Semantic Cut Elimination for the Logic of Bunched Implications and Structural Extensions

(as formalized in Coq)

Dan Frumin

Grolog, 13 Oct

What's in the title?

Semantic cut elimination for the logic of Bunched Implications with structural extensions, formalized in Coq.

What’s in the title?

Semantic cut elimination for the logic of Bunched Implications with structural extensions, formalized in Coq.

- BI: a logic for reasoning about (separation of) resources.

What's in the title?

Semantic cut elimination for the logic of Bunched Implications with structural extensions, formalized in Coq.

- BI: a logic for reasoning about (separation of) resources.
- Cut elimination: a proof of $\vdash \varphi$ only includes subformulas of φ.

What's in the title?

Semantic cut elimination for the logic of Bunched Implications with structural extensions, formalized in Coq.

- BI: a logic for reasoning about (separation of) resources.
- Cut elimination: a proof of $\vdash \varphi$ only includes subformulas of φ.
- Semantic proof: proof by interpreting syntax in a model.

What's in the title?

Semantic cut elimination for the logic of Bunched Implications with structural extensions, formalized in Coq.

- BI: a logic for reasoning about (separation of) resources.
- Cut elimination: a proof of $\vdash \varphi$ only includes subformulas of φ.
- Semantic proof: proof by interpreting syntax in a model.
- Structural extensions: extensions of the logic with certain axioms/rules.

What's in the title?

Semantic cut elimination for the logic of Bunched Implications with structural extensions, formalized in Coq.

- BI: a logic for reasoning about (separation of) resources.
- Cut elimination: a proof of $\vdash \varphi$ only includes subformulas of φ.
- Semantic proof: proof by interpreting syntax in a model.
- Structural extensions: extensions of the logic with certain axioms/rules.
- Formalized in Coq: axiom-free formalization at

  `https://github.com/co-dan/BI-cutelim`.

The logic of Bunched Implications

BI freely combines intuitionistic and linear connectives:

$$\varphi, \psi \in \mathit{Prop} ::= \mathsf{True} \mid \mathsf{False} \mid \varphi \vee \psi \mid \varphi \wedge \psi \mid \varphi \to \psi$$

The logic of Bunched Implications

BI freely combines intuitionistic and linear connectives:

$$\begin{aligned}\varphi, \psi \in \mathit{Prop} ::= {} & \mathsf{True} \mid \mathsf{False} \mid \varphi \vee \psi \mid \varphi \wedge \psi \mid \varphi \to \psi \\ & \mid \mathsf{Emp} \mid \varphi * \psi \mid \varphi \mathrel{-\!\!*} \psi\end{aligned}$$

Intuitionistic logic

The logic of Bunched Implications

BI freely combines intuitionistic and linear connectives:

$$\begin{aligned}\varphi, \psi \in \mathit{Prop} ::= {} & \mathsf{True} \mid \mathsf{False} \mid \varphi \vee \psi \mid \varphi \wedge \psi \mid \varphi \to \psi \\ & \mid \mathsf{Emp} \mid \varphi * \psi \mid \varphi \mathrel{-\!\!*} \psi\end{aligned}$$

Linear logic (fragment)

The logic of Bunched Implications

BI freely combines intuitionistic and linear connectives:

$$\varphi, \psi \in \mathit{Prop} ::= \mathsf{True} \mid \mathsf{False} \mid \varphi \vee \psi \mid \varphi \wedge \psi \mid \varphi \to \psi$$
$$\mid \mathsf{Emp} \mid \varphi * \psi \mid \varphi -\!\!* \psi$$

$$\mathsf{True} \wedge \varphi = \varphi \qquad \varphi \wedge (\varphi \to \psi) \vdash \psi$$
$$\mathsf{Emp} * \varphi = \varphi \qquad \varphi * (\varphi -\!\!* \psi) \vdash \psi$$

$$\varphi \wedge \psi \vdash \varphi \qquad \varphi \vdash \varphi \wedge \varphi$$
$$\varphi * \psi \nvdash \varphi \qquad \varphi \nvdash \varphi * \varphi$$

The logic of Bunched Implications

BI freely combines intuitionistic and linear connectives:

$$\varphi, \psi \in \mathit{Prop} ::= \mathsf{True} \mid \mathsf{False} \mid \varphi \vee \psi \mid \varphi \wedge \psi \mid \varphi \rightarrow \psi$$
$$\mid \mathsf{Emp} \mid \varphi * \psi \mid \varphi \mathrel{-\!\!*} \psi$$

Proposition represent ownership of resources

The logic of Bunched Implications

BI freely combines intuitionistic and linear connectives:

$$\varphi, \psi \in \mathit{Prop} ::= \mathsf{True} \mid \mathsf{False} \mid \varphi \vee \psi \mid \varphi \wedge \psi \mid \varphi \rightarrow \psi$$
$$\mid \mathsf{Emp} \mid \varphi * \psi \mid \varphi \mathrel{-\!\!*} \psi$$

Proposition represent ownership of resou

Both φ and ψ hold for owned resources

φ and ψ hold for separate/disjoint resources

Why BI?

BI has seen a lot of applications in CS, especially as a basis for *program logics* for programs with arrays/dynamic memory

- $\ell \mapsto v$: the current state has the location ℓ in memory, and it stores the value v
- $P * Q$: the current state can be divided into two disjoint parts, for which P and Q hold respecively

Why BI?

BI has seen a lot of applications in CS, especially as a basis for *program logics* for programs with arrays/dynamic memory

- $\ell \mapsto v$: the current state has the location ℓ in memory, and it stores the value v
- $P * Q$: the current state can be divided into two disjoint parts, for which P and Q hold respecively
- $\ell \mapsto v * \ell' \mapsto v'$: the locations ℓ and ℓ' do not alias each other
- $\ell \mapsto v \wedge \ell' \mapsto v'$: aliasing is allowed

Why BI?

BI has seen a lot of applications in CS, especially as a basis for *program logics* for programs with arrays/dynamic memory

- $\ell \mapsto v$: the current state has the location ℓ in memory, and it stores the value v
- $P * Q$: the current state can be divided into two disjoint parts, for which P and Q hold respecively
- $\ell \mapsto v * \ell' \mapsto v'$: the locations ℓ and ℓ' do not alias each other
- $\ell \mapsto v \wedge \ell' \mapsto v'$: aliasing is allowed
- $\ell_1 \mapsto (v_1, \ell_2) * \ell_2 \mapsto (v_2, \ell_3) * \cdots * \ell_n \mapsto (v_n, \ell_o) * \ell_o \mapsto \mathtt{NULL}$:
  a linked list without cycles

Sequent calculus

Sequent: $\Gamma \vdash \phi$

$$\frac{\Gamma; \varphi; \psi \vdash \chi}{\Gamma; \varphi \wedge \psi \vdash \chi} \qquad \frac{\Gamma_1 \vdash \varphi \qquad \Gamma_2 \vdash \psi}{\Gamma_1; \Gamma_2 \vdash \varphi \wedge \psi}$$

Sequent calculus

Left and right rules

$$\frac{\Gamma; \varphi; \psi \vdash \chi}{\Gamma; \varphi \wedge \psi \vdash \chi} \qquad \frac{\Gamma_1 \vdash \varphi \qquad \Gamma_2 \vdash \psi}{\Gamma_1; \Gamma_2 \vdash \varphi \wedge \psi}$$

$$\frac{\Gamma; \Gamma \vdash \chi}{\Gamma \vdash \chi} \qquad \frac{\Gamma \vdash \chi}{\Gamma; \Gamma' \vdash \chi}$$

Sequent calculus

Structural rules

$$\frac{\Gamma; \varphi \,;\, \psi \vdash \chi}{\Gamma; \varphi \wedge \psi \vdash \chi} \qquad \frac{\Gamma_1 \vdash \varphi \qquad \Gamma_2 \vdash \psi}{\Gamma_1 \,;\, \Gamma_2 \vdash \varphi \wedge \psi}$$

$$\frac{\Gamma \,;\, \Gamma \vdash \chi}{\Gamma \vdash \chi} \qquad \frac{\Gamma \vdash \chi}{\Gamma \,;\, \Gamma' \vdash \chi}$$

Sequent calculus

$$\frac{\Gamma; (\varphi \, , \, \psi) \vdash \chi}{\Gamma; \varphi * \psi \vdash \chi} \qquad \frac{\Gamma_1 \vdash \varphi \qquad \Gamma_2 \vdash \psi}{\Gamma_1 \, , \, \Gamma_2 \vdash \varphi * \psi}$$

$$\frac{\Gamma; \varphi \, ; \, \psi \vdash \chi}{\Gamma; \varphi \wedge \psi \vdash \chi} \qquad \frac{\Gamma_1 \vdash \varphi \qquad \Gamma_2 \vdash \psi}{\Gamma_1 \, ; \, \Gamma_2 \vdash \varphi \wedge \psi}$$

$$\frac{\Gamma \, ; \, \Gamma \vdash \chi}{\Gamma \vdash \chi} \qquad \frac{\Gamma \vdash \chi}{\Gamma \, ; \, \Gamma' \vdash \chi}$$

Sequent calculus

$$\frac{\Delta(\varphi \,,\, \psi) \vdash \chi}{\Delta(\varphi * \psi) \vdash \chi} \qquad \frac{\Gamma_1 \vdash \varphi \qquad \Gamma_2 \vdash \psi}{\Gamma_1 \,,\, \Gamma_2 \vdash \varphi * \psi}$$

$$\frac{\Delta(\varphi \,;\, \psi) \vdash \chi}{\Delta(\varphi \wedge \psi) \vdash \chi} \qquad \frac{\Gamma_1 \vdash \varphi \qquad \Gamma_2 \vdash \psi}{\Gamma_1 \,;\, \Gamma_2 \vdash \varphi \wedge \psi}$$

$$\frac{\Delta(\Gamma \,;\, \Gamma) \vdash \chi}{\Delta(\Gamma) \vdash \chi} \qquad \frac{\Delta(\Gamma) \vdash \chi}{\Delta(\Gamma \,;\, \Gamma') \vdash \chi}$$

$$\Gamma ::= \varphi \mid \Gamma \,;\, \Gamma \mid \Gamma \,,\, \Gamma \mid \ldots$$

Sequent calculus

$$\frac{\Delta \, \boldsymbol{,} \, \varphi \vdash \psi}{\Delta \vdash \varphi \mathrel{-\!\!*} \psi} \qquad \frac{\Delta \, \boldsymbol{;} \, \varphi \vdash \psi}{\Delta \vdash \varphi \to \psi}$$

BI sequent calculus

- Sequent calculus for BI externalizes $\wedge$ and $*$ as different connectives: **;** and **,**. Only **;** admits weakening and contraction.

BI sequent calculus

- Sequent calculus for BI externalizes $\wedge$ and $*$ as different connectives: **;** and **,**. Only **;** admits weakening and contraction.
- Because of that, contexts in the sequents are not lists/multisets, but *trees* (referred to as *bunches*);

BI sequent calculus

- Sequent calculus for BI externalizes $\wedge$ and $*$ as different connectives: **;** and **,**. Only **;** admits weakening and contraction.
- Because of that, contexts in the sequents are not lists/multisets, but *trees* (referred to as *bunches*);
- Left rules can be applied deep inside an arbitrary *bunched context*.

Cut rule

CUT

$$\frac{\Delta' \vdash \psi \qquad \Delta(\psi) \vdash \varphi}{\Delta(\Delta') \vdash \varphi}$$

Cut rule

$$\frac{\Delta' \vdash \psi \qquad \Delta(\psi) \vdash \varphi}{\Delta(\Delta') \vdash \varphi}\ \textsc{Cut}$$

Intuitions:

- ψ is an "intermediate lemma"

Cut rule

$$\frac{\Delta' \vdash \psi \qquad \Delta(\psi) \vdash \varphi}{\Delta(\Delta') \vdash \varphi}\ \textsc{cut}$$

Intuitions:

- ψ is an “intermediate lemma”
- provability relation is transitive

Cut elimination

Theorem

Everything that is provable, is also provable without the cut rule: $\vdash \varphi \implies \vdash_{\mathsf{cf}} \varphi$

Cut elimination

Theorem

Everything that is provable, is also provable without the cut rule: $\vdash \varphi \implies \vdash_{\mathsf{cf}} \varphi$

Why eliminate cut?

- makes the calculus *analytical* (subformula property): any derivation of $\varphi \vdash \psi$ only involves formula that are already present in φ and ψ
- important ingredient in the automated proof search toolbox

Cut elimination

Usually proofs of cut elimination involve analysis by inversion + terminating measure:

$$\dfrac{\dfrac{\cdots}{\Delta_1 \,;\, \Delta_2 \vdash \psi_1 \wedge \psi_2} \qquad \dfrac{\cdots}{\Delta(\psi_1 \wedge \psi_2) \vdash \varphi}}{\Delta(\Delta_1 \,;\, \Delta_2) \vdash \varphi}$$

Cut elimination

Usually proofs of cut elimination involve analysis by inversion + terminating measure:

$$\dfrac{\dfrac{?}{\Delta_1 \,;\, \Delta_2 \vdash \psi_1 \wedge \psi_2} \qquad \dfrac{?}{\Delta(\psi_1 \wedge \psi_2) \vdash \varphi}}{\Delta(\Delta_1 \,;\, \Delta_2) \vdash \varphi}$$

Cut elimination

Usually proofs of cut elimination involve analysis by inversion + terminating measure:

$$\dfrac{\dfrac{\Delta_1 \vdash \psi_1 \qquad \Delta_2 \vdash \psi_2}{\Delta_1 \,;\, \Delta_2 \vdash \psi_1 \wedge \psi_2} \qquad \dfrac{\Delta(\psi_1 \,;\, \psi_2) \vdash \varphi}{\Delta(\psi_1 \wedge \psi_2) \vdash \varphi}}{\Delta(\Delta_1 \,;\, \Delta_2) \vdash \varphi}$$

Cut elimination

Usually proofs of cut elimination involve analysis by inversion + terminating measure:

$$\dfrac{\dfrac{\Delta_1 \vdash \psi_1 \qquad \Delta_2 \vdash \psi_2}{\Delta_1 \,;\, \Delta_2 \vdash \psi_1 \wedge \psi_2} \qquad \dfrac{\Delta(\psi_1 \,;\, \psi_2) \vdash \varphi}{\Delta(\psi_1 \wedge \psi_2) \vdash \varphi}}{\Delta(\Delta_1 \,;\, \Delta_2) \vdash \varphi}$$

$$\rightsquigarrow \qquad \dfrac{\Delta_2 \vdash \psi_2 \qquad \dfrac{\Delta_1 \vdash \psi_1 \qquad \Delta(\psi_1 \,;\, \psi_2) \vdash \varphi}{\Delta(\Delta_1 \,;\, \psi_2) \vdash \varphi}}{\Delta(\Delta_1 \,;\, \Delta_2) \vdash \varphi}$$

Cut elimination

Usually proofs of cut elimination involve analysis by inversion + terminating measure:

$$\dfrac{\dfrac{\Delta_1 \vdash \psi_1 \qquad \Delta_2 \vdash \psi_2}{\Delta_1 \,;\, \Delta_2 \vdash \psi_1 \wedge \psi_2} \qquad \dfrac{?}{\Delta(\psi_1 \wedge \psi_2) \vdash \varphi}}{\Delta(\Delta_1 \,;\, \Delta_2) \vdash \varphi}$$

Cut elimination

Usually proofs of cut elimination involve analysis by inversion + terminating measure:

$$\dfrac{\dfrac{\Delta_1 \vdash \psi_1 \qquad \Delta_2 \vdash \psi_2}{\Delta_1 \,;\, \Delta_2 \vdash \psi_1 \wedge \psi_2} \qquad \dfrac{\Delta(\psi_1 \wedge \psi_2) \,;\, \varphi_1 \vdash \varphi_2}{\Delta(\psi_1 \wedge \psi_2) \vdash \varphi_1 \to \varphi_2}}{\Delta(\Delta_1 \,;\, \Delta_2) \vdash \varphi_1 \to \varphi_2}$$

Cut elimination

Usually proofs of cut elimination involve analysis by inversion + terminating measure:

$$\dfrac{\dfrac{\Delta_1 \vdash \psi_1 \qquad \Delta_2 \vdash \psi_2}{\Delta_1 \mathbin{;} \Delta_2 \vdash \psi_1 \wedge \psi_2} \qquad \dfrac{\Delta(\psi_1 \wedge \psi_2) \mathbin{;} \varphi_1 \vdash \varphi_2}{\Delta(\psi_1 \wedge \psi_2) \vdash \varphi_1 \to \varphi_2}}{\Delta(\Delta_1 \mathbin{;} \Delta_2) \vdash \varphi_1 \to \varphi_2}$$

$$\rightsquigarrow \qquad \dfrac{\dfrac{\Delta_1 \mathbin{;} \Delta_2 \vdash \psi_1 \wedge \psi_2 \qquad \Delta(\psi_1 \wedge \psi_2) \mathbin{;} \varphi_1 \vdash \varphi_2}{\Delta(\Delta_1 \mathbin{;} \Delta_2) \mathbin{;} \varphi_1 \vdash \varphi_2}}{\Delta(\Delta_1 \mathbin{;} \Delta_2) \vdash \varphi_1 \to \varphi_2}$$

Cut elimination

Usually proofs of cut elimination involve analysis by inversion + terminating measure:

$$\dfrac{\dfrac{?}{\Delta_1 \mathbin{;} \Delta_2 \vdash \psi_1 \wedge \psi_2} \qquad \dfrac{?}{\Delta(\psi_1 \wedge \psi_2) \vdash \varphi}}{\Delta(\Delta_1 \mathbin{;} \Delta_2) \vdash \varphi}$$

$\rightsquigarrow$ etc..

Limitations of the direct-style proof

- There are *a lot* of cases to consider, with a lot of syntactic details

Limitations of the direct-style proof

- There are *a lot* of cases to consider, with a lot of syntactic details
- Well-foundedness/termination measures can get complicated

Limitations of the direct-style proof

- There are *a lot* of cases to consider, with a lot of syntactic details
- Well-foundedness/termination measures can get complicated
- BI specific: the tree-like structure of bunches contribute to the complexity

Limitations of the direct-style proof

- There are *a lot* of cases to consider, with a lot of syntactic details
- Well-foundedness/termination measures can get complicated
- BI specific: the tree-like structure of bunches contribute to the complexity

For these reason, non-formalized proofs of cut elimination can be fragile and are known to be error-prone.

Limitations of the direct-style proof

- There are *a lot* of cases to consider, with a lot of syntactic details
- Well-foundedness/termination measures can get complicated
- BI specific: the tree-like structure of bunches contribute to the complexity

For these reason, non-formalized proofs of cut elimination can be fragile and are known to be error-prone.

On the other hand, formalizing these kind of proofs can also be tough...

Semantic proof of cut elimination

A *semantic* proof of cut elimination goes through some “universal” model $\mathcal{C}$ and the interpretation of sequent calculus in it.

$$\mathcal{C} \models \varphi \implies \vdash_{\mathsf{cf}} \varphi$$

Semantic proof of cut elimination

A *semantic* proof of cut elimination goes through some "universal" model $\mathcal{C}$ and the interpretation of sequent calculus in it.

$$\mathcal{C} \models \varphi \implies \vdash_{\mathsf{cf}} \varphi$$

BI algebra

A BI algebra $(\mathcal{C}, \leq)$ consists of operations $\top, \bot, \vee, \wedge, \to, \mathsf{Emp}, *, -\!\!*$ satisfying various laws.

Soundness: $\varphi \vdash \psi \implies [\![\varphi]\!] \leq [\![\psi]\!]$.

Intuition: Lindenbaum-Tarski algebra for completeness

Define $[\varphi] = \{\psi \mid \varphi \dashv\vdash \psi\}$, and $[\varphi] \leq_{\mathcal{L}} [\psi] \iff \varphi \vdash \psi$.

Intuition: Lindenbaum-Tarski algebra for completeness

Define $[\varphi] = \{\psi \mid \varphi \dashv\vdash \psi\}$, and $[\varphi] \leq_{\mathcal{L}} [\psi] \iff \varphi \vdash \psi$.

- $\mathcal{L} = \{[\varphi] \mid \varphi \in \mathit{Frml}\}$ with $\leq_{\mathcal{L}}$ is a BI algebra;
- Main property of $\mathcal{L}$: $[\![\varphi]\!] = [\varphi]$.

Intuition: Lindenbaum-Tarski algebra for completeness

Define $[\varphi] = \{\psi \mid \varphi \dashv\vdash \psi\}$, and $[\varphi] \leq_{\mathcal{L}} [\psi] \iff \varphi \vdash \psi$.

- $\mathcal{L} = \{[\varphi] \mid \varphi \in \mathit{Frml}\}$ with $\leq_{\mathcal{L}}$ is a BI algebra;
- Main property of $\mathcal{L}$: $[\![\varphi]\!] = [\varphi]$.
- Completeness: suppose $\varphi \models \psi$.

Intuition: Lindenbaum-Tarski algebra for completeness

Define $[\varphi] = \{\psi \mid \varphi \dashv\vdash \psi\}$, and $[\varphi] \leq_{\mathcal{L}} [\psi] \iff \varphi \vdash \psi$.

- $\mathcal{L} = \{[\varphi] \mid \varphi \in \mathit{Frml}\}$ with $\leq_{\mathcal{L}}$ is a BI algebra;
- Main property of $\mathcal{L}$: $[\![\varphi]\!] = [\varphi]$.
- Completeness: suppose $\varphi \models \psi$.
  - In particular: $[\![\varphi]\!] \leq_{\mathcal{L}} [\![\psi]\!]$, i.e. $[\varphi] \leq_{\mathcal{L}} [\psi]$;

Intuition: Lindenbaum-Tarski algebra for completeness

Define $[\varphi] = \{\psi \mid \varphi \dashv\vdash \psi\}$, and $[\varphi] \leq_{\mathcal{L}} [\psi] \iff \varphi \vdash \psi$.

- $\mathcal{L} = \{[\varphi] \mid \varphi \in \mathit{Frml}\}$ with $\leq_{\mathcal{L}}$ is a BI algebra;
- Main property of $\mathcal{L}$: $[\![\varphi]\!] = [\varphi]$.
- Completeness: suppose $\varphi \models \psi$.
    - In particular: $[\![\varphi]\!] \leq_{\mathcal{L}} [\![\psi]\!]$, i.e. $[\varphi] \leq_{\mathcal{L}} [\psi]$;
    - Conclusion: $\varphi \vdash \psi$.

Intuition: Lindenbaum-Tarski algebra for completeness

Define $[\varphi] = \{\psi \mid \varphi \dashv\vdash \psi\}$, and $[\varphi] \leq_{\mathcal{L}} [\psi] \iff \varphi \vdash \psi$.

- $\mathcal{L} = \{[\varphi] \mid \varphi \in \mathit{Frml}\}$ with $\leq_{\mathcal{L}}$ is a BI algebra;
- Main property of $\mathcal{L}$: $[\![\varphi]\!] = [\varphi]$.
- Completeness: suppose $\varphi \models \psi$.
  - In particular: $[\![\varphi]\!] \leq_{\mathcal{L}} [\![\psi]\!]$, i.e. $[\varphi] \leq_{\mathcal{L}} [\psi]$;
  - Conclusion: $\varphi \vdash \psi$.
- The “real” work is to show that $\mathcal{L}$ is indeed a model.

Attempt 1

What if we use $\vdash_{\mathsf{cf}}$ instead of $\vdash$ in the definition of $\mathcal{L}$?

Attempt 1

What if we use $\vdash_{\mathsf{cf}}$ instead of $\vdash$ in the definition of $\mathcal{L}$?

Need transitivity of $\leq$: $[\varphi] \leq [\psi] \leq [\chi] \implies [\varphi] \leq [\chi]$?

Attempt 1

What if we use $\vdash_{\mathsf{cf}}$ instead of $\vdash$ in the definition of $\mathcal{L}$?

Need transitivity of $\leq$: $[\varphi] \leq [\psi] \leq [\chi] \implies [\varphi] \leq [\chi]$?

Same as cut elimination: $\varphi \vdash_{\mathsf{cf}} \psi \vdash_{\mathsf{cf}} \chi \implies \varphi \vdash_{\mathsf{cf}} \chi$

Attempt 2

Attempted solution: use sets of predecessors.

$$\langle \varphi \rangle = \{\Delta \mid \Delta \vdash_{\mathsf{cf}} \varphi\} \in \wp(\mathit{Bunch}),$$

with the subset inclusion relation.

Attempt 2

Attempted solution: use sets of predecessors.

$$\langle \varphi \rangle = \{\Delta \mid \Delta \vdash_{\mathsf{cf}} \varphi\} \in \wp(\mathit{Bunch}),$$

with the subset inclusion relation.

Note that $\varphi \in \langle \varphi \rangle$. Hence, $\langle \varphi \rangle \subseteq \langle \psi \rangle$ implies

$$\varphi \in \langle \psi \rangle \iff \varphi \vdash_{\mathsf{cf}} \psi.$$

Attempt 2

Attempted solution: use sets of predecessors.

$$\boxed{\varphi \vdash_{\mathsf{cf}} \varphi} \langle \varphi \rangle = \{\Delta \mid \Delta \vdash_{\mathsf{cf}} \varphi\} \in \wp(\mathit{Bunch}),$$

with the subset inclusion relation.

Note that $\varphi \in \langle \varphi \rangle$. Hence, $\langle \varphi \rangle \subseteq \langle \psi \rangle$ implies

$$\varphi \in \langle \psi \rangle \iff \varphi \vdash_{\mathsf{cf}} \psi.$$

Attempt 3

Is $\mathcal{C} = (\{\langle\varphi\rangle \mid \varphi \in \mathit{Frml}\}, \subseteq)$ a BI algebra?

Attempt 3

Is $\mathcal{C} = (\{\langle\varphi\rangle \mid \varphi \in \mathit{Frml}\}, \subseteq)$ a BI algebra?

Not closed under $\cup$, $\cap$... Cannot inherit the algebra structure from $\wp(\mathit{Bunch})$.

For example, $(\varphi \vee \psi) \in \langle\varphi \vee \psi\rangle$, but does $(\varphi \vee \psi)$ belong to $\langle\varphi\rangle \cup \langle\psi\rangle$?

Attempt 3

Is $\mathcal{C} = (\{\langle\varphi\rangle \mid \varphi \in \mathit{Frml}\}, \subseteq)$ a BI algebra?

Not closed under $\cup$, $\cap$... Cannot inherit the algebra structure from $\wp(\mathit{Bunch})$.

For example, $(\varphi \vee \psi) \in \langle\varphi \vee \psi\rangle$, but does $(\varphi \vee \psi)$ belong to $\langle\varphi\rangle \cup \langle\psi\rangle$?

Solution: "the next best thing"

$$\langle\varphi\rangle \vee \langle\psi\rangle = \bigcap\{Y \in \mathcal{C} \mid \langle\varphi\rangle \cup \langle\psi\rangle \subseteq Y\}$$

The smallest set in $\mathcal{C}$ containing $\langle\varphi\rangle \cup \langle\psi\rangle$

Attempt 3.5 (successful and final)

Solution: close under arbitrary intersections:

$$\mathcal{C} = \{\bigcap_{i\in I}\langle\varphi_i\rangle \mid I \text{ arbitrary set}, \varphi_i \in \mathit{Frml}\} \subseteq \wp(\mathit{Bunch})$$

$$\mathsf{cl}(-) : \wp(\mathit{Bunch}) \to \mathcal{C}$$

$$\mathsf{cl}(X) = \bigcap\{\langle\varphi\rangle \mid X \subseteq \langle\varphi\rangle\}$$

Attempt 3.5 (successful and final)

Solution: close under arbitrary intersections:

$$\mathcal{C} = \{\bigcap_{i \in I} \langle \varphi_i \rangle \mid I \text{ arbitrary set}, \varphi_i \in \mathit{Frml}\} \subseteq \wp(\mathit{Bunch})$$

The smallest set in $\mathcal{C}$ containing X

$$\mathsf{cl}(-) : \wp(\mathit{Bunch}) \to \mathcal{C}$$

$$\mathsf{cl}(X) = \bigcap \{\langle \varphi \rangle \mid X \subseteq \langle \varphi \rangle\}$$

Attempt 3.5 (successful and final)

Solution: close under arbitrary intersections:

$$\mathcal{C} = \{\bigcap_{i\in I}\langle\varphi_i\rangle \mid I \text{ arbitrary set}, \varphi_i \in \textit{Frml}\} \subseteq \wp(\textit{Bunch})$$

$$\mathsf{cl}(-) : \wp(\textit{Bunch}) \to \mathcal{C}$$

$$\mathsf{cl}(X) = \bigcap\{\langle\varphi\rangle \mid X \subseteq \langle\varphi\rangle\}$$

Proposition

If $X \in \mathcal{C}$ with $\Delta_1, \ldots, \Delta_n \in X$ and

$$\frac{\Delta_1 \vdash \varphi \qquad \ldots \qquad \Delta_n \vdash \varphi}{\Delta' \vdash \varphi}$$

without the use of the cut rule, then $\Delta' \in X$.

Attempt 3.5 (successful and final)

Solution: close under arbitrary intersections:

$$\mathcal{C} = \{\bigcap_{i \in I} \langle \varphi_i \rangle \mid I \text{ arbitrary set}, \varphi_i \in \mathit{Frml}\} \subseteq \wp(\mathit{Bunch})$$

$$\mathsf{cl}(-) : \wp(\mathit{Bunch}) \to \mathcal{C}$$
$$\mathsf{cl}(X) = \bigcap \{\langle \varphi \rangle \mid X \subseteq \langle \varphi \rangle\}$$

Lift operations to $\mathcal{C}$:

$$X \wedge Y = X \cap Y \qquad X \to Y = \{\Delta \mid \forall \Delta' \in X.\, (\Delta \,;\, \Delta') \in Y\}$$
$$X \vee Y = \mathsf{cl}(X \cup Y)$$
$$X * Y = \mathsf{cl}(\{\Delta_1 \,,\, \Delta_2 \mid \Delta_1 \in X, \Delta_2 \in Y\}) \qquad X \mathrel{-\!\!*} Y = \{\Delta \mid \forall \Delta' \in X.\, (\Delta \,,\, \Delta') \in Y\}$$

Proposition

$\mathcal{C}$ is a BI algebra

Fundamental property

Fundamental property

$\varphi \in [\![\varphi]\!] \subseteq \langle\varphi\rangle$

Proof by induction on φ.

Fundamental property

Fundamental property

$\varphi \in [\![\varphi]\!] \subseteq \langle\varphi\rangle$

Proof by induction on φ.

Cut elimination

$\varphi \vdash \psi \implies \varphi \vdash_{\mathsf{cf}} \psi$

If $\varphi \vdash \psi$, then $[\![\varphi]\!] \subseteq [\![\psi]\!]$.

If $[\![\varphi]\!] \subseteq [\![\psi]\!]$, then $\varphi \in [\![\varphi]\!] \subseteq [\![\psi]\!] \subseteq \langle\psi\rangle \implies \varphi \vdash_{\mathsf{cf}} \psi$.

Extensibility

The semantic approach is, arguably, more extensible.

Extensibility

The semantic approach is, arguably, more extensible.

The key points in the proof:

- Invertibility of certain rules w.r.t. $\vdash_{cf}$.

Extensibility

The semantic approach is, arguably, more extensible.

The key points in the proof:

- Invertibility of certain rules w.r.t. $\vdash_{\mathsf{cf}}$.
- The resulting $\mathcal{C}$ is a BI algebra

Extensibility

The semantic approach is, arguably, more extensible.

The key points in the proof:

- Invertibility of certain rules w.r.t. $\vdash_{\mathsf{cf}}$.
- The resulting $\mathcal{C}$ is a BI algebra
- $\varphi \in [\![\varphi]\!] \subseteq \langle \varphi \rangle$

Extensions

We consider two different types of extensions:

Extensions

We consider two different types of extensions:

- BI + additional structural rules, e.g. affine BI

$$\frac{\Pi(\Delta) \vdash \varphi}{\Pi(\Delta \,\mathbf{,}\, \Delta') \vdash \varphi}$$

$\mathcal{C}$ is a BI algebra + some equations, e.g. $p * q \leq p$

Extensions

We consider two different types of extensions:

- BI + additional structural rules, e.g. affine BI

$$\frac{\Pi(\Delta) \vdash \varphi}{\Pi(\Delta \mathbin{,} \Delta') \vdash \varphi}$$

  $\mathcal{C}$ is a BI algebra + some equations, e.g. $p * q \leq p$

Extensions

We consider two different types of extensions:

- BI + additional structural rules, e.g. affine BI

$$\frac{\Pi(\Delta) \vdash \varphi}{\Pi(\Delta \mathbin{,} \Delta') \vdash \varphi}$$

  $\mathcal{C}$ is a BI algebra + some equations, e.g. $p * q \leq p$

- BI + $\Box$ modality: BI based on IS4

$\Box$L

$$\frac{\Delta(A) \vdash B}{\Delta(\Box A) \vdash B}$$

$\Box$R

$$\frac{\Box\Delta \vdash A}{\Box\Delta \vdash \Box A}$$

  $\mathcal{C}$ is a BI algebra with a modal operator

Extensions (analytic structural rules)

An analytic structural rule is of the form

$$\frac{\Pi(T_1[\Delta_1, \ldots, \Delta_n]) \vdash \varphi \qquad \ldots \qquad \Pi(T_m[\Delta_1, \ldots, \Delta_n]) \vdash \varphi}{\Pi(T[\Delta_1, \ldots, \Delta_n]) \vdash \varphi}$$

where $T_1, \ldots, T_m, T$ are *bunched terms* – bunches built out of connectives **,**, **;**, and variables $x_1, \ldots, x_n$, and T is *linear*

Extensions (analytic structural rules)

An analytic structural rule is of the form

$$\frac{\Pi(T_1[\Delta_1, \ldots, \Delta_n]) \vdash \varphi \qquad \ldots \qquad \Pi(T_m[\Delta_1, \ldots, \Delta_n]) \vdash \varphi}{\Pi(T[\Delta_1, \ldots, \Delta_n]) \vdash \varphi}$$

where $T_1, \ldots, T_m, T$ are *bunched terms* – bunches built out of connectives **,**, **;**, and variables $x_1, \ldots, x_n$, and T is *linear*

Corresponds to the axiom:

$$[\![T]\!](p_1, \ldots, p_n) \leq [\![T_1]\!](p_1, \ldots, p_n) \vee \cdots \vee [\![T_m]\!](p_1, \ldots, p_n).$$

Extensions (analytic structural rules)

How do we verify that

$$[\![T]\!](p_1, \ldots, p_n) \leq [\![T_1]\!](p_1, \ldots, p_n) \vee \cdots \vee [\![T_m]\!](p_1, \ldots, p_n).$$

holds in the model $\mathcal{C}$?

Proposition

For $X_1, X_2, \ldots, X_n \in \mathcal{C}$,

$$\mathsf{cl}(\{T[\Delta_1, \ldots, \Delta_n] \mid \Delta_i \in X_i, 1 \leq i \leq n\}) \subseteq [\![T]\!](X_1, \ldots, X_n).$$

And this becomes an equality when T is linear.

Analytic completion

$$\frac{\Pi(T_1[\Delta_1, \ldots, \Delta_n]) \vdash \varphi \qquad \ldots \qquad \Pi(T_m[\Delta_1, \ldots, \Delta_n]) \vdash \varphi}{\Pi(T[\Delta_1, \ldots, \Delta_n]) \vdash \varphi}$$

What if T is not linear?

Analytic completion

$$\frac{\Pi(T_1[\Delta_1, \ldots, \Delta_n]) \vdash \varphi \qquad \ldots \qquad \Pi(T_m[\Delta_1, \ldots, \Delta_n]) \vdash \varphi}{\Pi(T[\Delta_1, \ldots, \Delta_n]) \vdash \varphi}$$

What if T is not linear?

Then we can turn the above rule into an equivalent analytic rule.

Analytic completion

$$\frac{\Pi(\Delta) \vdash \varphi}{\Pi(\Delta \,\mathbf{,}\, \Delta) \vdash \varphi}$$

corresponds to $p * p \leq p$

Analytic completion

$$\frac{\Pi(\Delta) \vdash \varphi}{\Pi(\Delta \,;\, \Delta) \vdash \varphi}$$

corresponds to $p * p \leq p$

$$\Rightarrow$$

$$\frac{}{\Pi(\Delta_1 \,;\, \Delta_2) \vdash \varphi}$$

Analytic completion

$$\frac{\Pi(\Delta) \vdash \varphi}{\Pi(\Delta \,,\, \Delta) \vdash \varphi}$$

corresponds to $p * p \leq p$

$$\Rightarrow$$

$$\frac{\Pi(\Delta_1) \vdash \varphi \qquad \Pi(\Delta_2) \vdash \varphi}{\Pi(\Delta_1 \,,\, \Delta_2) \vdash \varphi}$$

corresponds to $p_1 * p_2 \leq p_1 \vee p_2$

Analytic completion

Clearly $p_1 * p_2 \leq p_1 \vee p_2$ implies $p * p \leq p$.

For the other way around:

$$p_1 * p_2 \leq \qquad\qquad\qquad\qquad\qquad\qquad .$$

Analytic completion

Clearly $p_1 * p_2 \leq p_1 \vee p_2$ implies $p * p \leq p$.

For the other way around:

$$p_1 * p_2 \leq (p_1 \vee p_2) * (p_1 \vee p_2) \leq \qquad\qquad .$$

Analytic completion

Clearly $p_1 * p_2 \leq p_1 \vee p_2$ implies $p * p \leq p$.

For the other way around:

$$p_1 * p_2 \leq (p_1 \vee p_2) * (p_1 \vee p_2) \leq p_1 \vee p_2.$$

Reflecting on the formalization

Coq formalization, ~1090 lines specs and ~3600 lines proof

Reflecting on the formalization

Coq formalization, ~1090 lines specs and ~3600 lines proof

- Good representation for $\mathcal{C}$ makes life easier

```
Record C := {
  CPred :> Bunch → Prop;
  CClosed : .... }
```

Reflecting on the formalization

Coq formalization, ~1090 lines specs and ~3600 lines proof

- Good representation for $\mathcal{C}$ makes life easier

```
Record C := {
  CPred :> Bunch → Prop;
  CClosed : .... }
```

- Extensive use of setoids and setoid rewriting, based on the typeclasses from the `stdpp` library

Reflecting on the formalization

Coq formalization, ~1090 lines specs and ~3600 lines proof

- Good representation for $\mathcal{C}$ makes life easier

```
Record C := {
  CPred :> Bunch → Prop;
  CClosed : .... }
```

- Extensive use of setoids and setoid rewriting, based on the typeclasses from the `stdpp` library
- Turn equations $\Delta = \Delta'(\Gamma)$ into inductive systems

```
Inductive bunch_decomp : bunch → bunch_ctx → bunch → Prop
```

Thank you

Thank you for your attention!

Let me know if you have questions, d.frumin@rug.nl.