsf{@}(x, z), \mathsf{@}(y, z))$$
$$\mathsf{e}(x, x) \to \top$$

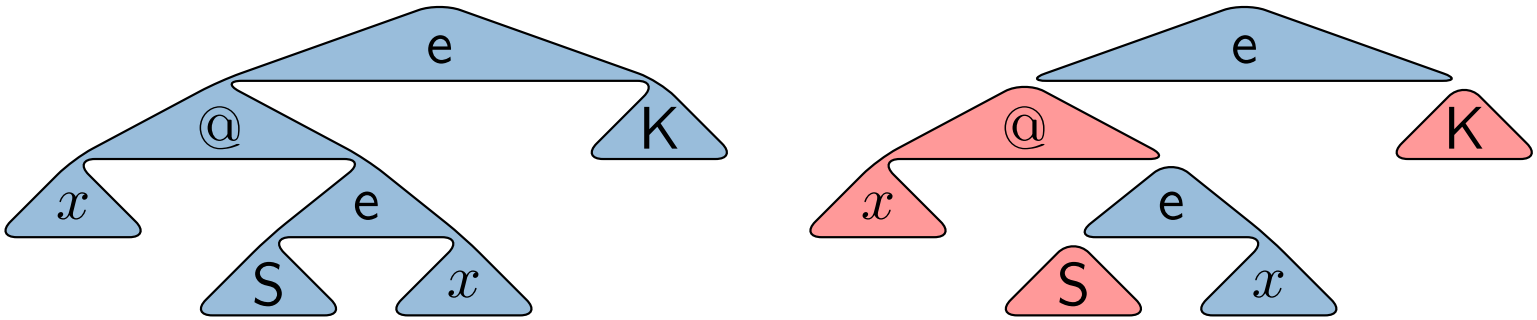
- $\mathsf{e}(\mathsf{@}(x, \mathsf{e}(\mathsf{S}, x)), \mathsf{K})$



Example

$$\mathsf{@}(\mathsf{@}(\mathsf{K}, x), y) \to x \qquad \mathsf{@}(\mathsf{@}(\mathsf{@}(\mathsf{S}, x), y), z) \to \mathsf{@}(\mathsf{@}(x, z), \mathsf{@}(y, z))$$
$$\mathsf{e}(x, x) \to \top$$

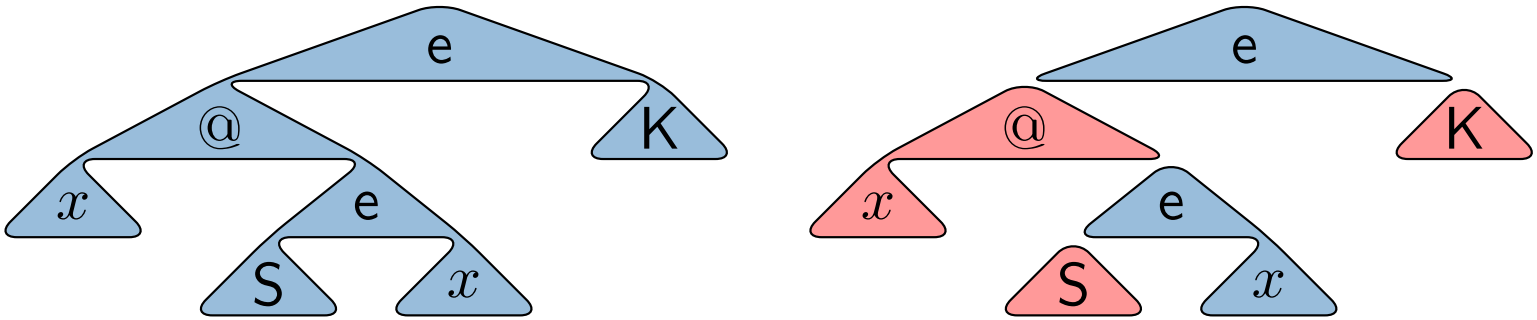
- $\mathsf{e}(\mathsf{@}(x, \mathsf{e}(\mathsf{S}, x)), \mathsf{K})$



Example

$$\mathsf{@}(\mathsf{@}(\mathsf{K}, x), y) \to x \qquad \mathsf{@}(\mathsf{@}(\mathsf{@}(\mathsf{S}, x), y), z) \to \mathsf{@}(\mathsf{@}(x, z), \mathsf{@}(y, z))$$
$$\mathsf{e}(x, x) \to \top$$

- $\mathsf{e}(\mathsf{@}(x, \mathsf{e}(\mathsf{S}, x)), \mathsf{K})$



- max-top $\mathsf{e}(\square, \square)$, aliens $\mathsf{@}(x, \mathsf{e}(\mathsf{S}, x))$ and K, rank 4

Related Results

Results

- Persistence (Aoto and Toyama 1997)
- Layer preservation (Ohlebusch 1994)
- Currying (Kahrs 1995)
- Order-sorted persistence (Aoto and Toyama 1996, F. *et al.* 2015)
- ...

Related Results

Results

- Persistence (Aoto and Toyama 1997)
- Layer preservation (Ohlebusch 1994)
- Currying (Kahrs 1995)
- Order-sorted persistence (Aoto and Toyama 1996, F. *et al.* 2015)
- ...

Proof idea

- $\Longrightarrow$ is easy
- recursively decompose terms into max-top and aliens
- use induction on rank
- ...details are complicated

Table of Contents

Layer Systems in a Nutshell

Goals

- abstract from all these proofs
- separate confluence proof and max-top properties

Layer Systems in a Nutshell

Goals

- abstract from all these proofs
- separate confluence proof and max-top properties

Idea

- layer system $\mathfrak{L}$: set of potential tops

Layer Systems in a Nutshell

Goals

- abstract from all these proofs
- separate confluence proof and max-top properties

Idea

- layer system $\mathfrak{L}$: set of potential tops
- result: if $\mathcal{R}$ is confluent on $\mathfrak{L}$, then $\mathcal{R}$ is confluent

Layer Systems

Concepts

- layer system $\mathfrak{L}$: set of multi-hole contexts
- top of t: $L \in \mathfrak{L}$ with $L \sqsubseteq t$
- max-top, aliens, rank
- weakly layered, layered

Layer Systems

Concepts

- layer system $\mathfrak{L}$: set of multi-hole contexts
- top of t: $L \in \mathfrak{L}$ with $L \sqsubseteq t$
- max-top, aliens, rank
- weakly layered, layered

Main Results

- If $\mathcal{R}$ is layered wrt. $\mathfrak{L}$ and terms of rank 1 are confluent, then $\mathcal{R}$ is confluent.
- ...

Layer Systems

Concepts

- layer system $\mathfrak{L}$: set of multi-hole contexts
- top of t: $L \in \mathfrak{L}$ with $L \sqsubseteq t$
- max-top, aliens, rank
- weakly layered, layered

Main Results

- If $\mathcal{R}$ is layered wrt. $\mathfrak{L}$ and terms of rank 1 are confluent, then $\mathcal{R}$ is confluent.
- ...

Applications

- modularity: $\mathcal{R}_1 \cup \mathcal{R}_2$ is layered by $\mathcal{T}(\mathcal{F}_1, \mathcal{V}) \cup \mathcal{T}(\mathcal{F}_2, \mathcal{V})$.
- ...

Layer Systems Definition

Definition

Under the following conditions, the TRS $\mathcal{R}$ is layered wrt. $\mathfrak{L}$:

- L_1 Every term in $\mathcal{T}(\mathcal{F},\mathcal{V})$ has a non-empty top
- L_2 If $x \in \mathcal{V}$ and $C \in \mathcal{C}$, then $C[x]_p \in \mathfrak{L}$ if and only if $C[\Box]_p \in \mathfrak{L}$
- L_3 If $L, N \in \mathfrak{L}$, $p \in \mathcal{P}\mathrm{os}_{\mathcal{F}}(L)$, and $L|_p \sqcup N$ is defined, then $L[L|_p \sqcup N]_p \in \mathfrak{L}$
- W If M is the max-top of s, $p \in \mathcal{P}\mathrm{os}_{\mathcal{F}}(M)$, and $s \to_{p,\ell\to r} t$ with $\ell \to r \in \mathcal{R}$, then $M \to_{p,\ell\to r} L$ for some $L \in \mathfrak{L}$
- C_1 In (W), either L is the max-top of t or $L = \Box$
- C_2 If $L, N \in \mathfrak{L}$ and $L \sqsubseteq N$, then $L[N|_p]_p \in \mathfrak{L}$ for any $p \in \mathcal{P}\mathrm{os}_{\Box}(L)$

Layer Systems Definition

Definition

Under the following conditions, the TRS $\mathcal{R}$ is layered wrt. $\mathfrak{L}$:

L_1
L_2
L_3

DON'T PANIC

W

it's formalized

C_1
C_2

Table of Contents

Challenges

The interesting challenge

- interface between confluence result and applications (enables division of labor)

Challenges

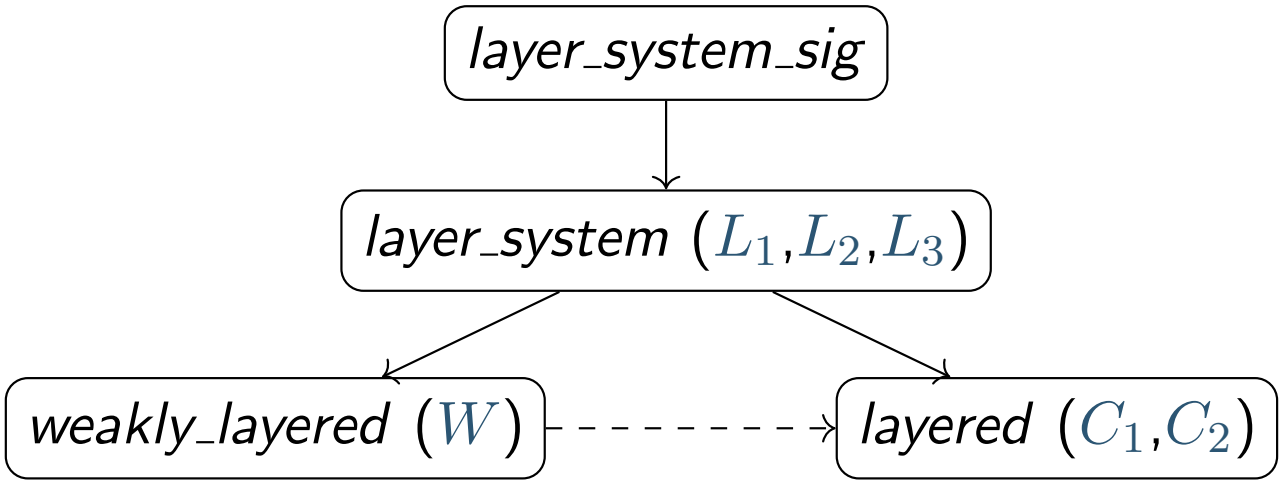
The interesting challenge

- interface between confluence result and applications
  (enables division of labor)

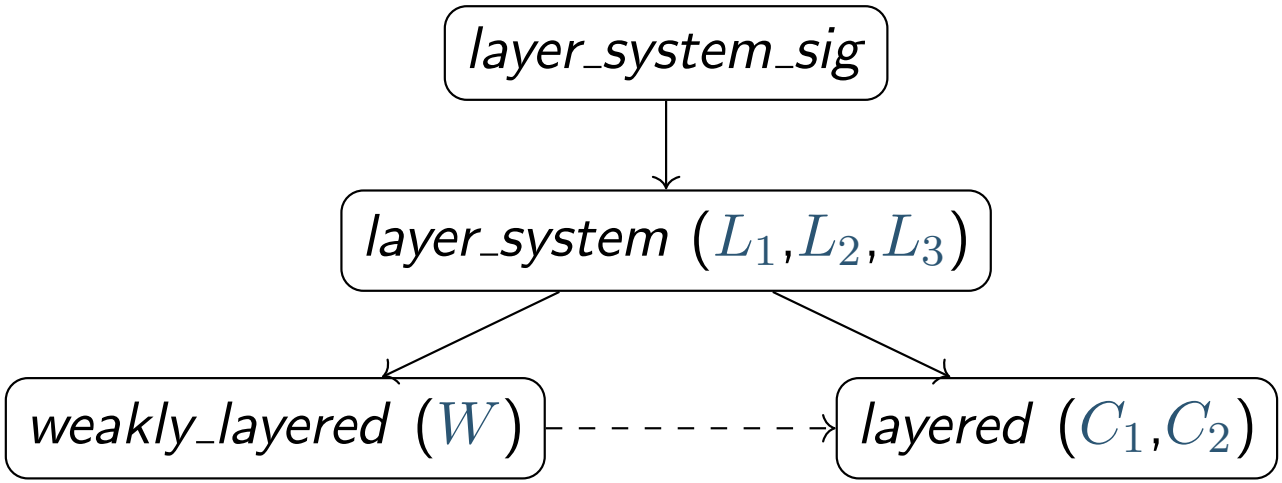
Miscellanea

- express properties algebraically
- *obvious*
  nice abstraction for multi-hole contexts
- motivation

Interface challenge



Interface challenge



Locales

- bundle assumptions and conclusions (the interface)
- can be instantiated (for applications)
- results based on the assumptions can be proved inside the locale (for main result)

Results and Effort

(BF) definitions, basic results about layers 3.2k

(BF) if $\mathcal{R}$ is layered by $\mathfrak{L}$, and $\mathcal{R}$ is confluent on $\mathfrak{L}$, then $\mathcal{R}$ is confluent 2.0k

(FR) for disjoint $\mathcal{R}_1$ and $\mathcal{R}_2$, $\mathcal{R}_1 \cup \mathcal{R}_2$ is layered by homogeneous terms
$\Longrightarrow$ modularity 0.8k

(FR) for many-sorted $\mathcal{R}$, $\mathcal{R}$ is layered by well-typed terms
$\Longrightarrow$ persistence 1.5k

(FR) for any $\mathcal{R}$, $\mathsf{Cu}(\mathcal{R})$ is layered by a layer system
$\Longrightarrow$ preservation of confluence by currying 3.8k

(BF) executable persistence check for CeTA 0.6k

total: 12k lines of proof

Table of Contents

Implementation

Notes

- part of CSI
- order-sorted persistence was available
- add many-sorted persistence
- add proof output

CSI + CeTA

Demo

Experiments

	CSI✓	+pd✓	+os	CSI
yes	148	153+	155	244
no	162	162	162	162
maybe	127	122	120	31
total	437	437	437	437

Conclusion

Done

- formalization of layer systems in Isabelle
- modularity, persistence, and currying
- certification for persistence-based decomposition
- important theoretical result

Conclusion

Done

- formalization of layer systems in Isabelle
- modularity, persistence, and currying
- certification for persistence-based decomposition
- important theoretical result

Open

- order-sorted persistence
- further applications
- currying is foundation for efficient GTRS confluence check

Conclusion

Done

- formalization of layer systems in Isabelle
- modularity, persistence, and currying
- certification for persistence-based decomposition
- important theoretical result

Open

- order-sorted persistence
- further applications
- currying is foundation for efficient GTRS confluence check

Thanks!