Stratifications and complexity in linear logic

Daniel Murfet

Curry-Howard correspondence

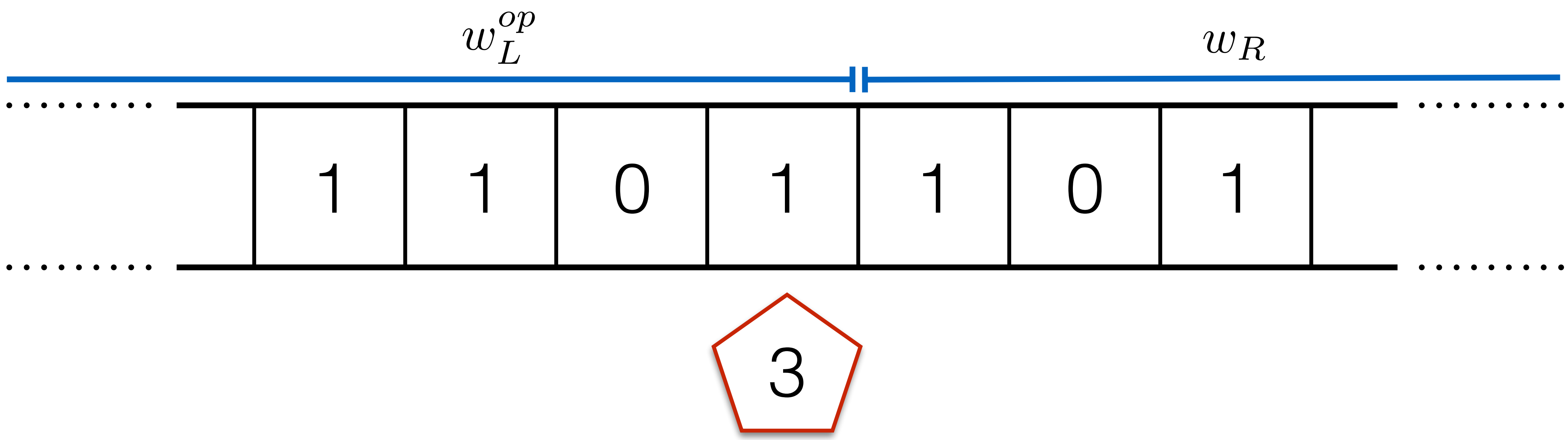
logic	programming	categories
formula	type	objects
sequent	input/output spec	—
proof	program	morphisms
cut-elimination	execution	—
contraction	copying	coproducts
stratification	complexity	**?**

this talk

Outline

1. Turing machines
2. Sequent calculus of linear logic
3. Programs (Turing machines) as proofs
4. **Stratification vs. complexity**

Turing machines

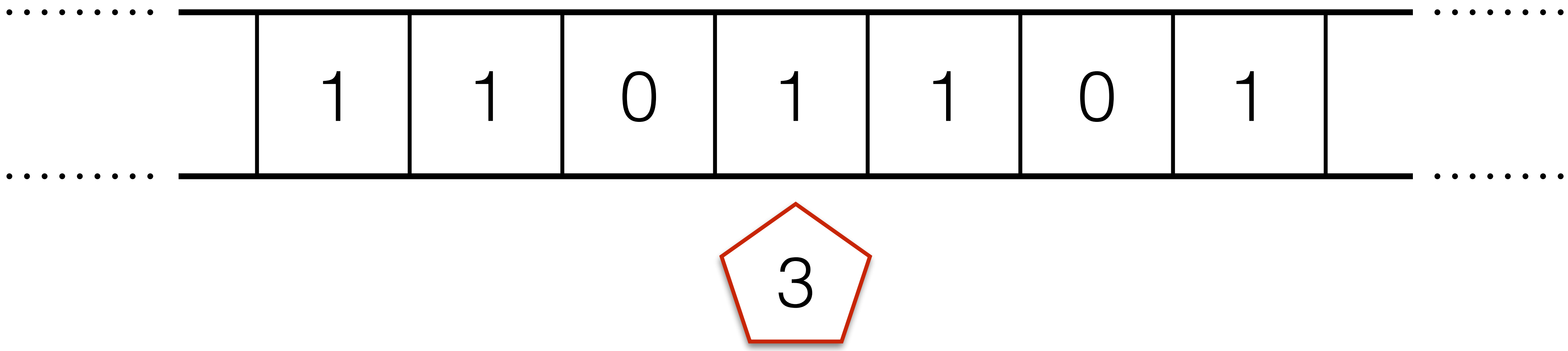


A configuration is $(w_L, w_R, a) \in \{0,1\}^* \times \{0,1\}^* \times \{1, \ldots, q\}$

binary integer	binary integer	q-boolean

Shown configuration: $(1011\cdots, 101\cdots, 3)$

Turing machines



A Turing machine T is a function

$$\delta_T : \{0,1\} \times \{1,\ldots,q\} \longrightarrow \{0,1\} \times \{1,\ldots,q\} \times \{L,R\}$$

read symbol | current state | write | new state | move to

$$\{0,1\}^* \times \{0,1\}^* \times \{1,\ldots,q\} \longrightarrow \{0,1\}^* \times \{0,1\}^* \times \{1,\ldots,q\}$$

Linear logic

- Discovered by Girard in the 1980s, linear logic is a substructural logic with contraction and weakening available only for formulas marked with an "exponential" connective, written "**!**".

- The usual connectives of logic (e.g. conjunction, implication) are decomposed into **!** together with a *linearised* version of that connective (called resp. tensor, linear implication).

- Under Curry-Howard, linear logic corresponds to a programming language with "resource management" and symmetric monoidal categories equipped with a special kind of comonad.

- We will use second-order intuitionistic linear logic with additives (as expressive as polymorphic lambda calculus).

Linear logic

variables: $\alpha, \beta, \gamma, \ldots$

formulas: $!F, F \otimes F', F \multimap F', F \& F', \forall \alpha F$, constants

$$\mathbf{int} = \forall \alpha \ !(\alpha \multimap \alpha) \multimap (\alpha \multimap \alpha)$$

$$\mathbf{bint} = \forall \alpha \ !(\alpha \multimap \alpha) \multimap \big(!(\alpha \multimap \alpha) \multimap (\alpha \multimap \alpha)\big)$$

Deduction rules for linear logic

(Axiom): $$\frac{}{A \vdash A}$$

(Cut): $$\frac{\Gamma \vdash A \quad \Delta', A, \Delta \vdash B}{\Delta', \Gamma, \Delta \vdash B}\,\text{cut}$$

(Exchange): $$\frac{\Gamma, A, B, \Delta \vdash C}{\Gamma, B, A, \Delta \vdash C}$$

(Left $\otimes$): $$\frac{\Gamma, A, B, \Delta \vdash C}{\Gamma, A \otimes B, \Delta \vdash C}\,\otimes\text{-}L$$

(Right $\otimes$): $$\frac{\Gamma \vdash A \quad \Delta \vdash B}{\Gamma, \Delta \vdash A \otimes B}\,\otimes\text{-}R$$

(Right $\multimap$): $$\frac{A, \Gamma \vdash B}{\Gamma \vdash A \multimap B}\,\multimap R$$

(Left $\multimap$): $$\frac{\Gamma \vdash A \quad \Delta', B, \Delta \vdash C}{\Delta', \Gamma, A \multimap B, \Delta \vdash C}\,\multimap L$$

(Promotion): $$\frac{!\Gamma \vdash A}{!\Gamma \vdash !A}\,\text{prom}$$

(Dereliction): $$\frac{\Gamma, A, \Delta \vdash B}{\Gamma, !A, \Delta \vdash B}\,\text{der}$$

(Weakening): $$\frac{\Gamma, \Delta \vdash B}{\Gamma, !A, \Delta \vdash B}\,\text{weak}$$

(Contraction): $$\frac{\Gamma, !A, !A, \Delta \vdash B}{\Gamma, !A, \Delta \vdash B}\,\text{ctr}$$

$$\frac{\Gamma, A[B/x] \vdash C}{\Gamma, \forall x \,.\, A \vdash C}\,\forall L$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x \,.\, A}\,\forall R$$

a sequent is $\Gamma \vdash A$ for a sequence of formulae Γ, where $\vdash$ is the “turnstile”

Binary integers

$$\mathbf{bint} = \forall\alpha\ !(\alpha \multimap \alpha) \multimap (!(\alpha \multimap \alpha) \multimap (\alpha \multimap \alpha))$$

$$S \in \{0,1\}^* \longmapsto \text{proof } t_S \text{ of } \vdash \mathbf{bint}$$

$$\dfrac{\dfrac{}{\alpha \vdash \alpha} \quad \dfrac{}{\alpha \vdash \alpha}}{\alpha, \alpha \multimap \alpha \vdash \alpha}\ \multimap L$$

$$\dfrac{\dfrac{}{\alpha \vdash \alpha} \quad \alpha, \alpha \multimap \alpha \vdash \alpha}{\alpha, \alpha \multimap \alpha, \alpha \multimap \alpha \vdash \alpha}\ \multimap L$$

$$\dfrac{\dfrac{}{\alpha \vdash \alpha} \quad \alpha, \alpha \multimap \alpha, \alpha \multimap \alpha \vdash \alpha}{\alpha, \alpha \multimap \alpha, \alpha \multimap \alpha, \alpha \multimap \alpha \vdash \alpha}\ \multimap L$$

$$\dfrac{\alpha, \alpha \multimap \alpha, \alpha \multimap \alpha, \alpha \multimap \alpha \vdash \alpha}{\alpha \multimap \alpha, \alpha \multimap \alpha, \alpha \multimap \alpha \vdash \alpha \multimap \alpha}\ \multimap R$$

$$\dfrac{\alpha \multimap \alpha, \alpha \multimap \alpha, \alpha \multimap \alpha \vdash \alpha \multimap \alpha}{!(\alpha \multimap \alpha), !(\alpha \multimap \alpha), !(\alpha \multimap \alpha) \vdash \alpha \multimap \alpha}\ \text{der}$$

$$\dfrac{!(\alpha \multimap \alpha), !(\alpha \multimap \alpha), !(\alpha \multimap \alpha) \vdash \alpha \multimap \alpha}{!(\alpha \multimap \alpha), !(\alpha \multimap \alpha) \vdash \alpha \multimap \alpha}\ \text{ctr}$$

$$\dfrac{!(\alpha \multimap \alpha), !(\alpha \multimap \alpha) \vdash \alpha \multimap \alpha}{!(\alpha \multimap \alpha) \vdash !(\alpha \multimap \alpha) \multimap (\alpha \multimap \alpha)}\ \multimap R$$

$$\dfrac{!(\alpha \multimap \alpha) \vdash !(\alpha \multimap \alpha) \multimap (\alpha \multimap \alpha)}{\vdash !(\alpha \multimap \alpha) \multimap (!(\alpha \multimap \alpha) \multimap (\alpha \multimap \alpha))}\ \multimap R$$

t_{001}

Aside on linear logic

$$\pi$$

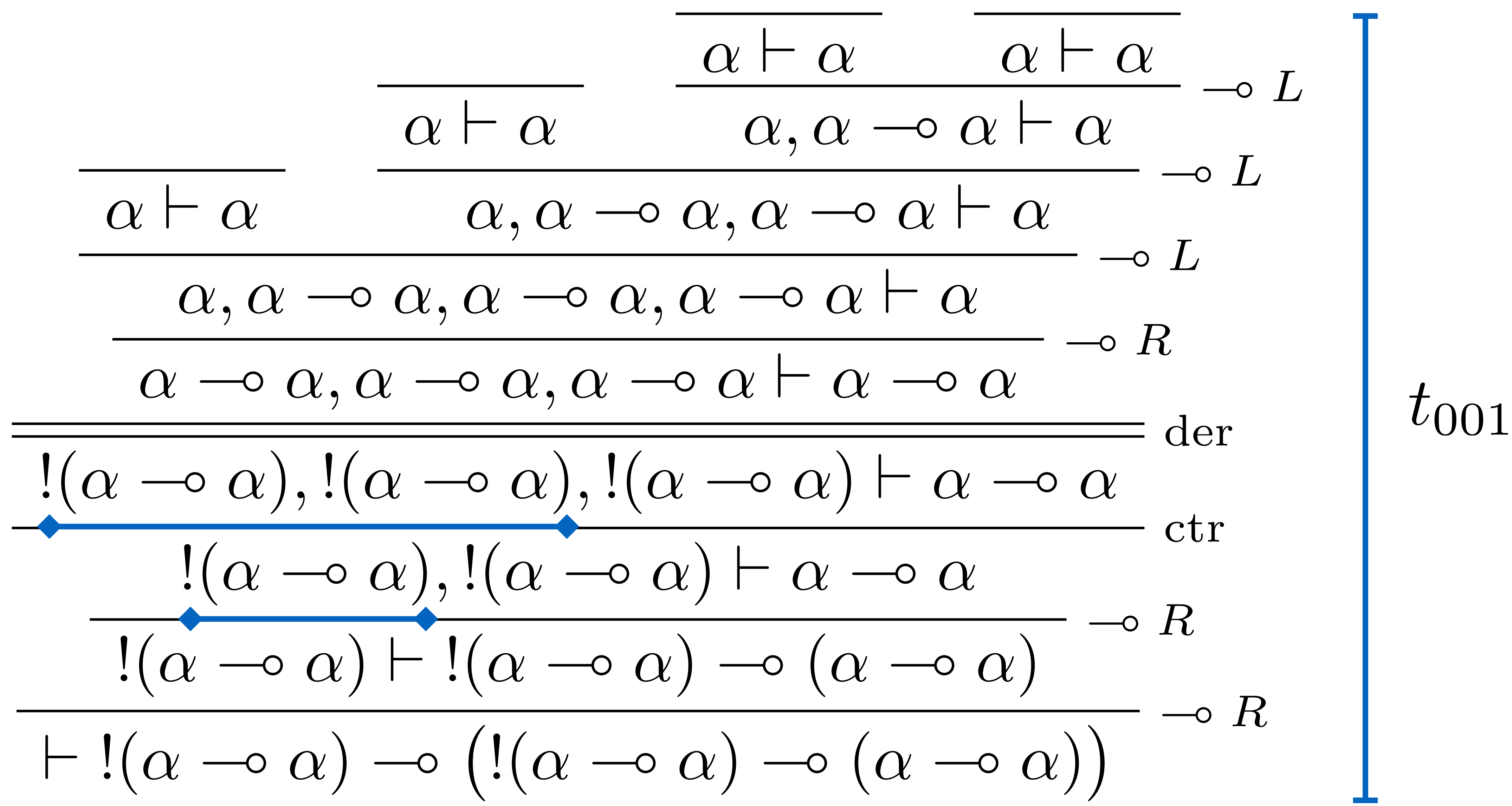
$$\vdots$$

$$!A, B \vdash C$$

Binary integers

$$\mathbf{bint} = \forall\alpha\ !(\alpha \multimap \alpha) \multimap (!(\alpha \multimap \alpha) \multimap (\alpha \multimap \alpha))$$

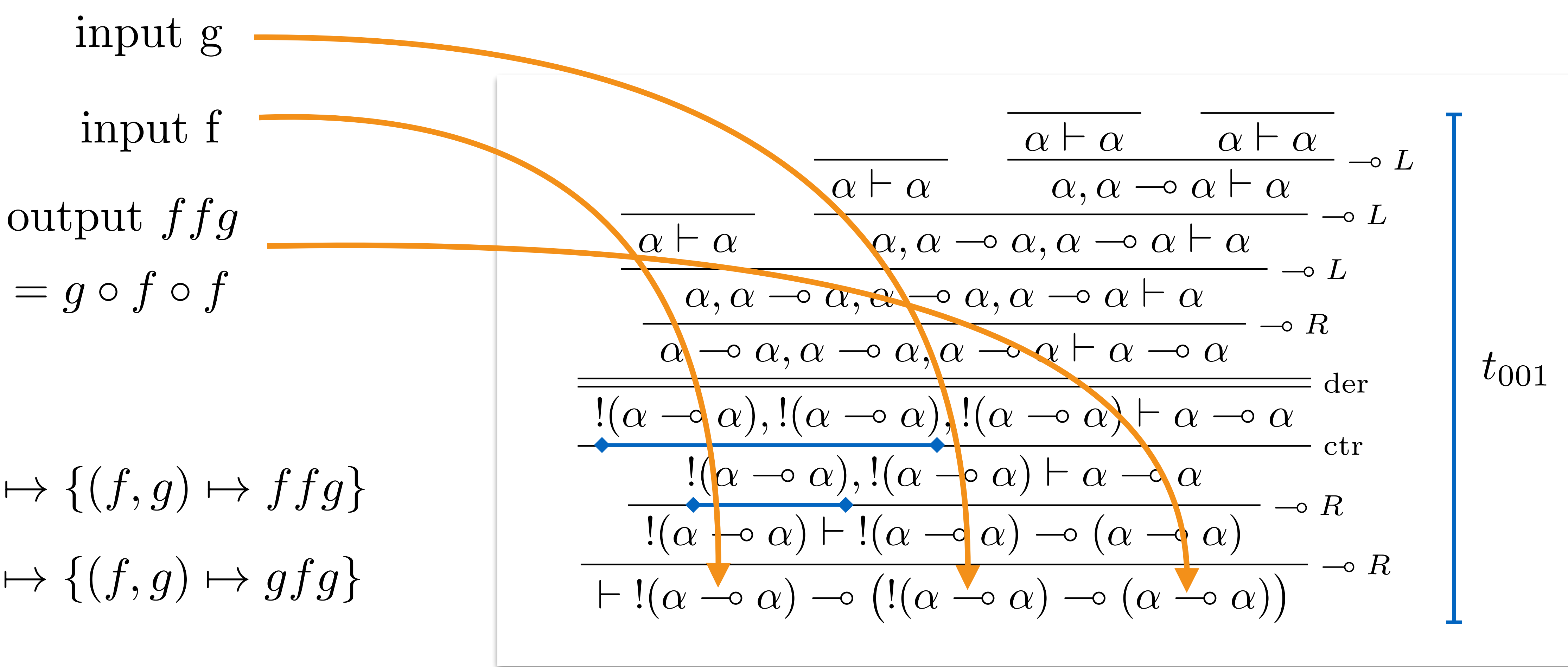
$$S \in \{0,1\}^* \longmapsto \text{proof } t_S \text{ of } \vdash \mathbf{bint}$$



Binary integers

$$\mathbf{bint} = \forall \alpha \; !(\alpha \multimap \alpha) \multimap (!(\alpha \multimap \alpha) \multimap (\alpha \multimap \alpha))$$

$$S \in \{0,1\}^* \longmapsto \text{proof } t_S \text{ of } \vdash \mathbf{bint}$$



$001 \mapsto \{(f,g) \mapsto ffg\}$

$101 \mapsto \{(f,g) \mapsto gfg\}$

Stratified Linear logic

variables: $\alpha, \beta, \gamma, \dots$

formulas: $!F, \S F, F \otimes F, F \multimap F, F \& F, \forall \alpha F,$ constants

$$\mathbf{bint}^{\S} = \forall \alpha \; !(\alpha \multimap \alpha) \multimap \big(!(\alpha \multimap \alpha) \multimap \S(\alpha \multimap \alpha)\big)$$

$$\mathbf{int}^{\S} = \forall \alpha \; !(\alpha \multimap \alpha) \multimap \S(\alpha \multimap \alpha)$$

Deduction rules for stratified linear logic

same rules as before… e.g.

$$\text{(Axiom)}: \quad \frac{}{\underset{i}{A} \vdash \underset{i}{A}}$$

$$\text{(Cut)}: \quad \frac{\Gamma \vdash \overset{i}{A} \qquad \Delta', \overset{i}{A}, \Delta \vdash B}{\Delta', \Gamma, \Delta \vdash B}\ \text{cut}$$

$$\text{(Right} \multimap\text{)}: \quad \frac{\overset{i}{A}, \Gamma \vdash \overset{i}{B}}{\Gamma \vdash A \underset{i}{\multimap} B}\ {\multimap}\, R$$

$$\text{(Left} \multimap\text{)}: \quad \frac{\Gamma \vdash \overset{i}{A} \qquad \Delta', \overset{i}{B}, \Delta \vdash C}{\Delta', \Gamma, A \underset{i}{\multimap} B, \Delta \vdash C}\ {\multimap}\, L$$

$$\text{(Promotion)}: \quad \frac{!\Gamma \vdash \overset{i+1}{A}}{!\Gamma \vdash \underset{i}{!A}}\ \text{prom} \qquad |\Gamma| = 1$$

$$\text{(Dereliction)}: \quad \frac{\Gamma, \overset{i+1}{A}, \Delta \vdash B}{\Gamma, \underset{i}{!A}, \Delta \vdash B}\ \text{der}$$

$$\text{(Weakening)}: \quad \frac{\Gamma, \Delta \vdash B}{\Gamma, \underset{i}{!A}, \Delta \vdash B}\ \text{weak}$$

$$\text{(Contraction)}: \quad \frac{\Gamma, \overset{i}{!A}, \overset{i}{!A}, \Delta \vdash B}{\Gamma, \underset{i}{!A}, \Delta \vdash B}\ \text{ctr}$$

plus

$$\frac{\Gamma, \overset{i+1}{A} \vdash B}{\Gamma, \underset{i}{\S A} \vdash B} \qquad \frac{\Gamma, A \vdash \overset{i+1}{B}}{\Gamma, A \vdash \underset{i}{\S B}}$$

A proof in the stratified sequent calculus is a proof in the usual sense, together with a *stratification,* which is an assignment of integers to all occurrences of formulas, such that conclusions are assigned 0 and the assignment changes across deduction rules are as shown in blue.

Binary integers

$$\mathbf{bint} = \forall\alpha\ !(\alpha \multimap \alpha) \multimap \big(!(\alpha \multimap \alpha) \multimap (\alpha \multimap \alpha)\big)$$

$$S \in \{0,1\}^* \longmapsto \text{proof } t_S \text{ of } \vdash \mathbf{bint}$$

$$\dfrac{}{\alpha \vdash \alpha} \qquad \dfrac{}{\alpha \vdash \alpha} \qquad \dfrac{\dfrac{}{\alpha \vdash \alpha} \quad \dfrac{}{\alpha \vdash \alpha}}{\alpha, \alpha \multimap \alpha \vdash \alpha} \multimap L$$

$$\dfrac{\alpha \vdash \alpha \qquad \alpha, \alpha \multimap \alpha \vdash \alpha}{\alpha, \alpha \multimap \alpha, \alpha \multimap \alpha \vdash \alpha} \multimap L$$

$$\dfrac{\alpha \vdash \alpha \qquad \alpha, \alpha \multimap \alpha, \alpha \multimap \alpha \vdash \alpha}{\alpha, \alpha \multimap \alpha, \alpha \multimap \alpha, \alpha \multimap \alpha \vdash \alpha} \multimap L$$

$$\dfrac{\alpha, \alpha \multimap \alpha, \alpha \multimap \alpha, \alpha \multimap \alpha \vdash \alpha}{\alpha \multimap \alpha, \alpha \multimap \alpha, \alpha \multimap \alpha \vdash \alpha \multimap \alpha} \multimap R$$

$$\dfrac{\alpha \multimap \alpha, \alpha \multimap \alpha, \alpha \multimap \alpha \vdash \alpha \multimap \alpha}{!(\alpha \multimap \alpha), !(\alpha \multimap \alpha), !(\alpha \multimap \alpha) \vdash \alpha \multimap \alpha} \text{der}$$

$$\dfrac{!(\alpha \multimap \alpha), !(\alpha \multimap \alpha), !(\alpha \multimap \alpha) \vdash \alpha \multimap \alpha}{!(\alpha \multimap \alpha), !(\alpha \multimap \alpha) \vdash \alpha \multimap \alpha} \text{ctr}$$

$$\dfrac{!(\alpha \multimap \alpha), !(\alpha \multimap \alpha) \vdash \alpha \multimap \alpha}{!(\alpha \multimap \alpha) \vdash !(\alpha \multimap \alpha) \multimap (\alpha \multimap \alpha)} \multimap R$$

$$\dfrac{!(\alpha \multimap \alpha) \vdash !(\alpha \multimap \alpha) \multimap (\alpha \multimap \alpha)}{\vdash !(\alpha \multimap \alpha) \multimap \big(!(\alpha \multimap \alpha) \multimap (\alpha \multimap \alpha)\big)} \multimap R$$

t_{001}

Binary integers (stratified)

$$\mathbf{bint}^{\S} = \forall\alpha\ !(\alpha \multimap \alpha) \multimap (!(\alpha \multimap \alpha) \multimap \S(\alpha \multimap \alpha))$$

$$S \in \{0,1\}^* \longmapsto \text{proof } t^{\S}_{S} \text{ of } \vdash \mathbf{bint}^{\S}$$

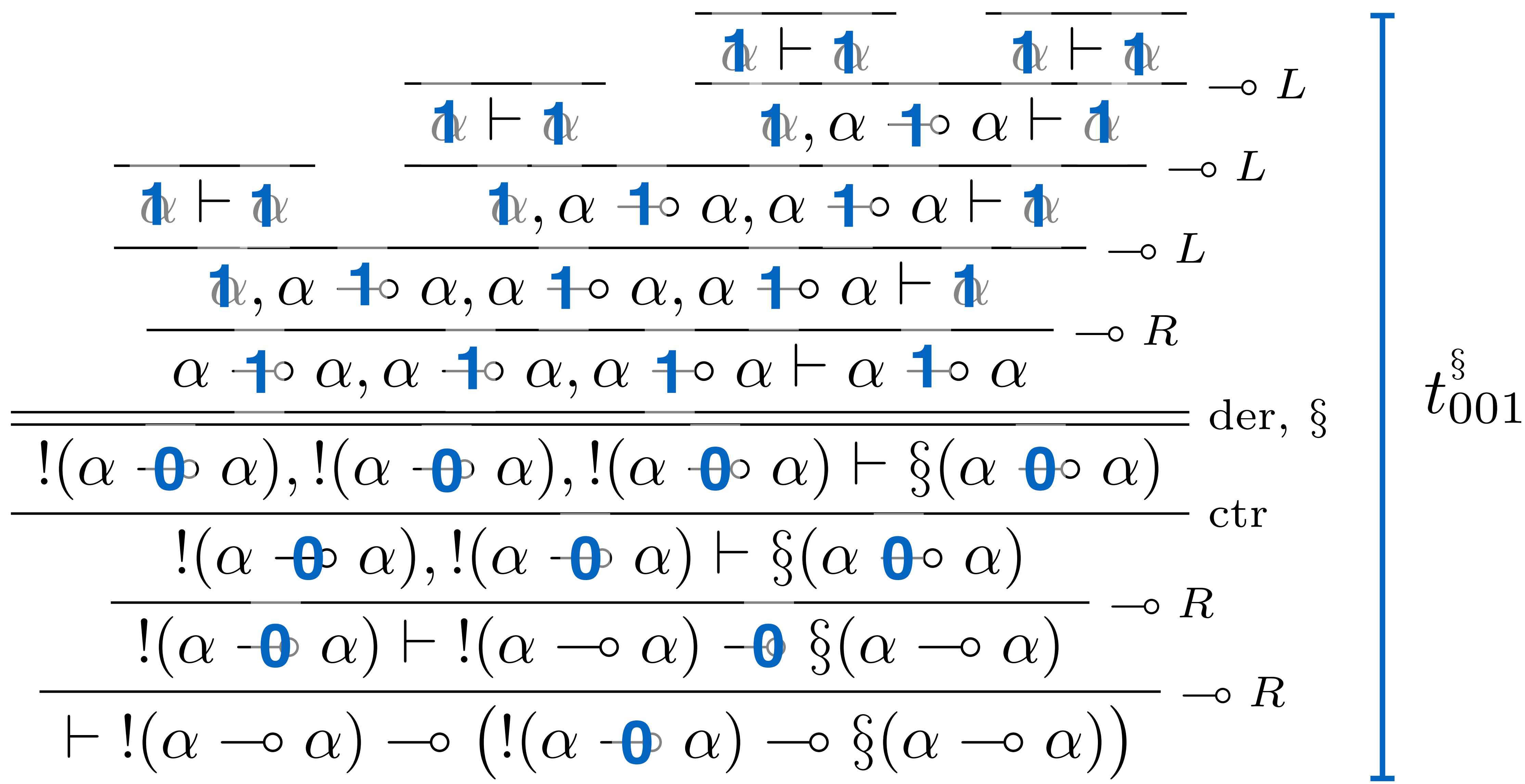
$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\alpha \vdash \alpha} \qquad \dfrac{\dfrac{}{\alpha \vdash \alpha} \qquad \dfrac{\dfrac{}{\alpha \vdash \alpha} \qquad \dfrac{}{\alpha \vdash \alpha}}{\alpha, \alpha \multimap \alpha \vdash \alpha}\multimap L}{\alpha, \alpha \multimap \alpha, \alpha \multimap \alpha \vdash \alpha}\multimap L}{\alpha, \alpha \multimap \alpha, \alpha \multimap \alpha, \alpha \multimap \alpha \vdash \alpha}\multimap L}{\alpha \multimap \alpha, \alpha \multimap \alpha, \alpha \multimap \alpha \vdash \alpha \multimap \alpha}\multimap R}{\dfrac{!(\alpha \multimap \alpha), !(\alpha \multimap \alpha), !(\alpha \multimap \alpha) \vdash \S(\alpha \multimap \alpha)}{!(\alpha \multimap \alpha), !(\alpha \multimap \alpha) \vdash \S(\alpha \multimap \alpha)}\text{ctr}}\text{der}, \S}{!(\alpha \multimap \alpha) \vdash !(\alpha \multimap \alpha) \multimap \S(\alpha \multimap \alpha)}\multimap R}{\vdash !(\alpha \multimap \alpha) \multimap (!(\alpha \multimap \alpha) \multimap \S(\alpha \multimap \alpha))}\multimap R$$

$$t^{\S}_{001}$$

Binary integers (stratified)

$$\mathbf{bint}^{\S} = \forall \alpha \; !(\alpha \multimap \alpha) \multimap (!(\alpha \multimap \alpha) \multimap \S(\alpha \multimap \alpha))$$

$$S \in \{0,1\}^* \longmapsto \text{proof } t^{\S}_S \text{ of } \vdash \mathbf{bint}^{\S}$$



Integers

$$\mathbf{int} = \forall\alpha\ !(\alpha \multimap \alpha) \multimap (\alpha \multimap \alpha)$$

$\forall n \in \mathbb{N}$ there is a proof $\underline{n}$ of $\vdash \mathbf{int}$

Addition is a proof of $\mathbf{int}, \mathbf{int} \vdash \mathbf{int}$

Multiplication is a proof of $\mathbf{int}, \mathbf{int} \vdash \mathbf{int}$

A polynomial of degree k is a proof of $\mathbf{int} \vdash \mathbf{int}$

Integers (stratified)

$$\mathbf{int}^{\S} = \forall \alpha \; !(\alpha \multimap \alpha) \multimap \S(\alpha \multimap \alpha)$$

$\forall n \in \mathbb{N}$ there is a proof $\underline{n}^{\S}$ of $\vdash \mathbf{int}^{\S}$

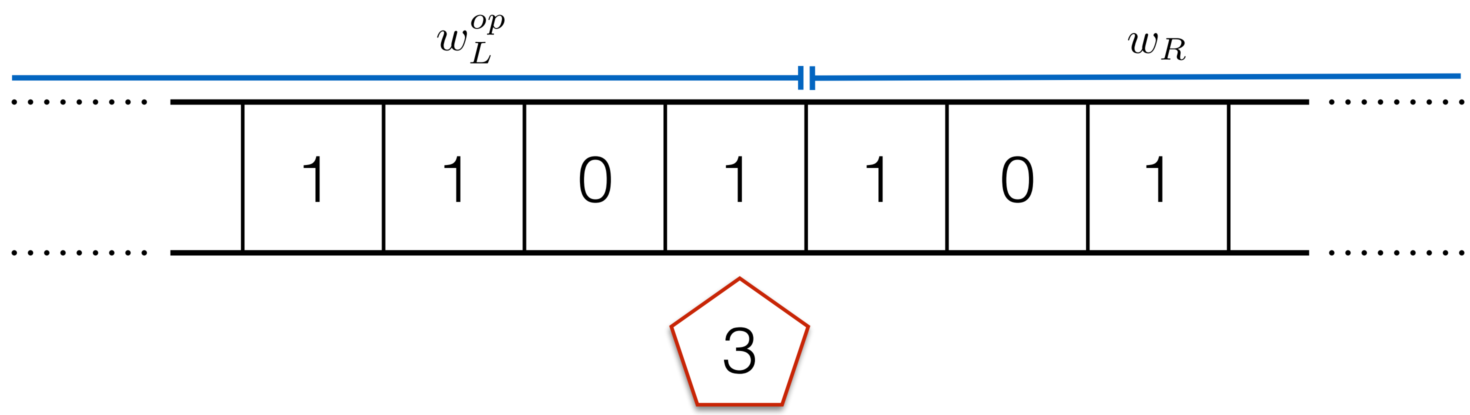
(note that $!(\alpha \multimap \alpha) \multimap (\alpha \multimap \alpha)$ is not provable)

Addition is a proof of $\mathbf{int}^{\S}, \mathbf{int}^{\S} \vdash \mathbf{int}^{\S}$

Multiplication is a proof of $\mathbf{int}^{\S}, \mathbf{int}^{\S} \vdash \S\mathbf{int}^{\S}$

A polynomial of degree k is a proof of $\mathbf{int}^{\S} \vdash \S^{k}\mathbf{int}^{\S}$

Turing machines as proofs



$$\mathbf{Tur} = \mathbf{bint} \otimes \mathbf{bint} \otimes \mathbf{bool}_q$$

Configuration (w_L, w_R, q) of Turing machine $\longmapsto$ proof of $\vdash \mathbf{Tur}$

Instructions for a Turing machine $T \longmapsto$ proof of $\vdash \mathbf{Tur} \multimap \mathbf{Tur}$

Running a Turing machine

(Identify a Turing machine T with a proof of $\vdash \mathbf{Tur} \multimap \mathbf{Tur}$)

$$
\dfrac{
\dfrac{
\dfrac{\begin{array}{c} T \\ \vdots \end{array}}{\vdash \mathbf{Tur} \multimap \mathbf{Tur}}
}{\vdash !(\mathbf{Tur} \multimap \mathbf{Tur})}\ \text{prom}
\qquad
\dfrac{
\dfrac{\begin{array}{c} \text{prepare initial state} \\ \vdots \end{array}}{\mathbf{bint} \vdash \mathbf{Tur}}
\qquad
\dfrac{}{\mathbf{Tur} \vdash \mathbf{Tur}}
}{\mathbf{bint}, \mathbf{Tur} \multimap \mathbf{Tur} \vdash \mathbf{Tur}}\ \multimap L
}{
\dfrac{\mathbf{bint}, !(\mathbf{Tur} \multimap \mathbf{Tur}) \multimap (\mathbf{Tur} \multimap \mathbf{Tur}) \vdash \mathbf{Tur}}{\mathbf{bint}, \mathbf{int} \vdash \mathbf{Tur}}\ \forall\, \mathrm{L}
}\ \multimap L
$$

input binary integer

number of steps n to run

config of Turing machine after n steps

Running a Turing machine (stratified)

$$\mathbf{Tur}^{\S} = \mathbf{bint}^{\S} \otimes \mathbf{bint}^{\S} \otimes \mathbf{bool}_q^{\S}$$

$$\dfrac{\dfrac{\begin{matrix} T \\ \vdots \\ \vdash \mathbf{Tur}^{\S} \multimap \mathbf{Tur}^{\S} \end{matrix}}{\vdash !(\mathbf{Tur}^{\S} \multimap \mathbf{Tur}^{\S})}\,\text{prom} \qquad \dfrac{\dfrac{\begin{matrix} \text{prepare initial state} \\ \vdots \\ \mathbf{bint}^{\S} \vdash \mathbf{Tur}^{\S} \end{matrix} \quad \dfrac{}{\mathbf{Tur}^{\S} \vdash \mathbf{Tur}^{\S}}}{\mathbf{bint}^{\S}, \mathbf{Tur}^{\S} \multimap \mathbf{Tur}^{\S} \vdash \mathbf{Tur}^{\S}}\,\multimap L}{\S\mathbf{bint}^{\S}, \S(\mathbf{Tur}^{\S} \multimap \mathbf{Tur}^{\S}) \vdash \S\mathbf{Tur}^{\S}}\,\S}{\dfrac{\S\mathbf{bint}^{\S}, !(\mathbf{Tur}^{\S} \multimap \mathbf{Tur}^{\S}) \multimap \S(\mathbf{Tur}^{\S} \multimap \mathbf{Tur}^{\S}) \vdash \S\mathbf{Tur}^{\S}}{\S\mathbf{bint}^{\S}, \mathbf{int}^{\S} \vdash \S\mathbf{Tur}^{\S}}\,\forall\,\mathrm{L}}\,\multimap L$$

Theorem (Girard)

A function $\{0,1\}^* \longrightarrow \{0,1\}^*$ is "polytime" if and only if it can be typed as a proof π of $\mathbf{bint} \vdash \mathbf{bint}$ which admits a stratification.

$$\begin{array}{c} \pi^{\S} \\ \vdots \\ \mathbf{bint}^{\S} \vdash \S^{k+2}\mathbf{bint}^{\S} \end{array} \quad \textbf{stratifies} \quad \begin{array}{c} \pi \\ \vdots \\ \mathbf{bint} \vdash \mathbf{bint} \end{array}$$

Theorem (Girard)

> A function $\{0,1\}^* \longrightarrow \{0,1\}^*$ is "polytime" if and only if it can be typed as a proof π of $\mathbf{bint} \vdash \mathbf{bint}$ which admits a stratification.

$f : \{0,1\}^* \longrightarrow \{0,1\}^*$ computed by a Turing machine T with polyclock P

$$\dfrac{\overset{\text{length}}{\vdots}\quad\quad \overset{\text{P}}{\vdots}}{\mathbf{bint} \vdash \mathbf{int} \quad\quad \mathbf{int} \vdash \mathbf{int}}$$

$$\dfrac{\mathbf{bint} \vdash \mathbf{int} \quad\quad \mathbf{int} \vdash \mathbf{int}}{\mathbf{bint} \vdash \mathbf{int}}\ \text{cut}$$

$$\dfrac{}{\mathbf{bint} \vdash \mathbf{bint}}$$

$$\dfrac{\mathbf{bint} \vdash \mathbf{bint} \quad\quad \mathbf{bint} \vdash \mathbf{int}}{\mathbf{bint} \otimes \mathbf{bint} \vdash \mathbf{bint} \otimes \mathbf{int}}\ \otimes R, \otimes L$$

$$\dfrac{\overset{\text{copy}}{\vdots}}{\mathbf{bint} \vdash \mathbf{bint} \otimes \mathbf{bint}}$$

$$\dfrac{\mathbf{bint} \vdash \mathbf{bint} \otimes \mathbf{bint} \quad\quad \mathbf{bint} \otimes \mathbf{bint} \vdash \mathbf{bint} \otimes \mathbf{int}}{\mathbf{bint} \vdash \mathbf{bint} \otimes \mathbf{int}}\ \text{cut}$$

$$\dfrac{\overset{\text{iterate T}}{\vdots}}{\mathbf{bint}, \mathbf{int} \vdash \mathbf{Tur}}$$

$$\dfrac{\mathbf{bint}, \mathbf{int} \vdash \mathbf{Tur}}{\mathbf{bint} \otimes \mathbf{int} \vdash \mathbf{Tur}}$$

$$\dfrac{\mathbf{bint} \vdash \mathbf{bint} \otimes \mathbf{int} \quad\quad \mathbf{bint} \otimes \mathbf{int} \vdash \mathbf{Tur}}{\mathbf{bint} \vdash \mathbf{Tur}}$$

Theorem (Girard)

> A function $\{0,1\}^* \longrightarrow \{0,1\}^*$ is "polytime" if and only if it can be typed as a proof π of $\mathbf{bint} \vdash \mathbf{bint}$ which admits a stratification.

$f : \{0,1\}^* \longrightarrow \{0,1\}^*$ computed by a Turing machine T with polyclock P

$$\dfrac{\dfrac{\dfrac{\text{copy}}{\vdots}\quad \mathbf{bint} \vdash \mathbf{bint} \otimes \mathbf{bint} \qquad \dfrac{\dfrac{}{\mathbf{bint} \vdash \mathbf{bint}} \qquad \dfrac{\dfrac{\text{length}}{\vdots}\ \mathbf{bint} \vdash \mathbf{int} \qquad \dfrac{\text{P}}{\vdots}\ \mathbf{int} \vdash \mathbf{int}}{\mathbf{bint} \vdash \mathbf{int}}\,\text{cut}}{\mathbf{bint} \otimes \mathbf{bint} \vdash \mathbf{bint} \otimes \mathbf{int}}\,\otimes R, \otimes L}{\mathbf{bint} \vdash \mathbf{bint} \otimes \mathbf{int}}\,\text{cut} \qquad \dfrac{\dfrac{\text{iterate T}}{\vdots}\ \mathbf{bint}, \mathbf{int} \vdash \mathbf{Tur}}{\mathbf{bint} \otimes \mathbf{int} \vdash \mathbf{Tur}}}{\mathbf{bint} \vdash \mathbf{Tur}}$$

$$\dfrac{\mathbf{bint} \vdash \mathbf{Tur} \qquad \dfrac{\text{read off output}}{\vdots}\ \mathbf{Tur} \vdash \mathbf{bint}}{\mathbf{bint} \vdash \mathbf{bint}} \quad \pi$$

Upshot: π computes f

Theorem (Girard)

A function $\{0,1\}^* \longrightarrow \{0,1\}^*$ is "polytime" if and only if it can be typed as a proof π of $\mathbf{bint} \vdash \mathbf{bint}$ which admits a stratification.

$f : \{0,1\}^* \longrightarrow \{0,1\}^*$ computed by a Turing machine T with polyclock P

copy	P	iterate T
$\vdots$	$\vdots$	$\vdots$
$\mathbf{bint}^{\S} \vdash \S(\mathbf{bint}^{\S} \otimes \mathbf{bint}^{\S})$	$\mathbf{int}^{\S} \vdash \S^k \mathbf{int}^{\S}$	$\S\mathbf{bint}^{\S}, \mathbf{int}^{\S} \vdash \S\mathbf{Tur}^{\S}$

$\pi^{\S}$		π
$\vdots$	**stratifies**	$\vdots$
$\mathbf{bint}^{\S} \vdash \S^{k+2}\mathbf{bint}^{\S}$		$\mathbf{bint} \vdash \mathbf{bint}$

Summary

- There is a notion of *stratification* for proofs
- Turing machines can be encoded into linear logic
- If a Turing machine is polytime, the stratification of the clock polynomial gives a stratification of the corresponding proof in linear logic.
- Theorem: a function of binary integers is polytime iff. it admits a stratification.

References

J.Y. Girard, "*Light linear logic*", Information and Computation 14, 1995.

P. Baillot, D. Mazza "*Linear logic by levels and bounded time complexity*", Theoretical Computer Science 411.2, 2010.

P. Boudes, D. Mazza, and L. Tortora de Falco, *An abstract approach to stratification in linear logic*, Information and Computation 241, 2015.

D. Murfet, *Logic and linear algebra: an introduction*, arXiv: 1407.2650.

Slides of this lecture available at therisingsea.org