On subexponentials, focusing and modalities in concurrent systems

Vivek Nigam

Federal University of Paraíba, Brazil

co-joint work with Carlos Olarte and Elaine Pimentel

Linear Logic Basics

Multiplicative Fragment

$$\frac{\Gamma, F, G \longrightarrow H}{\Gamma, F \otimes G \longrightarrow H}\ \otimes_L \qquad \frac{\Gamma_1 \longrightarrow F \quad \Gamma_2 \longrightarrow G}{\Gamma_1, \Gamma_2 \longrightarrow F \otimes G}\ \otimes_R$$

$$\frac{\Gamma_1 \longrightarrow F \quad \Gamma_2, G \longrightarrow H}{\Gamma_1, \Gamma_2, F \multimap G \longrightarrow H}\ \multimap_L \qquad \frac{\Gamma, F \longrightarrow G}{\Gamma \longrightarrow F \multimap G}\ \multimap_R$$

Linear Logic Basics

Multiplicative Fragment

$$\frac{\Gamma, F, G \longrightarrow H}{\Gamma, F \otimes G \longrightarrow H} \otimes_L \qquad \frac{\Gamma_1 \longrightarrow F \quad \Gamma_2 \longrightarrow G}{\Gamma_1, \Gamma_2 \longrightarrow F \otimes G} \otimes_R$$

$$\frac{\Gamma_1 \longrightarrow F \quad \Gamma_2, G \longrightarrow H}{\Gamma_1, \Gamma_2, F \multimap G \longrightarrow H} \multimap_L \qquad \frac{\Gamma, F \longrightarrow G}{\Gamma \longrightarrow F \multimap G} \multimap_R$$

Contraction and weakening are controled by the exponentials $!$ and $?$.

$$\frac{\Gamma, !P, !P \longrightarrow G}{\Gamma, !P \longrightarrow G} C \qquad \frac{\Gamma \longrightarrow G}{\Gamma, !P \longrightarrow G} W$$

Subexponentials

Linear Logic Exponentials are Not Canonical

Subexponentials

Linear Logic Exponentials are Not Canonical

$!^b, !^r$ and $?^b, ?^r$:

Subexponentials

Linear Logic Exponentials are Not Canonical

$!^b, !^r$ and $?^b, ?^r$:

$$!^b F \not\equiv !^r F \qquad ?^b F \not\equiv ?^r F$$

Subexponentials

Linear Logic Exponentials are Not Canonical

$!^b, !^r$ and $?^b, ?^r$:

Subexponentials

$$!^b F \not\equiv\ !^r F \qquad ?^b F \not\equiv\ ?^r F$$

All other connectives are canonical.

Subexponentials

Linear Logic Exponentials are Not Canonical

$!^b, !^r$ and $?^b, ?^r$:

Subexponentials

$$!^b F \not\equiv !^r F \qquad ?^b F \not\equiv ?^r F$$

All other connectives are canonical.

Subexponential Signature

$$\langle I, \preceq, U \rangle$$

where $U \subseteq I$ and is closed under $\preceq$.

Subexponentials with index $a \in U$ can weaken and contract:

$$\frac{\Gamma, !^a P, !^a P \longrightarrow G}{\Gamma, !^a P \longrightarrow G}\ C \qquad \frac{\Gamma \longrightarrow G}{\Gamma, !^a P \longrightarrow G}\ W$$

Subexponentials

Linear Logic Exponentials are Not Canonical

$!^b, !^r$ and $?^b, ?^r$:

Subexponentials

$$!^b F \not\equiv\ !^r F \qquad ?^b F \not\equiv\ ?^r F$$

All other connectives are canonical.

Subexponential Signature

$$\langle I, \preceq, U \rangle$$

where $U \subseteq I$ and is closed under $\preceq$.

Subexponentials with index $a \in U$ can weaken and contract:

$$\frac{\Gamma, !^a P, !^a P \longrightarrow G}{\Gamma, !^a P \longrightarrow G}\ C \qquad \frac{\Gamma \longrightarrow G}{\Gamma, !^a P \longrightarrow G}\ W$$

In fact, signatures are of the form:

$$\langle I, \preceq, C, W \rangle$$

Subexponentials

Linear Logic Exponentials are Not Canonical

$!^b, !^r$ and $?^b, ?^r$:

Subexponentials

$!^b F \not\equiv !^r F \qquad ?^b F \not\equiv ?^r F$

All other connectives are canonical.

Subexponential Signature

$$\langle I, \preceq, U \rangle$$

where $U \subseteq I$ and is closed under $\preceq$.

Subexponentials with index $a \in U$ can weaken and contract:

$$\frac{\Gamma, !^a P, !^a P \longrightarrow G}{\Gamma, !^a P \longrightarrow G}\ C \qquad \frac{\Gamma \longrightarrow G}{\Gamma, !^a P \longrightarrow G}\ W$$

Introduction Rules

$$\frac{!^{x_1} F_1, \ldots !^{x_n} F_n \longrightarrow G}{!^{x_1} F_1, \ldots !^{x_n} F_n \longrightarrow !^a G}\ !^a{}_R$$

$$\frac{!^{x_1} F_1, \ldots !^{x_n} F_n, F \longrightarrow ?^{x_{n+1}} G}{!^{x_1} F_1, \ldots !^{x_n} F_n, ?^a F \longrightarrow ?^{x_{n+1}} G}\ ?^a{}_L$$

where $a \preceq x_i$ for all i.

Subexponentials

Linear Logic Exponentials are Not Canonical

$!^b, !^r$ and $?^b, ?^r$: **Subexponentials**

$$!^b F \not\equiv !^r F \qquad ?^b F \not\equiv ?^r F$$

All other connectives are canonical.

Subexponential Signature

$$\langle I, \preceq, U \rangle$$

where $U \subseteq I$ and is closed under $\preceq$.

Subexponentials with index $a \in U$ can weaken and contract:

$$\frac{\Gamma, !^a P, !^a P \longrightarrow G}{\Gamma, !^a P \longrightarrow G}\ C \qquad \frac{\Gamma \longrightarrow G}{\Gamma, !^a P \longrightarrow G}\ W$$

Introduction Rules

$$\frac{!^{x_1} F_1, \ldots !^{x_n} F_n \longrightarrow G}{!^{x_1} F_1, \ldots !^{x_n} F_n \longrightarrow !^a G}\ !^a{}_R$$

$$\frac{!^{x_1} F_1, \ldots !^{x_n} F_n, F \longrightarrow ?^{x_{n+1}} G}{!^{x_1} F_1, \ldots !^{x_n} F_n, ?^a F \longrightarrow ?^{x_{n+1}} G}\ ?^a{}_L$$

where $a \preceq x_i$ for all i.

Theorem: For any subexponential signature, Σ, $SELL_\Sigma$ admits cut-elimination.

Differences to Linear Logic

- The combination of subexponentials yields an **unbounded number** of **logically distinct prefixes** as one can combine subexponentials with different labels, *e.g.*, $!^{l_1}, !^{l_2}, \ldots, !^{l_1} ?^{l_1}, !^{l_1} ?^{l_2}, !^{l_1} ?^{l_3}, \ldots$;

- Subexponential labels can be **quantified over** leading to new universal and existential quantifiers $\Cap$ and $\Cup$;

- The preorder $\preceq$ among subexponentials can be constructed using more **involved structures**, e.g, c-semirings.

Some Applications

- A framework for **proof systems**;
- A framework for **authorization logics**;
- A framework for **concurrent constraint programming languages**.

Sequents

In **linear logic**, there are two types of fórmulas **bounded** and **unbounded**. Sequents normally have the form:

$$\Theta \mid \Gamma \longrightarrow F$$

Sequents

In **linear logic**, there are two types of fórmulas **bounded** and **unbounded**. Sequents normally have the form:

$$\Theta \mid \Gamma \longrightarrow F$$

SELL has **as many contexts** as subexponential labels:

$$I = \{l_1, \ldots, l_n, \ldots, l_{m+n}\} \qquad U = \{l_1, \ldots, l_n\}$$

$$\underbrace{\Theta_1 \mid \cdots \mid \Theta_n}_{\text{Unbounded}} \mid \underbrace{\Gamma_{n+1} \mid \cdots \mid \Gamma_{n+m}}_{\text{Bounded}} \mid \Gamma \longrightarrow F$$

Sequents

In **linear logic**, there are two types of fórmulas **bounded** and **unbounded**. Sequents normally have the form:

$$\Theta \mid \Gamma \longrightarrow F$$

SELL has **as many contexts** as subexponential labels:

$$I = \{l_1, \ldots, l_n, \ldots, l_{m+n}\} \qquad U = \{l_1, \ldots, l_n\}$$

$$\underbrace{\Theta_1 \mid \cdots \mid \Theta_n}_{\text{Unbounded}} \mid \underbrace{\Gamma_{n+1} \mid \cdots \mid \Gamma_{n+m}}_{\text{Bounded}} \mid \Gamma \longrightarrow F$$

LL is an instance of SELL, where $I = U = \{u\}$. For the Linear K system from Frank's talk set $I = \{u\}$ and $U = \emptyset$.

We also have a focused proof system for SELL.

Rules

Bounded contexts are split, while unbounded are contracted:

$$\frac{\Theta_{1..n} \mid \Gamma_{n+1} \mid \cdots \mid \Gamma_{n+m} \mid \Gamma \longrightarrow F_1 \quad \Theta_{1..n} \mid \Gamma'_{n+1} \mid \cdots \mid \Gamma'_{n+m} \mid \Gamma \longrightarrow F_2}{\Theta_{1..n} \mid \Gamma_{n+1}\Gamma'_{n+1} \mid \cdots \mid \Gamma_{n+m}\Gamma'_{n+m} \mid \Gamma\Gamma' \longrightarrow F_1 \otimes F_2}$$

Rules

Bounded contexts are split, while unbounded are contracted:

$$\frac{\Theta_{1..n} \mid \Gamma_{n+1} \mid \cdots \mid \Gamma_{n+m} \mid \Gamma \longrightarrow F_1 \qquad \Theta_{1..n} \mid \Gamma'_{n+1} \mid \cdots \mid \Gamma'_{n+m} \mid \Gamma \longrightarrow F_2}{\Theta_{1..n} \mid \Gamma_{n+1}\Gamma'_{n+1} \mid \cdots \mid \Gamma_{n+m}\Gamma'_{n+m} \mid \Gamma\Gamma' \longrightarrow F_1 \otimes F_2}$$

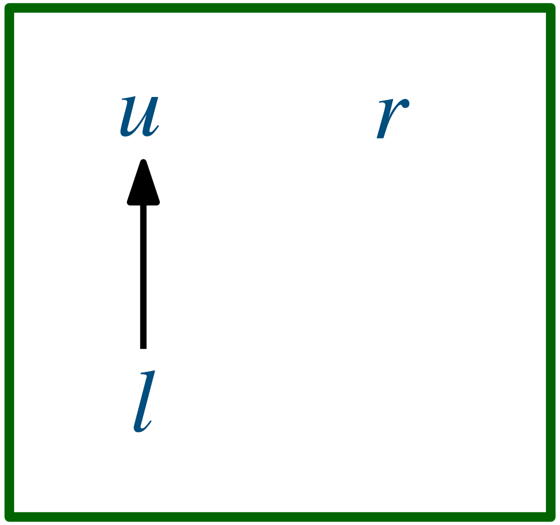
Unbounded contexts may be contracted when necessary:

$$\frac{}{\Theta_{1..n} \mid \cdot \mid \cdots \mid A \mid \cdot \mid \cdot \longrightarrow A}\ I$$

Preorder

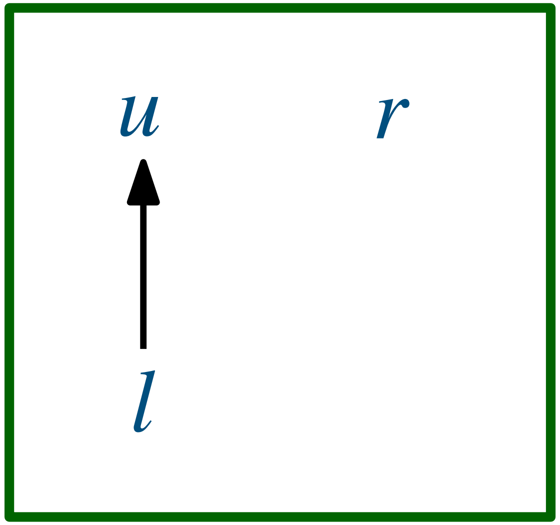
Preorder

Consider $I = \{u, l, r\}$, $U = \{u\}$ and the pre-order:



Preorder

Consider $I = \{u, l, r\}$, $U = \{u\}$ and the pre-order:



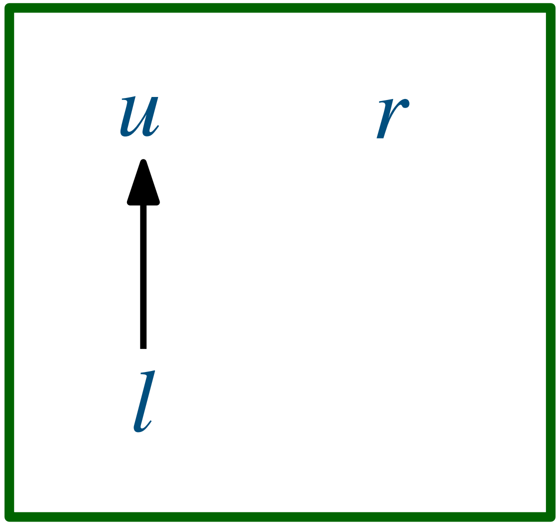
$$\frac{\Theta_u \mid \Gamma_l \mid \cdot \mid \cdot \longrightarrow F}{\Theta_u \mid \Gamma_l \mid \cdot \mid \cdot \longrightarrow\, !^l F}\ !_R$$

$$\frac{\cdot \mid \cdot \mid \Gamma_r \mid \cdot \longrightarrow F}{\Theta_u \mid \cdot \mid \Gamma_r \mid \cdot \longrightarrow\, !^r F}\ !_R$$

$$\frac{\Theta_u \mid \cdot \mid \cdot \mid \cdot \longrightarrow F}{\Theta_u \mid \cdot \mid \cdot \mid \cdot \longrightarrow\, !^u F}\ !_R$$

Preorder

Consider $I = \{u, l, r\}$, $U = \{u\}$ and the pre-order:



$$\frac{\Theta_u \mid \Gamma_l \mid \cdot \mid \cdot \longrightarrow F}{\Theta_u \mid \Gamma_l \mid \cdot \mid \cdot \longrightarrow\ !^l F}\ !_R$$

$$\frac{\cdot \mid \cdot \mid \Gamma_r \mid \cdot \longrightarrow F}{\Theta_u \mid \cdot \mid \Gamma_r \mid \cdot \longrightarrow\ !^r F}\ !_R$$

$$\frac{\Theta_u \mid \cdot \mid \cdot \mid \cdot \longrightarrow F}{\Theta_u \mid \cdot \mid \cdot \mid \cdot \longrightarrow\ !^u F}\ !_R$$

Similarly with left $?$ introduction rules:

$$\frac{\Theta_u \mid \Gamma_l \mid \cdot \mid G \longrightarrow\ ?^l F}{\Theta_u \mid ?^l G, \Gamma_l \mid \cdot \mid \cdot \longrightarrow\ ?^l F}\ !_R$$

Classical SELL

Sometimes it will be convenient to use the **classical version of SELL**.

Classical SELL

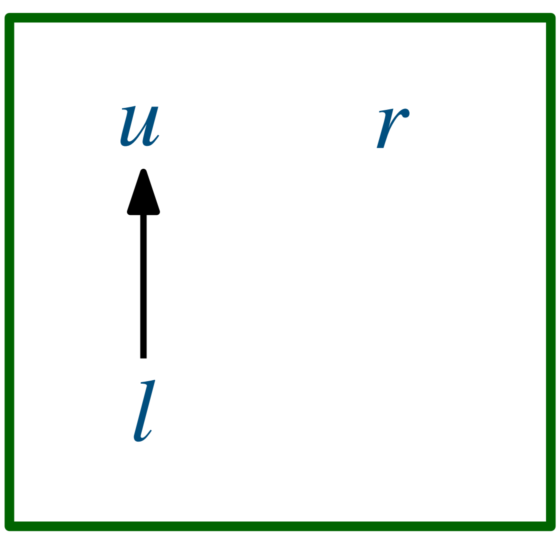
Sometimes it will be convenient to use the **classical version of SELL**.

Sequents

$I = \{l_1, \ldots, l_n, \ldots, l_{m+n}\}$ $\qquad$ $U = \{l_1, \ldots, l_n\}$

$$\vdash \Theta_1 \mid \cdots \mid \Theta_n \mid \Gamma_{n+1} \mid \cdots \mid \Gamma_{n+m} \mid \Gamma$$

Rules



$$\frac{}{\vdash \Theta_{1..n} \mid \cdot \mid \cdots \mid A \mid \cdot \mid A^\perp}\ I$$

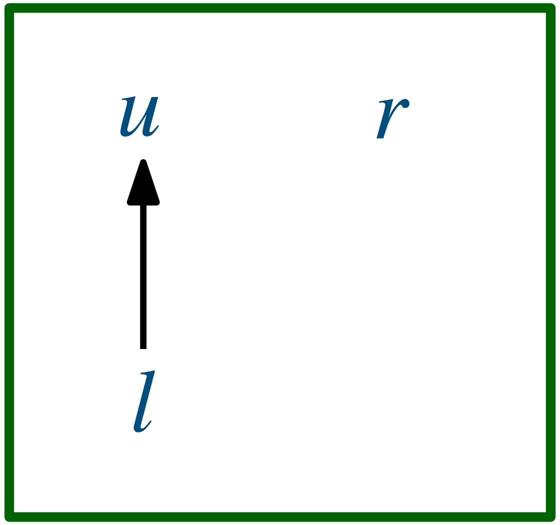
$$\frac{\vdash \Theta_u \mid \Gamma_l \mid \cdot \mid F}{\vdash \Theta_u \mid !^l F, \Gamma_l \mid \cdot \mid \cdot}\ !_R$$

Agenda

Subexponential Prefixes

- Subexponential Quantification
- Algebras for Subexponential Relations
- Conclusions and Future Work

Prefixes



$$\frac{\Theta_u \mid \Gamma_l \mid \cdot \mid \cdot \longrightarrow F}{\Theta_u \mid \Gamma_l \mid \cdot \mid \cdot \longrightarrow\ !^l F}\ !_R$$

$$\frac{\cdot \mid \cdot \mid \Gamma_r \mid \cdot \longrightarrow F}{\Theta_u \mid \cdot \mid \Gamma_r \mid \cdot \longrightarrow\ !^r F}\ !_R$$

$$\frac{\Theta_u \mid \cdot \mid \cdot \mid \cdot \longrightarrow F}{\Theta_u \mid \cdot \mid \cdot \mid \cdot \longrightarrow\ !^u F}\ !_R$$

- We are able to erase some types of unbounded formulas in the context;
- We are able to check whether only some types of formulas are present in the context.

Prefixes

Classical SELL as a Framework for Proof Systems

Prefixes

Classical SELL as a Framework for Proof Systems

Object Sequent $F_1, \ldots, F_n \longrightarrow G_1, \ldots, G_m$

$I = \{u, l, r\}$ $\lfloor \cdot \rfloor, \lceil \cdot \rceil : form \to o$

Meta Sequent $\vdash \Theta \mid \lfloor F_1 \rfloor, \ldots \lfloor F_n \rfloor \mid \lceil G_1 \rceil, \ldots, \lceil G_n \rceil \mid \cdot$

Encoding of the rules of the proof system, like a logic program.

Prefixes

- We are able to erase some types of unbounded formulas in the context.

Prefixes

- We are able to erase some types of unbounded formulas in the context.

Consider the following rule from **the multi-conclusion proof system** for intuitionistic logic:

$$\frac{\Gamma, F \longrightarrow G}{\Gamma \longrightarrow \Delta, F \supset G} \Rightarrow_R$$

Prefixes

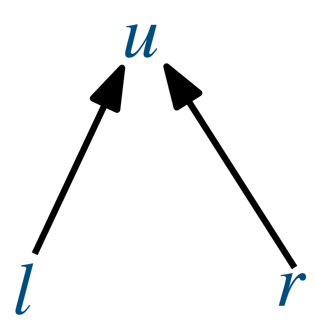
- We are able to erase some types of unbounded formulas in the context.

Consider the following rule from **the multi-conclusion proof system** for intuitionistic logic:

$$\frac{\Gamma, F \longrightarrow G}{\Gamma \longrightarrow \Delta, F \supset G} \Rightarrow_R$$

SELL Encoding

$u, l, r \in U$



$$\exists A.\exists B.\lceil A \supset B \rceil^{\perp} \otimes !^{l}(?^{l}\lfloor A \rfloor \parr ?^{r}\lceil B \rceil)$$

Prefixes

- We are able to erase some types of unbounded formulas in the context.

$$\dfrac{\dfrac{\Xi \qquad \dfrac{\dfrac{\vdash \Theta \mid \lfloor \Gamma, F \rfloor \mid \lceil G \rceil \mid}{\vdash \Theta \mid \lfloor \Gamma \rfloor \mid \cdot \mid \lfloor F \rfloor \parr ?^r \lceil G \rceil}}{\vdash \Theta \mid \lfloor \Gamma \rfloor \mid \lceil F \supset G, \Delta \rceil \mid !^l(?^l \lfloor F \rfloor \parr ?^r \lceil G \rceil)}}{\vdash \Theta \mid \lfloor \Gamma \rfloor \mid \lceil F \supset G, \Delta \rceil \mid \lceil F \supset G \rceil^\perp \otimes !^l(?^l \lfloor F \rfloor \parr ?^r \lceil G \rceil)}}{\dfrac{\vdash \Theta \mid \lfloor \Gamma \rfloor \mid \lceil F \supset G, \Delta \rceil \mid \exists A.\exists B.\lceil A \supset B \rceil^\perp \otimes !^l(?^l \lfloor A \rfloor \parr ?^r \lceil B \rceil)}{\vdash \Theta \mid \lfloor \Gamma \rfloor \mid \lceil F \supset G, \Delta \rceil \mid \cdot}}$$

The r-context is erased.

Prefixes

- We are able to erase some types of unbounded formulas in the context.

$$
\dfrac{\dfrac{\Xi \qquad \dfrac{\dfrac{\vdash \Theta \mid \lfloor \Gamma, F \rfloor \mid \lceil G \rceil \mid}{\vdash \Theta \mid \lfloor \Gamma \rfloor \mid \cdot \mid \lfloor F \rfloor \parr ?^{r}\lceil G \rceil}}{\vdash \Theta \mid \lfloor \Gamma \rfloor \mid \lceil F \supset G, \Delta \rceil \mid !^{l}(?^{l}\lfloor F \rfloor \parr ?^{r}\lceil G \rceil)}}{\vdash \Theta \mid \lfloor \Gamma \rfloor \mid \lceil F \supset G, \Delta \rceil \mid \lceil F \supset G \rceil^{\perp} \otimes !^{l}(?^{l}\lfloor F \rfloor \parr ?^{r}\lceil G \rceil)}}{\dfrac{\vdash \Theta \mid \lfloor \Gamma \rfloor \mid \lceil F \supset G, \Delta \rceil \mid \exists A.\exists B.\lceil A \supset B \rceil^{\perp} \otimes !^{l}(?^{l}\lfloor A \rfloor \parr ?^{r}\lceil B \rceil)}{\vdash \Theta \mid \lfloor \Gamma \rfloor \mid \lceil F \supset G, \Delta \rceil \mid \cdot}}
$$

The r-context is erased.

From the **focusing discipline**, in fact, this is the **only way to introduce this formula**. **Adequacy on the Level of Derivations**.

Prefixes

- We are able to check whether only some types of formulas are present in the context.

Prefixes

- We are able to check whether only some types of formulas are present in the context.

Consider the following rule from **the multi-conclusion proof system** for intuitionistic logic:

$$\frac{\Gamma, \bigcirc F, F \longrightarrow \bigcirc G}{\Gamma, \bigcirc F \longrightarrow \bigcirc G}\ \bigcirc L$$

Prefixes

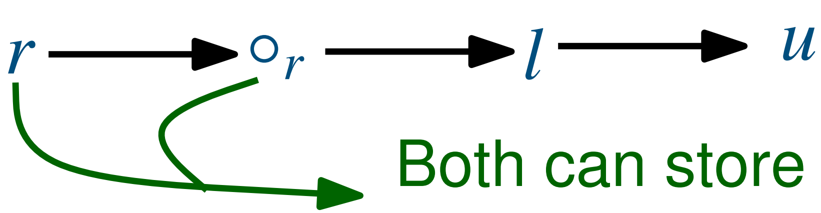
- We are able to check whether only some types of formulas are present in the context.

Consider the following rule from **the multi-conclusion proof system** for intuitionistic logic:

$$\frac{\Gamma, \bigcirc F, F \longrightarrow \bigcirc G}{\Gamma, \bigcirc F \longrightarrow \bigcirc G}\ \bigcirc L$$

SELL Encoding

$u, l \in U$



Both can store the formula on the r.h.s, but only $\circ_r$ can store a $\bigcirc$ formula.

$$\exists A. \lfloor \bigcirc A \rfloor^{\perp} \otimes !^{\circ_r} ?^{l} \lfloor A \rfloor$$

Prefixes

- We are able to check whether only some types of formulas are present in the context.

$$
\begin{array}{c}
\vdash \Theta \mid \lfloor \Gamma, \bigcirc F, F \rfloor \mid \cdot \mid \lceil \bigcirc G \rceil \mid \cdot \\
\hline
\vdash \Theta \mid \lfloor \Gamma, \bigcirc F \rfloor \mid \cdot \mid \lceil \bigcirc G \rceil \mid ?^{l} \lfloor F \rfloor \\
\hline
\Xi \qquad \vdash \Theta \mid \lfloor \Gamma, \bigcirc F \rfloor \mid \cdot \mid \lceil \bigcirc G \rceil \mid !^{\circ_r} ?^{l} \lfloor F \rfloor \\
\hline
\vdash \Theta \mid \lfloor \Gamma, \bigcirc F \rfloor \mid \cdot \mid \lceil \bigcirc G \rceil \mid \lfloor \bigcirc F \rfloor^{\perp} \otimes !^{\circ_r} ?^{l} \lfloor F \rfloor \\
\hline
\vdash \Theta \mid \lfloor \Gamma, \bigcirc F \rfloor \mid \cdot \mid \lceil \bigcirc G \rceil \mid \exists A. \lfloor \bigcirc A \rfloor^{\perp} \otimes !^{\circ_r} ?^{l} \lfloor A \rfloor \\
\hline
\vdash \Theta \mid \lfloor \Gamma, \bigcirc F \rfloor \mid \cdot \mid \lceil \bigcirc G \rceil \mid \cdot
\end{array}
$$

Only if the right formula is in the $\circ_r$ context.

More details in our JLC 2016 paper.

Putting this together

Intuitionistic SELL as a Framework for Linear Authorization Logics

Putting this together

Intuitionistic SELL as a Framework for Linear Authorization Logics

Three Families of Modalities [Garg et al.]

K says P K knows P K has P

Putting this together

Intuitionistic SELL as a Framework for Linear Authorization Logics

Three Families of Modalities [Garg et al.]

K says P $\qquad$ K knows P $\qquad$ K has P

A lax modality denoting that the principal K affirms the formula P:

$$\frac{\Gamma, P \longrightarrow K \text{ says } G}{\Gamma, K \text{ says } P \longrightarrow K \text{ says } G}\ \text{says}_L \qquad \frac{\Gamma \longrightarrow P}{\Gamma \longrightarrow K \text{ says } P}\ \text{says}_R$$

Putting this together

Intuitionistic SELL as a Framework for Linear Authorization Logics

Three Families of Modalities [Garg et al.]

K says P $\qquad$ K knows P $\qquad$ K has P

Since knowledge is unrestricted, one is allowed to contract as well as weaken it:

$$\frac{\Gamma \longrightarrow G}{\Gamma, K \text{ knows } P \longrightarrow G}\ W \qquad \frac{\Gamma, K \text{ knows } P, K \text{ knows } P \longrightarrow G}{\Gamma, K \text{ knows } P \longrightarrow G}\ C$$

Putting this together

Intuitionistic SELL as a Framework for Linear Authorization Logics

Three Families of Modalities [Garg et al.]

K says P K knows P K has P

An unbounded modality denoting that the principal K has the consumable resource P:

$$\frac{\Gamma, P \longrightarrow G}{\Gamma, K \text{ has } P \longrightarrow G}\ \text{has}_L \qquad \frac{\Psi, \Delta \longrightarrow P}{\Psi, \Delta \longrightarrow K \text{ has } P}\ \text{has}_R$$

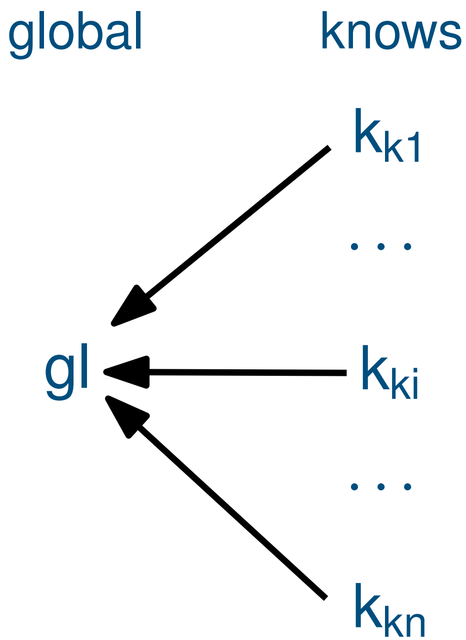
where Ψ contains only formulas of the form K knows F, while Δ contains only formulas of the form K has F.

Putting this together

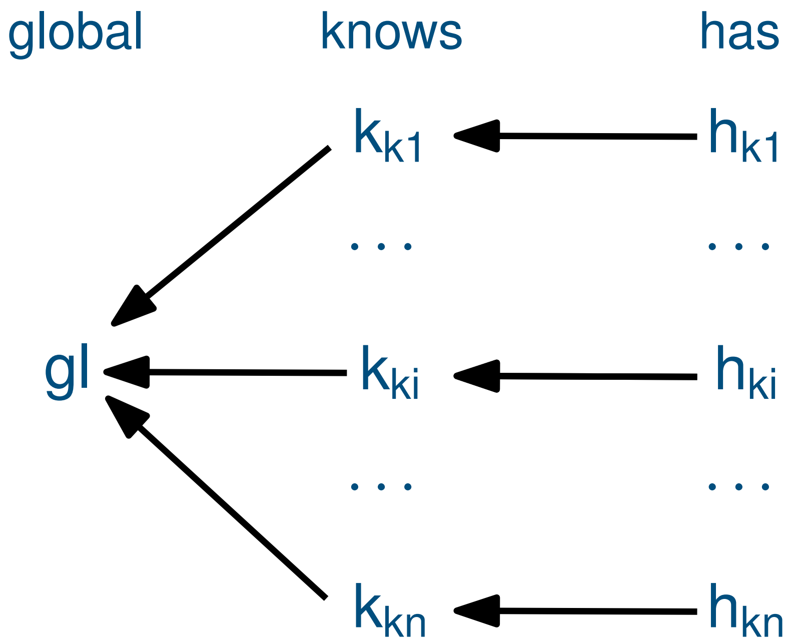
global

gl

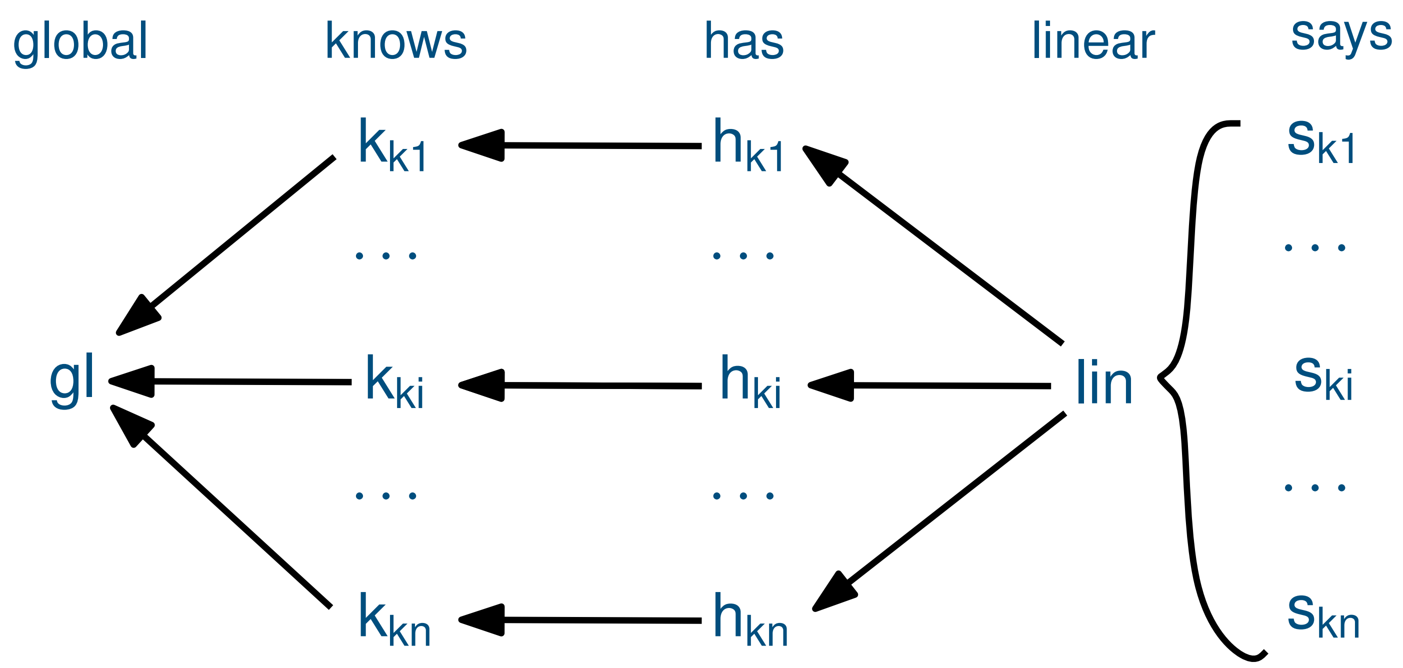
Putting this together



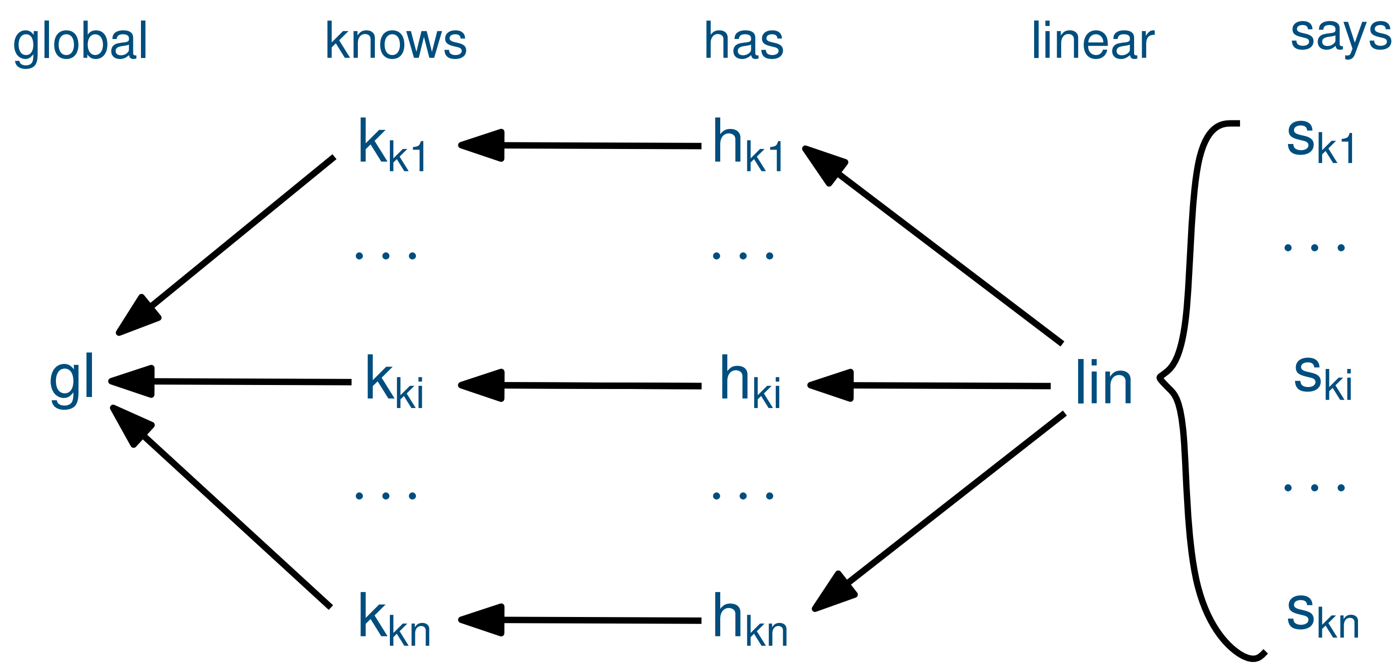
Putting this together



Putting this together



Putting this together



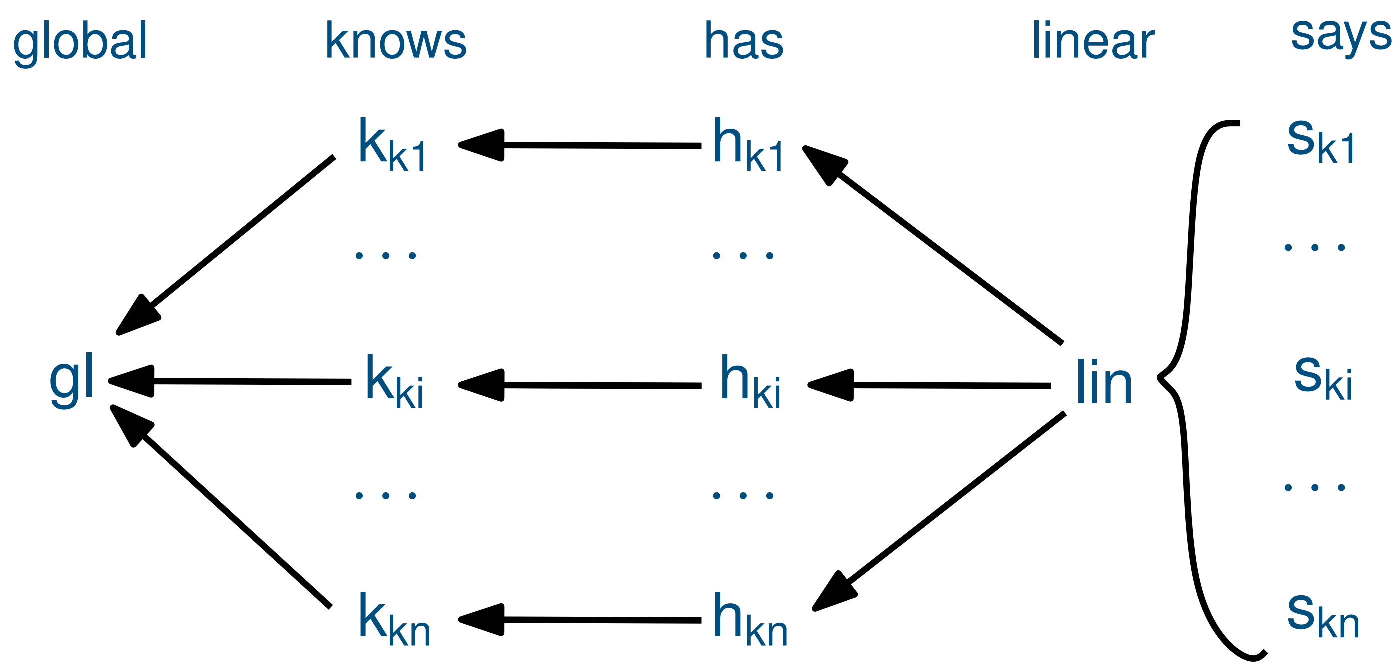
$$[\![F \text{ knows } K]\!]_L = !^{k_K}[\![F]\!]_L \qquad [\![F \text{ knows } K]\!]_R = !^{k_K}[\![F]\!]_R$$

$$[\![F \text{ has } K]\!]_L = !^{h_K}[\![F]\!]_L \qquad [\![F \text{ has } K]\!]_R = !^{h_K}[\![F]\!]_R$$

$$[\![F \text{ says } K]\!]_L = !^{lin}?^{s_k}[\![F]\!]_L$$

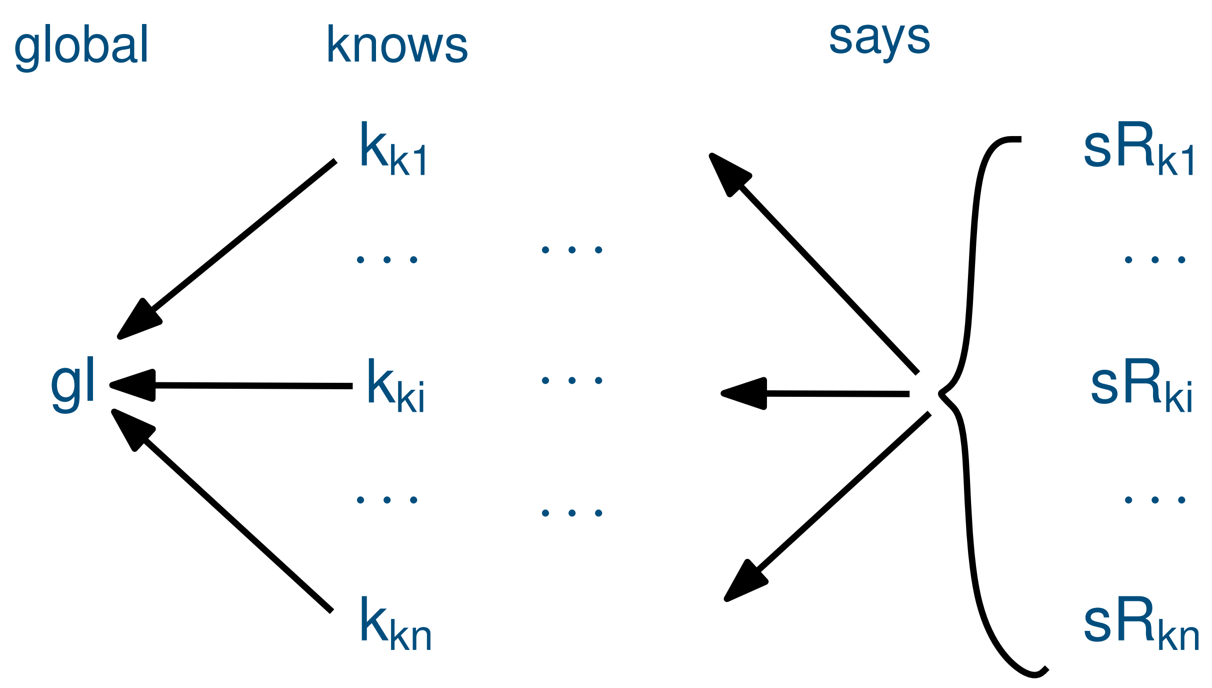
$$[\![F \text{ says } K]\!]_R = ?^{s_k}[\![F]\!]_R$$

Putting this together

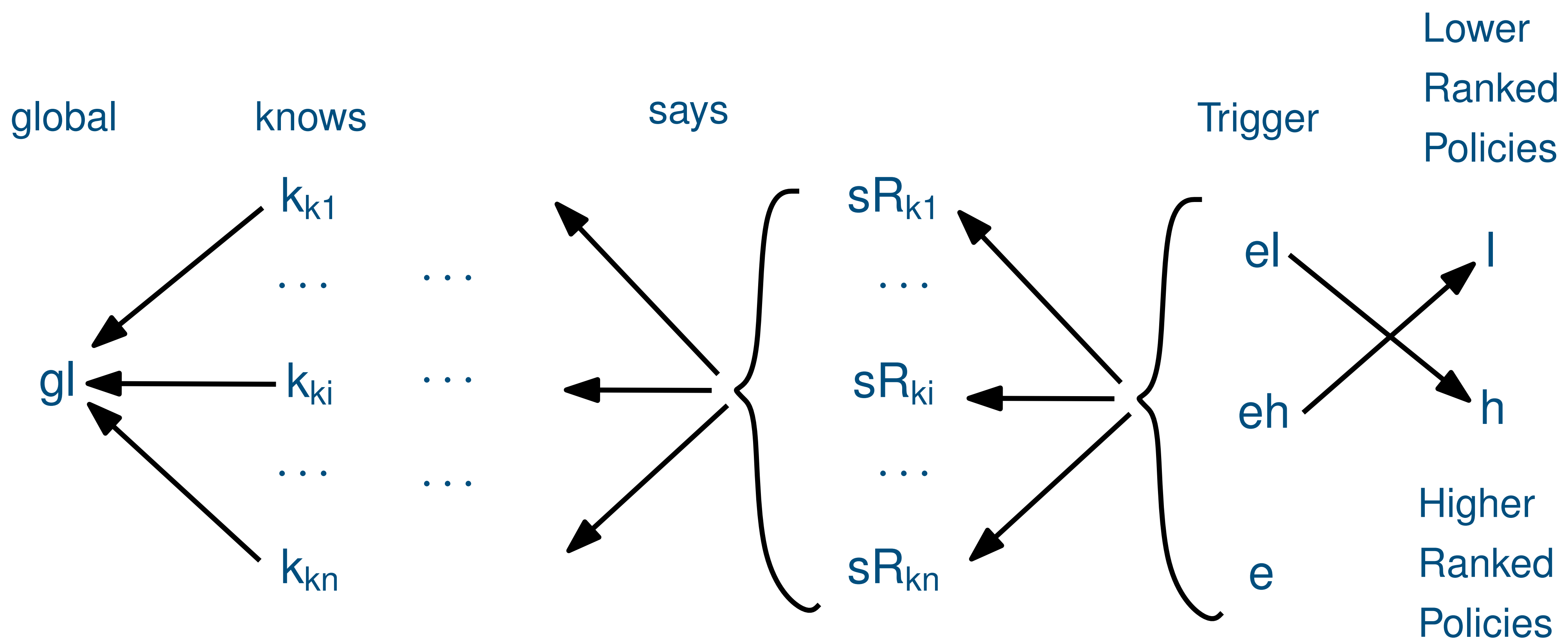


Theorem: The sequent $\Gamma \longrightarrow F$ is provable in linear authorization logic if and only if the sequent $[\![\Gamma]\!]_L \longrightarrow [\![F]\!]_R$ is provable in SELL.

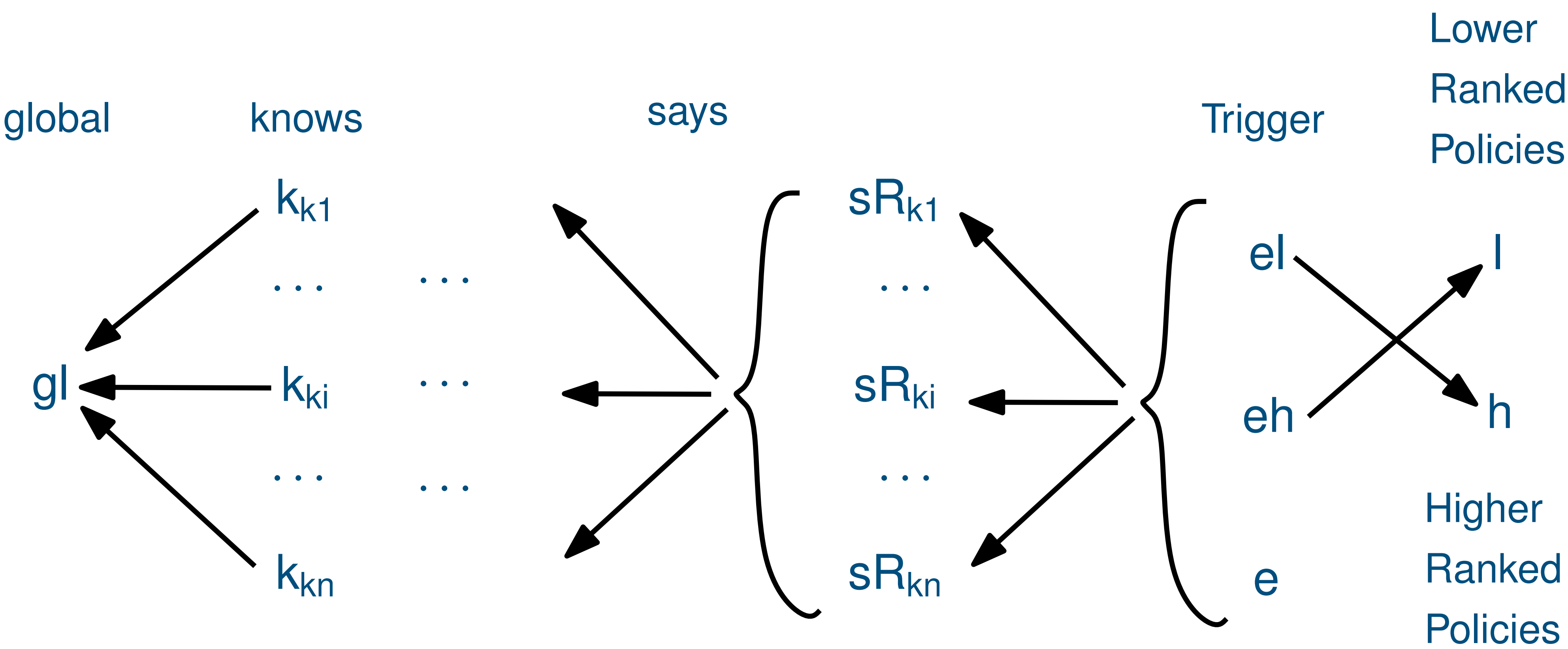
Putting this together



Putting this together



Putting this together



$$\dfrac{\dfrac{\Gamma \longrightarrow F}{\Gamma \longrightarrow\ !^{\mathsf{el}} F}\ !^{\mathsf{el}}{}_R}{\Gamma, !^{\mathsf{l}}\{\Gamma_L\} \longrightarrow\ !^{\mathsf{el}} F}\ n \times W$$

More details in my TCS 2014 paper.

Agenda

- Subexponential Prefixes
- **Subexponential Quantification**
- Algebras for Subexponential Relations
- Conclusions and Future Work

Adding Subexponential Quantifiers

Subexponential quantification **adds expressiveness to SELL**, but one needs to be **careful that SELL's nice properties**, *e.g.*, cut-elimination and focusing discipline, are still preserved.

Adding Subexponential Quantifiers

Subexponential quantification **adds expressiveness to SELL**, but one needs to be **careful that SELL's nice properties**, *e.g.*, cut-elimination and focusing discipline, are still preserved.

- The ideia is to **emulate the cut-elimination reductions** for the first-order quantifiers.
- Quantification may create generic variables, we call **Subexponential Variables**;
- However, subexponentials are organized into a pre-order, so we need more information on the variables. **We add a typing to subexponentials.**

Adding Subexponential Quantifiers

Signatures are of the form:

$$\langle I, \preceq, F, U \rangle$$

Adding Subexponential Quantifiers

Signatures are of the form:

$$\langle I, \preceq, F, U \rangle$$

- **Subexponential variables** are typed: $l : a$ means that l is in the ideal of a, *i.e.*, $l \in \downarrow a$.

Adding Subexponential Quantifiers

Signatures are of the form:

$$\langle I, \preceq, F, U \rangle$$

- **Subexponential variables** are typed: $l : a$ means that l is in the ideal of a, *i.e.*, $l \in \downarrow a$.
- $F = \{\mathfrak{f}_1, \ldots, \mathfrak{f}_n\}$ is a set of **subexponential index families**. In particular, $\mathfrak{f} \in F$ takes an element $a \in I$ and returns a subexponential index $\mathfrak{f}(a)$.

Adding Subexponential Quantifiers

Signatures are of the form:

$$\langle I, \preceq, F, U \rangle$$

- **Subexponential variables** are typed: $l : a$ means that l is in the ideal of a, *i.e.*, $l \in \downarrow a$.
- $F = \{\mathfrak{f}_1, \ldots, \mathfrak{f}_n\}$ is a set of **subexponential index families**. In particular, $\mathfrak{f} \in F$ takes an element $a \in I$ and returns a subexponential index $\mathfrak{f}(a)$.
- $U \subseteq \{\mathfrak{f}(a) \mid a \in I, \mathfrak{f} \in F\}$ is a set of **unbounded subexponentials**. As before, it is upwardly closed with respect to $\preceq$: if $b \preceq a$, where $a, b \in I$, and $\mathfrak{f}(b) \in U$ then $\mathfrak{f}(a) \in U$.

Adding Subexponential Quantifiers

$\Cap$ – Universal quantifier;

$\Cup$ – Existential quantifier;

Adding Subexponential Quantifiers

$\Cap$ – Universal quantifier;

$\Cup$ – Existential quantifier;

$$\frac{\mathcal{A}; \Gamma, P[l/x] \vdash G}{\mathcal{A}; \Gamma, \Cap x : a.P \vdash G}\ \Cap_L \qquad \frac{\mathcal{A}, l_e : a; \Gamma \vdash P[l_e/x]}{\mathcal{A}; \Gamma \vdash \Cap x : a.P}\ \Cap_R$$

$$\frac{\mathcal{A}, l_e : a; \Gamma, P[l_e/x] \vdash G}{\mathcal{A}; \Gamma, \Cup x : a.P \vdash G}\ \Cup_L \qquad \frac{\mathcal{A}; \Gamma \vdash P[l/x]}{\mathcal{A}; \Gamma \vdash \Cup x : a.P}\ \Cup_R$$

Adding Subexponential Quantifiers

$\Cap$ – Universal quantifier;

$\Cup$ – Existential quantifier;

$$\frac{\mathcal{A}; \Gamma, P[l/x] \vdash G}{\mathcal{A}; \Gamma, \Cap x : a.P \vdash G}\ \Cap_L \qquad \frac{\mathcal{A}, l_e : a; \Gamma \vdash P[l_e/x]}{\mathcal{A}; \Gamma \vdash \Cap x : a.P}\ \Cap_R$$

$$\frac{\mathcal{A}, l_e : a; \Gamma, P[l_e/x] \vdash G}{\mathcal{A}; \Gamma, \Cup x : a.P \vdash G}\ \Cup_L \qquad \frac{\mathcal{A}; \Gamma \vdash P[l/x]}{\mathcal{A}; \Gamma \vdash \Cup x : a.P}\ \Cup_R$$

$$\frac{\mathcal{A};\ !^{\mathfrak{f}(l_1 : a_1)} F_1, \ldots !^{\mathfrak{f}(l_n : a_n)} F_n \longrightarrow G}{\mathcal{A};\ !^{\mathfrak{f}(l_1 : a_1)} F_1, \ldots, !^{\mathfrak{f}(l_n : a_n)} F_n \longrightarrow\ !^{\mathfrak{f}(l : a)} G} \qquad \mathfrak{f}(l : a) \preceq_{\mathcal{A}} \mathfrak{f}(l_i : a_i)$$

where $\mathfrak{f}(l : a) \preceq_{\mathcal{A}} \mathfrak{f}(l_i : a_i)$ means $l_i \in\uparrow l$.

Adding Subexponential Quantifiers

Theorem For any signature Σ, the proof system $\text{SELL}^{\Cap}$ admits cut-elimination.

$\text{SELL}^{\Cap}$ **also has a complete focused proof system.**

Adding Subexponential Quantifiers

Intuitionistic SELL as a Framework for Concurrent Constraint Programming

Adding Subexponential Quantifiers

Intuitionistic SELL as a Framework for Concurrent Constraint Programming

A simple and powerful model of concurrency **tied to logic**:

- Systems are specified by constraints representing **partial information** on the variables of the system.
- Agents **tell** and **ask** constraints on a shared store of constraints.
- CCP is **parametric** in a Constraint System (e.g. $x > 42 \vdash_\Delta x > 0$).

Adding Subexponential Quantifiers

Intuitionistic SELL as a Framework for Concurrent Constraint Programming

CCP has been extended to deal with different application domains:

- tcc: Reactive and timed systems;
- lccp: Linearity and resources;
- ntcc: Time, non-determinsim and asynchrony;
- utcc: Mobility;
- eccp and sccp: Epistemic and Spatial reasoning.

Adding Subexponential Quantifiers

Intuitionistic SELL as a Framework for Concurrent Constraint Programming

CCP has been extended to deal with different application domains:

- tcc: Reactive and timed systems;
- lccp: Linearity and resources;
- ntcc: Time, non-determinsim and asynchrony;
- utcc: Mobility;
- eccp and sccp: Epistemic and Spatial reasoning.

All these systems can be encoded in SELL$^{\Cap}$. In fact, we show how to combine some of them.

Adding Subexponential Quantifiers

Intuitionistic SELL as a Framework for Concurrent Constraint Programming

- $!^s P$ is **located** at s (epistemic and temporal);
- $!^s ?^s P$ is **confined** to s (spatial);
- $\Cap l : a\ P$ – P can move to locations below (outside) a (mobility).

Adding Subexponential Quantifiers

Intuitionistic SELL as a Framework for Concurrent Constraint Programming

All our encodings have a **strong level of adequacy**: proof search and the execution of encoded programs **match exactly**.

Adding Subexponential Quantifiers

Intuitionistic SELL as a Framework for Concurrent Constraint Programming

All our encodings have a **strong level of adequacy**: proof search and the execution of encoded programs **match exactly**.

More details in our CONCUR 2013 paper.

Agenda

- Subexponential Prefixes
- Subexponential Quantification
- **Algebras for Subexponential Relations**
- Conclusions and Future Work

Algebra for Subexponential Relations

Until now, $\preceq$ was **quite simple**. We can add more structure it **to capture even more computational behaviors**.

Algebra for Subexponential Relations

C-Semiring is a tuple $\langle \mathcal{A}, +, \times, \bot_A, \top_A \rangle$

- $+$: commutative, associative, idempotent, $\bot_A$-unit, $\top_A$-absorbing
- $\times$ is associative, commutative, distribute over $+$, $\top_A$-unit, $\bot_A$-absorbing

Let $\leq_A$ be defined as $a \leq_A b$ iff $a + b = b$. Then, $\langle \mathcal{A}, \leq_A \rangle$ is a complete lattice where:

- $+$ and $\times$ are monotone on $\leq_A$, $+$ is the *lub operator.*

If $\times$ is idempotent, then

- $\langle \mathcal{A}, \leq_A \rangle$ is a complete distribute lattice, $\times$ is its *glb.*

Algebra for Subexponential Relations

C-Semiring is a tuple $\langle \mathcal{A}, +, \times, \bot_A, \top_A \rangle$

Choses the "best"valuation.

Combines constraints

Algebra for Subexponential Relations

C-Semiring is a tuple $\langle \mathcal{A}, +, \times, \bot_A, \top_A \rangle$

Choses the "best"valuation. (+)

Combines constraints (×)

- Crisp: $S_c = \langle \{\texttt{true}, \textit{false}\}, \vee, \wedge, \textit{false}, \texttt{true} \rangle$
- Fuzzy: $S_F = \langle [0, 1], max, min, 0, 1 \rangle$ – Preferences
- Probabilistic: $S_P = \langle [0, 1], max, \times, 0, 1 \rangle$
- Weighted: $S_w = \langle \mathcal{R}^-, max, +, -\infty, 0 \rangle$ – Costs

Algebra for Subexponential Relations

C-Semiring is a tuple $\langle \mathcal{A}, +, \times, \bot_A, \top_A \rangle$

Choses the "best"valuation. (+)

Combines constraints (×)

- Crisp: $S_c = \langle \{\mathtt{true}, \mathit{false}\}, \vee, \wedge, \mathit{false}, \mathtt{true} \rangle$
- Fuzzy: $S_F = \langle [0,1], max, min, 0, 1 \rangle$ – Preferences
- Probabilistic: $S_P = \langle [0,1], max, \times, 0, 1 \rangle$
- Weighted: $S_w = \langle \mathcal{R}^-, max, +, -\infty, 0 \rangle$ – Costs

An example of Fuzzy constraints:

x	y	$x < y$	$x > 1$	$c_1 \otimes c_2$
1	1	0.5	0.2	0.2
1	2	1.0	0.2	0.2
2	1	0.2	1.0	0.2
2	2	0.5	1.0	0.5

$\sum v_i = 0.5$. Best solution=0.5

Algebra for Subexponential Relations

All the nice properties are preserved, *i.e.*,
cut-elimination, focusing discipline, adequacy, etc.

Algebra for Subexponential Relations

All the nice properties are preserved, *i.e.*, cut-elimination, focusing discipline, adequacy, etc.

More details in our ICLP 2014 paper. In our TCS paper, we show how soft constraints can be combined with spatial, epistemic and temporal modalities.

Agenda

- Subexponential Prefixes
- Subexponential Quantification
- Algebras for Subexponential Relations

Conclusions and Future Work

Conclusions and Future Work

- We reviewed SELL a linear logic framework with subexponentials and its extensions.
- We briefly explained how SELL can be used as a framework for Proof Systems, Authorization Logics, and CCP.

Conclusions and Future Work

As future work, we are investigating:

- **Verification of SELL specifications**: Linear logic does help in proving properties about proof systems, such as cut-elimination, when rules permute, etc. More is needed to understand how one can profit when specifying other types of systems.
- **Other algebras for $\leq$**: Investigate mechanisms to combine modalities in a more systematic fashion.
- **Other forms of quantification**: There seems to be a number of forms of quantifying subexponentials. We need to understand these better.
- **Other applications**: Cyber-Physical security protocols, verification of drone strategies.

Questions