Semantic Cut Elimination for the Logic of Bunched Implications

(as formalized in Coq)

Dan Frumin

CPP 2022

University of Groningen

What's in the title?

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

What's in the title?

Semantic cut elimination for the logic of Bunched Implications, 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, 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, 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, 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.
- 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:

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

Intuitionistic logic

BI freely combines intuitionistic and linear connectives:

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

Linear logic (fragment)

The logic of Bunched Implications

BI freely combines intuitionistic and linear connectives:

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

Proposition represent owenership of resources

Sequent calculus

$\boxed{\text{Sequent: } \Gamma \vdash \phi}$

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

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

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

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

Sequent calculus

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

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

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

Sequent calculus

$$\frac{\Delta(\varphi \mathbin{,} \psi) \vdash \chi}{\Delta(\varphi * \psi) \vdash \chi}$$

$$\frac{\Gamma_1 \vdash \varphi \qquad \Gamma_2 \vdash \psi}{\Gamma_1 \mathbin{,} \Gamma_2 \vdash \varphi \wedge \psi}$$

$$\frac{\Delta(\varphi \mathbin{;} \psi) \vdash \chi}{\Delta(\varphi \wedge \psi) \vdash \chi}$$

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

$$\frac{\Delta(\Gamma \mathbin{;} \Gamma) \vdash \chi}{\Delta(\Gamma) \vdash \chi}$$

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

$$\boxed{\Gamma ::= \varphi \mid \Gamma \mathbin{;} \Gamma \mid \Gamma \mathbin{,} \Gamma \mid \ldots}$$

Cut rule

CUT

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

Cut rule

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

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:

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

Cut elimination

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

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

Cut elimination

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

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

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

Cut elimination

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

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

$\rightsquigarrow$ 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 $\top, \bot, \vee, \wedge, \to, \mathrm{Emp}, *, -\!\!*$ 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.

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

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

Attempt 3

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

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

Attempt 3

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

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

Solution: close under arbitrary intersections:

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

Attempt 3

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

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

Solution: close under arbitrary intersections:

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

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

Attempt 3

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

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

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

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

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

Attempt 3

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

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

Solution: close under arbitrary intersec[tions]

$$\mathcal{C} = \{\bigcap_{i \in I} \langle\varphi_i\rangle \mid I \text{ arbitrary}$$

Lift operations to $\mathcal{C}$:

$$X \wedge Y = X \cap Y$$
$$X \vee Y = \mathsf{cl}(X \cup Y)$$
$$X * Y = \mathsf{cl}(\{\Delta_1 \,\mathbf{,}\, \Delta_2 \mid \Delta_1 \in X, \Delta_2 \in Y\})$$

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

Attempt 3

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

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

Solution: close under arbitrary intersec

$$\mathcal{C} = \{\bigcap_{i\in I}\langle\varphi_i\rangle \mid I \text{ arbitrary}$$

Lift operations to $\mathcal{C}$:

$$X \wedge Y = X \cap Y$$
$$X \vee Y = \mathsf{cl}(X \cup Y)$$
$$X * Y = \mathsf{cl}(\{\Delta_1 \,;\, \Delta_2 \mid \Delta_1 \in X, \Delta_2 \in Y\})$$

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

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

Satisfies $[\![\varphi]\!] \subseteq [\![\psi]\!] \implies \varphi \vdash_{\mathsf{cf}} \psi$

Sum up

- Semantic proof of cut elimination through $\mathcal{C}$

Sum up

- Semantic proof of cut elimination through $\mathcal{C}$
- More modular proof

Sum up

- Semantic proof of cut elimination through $\mathcal{C}$
- More modular proof
- Extensions: structural rules, $\Box$ modality.

Reflecting on the formalization

Coq formalization, ~650 lines specs and ~2500 lines proof

Reflecting on the formalization

Coq formalization, ~650 lines specs and ~2500 lines proof

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

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

Reflecting on the formalization

Coq formalization, ~650 lines specs and ~2500 lines proof

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

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

- Setoids and setoid rewriting were helpful, useful type classes in `stdpp`

Reflecting on the formalization

Coq formalization, ~650 lines specs and ~2500 lines proof

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

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

- Setoids and setoid rewriting were helpful, useful type classes in `stdpp`
- Turn equations $\Delta = \Delta'(\Gamma)$ into inductive systems

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

Thank you

Thank you for listening!

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