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

\[
\frac{\Gamma, F, G \rightarrow H}{\Gamma, F \otimes G \rightarrow H} \quad \otimes_L
\]

\[
\frac{\Gamma_1 \rightarrow F \quad \Gamma_2 \rightarrow G}{\Gamma_1, \Gamma_2 \rightarrow F \otimes G} \quad \otimes_R
\]

\[
\frac{\Gamma_1 \rightarrow F \quad \Gamma_2, G \rightarrow H}{\Gamma_1, \Gamma_2, F \multimap G \rightarrow H} \quad \multimap_L
\]

\[
\frac{\Gamma, F \rightarrow G}{\Gamma \rightarrow F \multimap G} \quad \multimap_R
\]
## Linear Logic Basics

### Multiplicative Fragment

<table>
<thead>
<tr>
<th>Rule</th>
<th>Formulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\otimes_L$</td>
<td>$\Gamma, F, G \rightarrow H \quad \rightarrow \quad \Gamma, F \otimes G \rightarrow H$</td>
</tr>
<tr>
<td>$\otimes_R$</td>
<td>$\Gamma_1 \rightarrow F \quad \quad \Gamma_2 \rightarrow G \quad \rightarrow \quad \Gamma_1, \Gamma_2 \rightarrow F \otimes G$</td>
</tr>
<tr>
<td>$\multimap_L$</td>
<td>$\Gamma_1 \rightarrow F \quad \Gamma_2, G \rightarrow H \quad \rightarrow \quad \Gamma_1, \Gamma_2, F \multimap G \rightarrow H$</td>
</tr>
<tr>
<td>$\multimap_R$</td>
<td>$\Gamma, F \rightarrow G \quad \rightarrow \quad \Gamma \rightarrow F \multimap G$</td>
</tr>
</tbody>
</table>

Contraction and weakening are controlled by the exponentials ${\otimes}$ and ${\multimap}$.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Formulation</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C$</td>
<td>$\Gamma, !P, !P \rightarrow G \quad \rightarrow \quad \Gamma, !P \rightarrow G$</td>
</tr>
<tr>
<td>$W$</td>
<td>$\Gamma \rightarrow G \quad \rightarrow \quad \Gamma, !P \rightarrow G$</td>
</tr>
</tbody>
</table>
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 $?^b, ?^r$:

$!^b F \not\equiv !^r F \quad ?^b F \not\equiv ?^r F$
Subexponentials

Linear Logic Exponentials are Not Canonical

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

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

All other connectives are canonical.
Subexponentials

Linear Logic Exponentials are Not Canonical

\(!^b, !^r\) and \(?^b, ?^r\):

\[ !^b F \neq !^r F \quad ?^b F \neq ?^r F \]

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:

\[
\frac{\Gamma, !^a P, !^a P \rightarrow G}{\Gamma, !^a P \rightarrow G} \quad C \quad \frac{\Gamma \rightarrow G}{\Gamma, !^a P \rightarrow G} \quad W
\]
**Subexponentials**

Linear Logic Exponentials are Not Canonical

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

Subexponentials

$!^b F \neq !^r F$

$?^b F \neq ?^r F$

All other connectives are canonical.

Subexponential Signature

$\langle I, \leq, U \rangle$

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

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

\[
\begin{align*}
\Gamma, !^a P, !^a P & \rightarrow G \\
\Gamma, !^a P & \rightarrow G
\end{align*}
\]

$C$

\[
\begin{align*}
\Gamma & \rightarrow G \\
\Gamma, !^a P & \rightarrow G
\end{align*}
\]

$W$

In fact, signatures are of the form:

$\langle I, \leq, C, W \rangle$
Subexponentials

Linear Logic Exponentials are Not Canonical

\(!^b, !^r\) and \(?^b, ?^r\):

Subexponentials

\(!^b F \neq !^r F\)

\(?^b F \neq ?^r F\)

All other connectives are canonical.

Subexponential Signature

\(\langle I, \leq, U \rangle\)

where \(U \subseteq I\) and is closed under \(\leq\).

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

\[
\Gamma, !^a P, !^a P \rightarrow G \\
\Gamma, !^a P \rightarrow G \\
\Gamma, !^a P \rightarrow G \\
\Gamma, !^a P \rightarrow G
\]

C

W

Introduction Rules

\[
\frac{!^x_1 F_1, \ldots, !^x_n F_n \rightarrow G}{!^a G} !^a R
\]

\[
\frac{!^x_1 F_1, \ldots, !^x_n F_n, F \rightarrow ?^x_{n+1} G}{?^a F \rightarrow ?^x_{n+1} G} ?^a L
\]

where \(a \leq x_i\) for all \(i\).
Subexponentials

Linear Logic Exponentials are **Not Canonical**

\[ !^b, !^r \text{ and } ?^b, ?^r : \]

- Subexponentials
  - \( !^b F \neq !^r F \)
  - \( ?^b F \neq ?^r F \)

All other connectives are canonical.

### Subexponential Signature

\[ \langle I, \leq, U \rangle \]

where \( U \subseteq I \) and is closed under \( \leq \).

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

- **Introduction Rules**
  - \( !^x_1 F_1, \ldots, !^x_n F_n \rightarrow G \)
  - \( !^a G \rightarrow !^r F \)

\[
\frac{!^x_1 F_1, \ldots, !^x_n F_n \rightarrow G}{!^x_1 F_1, \ldots, !^x_n F_n \rightarrow !^a G}
\]

- \( !^x_1 F_1, \ldots, !^x_n F_n, F \rightarrow ?^{x+n+1} G \)
  - \( ?^a L \)

\[
\frac{!^x_1 F_1, \ldots, !^x_n F_n, ?^a F \rightarrow ?^{x+n+1} G}{!^x_1 F_1, \ldots, !^x_n F_n, ?^a F \rightarrow ?^{x+n+1} G}
\]

where \( a \leq x_i \) for all \( i \).

**Theorem:** For any subexponential signature, \( \Sigma \), \( \text{SELL}_\Sigma \) 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 \( \forall \) and \( \exists \);

• 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:

$$\Theta \mid \Gamma \rightarrow F$$
In **linear logic**, there are two types of formulas **bounded** and **unbounded**. Sequents normally have the form:

\[ \Theta \mid \Gamma \rightarrow F \]

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

\[ I = \{l_1, \ldots, l_n, \ldots, l_{m+n}\} \quad U = \{l_1, \ldots, l_n\} \]

\[ \Theta_1 \mid \cdots \mid \Theta_n \mid \Gamma_{n+1} \mid \cdots \mid \Gamma_{n+m} \mid \Gamma \rightarrow F \]

Unbounded \hspace{5cm} Bounded
Sequents

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

$$ \Theta \mid \Gamma \rightarrow F $$

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

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

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

**Unbounded** \hspace{2cm} **Bounded**

**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.*
Bounded contexts are split, while unbounded are contracted:

\[ \Theta_{1..n} \mid \Gamma_{n+1} \mid \cdots \mid \Gamma_{n+m} \mid \Gamma \rightarrow F_1 \quad \Theta_{1..n} \mid \Gamma'_{n+1} \mid \cdots \mid \Gamma'_{n+m} \mid \Gamma \rightarrow F_2 \]

\[ \Theta_{1..n} \mid \Gamma_{n+1} \Gamma'_{n+1} \mid \cdots \mid \Gamma_{n+m} \Gamma'_{n+m} \mid \Gamma \Gamma' \rightarrow F_1 \otimes F_2 \]
Bounded contexts are split, while unbounded are contracted:

\[
\Theta_{1..n} | \Gamma_{n+1} | \cdots | \Gamma_{n+m} | \Gamma \rightarrow F_1 \quad \Theta_{1..n} | \Gamma'_{n+1} | \cdots | \Gamma'_{n+m} | \Gamma \rightarrow F_2
\]

\[
\Theta_{1..n} | \Gamma_{n+1} \Gamma'_{n+1} | \cdots | \Gamma_{n+m} \Gamma'_{n+m} | \Gamma \Gamma' \rightarrow F_1 \otimes F_2
\]

Unbounded contexts may be contracted when necessary:

\[
\Theta_{1..n} | \cdot | \cdots | A | \cdot | \cdot \rightarrow A \quad I
\]
Preorder
Consider $I = \{u, l, r\}$, $U = \{u\}$ and the pre-order:
Consider $I = \{u, l, r\}$, $U = \{u\}$ and the pre-order:

\[
\Theta_u | \Gamma_l | \cdot | \cdot \rightarrow F \\
\Theta_u | \Gamma_l | \cdot | \cdot \rightarrow \! \! l ! \!/ F \\
\cdot | \cdot | \Gamma_r | \cdot \rightarrow F \\
\Theta_u | \cdot | \Gamma_r | \cdot \rightarrow \! \! r ! \!/ F \\
\Theta_u | \cdot | \cdot | \cdot \rightarrow F \\
\Theta_u | \cdot | \cdot | \cdot \rightarrow \! \! u ! \!/ F \\
\Theta_u | \cdot | \cdot | \cdot \rightarrow \! \! u ! \!/ F
\]
Consider $I = \{u, l, r\}$, $U = \{u\}$ and the pre-order:

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

Similarly with left $?$ introduction rules:

$$\Theta_u \mid \Gamma_l \mid \cdot \mid \cdot \rightarrow F \quad !_R$$

$$\Theta_u \mid \Gamma_l \mid \cdot \mid \cdot \rightarrow !lF \quad !_R$$

$$\cdot \mid \cdot \mid \Gamma_r \mid \cdot \rightarrow F \quad !_R$$

$$\Theta_u \mid \cdot \mid \Gamma_r \mid \cdot \rightarrow !_rF \quad !_R$$

$$\Theta_u \mid \cdot \mid \cdot \mid \cdot \rightarrow F \quad !_R$$

$$\Theta_u \mid \cdot \mid \cdot \mid \cdot \rightarrow !_uF \quad !_R$$

Similarly with left $?$ introduction rules:

$$\Theta_u \mid \Gamma_l \mid \cdot \mid G \rightarrow ?lF \quad !_R$$

$$\Theta_u \mid ?lG, \Gamma_l \mid \cdot \mid \cdot \rightarrow ?lF \quad !_R$$
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**

\[ I = \{l_1, \ldots, l_n, \ldots, l_{m+n}\} \quad U = \{l_1, \ldots, l_n\} \]

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

**Rules**

\[ \vdash \Theta_{1..n} \mid \cdots \mid A \mid \cdots \mid A^\perp \quad I \]

\[ \vdash \Theta_u \mid \Gamma_l \mid \cdots \mid F \]

\[ \vdash \Theta_u \mid !l F, \Gamma_l \mid \cdots \quad !R \]
Agenda

Subexponential Prefixes

- Subexponential Quantification
- Algebras for Subexponential Relations
- Conclusions and Future Work
• We are able to check whether only some types of formulas are present in the context.

• We are able to erase some types of unbounded formulas in the context;
Prefixes

Classical SELL as a Framework for Proof Systems
Prefixes

**Classical SELL as a Framework for Proof Systems**

Object Sequent \( F_1, \ldots, F_n \rightarrow G_1, \ldots, G_m \)

\[ I = \{u, l, r\} \quad \llbracket \cdot \rrbracket, \llceil \cdot \rrceil : \text{form} \rightarrow o \]

Meta Sequent \( \vdash \emptyset \mid [F_1], \ldots, [F_n] \mid [G_1], \ldots, [G_n] \mid \cdot \)

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:

\[
\frac{\Gamma, F \rightarrow G}{\Gamma \rightarrow \Delta, F \supset G} \Rightarrow_R
\]
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:

\[ \frac{\Gamma, F \rightarrow G}{\Gamma \rightarrow \Delta, F \supset G} \Rightarrow_R \]

SELL Encoding

\[ \exists A. \exists B. [A \supset B]^\perp \otimes !^l(?^l[A] \otimes ?^r[B]) \]
Prefixes

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

\[
\begin{align*}
&\vdash \Theta | [\Gamma, F] | [G] | \\
&\vdash \Theta | [\Gamma] | \cdot | [F] \otimes ?' [G] \\
&\vdash \Theta | [\Gamma] | [F \supset G, \Delta] | ! l (? l [F] \otimes ?' [G]) \\
&\vdash \Theta | [\Gamma] | [F \supset G, \Delta] | [F \supset G] | ! l (? l [F] \otimes ?' [G]) \\
&\vdash \Theta | [\Gamma] | [F \supset G, \Delta] | \exists A. \exists B. [A \supset B] | ! l (? l [A] \otimes ?' [B]) \\
&\vdash \Theta | [\Gamma] | [F \supset G, \Delta] | \\
\end{align*}
\]

The \( r \)-context is erased.
Prefixes

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

\[
\begin{align*}
\vdash \Theta | [\Gamma, F] | [G] | &
\vdash \Theta | [\Gamma] | [F] \otimes ?' [G] \\
\equiv &
\vdash \Theta | [\Gamma] | [F \\supset G, \Delta] | !'(?^[F] \otimes ?'[G])
\end{align*}
\]

\[
\begin{align*}
\vdash \Theta | [\Gamma] | [F \supset G, \Delta] | [F \supset G] \perp \otimes !'(?^[F] \otimes ?'[G])
\vdash \Theta | [\Gamma] | [F \supset G, \Delta] | \exists A. \exists B. [A \supset B] ^\perp \otimes !'(?^[A] \otimes ?'[B])
\end{align*}
\]

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:

\[
\frac{\Gamma, \bigcirc F, F \rightarrow \bigcirc G}{\Gamma, \bigcirc F \rightarrow \bigcirc G} \quad \bigcirc L
\]
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:

\[
\begin{align*}
\Gamma, \bigcirc F, F & \rightarrow \bigcirc G \\
\Gamma, \bigcirc F & \rightarrow \bigcirc G
\end{align*}
\]

**SELL Encoding**

\( u, l \in U \)

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

\( \exists A. [\bigcirc A] \downarrow \otimes !_{\circ_r} ?^l [A] \)
We are able to check whether only some types of formulas are present in the 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.]

\[ K \text{ says } P \quad K \text{ knows } P \quad K \text{ has } P \]

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

\[
\Gamma, P \rightarrow K \text{ says } G \\
\Gamma, K \text{ says } P \rightarrow K \text{ says } G \\
\Gamma \rightarrow P \\
\Gamma \rightarrow K \text{ says } P
\]

\( \text{say}_{L} \quad \text{say}_{R} \)
Putting this together

**Intuitionistic SELL** as a Framework for Linear Authorization Logics

Three Families of Modalities [Garg et al.]

\[
\begin{align*}
K \text{ says } P & \quad K \text{ knows } P & \quad K \text{ has } P
\end{align*}
\]

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

\[
\begin{align*}
\Gamma \rightarrow G & \quad W & \Gamma, K \text{ knows } P, K \text{ knows } P \rightarrow G & \quad C
\end{align*}
\]
Putting this together

Intuitionistic SELL as a Framework for Linear Authorization Logics

Three Families of Modalities [Garg et al.]

\[ K \text{ says } P \quad K \text{ knows } P \quad K \text{ has } P \]

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

\[
\frac{\Gamma, P \rightarrow G}{\Gamma, K \text{ has } P \rightarrow G} \quad \text{has}_L \quad \frac{\Psi, \Delta \rightarrow P}{\Psi, \Delta \rightarrow K \text{ has } P} \quad \text{has}_R
\]

where \( \Psi \) contains only formulas of the form \( K \text{ knows } F \), while \( \Delta \) contains only formulas of the form \( K \text{ has } F \).
Putting this together

global

gl
Putting this together

gl knows

k_{k1}

... 

k_{ki}

... 

k_{kn}
Putting this together

global knows has

\[
\begin{align*}
&k_{k_1} &\rightarrow &h_{k_1} \\
&\ldots &\rightarrow &\ldots \\
&k_{k_i} &\rightarrow &h_{k_i} \\
&\ldots &\rightarrow &\ldots \\
&k_{k_n} &\rightarrow &h_{k_n}
\end{align*}
\]
Putting this together

global knows has linear says

\[ g_l \rightarrow k_{k_1} \rightarrow h_{k_1} \rightarrow \ldots \rightarrow h_{k_i} \rightarrow k_{k_i} \rightarrow \ldots \rightarrow h_{k_n} \rightarrow k_{k_n} \rightarrow \{ s_{k_1}, \ldots, s_{k_i}, \ldots, s_{k_n} \} \]
Putting this together

\[
\begin{align*}
[[F \text{ knows } K]]_L &= !^{k_K} [[F]]_L \\
[[F \text{ has } K]]_L &= !^{h_K} [[F]]_L \\
[[F \text{ says } K]]_L &= !^{lin} ?^{s_k} [[F]]_L \\
[[F \text{ says } K]]_R &= ?^{s_k} [[F]]_R
\end{align*}
\]
Theorem: The sequent $\Gamma \rightarrow F$ is provable in linear authorization logic if and only if the sequent $\llbracket \Gamma \rrbracket_L \rightarrow \llbracket F \rrbracket_R$ is provable in SELL.
Putting this together

global knows says

\[ \begin{align*}
gl & \quad k_{k1} \\
& \quad \cdots \quad \cdots \\
& \quad k_{ki} \\
& \quad \cdots \quad \cdots \\
& \quad k_{kn}
\end{align*} \]

\[ \begin{align*}
sR_{k1} \\
& \quad \cdots \\
sR_{ki} \\
& \quad \cdots \\
sR_{kn}
\end{align*} \]
Putting this together

- global knows
  - $k_{k1}$
  - $\ldots$
  - $\ldots$
  - $k_{kn}$

- says
  - $sR_{k1}$
  - $\ldots$
  - $sR_{ki}$
  - $sR_{kn}$

- Trigger
  - $el$
  - $eh$
  - $e$
  - $l$
  - $h$

Lower Ranked Policies
Higher Ranked Policies
Putting this together says:

```
\begin{align*}
\Gamma &\to F \\
\Gamma &\to !^e \![F]_R \\
\Gamma, {!^l\{\Gamma_L\}} &\to !^e \![F]_n \times W
\end{align*}
```

More details in my TCS 2014 paper.
Agenda

- Subexponential Prefixes

Subexponential Quantification

- Algebras for Subexponential Relations
- Conclusions and Future Work
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.
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 idea 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:

$$\langle I, \leq, F, U \rangle$$
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., \( l \in \downarrow a \).
Signatures are of the form:

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

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

- $F = \{\bar{f}_1, \ldots, \bar{f}_n\}$ is a set of **subexponential index families**. In particular, $\bar{f} \in F$ takes an element $a \in I$ and returns a subexponential index $\bar{f}(a)$. 
Adding Subexponential Quantifiers

Signatures are of the form:

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

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

- \( F = \{ f_1, \ldots, f_n \} \) is a set of **subexponential index families**. In particular, \( f \in F \) takes an element \( a \in I \) and returns a subexponential index \( f(a) \).

- \( U \subseteq \{ f(a) \mid a \in I, f \in F \} \) is a set of **unbounded subexponentials**. As before, it is upwardly closed with respect to \( \leq \): if \( b \leq a \), where \( a, b \in I \), and \( f(b) \in U \) then \( f(a) \in U \).
Adding Subexponential Quantifiers

∩ – Universal quantifier;
∪ – Existential quantifier;
Adding Subexponential Quantifiers

\( \forall \) – Universal quantifier;

\( \exists \) – Existential quantifier;

\[
\frac{\mathcal{A}; \Gamma, P[l/x] \vdash G}{\mathcal{A}; \Gamma, \forall x : a.P \vdash G} \quad \text{\( \forall_L \)}
\]

\[
\frac{\mathcal{A}; \Gamma \vdash P[l_e/x]}{\mathcal{A}; \Gamma \vdash \forall x : a.P} \quad \text{\( \forall_R \)}
\]

\[
\frac{\mathcal{A}, l_e : a; \Gamma, P[l_e/x] \vdash G}{\mathcal{A}, \forall x : a.P \vdash G} \quad \text{\( \exists_L \)}
\]

\[
\frac{\mathcal{A}; \Gamma \vdash P[l/x]}{\mathcal{A}; \Gamma \vdash \exists x : a.P} \quad \text{\( \exists_R \)}
\]
Adding Subexponential Quantifiers

\[ \forall - \text{Universal quantifier; } \]
\[ \exists - \text{Existential quantifier; } \]

\[ \frac{A; \Gamma, P[l/x] \vdash G}{A; \Gamma, \forall x : a. P \vdash G} \quad \forall_L \]

\[ \frac{A, l_e : a; \Gamma \vdash P[l_e/x]}{A; \Gamma \vdash \forall x : a. P} \quad \forall_R \]

\[ \frac{A, l_e : a; \Gamma, P[l_e/x] \vdash G}{A; \Gamma, \exists x : a. P \vdash G} \quad \exists_L \]

\[ \frac{A; \Gamma \vdash P[l/x]}{A; \Gamma \vdash \exists x : a. P} \quad \exists_R \]

\[ \frac{A; \forall(l_1 : a_1) F_1, \ldots, \forall(l_n : a_n) F_n \rightarrow G}{A; \forall(l_1 : a_1) F_1, \ldots, \forall(l_n : a_n) F_n \rightarrow \forall(l : a) G} \]

\[ \frac{\forall(l : a) \leq_A \forall(l_i : a_i)}{\forall(l : a) \leq_A \forall(l_i : a_i) \text{ means } l_i \in \uparrow l} \]
Theorem For any signature $\Sigma$, the proof system $\text{SELL}^n$ admits cut-elimination.

$\text{SELL}^n$ 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-determinism 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:

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

All these systems can be encoded in SELL\textsuperscript{®}. In fact, we show how to combine some of them.
Adding Subexponential Quantifiers

Intuitionistic SELL as a Framework for Concurrent Constraint Programming

- $!^sP$ is **located** at $s$ (epistemic and temporal);
- $!^s?^sP$ is **confined** to $s$ (spatial);
- $\cap l : a P \rightarrow P$ 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
Until now, \( \leq \) was quite simple. We can add more structure it to capture even more computational behaviors.
C-Semiring is a tuple \( \langle \mathcal{A}, +, \times, \perp, \top \rangle \)

- \( + \): commutative, associative, idempotent, \( \perp \)-unit, \( \top \)-absorbing

- \( \times \) is associative, commutative, distribute over \( + \), \( \top \)-unit, \( \perp \)-absorbing

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

- \( + \) and \( \times \) are monotone on \( \leq \), \( + \) is the lub operator.

If \( \times \) is idempotent, then

- \( \langle \mathcal{A}, \leq \rangle \) is a complete distribute lattice, \( \times \) is its glb.
C-Semiring is a tuple $\langle \mathcal{A}, +, \times, \perp_A, \top_A \rangle$.

Chooses the "best" valuation.

Combines constraints.
C-Semiring is a tuple \( \langle \mathbb{A}, +, \times, \bot_A, \top_A \rangle \)

Choses the "best" valuation.

- Crisp: \( S_c = \langle \{\text{true, false}\}, \lor, \land, \text{false, true} \rangle \)
- Fuzzy: \( S_F = \langle [0, 1], \max, \min, 0, 1 \rangle \) – Preferences
- Probabilistic: \( S_P = \langle [0, 1], \max, \times, 0, 1 \rangle \)
- Weighted: \( S_w = \langle \mathbb{R}^-, \max, +, -\infty, 0 \rangle \) – Costs

Combines constraints
Algebra for Subexponential Relations

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

Choses the "best" valuation.

Combines constraints

- **Crisp**: $S_c = \langle \{\text{true, false}\}, \lor, \land, \text{false, true} \rangle$
- **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:

<table>
<thead>
<tr>
<th>x</th>
<th>y</th>
<th>$x &lt; y$</th>
<th>$x &gt; 1$</th>
<th>$c_1 \otimes c_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>0.5</td>
<td>0.2</td>
<td>0.2</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>1.0</td>
<td>0.2</td>
<td>0.2</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>0.2</td>
<td>1.0</td>
<td>0.2</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0.5</td>
<td>1.0</td>
<td>0.5</td>
</tr>
</tbody>
</table>

$\sum v_i = 0.5$. Best solution=0.5
All the nice properties are preserved, *i.e.*, cut-elimination, focusing discipline, adequacy, etc.
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 $\preceq$**: 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