Proof nets for first-order additive linear logic

Willem Heijltjes
University of Bath

Dominic Hughes
UC Berkeley

Lutz Straßburger
Inria Saclay



Joint meeting CRECOGI / GDRI LL / Elica — Paris — October 8–11, 2018

Additive linear logic

Additive linear logic

Formulas

$$A \ ::= \ a \ \mid \ \bar{a} \ \mid \ A + A \ \mid \ A \times A$$

Additive linear logic

Formulas

$$A \;::=\; a \;\mid\; \bar{a} \;\mid\; A + A \;\mid\; A \times A$$

Sequents

$$\vdash A, B$$

Additive linear logic

Formulas

$$A \ ::= \ a \ \mid \ \overline{a} \ \mid \ A + A \ \mid \ A \times A$$

Sequents

$$\vdash A, B$$

Proofs

$$\frac{}{\vdash a, \overline{a}}\,\mathrm{ax} \qquad \frac{\vdash A, B_i}{\vdash A, B_1 + B_2}\,{+}\mathrm{R}, i \qquad \frac{\vdash A, B \quad \vdash A, C}{\vdash A, B \times C}\,{\times}\mathrm{R}$$

Features

Compact: Proof search on $\vdash A, B$ is $\mathcal{O}(|A| \times |B|)$ propositionally[1], and *NP-complete* for first-order[2]

[1] [Galmiche & Marion 1995] [2] [Heijltjes & Hughes 2015]

Features

Compact: Proof search on $\vdash A, B$ is $\mathcal{O}(|A| \times |B|)$ propositionally[1], and *NP-complete* for first-order[2]

Rich: Additives $+/\times$ (binary choice),
Duality $\overline{\overline{A}} = A$ (player/opponent),
meta-level linear implication/par $\vdash A, B$ (parallellism)

[1] [Galmiche & Marion 1995] [2] [Heijltjes & Hughes 2015]

Features

Compact: Proof search on $\vdash A, B$ is $\mathcal{O}(|A| \times |B|)$ propositionally[1], and *NP-complete* for first-order[2]

Rich: Additives $+/\times$ (binary choice),
Duality $\overline{\overline{A}} = A$ (player/opponent),
meta-level linear implication/par $\vdash A, B$ (parallellism)

Interesting: Two-player parallel games,
Communication along a two-way channel,
the Blass problem (sequential strategies don't compose associatively)[3]

[1][Galmiche & Marion 1995] [2][Heijltjes & Hughes 2015] [3][Abramsky 2003]

Features

Compact: Proof search on $\vdash A, B$ is $\mathcal{O}(|A| \times |B|)$ propositionally[1], and *NP-complete* for first-order[2]

Rich: Additives $+/\times$ (binary choice),
Duality $\overline{\overline{A}} = A$ (player/opponent),
meta-level linear implication/par $\vdash A, B$ (parallellism)

Interesting: Two-player parallel games,
Communication along a two-way channel,
the Blass problem (sequential strategies don't compose associatively)[3]

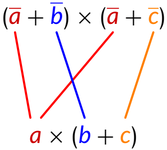
Well-behaved: Canonical proof nets[4], also with units[5],
Fixed-point formulae (mu-lattice hierarchy)[6]

[1][Galmiche & Marion 1995] [2][Heijltjes & Hughes 2015] [3][Abramsky 2003]
[4][Hughes & Van Glabbeek 2005] [5][Heijltjes 2011] [6][Santocanale 2002]

Proof nets and cut elimination

Proof nets and cut elimination

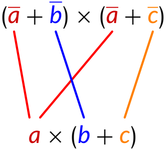
Proof net = sequent + linking



$$
\dfrac{
\dfrac{\dfrac{\dfrac{}{\vdash \overline{a}, a}\,\text{ax}}{\vdash \overline{a} + \overline{b}, a}\,{+}\text{R},1
\qquad
\dfrac{\dfrac{\dfrac{}{\vdash \overline{b}, b}\,\text{ax}}{\vdash \overline{b}, b + c}\,{+}\text{R},1}{\vdash \overline{a} + \overline{b}, b + c}\,{+}\text{R},2}
{\vdash \overline{a} + \overline{b}, a \times (b + c)}\,{\times}\text{R}
\qquad
\dfrac{\dfrac{\dfrac{}{\vdash \overline{a}, a}\,\text{ax}}{\vdash \overline{a} + \overline{c}, a}\,{+}\text{R},1
\qquad
\dfrac{\dfrac{\dfrac{}{\vdash \overline{c}, c}\,\text{ax}}{\vdash \overline{c}, b + c}\,{+}\text{R},2}{\vdash \overline{a} + \overline{c}, b + c}\,{+}\text{R},2}
{\vdash \overline{a} + \overline{c}, a \times (b + c)}\,{\times}\text{R}
}{\vdash (\overline{a} + \overline{b}) \times (\overline{a} + \overline{c}), a \times (b + c)}\,{\times}\text{R}
$$

Proof nets and cut elimination

Proof net = sequent + linking



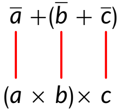
$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \bar{a}, a}\,\mathrm{ax}}{\vdash \bar{a} + \bar{b}, a}\,{+}\mathrm{R},1 \qquad \dfrac{\dfrac{\dfrac{}{\vdash \bar{b}, b}\,\mathrm{ax}}{\vdash \bar{b}, b + c}\,{+}\mathrm{R},1}{\vdash \bar{a} + \bar{b}, b + c}\,{+}\mathrm{R},2}{\vdash \bar{a} + \bar{b}, a \times (b + c)}\,{\times}\mathrm{R} \qquad \dfrac{\dfrac{\dfrac{}{\vdash \bar{a}, a}\,\mathrm{ax}}{\vdash \bar{a} + \bar{c}, a}\,{+}\mathrm{R},1 \qquad \dfrac{\dfrac{\dfrac{}{\vdash \bar{c}, c}\,\mathrm{ax}}{\vdash \bar{c}, b + c}\,{+}\mathrm{R},2}{\vdash \bar{a} + \bar{c}, b + c}\,{+}\mathrm{R},2}{\vdash \bar{a} + \bar{c}, a \times (b + c)}\,{\times}\mathrm{R}}{\vdash (\bar{a} + \bar{b}) \times (\bar{a} + \bar{c}), a \times (b + c)}\,{\times}\mathrm{R}$$

More examples:

diagonal

injection

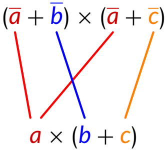
symmetry



associativity

Proof nets and cut elimination

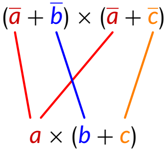
Proof net = sequent + linking



$$
\dfrac{
  \dfrac{
    \dfrac{\dfrac{}{\vdash \overline{a}, a}\,\text{ax}}{\vdash \overline{a} + \overline{b}, a}\,{+}\text{R,1}
    \qquad
    \dfrac{\dfrac{\dfrac{}{\vdash \overline{b}, b}\,\text{ax}}{\vdash \overline{b}, b + c}\,{+}\text{R,1}}{\vdash \overline{a} + \overline{b}, b + c}\,{+}\text{R,2}
  }{\vdash \overline{a} + \overline{b}, a \times (b + c)}\,{\times}\text{R}
  \qquad
  \dfrac{
    \dfrac{\dfrac{}{\vdash \overline{a}, a}\,\text{ax}}{\vdash \overline{a} + \overline{c}, a}\,{+}\text{R,1}
    \qquad
    \dfrac{\dfrac{\dfrac{}{\vdash \overline{c}, c}\,\text{ax}}{\vdash \overline{c}, b + c}\,{+}\text{R,2}}{\vdash \overline{a} + \overline{c}, b + c}\,{+}\text{R,2}
  }{\vdash \overline{a} + \overline{c}, a \times (b + c)}\,{\times}\text{R}
}{\vdash (\overline{a} + \overline{b}) \times (\overline{a} + \overline{c}), a \times (b + c)}\,{\times}\text{R}
$$

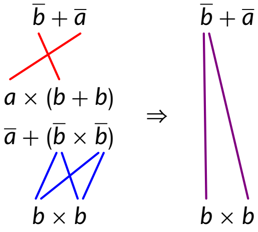
Proof nets and cut elimination

Proof net = sequent + linking



$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \bar{a}, a}\,\text{ax}}{\vdash \bar{a} + \bar{b}, a}\,{+}\text{R},1 \qquad \dfrac{\dfrac{\dfrac{}{\vdash \bar{b}, b}\,\text{ax}}{\vdash \bar{b}, b + c}\,{+}\text{R},1}{\vdash \bar{a} + \bar{b}, b + c}\,{+}\text{R},2}{\vdash \bar{a} + \bar{b}, a \times (b + c)}\,{\times}\text{R} \qquad \dfrac{\dfrac{\dfrac{}{\vdash \bar{a}, a}\,\text{ax}}{\vdash \bar{a} + \bar{c}, a}\,{+}\text{R},1 \qquad \dfrac{\dfrac{\dfrac{}{\vdash \bar{c}, c}\,\text{ax}}{\vdash \bar{c}, b + c}\,{+}\text{R},2}{\vdash \bar{a} + \bar{c}, b + c}\,{+}\text{R},2}{\vdash \bar{a} + \bar{c}, a \times (b + c)}\,{\times}\text{R}}{\vdash (\bar{a} + \bar{b}) \times (\bar{a} + \bar{c}), a \times (b + c)}\,{\times}\text{R}$$

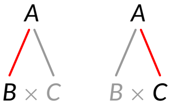
Cut elimination = relational composition



Correctness

Correctness

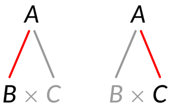
Slicing:



[Hughes & Van Glabbeek 2003]

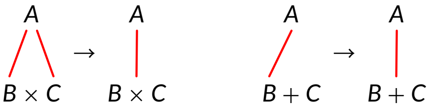
Correctness

Slicing:



[Hughes & Van Glabbeek 2003]

Coalescence:



[Heijltjes & Hughes 2015]

additive linear logic

Formulas

$$A \ ::= \ a \ \mid \ \overline{a} \ \mid \ A + A \ \mid \ A \times A$$

Sequents

$$\vdash A, B$$

Proofs

$$\dfrac{}{\vdash a, \overline{a}}\ \mathrm{ax} \qquad \dfrac{\vdash A, B_i}{\vdash A, B_1 + B_2}\ {+}\mathrm{R},i \qquad \dfrac{\vdash A, B \quad \vdash A, C}{\vdash A, B \times C}\ {\times}\mathrm{R}$$

First-order additive linear logic

Formulas

$$A \ ::= \ a \ | \ \overline{a} \ | \ A + A \ | \ A \times A \ | \ \exists x.A \ | \ \forall x.A$$

$$a \ ::= \ P(t_1, \ldots, t_n)$$

$$t \ ::= \ f(t_1, \ldots, t_n) \ | \ x$$

Sequents

$$\vdash A, B$$

Proofs

$$\frac{}{\vdash a, \overline{a}}\,\text{ax} \qquad \frac{\vdash A, B_i}{\vdash A, B_1 + B_2}\,{+}\text{R},i \qquad \frac{\vdash A, B \quad \vdash A, C}{\vdash A, B \times C}\,{\times}\text{R}$$

$$\frac{\vdash A, B[t/x]}{\vdash A, \exists x.B}\,\exists\text{R},t \qquad \frac{\vdash A, B}{\vdash A, \forall x.B}\,\forall\text{R}\ (x \notin \text{FV}(A))$$

What is first-order quantification in proofs?

What is first-order quantification in proofs?

Commonly: *expansion + substitution*[1]

$$\exists x.A \quad \Rightarrow \quad A[t_1/x] + \ldots + A[t_n/x]$$

[1] For classical logic: [Herbrand 1930, Miller 1987, Heijltjes 2010]

What is first-order quantification in proofs?

Commonly: *expansion + substitution*[1]

$$\exists x.A \quad \Rightarrow \quad A[t_1/x] + \ldots + A[t_n/x]$$

$$\dfrac{\dfrac{\dfrac{}{\vdash \overline{P}(s), P(s)}}{\vdash \exists x.\overline{P}(x), P(s)}\ \exists\mathrm{R}, s \qquad \dfrac{\dfrac{}{\vdash \overline{P}(t), P(t)}}{\vdash \exists x.\overline{P}(x), P(t)}\ \exists\mathrm{R}, t}{\vdash \exists x.\overline{P}(x), P(s) \times P(t)}\ \times\mathrm{R}$$

[1]For classical logic: [Herbrand 1930, Miller 1987, Heijltjes 2010]

What is first-order quantification in proofs?

Commonly: *expansion + substitution*[1]

$$\exists x.A \quad \Rightarrow \quad A[t_1/x] + \ldots + A[t_n/x]$$

$$\dfrac{\dfrac{\dfrac{}{\vdash \overline{P}(s), P(s)}}{\vdash \exists x.\overline{P}(x), P(s)}\ \exists\mathrm{R},s \qquad \dfrac{\dfrac{}{\vdash \overline{P}(t), P(t)}}{\vdash \exists x.\overline{P}(x), P(t)}\ \exists\mathrm{R},t}{\vdash \exists x.\overline{P}(x), P(s) \times P(t)}\ \times\mathrm{R}$$

Problem: Incompatible with *sequent + linking* and *relational composition*

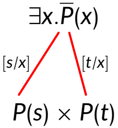
Both *expansion* and *substitution* destroy the original formula

[1]For classical logic: [Herbrand 1930, Miller 1987, Heijltjes 2010]

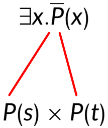
Two solutions

$$\dfrac{\dfrac{\dfrac{}{\vdash \overline{P}(s), P(s)}}{\vdash \exists x.\overline{P}(x), P(s)}\ {\scriptstyle \exists\mathrm{R},s} \qquad \dfrac{\dfrac{}{\vdash \overline{P}(t), P(t)}}{\vdash \exists x.\overline{P}(x), P(t)}\ {\scriptstyle \exists\mathrm{R},t}}{\vdash \exists x.\overline{P}(x), P(s) \times P(t)}\ {\scriptstyle \times\mathrm{R}}$$

Witness nets: explicit substitution



Unification nets: first-order unification[1]



[1]For MLL: [Hughes 2018]

Proof identity

If *any* witness will do, is the choice significant?

$$\dfrac{\dfrac{}{\vdash P(s), \overline{P}(s)}}{\vdash \exists x.P(x), \exists y.\overline{P}(y)} \quad \stackrel{?}{\equiv} \quad \dfrac{\dfrac{}{\vdash P(t), \overline{P}(t)}}{\vdash \exists x.P(x), \exists y.\overline{P}(y)}$$

Proof identity

If *any* witness will do, is the choice significant?

$$\dfrac{\dfrac{}{\vdash P(s), \overline{P}(s)}}{\vdash \exists x.P(x), \exists y.\overline{P}(y)} \quad \stackrel{?}{\equiv} \quad \dfrac{\dfrac{}{\vdash P(t), \overline{P}(t)}}{\vdash \exists x.P(x), \exists y.\overline{P}(y)}$$

What if the quantifier is *vacuous*?

$$\dfrac{\dfrac{}{\vdash P, \overline{P}}}{\vdash \exists x.P, \overline{P}}\,\exists\mathrm{R},s \quad \stackrel{?}{\equiv} \quad \dfrac{\dfrac{}{\vdash P, \overline{P}}}{\vdash \exists x.P, \overline{P}}\,\exists\mathrm{R},t$$

Proof identity

If *any* witness will do, is the choice significant?

$$\dfrac{\dfrac{}{\vdash P(s), \overline{P}(s)}}{\vdash \exists x.P(x), \exists y.\overline{P}(y)} \quad \stackrel{?}{\equiv} \quad \dfrac{\dfrac{}{\vdash P(t), \overline{P}(t)}}{\vdash \exists x.P(x), \exists y.\overline{P}(y)}$$

What if the quantifier is *vacuous*?

$$\dfrac{\dfrac{}{\vdash P, \overline{P}}}{\vdash \exists x.P, \overline{P}}\,\exists\mathrm{R},s \quad \stackrel{?}{\equiv} \quad \dfrac{\dfrac{}{\vdash P, \overline{P}}}{\vdash \exists x.P, \overline{P}}\,\exists\mathrm{R},t$$

What if a quantified variable occurs only in a *weakened* formula?

$$\dfrac{\dfrac{\dfrac{}{\vdash P, \overline{P}}}{\vdash P{+}Q(s), \overline{P}}\,{+}\mathrm{R},1}{\vdash \exists x.P{+}Q(x), \overline{P}}\,\exists\mathrm{R},s \quad \stackrel{?}{\equiv} \quad \dfrac{\dfrac{\dfrac{}{\vdash P, \overline{P}}}{\vdash P{+}Q(t), \overline{P}}\,{+}\mathrm{R},1}{\vdash \exists x.P{+}Q(x), \overline{P}}\,\exists\mathrm{R},t$$

Generality

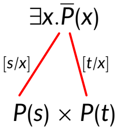
Witness nets: make *none* of these identifications (like sequent calculus)

Unification nets: make *all* of these identifications

Witness nets and Unification nets

Witness nets and Unification nets

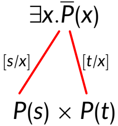
Witness net = sequent + linking with substitution



$$\dfrac{\dfrac{\dfrac{}{\vdash \overline{P}(s), P(s)}}{\vdash \exists x.\overline{P}(x), P(s)}\,{\scriptstyle \exists\mathrm{R}, s} \qquad \dfrac{\dfrac{}{\vdash \overline{P}(t), P(t)}}{\vdash \exists x.\overline{P}(x), P(t)}\,{\scriptstyle \exists\mathrm{R}, t}}{\vdash \exists x.\overline{P}(x), P(s) \times P(t)}\,{\scriptstyle \times\mathrm{R}}$$

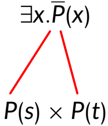
Witness nets and Unification nets

Witness net = sequent + linking with substitution



$$\dfrac{\dfrac{\overline{\vdash \overline{P}(s), P(s)}}{\vdash \exists x.\overline{P}(x), P(s)}\,\exists\mathrm{R},s \qquad \dfrac{\overline{\vdash \overline{P}(t), P(t)}}{\vdash \exists x.\overline{P}(x), P(t)}\,\exists\mathrm{R},t}{\vdash \exists x.\overline{P}(x), P(s) \times P(t)}\,\times\mathrm{R}$$

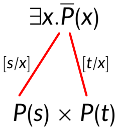
Unification net = sequent + linking



$$\dfrac{\dfrac{\overline{\vdash \overline{P}(s), P(s)}}{\vdash \exists x.\overline{P}(x), P(s)}\,\exists\mathrm{R},s \qquad \dfrac{\overline{\vdash \overline{P}(t), P(t)}}{\vdash \exists x.\overline{P}(x), P(t)}\,\exists\mathrm{R},t}{\vdash \exists x.\overline{P}(x), P(s) \times P(t)}\,\times\mathrm{R}$$

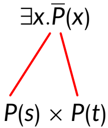
Witness nets and Unification nets

Witness net = sequent + linking with substitution



$$\dfrac{\dfrac{\dfrac{}{\vdash \overline{P}(s), P(s)}}{\vdash \exists x.\overline{P}(x), P(s)}\,\exists\mathrm{R},s \qquad \dfrac{\dfrac{}{\vdash \overline{P}(t), P(t)}}{\vdash \exists x.\overline{P}(x), P(t)}\,\exists\mathrm{R},t}{\vdash \exists x.\overline{P}(x), P(s) \times P(t)}\,\times\mathrm{R}$$

Unification net = sequent + linking

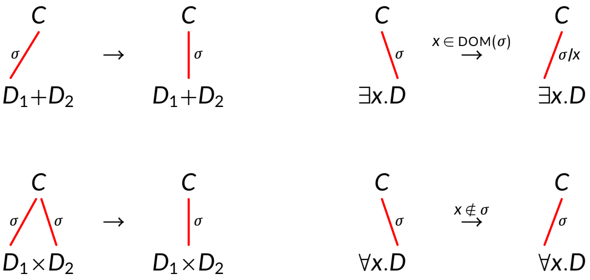


$$\dfrac{\dfrac{\dfrac{}{\vdash \overline{P}(s), P(s)}}{\vdash \exists x.\overline{P}(x), P(s)}\,\exists\mathrm{R},s \qquad \dfrac{\dfrac{}{\vdash \overline{P}(t), P(t)}}{\vdash \exists x.\overline{P}(x), P(t)}\,\exists\mathrm{R},t}{\vdash \exists x.\overline{P}(x), P(s) \times P(t)}\,\times\mathrm{R}$$

(such that "sequent + linking with mgu" forms a witness net)

Coalescence for witness nets

Coalescence for witness nets (rewrite rules)



Coalescence for witness nets (example)

$$\forall x.\ \exists y.\ \overline{P}(x,y)$$

$$[x/z, s/y] \qquad\qquad [x/z, t/y]$$

$$\exists z.\ P(z,s) \times P(z,t)$$

Coalescence for witness nets (example)

$$\forall x.\ \exists y.\ \overline{P}(x,y)$$

$[x/z,s/y]$ $[x/z,t/y]$

$$\exists z.\ P(z,s) \times P(z,t)$$

$$\dfrac{}{\vdash \overline{P}(x,s),\, P(x,s)} \qquad \dfrac{}{\vdash \overline{P}(x,t),\, P(x,t)}$$

Coalescence for witness nets (example)

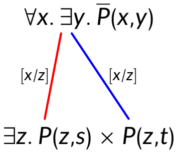
$$\forall x.\ \exists y.\ \overline{P}(x,y)$$

$[x/z]$ $\quad$ $[x/z, t/y]$

$$\exists z.\ P(z,s) \times P(z,t)$$

$$\dfrac{\dfrac{}{\vdash \overline{P}(x,s),\ P(x,s)}}{\vdash \exists y. \overline{P}(x,y),\ P(x,s)}\ \exists\mathrm{R}, s \qquad\qquad \dfrac{}{\vdash \overline{P}(x,t),\ P(x,t)}$$

Coalescence for witness nets (example)



$$\dfrac{\dfrac{}{\vdash \overline{P}(x,s),\, P(x,s)}}{\vdash \exists y.\overline{P}(x,y),\, P(x,s)}\;\exists\mathrm{R},s \qquad \dfrac{\dfrac{}{\vdash \overline{P}(x,t),\, P(x,t)}}{\vdash \exists y.\overline{P}(x,y),\, P(x,t)}\;\exists\mathrm{R},t$$

Coalescence for witness nets (example)

$$\begin{tikzcd} \forall x.\, \exists y.\, \overline{P}(x,y) \arrow[d, dash, "{[x/z]}"] \\ \exists z.\, P(z,s) \times P(z,t) \end{tikzcd}$$

$$\dfrac{\dfrac{\dfrac{}{\vdash \overline{P}(x,s),\, P(x,s)}}{\vdash \exists y.\overline{P}(x,y),\, P(x,s)}{\scriptstyle \exists\mathrm{R},s} \qquad \dfrac{\dfrac{}{\vdash \overline{P}(x,t),\, P(x,t)}}{\vdash \exists y.\overline{P}(x,y),\, P(x,t)}{\scriptstyle \exists\mathrm{R},t}}{\vdash \exists y.\overline{P}(x,y),\, P(x,s) \times P(x,t)}{\scriptstyle \times\mathrm{R}}$$

Coalescence for witness nets (example)

$$\forall x.\ \exists y.\ \overline{P}(x,y)$$

$$\exists z.\ P(z,s) \times P(z,t)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \overline{P}(x,s),\, P(x,s)}}{\vdash \exists y.\overline{P}(x,y),\, P(x,s)}\;\exists\mathrm{R},s \qquad \dfrac{\dfrac{}{\vdash \overline{P}(x,t),\, P(x,t)}}{\vdash \exists y.\overline{P}(x,y),\, P(x,t)}\;\exists\mathrm{R},t}{\vdash \exists y.\overline{P}(x,y),\, P(x,s) \times P(x,t)}\;\times\mathrm{R}}{\vdash \exists y.\overline{P}(x,y),\, \exists z.P(z,s) \times P(z,t)}\;\exists\mathrm{R},x$$

Coalescence for witness nets (example)

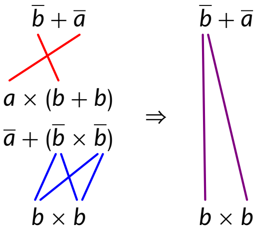
$$\forall x.\ \exists y.\ \overline{P}(x,y)$$

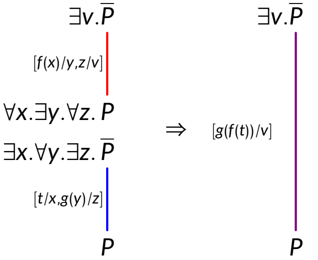
$$\exists z.\ P(z,s) \times P(z,t)$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\vdash \overline{P}(x,s), P(x,s)}}{\vdash \exists y.\overline{P}(x,y), P(x,s)}\ {\scriptstyle \exists R, s} \qquad \dfrac{\dfrac{}{\vdash \overline{P}(x,t), P(x,t)}}{\vdash \exists y.\overline{P}(x,y), P(x,t)}\ {\scriptstyle \exists R, t}}{\vdash \exists y.\overline{P}(x,y), P(x,s) \times P(x,t)}\ {\scriptstyle \times R}}{\vdash \exists y.\overline{P}(x,y), \exists z.P(z,s) \times P(z,t)}\ {\scriptstyle \exists R, x}}{\vdash \forall x.\exists y.\overline{P}(x,y), \exists z.P(z,s) \times P(z,t)}\ {\scriptstyle \forall R}$$

Composition / cut elimination

relational composition $+$ composition of substitution





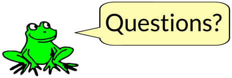
Summary

	Monomial nets[1]	Witness nets[2]	Unification nets[2]
Canonicity	?	✓	✓
Generality	✗	✗	✓
Direct composition	✗	✓	✓
Coalescence	?	✓	✓
Slicing	✓	✓	?

[1] [Girard 1987, 1996] [2] [Inria RR-9201]

Summary

	Monomial nets[1]	Witness nets[2]	Unification nets[2]
Canonicity	?	✓	✓
Generality	✗	✗	✓
Direct composition	✗	✓	✓
Coalescence	?	✓	✓
Slicing	✓	✓	?



[1][Girard 1987, 1996]   [2][Inria RR-9201]