

(Veja o PDF IntroProof.)

lec01
2025-08-18

lec02
2025-08-20

lec03
2025-08-22

Int . Especificação

(Int ; $\overset{+}{2}$, $\overset{-}{1}$, $\overset{0}{0}$, $\overset{\cdot}{2}$, $\overset{1}{0}$)

↑ aridades

Int : Type

$\overset{+}{-}$: Int $\times$ Int $\rightarrow$ Int

$\overset{-}{-}$: Int $\rightarrow$ Int

$\overset{\cdot}{-}$: Int $\times$ Int $\rightarrow$ Int

0 : Int

1 : Int

(v1 / ?)

lec04
2025-08-22

Operação n-ária no α

$$\underbrace{(\alpha \times \dots \times \alpha)}_{n \text{ cópias}} \rightarrow \alpha$$

Açúcares sintácticos

lec05
2025-08-25

Tendo $x, y, z : \text{Int}$, o que significam as expressões?:

$$x + y \cdot z \equiv ?$$

$$x + y + z \equiv ?$$

$$x \cdot y \cdot z \equiv ?$$

$$xy \equiv ?$$

NADA! Por enquanto é lixo: nem compila!

Atribuímos: $\left. \begin{array}{l} \text{precedência sintáctica} \\ \text{associatividade sintáctica} \end{array} \right\}$

- $(\cdot)$ tem precedência sobre $(+)$
- $(+)$ associa à L
- $(\cdot)$ associa à L
- justaposição: $(\cdot)$

Assim, agora temos:

- $x + y \cdot z \stackrel{\text{sug}}{\equiv} x + (y \cdot z)$
- $x + y + z \stackrel{\text{sug}}{\equiv} (x + y) + z$
- $x \cdot y \cdot z \stackrel{\text{sug}}{\equiv} (x \cdot y) \cdot z$
- $xy \stackrel{\text{sug}}{\equiv} x \cdot y$

Como usar funções $(\rightarrow)-E$

$$\frac{f : \alpha \rightarrow \beta \quad a : \alpha}{f \ a : \beta} (\rightarrow)-E$$

$\uparrow$
aplicação de função

Precedência?

Associatividade sintáctica?

Subtração (operação definida)

$$-_- : \text{Int} \times \text{Int} \rightarrow \text{Int}$$

$$x - y \stackrel{\text{def}}{=} x + \underbrace{(-y)}_{: \text{Int} ?}$$

Queremos o conforto:

$$\frac{x : \text{Int} \quad \frac{y : \text{Int}}{-y : \text{Int}}}{x + (-y) : \text{Int}} \quad ?$$

$$\frac{\dots ? \dots}{-y : \text{Int}}$$

Sem ele:

$$\frac{(+): \text{Int} \times \text{Int} \rightarrow \text{Int} \quad \frac{x : \text{Int} \quad -y : \text{Int}}{\langle x, -y \rangle : \text{Int} \times \text{Int}}}{\underbrace{x + (-y)}_{\text{III}} : \text{Int}} \quad (+) _ \langle x, -y \rangle$$

Quantos inteiros garanta a spec.?

Resposta errada: é garantida uma infinidade de inteiros:

$0, -0, -(-0), -(-(-0)), \dots : \text{Int}$

↑
quantidade infinita de expressões que denotam inteiros

Melhor resposta: pelo menos um inteiro é garantido.

Sem leis talvez $0 = 1$ ou $(\forall x, y) [x = y]$ ou ..

Leis (axiomas)

$$(+) - \text{ass} : (\forall x : \text{Int}) (\forall y) (\forall z) [(x+y)+z = x+(y+z)]$$

(+) associativa

$$(+) - \text{com} : x + y = y + x$$

(+) comutativa

$$(\heartsuit) : \alpha \times \alpha \rightarrow \alpha$$

$$(\heartsuit) \text{ associativa} \stackrel{\text{def}}{\iff} (\forall a, b, c) [(a+b)+c = a+(b+c)]$$

$$0 - \text{idR} - (+) : x + 0 = x$$

0 é uma (+)-identidade-R

$$(-) - \text{invR} - (+) : x + (-x) = 0$$

$(-x)$ é um (+)-inverso-R de x

$(\cdot)$ -ass : ...

$(\cdot)$ -com : ...

1 -idR- $(\cdot)$: ...

(Int ; $\underbrace{+, -, 0}_{\text{parte aditiva}}, \underbrace{\cdot, 1}_{\text{parte multiplicativa}}$)

$(+)$ -distR- $(\cdot)$: $(x + y) \cdot d = x \cdot d + y \cdot d$

$(\cdot)$ distribui sobre $(+)$ à direita

(distributividade 2-ária)

(Aqui termina a Spec-Int v1/?.

Teoremas (consequências dos axiomas)

$$\Theta. (\forall x) [0 + x = x]$$

•
•

$$\Theta. x \cdot 0 = 0 \iff 0 \text{ absorve } (\cdot) \text{ pela direita}$$

$$\Theta. -(-x) = x \iff (-) \text{ é uma involução}$$

•
•
•

<

... -2 -1 0 1 2 ...

Θ. Demonstre: $(\forall x: \text{Int}) [0 + x = x]$

DEMONS

DADOS

ALVO

Seja a: Int.

a: Int

~~$(\forall x: \text{Int}) [0 + x = x]$~~

$0 + a = a$

E agora?

Não tenho como continuar:

- não sei como atacar $(=)$;
- parece que estou sem dados.

Igualdade ($=_\alpha$)

lec06
2025-08-27

$$\frac{a : \alpha \quad b : \alpha}{a =_\alpha b : \text{Prop}} \quad (=_\alpha)\text{-F}$$

- $(=_\alpha)$ relação de equivalência:

$$\frac{}{a = a} \quad \text{Ref}[a]$$

$$\frac{a = b \quad b = c}{a = c} \quad \text{Trans}$$

$$\frac{a = b}{b = a} \quad \text{Sym}$$

- substituição:

$$\frac{a = b \quad \dots a \dots \overset{\text{2ª ocorrência de } a}{a} \dots a \dots}{\dots a \dots b \dots a \dots} \quad \text{Subst}[2]$$

HW ↗

↑
podemos inferir
essas duas!

Metateorema:

Não precisamos a sym .

Basta mostrar como conseguir o que ela consegue:
inferir $b = a$ com única hipótese $a = b$.

Ó: duas folhas abertas. A $a = b$ tá OK mas precisamos "fechar" a outra.

$$\frac{\begin{array}{c} a = b \end{array} \quad \begin{array}{c} a = a \end{array}}{b = a} \text{Subst}[1]$$

$$\frac{a = b \quad \frac{a = a}{\text{Refl}}}{b = a} \text{Subst}[1]$$

Θ. Demonstre: $(\forall x: \text{Int}) [0 + x = x]$

DEMONS

Seja a: Int.

Aplique ((+)-com)

com

$x := 0$
 $y := a$

← para ajudar o leitor
← necessário

para obter $0 + a = a + 0$.

⋮

(queremos

"macros"/açúcar)

DADOS

a: Int

$$0 + a = a + 0$$

$$a + 0 = a$$

$$0 + a = a$$

ALVO

~~$$(\forall x: \text{Int}) [0 + x = x]$$~~

$$0 + a = a$$

$$(0\text{-idR-}(+)) \sqcup a \xrightarrow{\text{fornece}} a + 0 = a$$

↑
aplicação da $(0\text{-idR-}(+))$ no a

Calculamos

Θ. Demonstre: $(\forall x: \text{Int}) [0 + x = x]$

DEMONS

Seja a: Int. -- ALVO: $0 + a = a$

Calculamos:

$$a = a + 0 \quad [(0\text{-idR-}(+)) \sqsubset a]$$

$$= 0 + a \quad [((+)\text{-com}) \sqsubset a \sqsubset 0]$$

← Halmos tombstone
■ (matamos o teorema)

$$(((+)\text{-com}) \sqsubset a) \sqsubset 0$$

↑
atribuimos ao $\sqsubset$ associatividade sintáctica à L.

DADOS

a: Int

$$a = 0 + a$$

ALVO

~~÷~~

$$0 + a = a$$

Aplicações "parciais"

$$((+) - \text{com}) \quad : \quad (\forall x) [(\forall y) [x + y = y + x]]$$

$$((+) - \text{com}) \quad 1 \quad : \quad (\forall y) [1 + y = y + 1]$$

$$((+) - \text{com}) \quad 1) \quad 42 \quad : \quad 1 + 42 = 42 + 1$$

Curritificação teaser

versão descurritificada

versão curritificada

$$\hat{f} : (\alpha \times \beta \times \gamma) \rightarrow \delta$$

$$\hat{f} \underbrace{\langle a, b, c \rangle}_{: \alpha \times \beta \times \gamma} : \delta$$

$$f : \alpha \rightarrow (\beta \rightarrow (\gamma \rightarrow \delta))$$

$$f \underbrace{a}_{: \alpha} : \beta \rightarrow (\gamma \rightarrow \delta)$$

$$(f \underbrace{a}_{: \alpha} \underbrace{b}_{: \beta}) : \gamma \rightarrow \delta$$

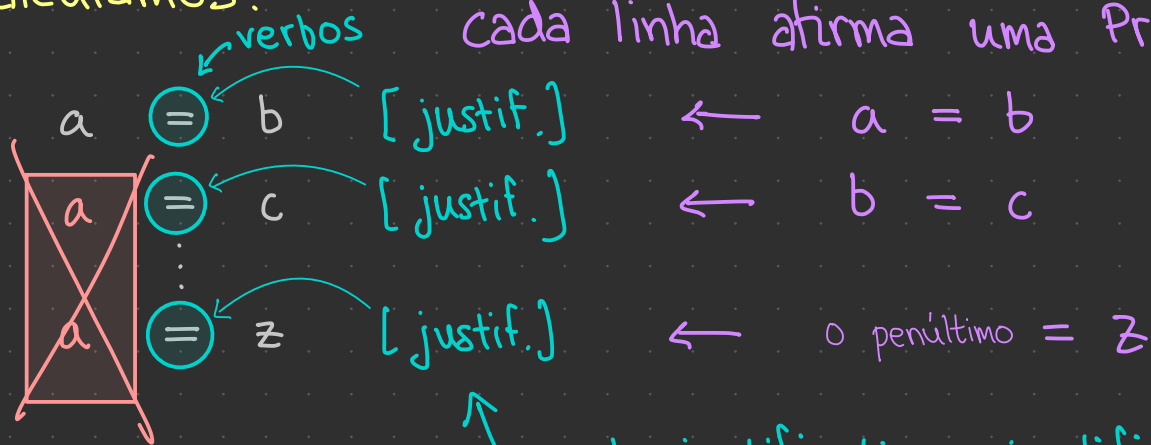
$$((f \underbrace{a}_{: \alpha} \underbrace{b}_{: \beta}) \underbrace{c}_{: \gamma}) : \delta$$

$$(\alpha \times \beta \rightarrow \delta) \xrightarrow{\text{curry}} (\alpha \rightarrow (\beta \rightarrow \delta))$$
$$\xleftarrow{\text{uncurry}}$$

Como escrever cálculos

Calculamos:

cada linha afirma uma Prop:



aqui não são
implícitas cópias
de a ! É assim:

$$a^{(j1)} = b^{(j2)} = c^{(j3)} = d^{(j4)} = z \quad \rightsquigarrow$$

$$\begin{array}{rcl} a & = & b \quad [j1] \\ & = & c \quad [j2] \\ & = & d \quad [j3] \\ & = & z \quad [j4] \end{array}$$

Três estilos de escrever cálculos:

(não improvise!)

$$\begin{array}{lcl} \text{obj}_1 & = & \text{obj}_2 \quad [\text{just.}] \\ & = & \text{obj}_3 \quad [\text{just.}] \\ & = & \text{obj}_4 \quad [\text{just.}] \\ & \vdots & \\ & = & \text{obj}_n \quad [\text{just.}] \end{array}$$

↑
popular entre matemáticos
com papéis ou quadros
bem largos.

(Se a exp. a é larga
vai ser chato indentar!)

$$\begin{array}{lcl} \text{obj}_1 & = & \text{obj}_2 \quad [\text{just.}] \\ & = & \text{obj}_3 \quad [\text{just.}] \\ & = & \text{obj}_4 \quad [\text{just.}] \\ & \vdots & \\ & = & \text{obj}_n \quad [\text{just.}] \end{array}$$

↑
ideal escrevendo no computador
ou tendo largura curta.

$$\begin{array}{lcl} \text{obj}_1 & = & \{\text{just.}\} \\ \text{obj}_2 & = & \{\text{just.}\} \\ \text{obj}_3 & = & \{\text{just.}\} \\ & \vdots & \\ \text{obj}_n & = & \{\text{just.}\} \end{array}$$

↑
popular em
programação funcional

Unicidade

(Demonstramos
"por fight club")

DADOS

$a : \text{Int}$

$b : \text{Int}$

$a (+)\text{-id}$ & $b (+)\text{-id}$

Θ. Unicidade de $(+)\text{-id}$

$$(\forall u, v) [\overset{\updownarrow}{u, v (+)\text{-id}} \Rightarrow u = v]$$

Seja a : Int.

Seja b : Int.

} ou: Sejam a, b : Int. ← DUAS linhas de código!

ALVO

Suponha $a (+)\text{-id}$ & $b (+)\text{-id}$.

$$(\forall u, v) [u, v (+)\text{-id} \Rightarrow u = v]$$

$$(\forall v) [a, v (+)\text{-id} \Rightarrow a = v]$$

$$a, b (+)\text{-id} \Rightarrow a = b$$

$$a = b$$

Preciso escolher um nome "fresco" (fresh); um que não está sendo usado no escopo.

(Veja lec04 no PDF IntroProof.)
2025-08-29

lec07
2025-08-29

(Veja lec05 no PDF IntroProof.)
2025-09-01

lec08
2025-09-01

(Veja lec06 no PDF IntroProof.)
2025-09-03

lec09
2025-09-03

(Veja lec07 no PDF IntroProof.)
2025-09-05

lec10
2025-09-05

Unicidade

$$(\forall u, v) [u, v (+)\text{-id} \Rightarrow u = v]$$

lec11

2025-09-05

Θ. Unicidade de $(+)\text{-id}$

Sejam $a, b : \text{Int}$.

Suponha $a (+)\text{-id}$ & $b (+)\text{-id}$.

~~Ext-L de $a (+)\text{-id}$ & $b (+)\text{-id}$~~

~~Como $a (+)\text{-id}$ & $b (+)\text{-id}$, Logo $a (+)\text{-id}$ ^(ha) [Ext-L]~~

~~Como $a (+)\text{-id}$ & $b (+)\text{-id}$, logo $b (+)\text{-id}$ ^(hb) [Ext-R]~~

Logo $a (+)\text{-id}$ ^(ha) e $b (+)\text{-id}$ ^(hb) [Ext-L ; Ext-R]

DADOS

$a : \text{Int}$

$b : \text{Int}$

$a (+)\text{-id}$ & $b (+)\text{-id}$

ALVO

$a =_{\text{Int}} b$

Θ. Unicidade de (+)-id

DEMONS:

Sejam $a, b : \text{Int}$.

Suponha a (+)-id & b (+)-id.

Logo a (+)-id^(ha) e b (+)-id^(hb). [Ext-L; Ext-R]

Calculamos:

a

$$= a + b \quad [(hb \ a) \cdot r]$$

$$= b \quad [(ha \ b) \cdot l]$$

DADOS

$a : \text{Int}$

$b : \text{Int}$

a (+)-id & b (+)-id

$ha : a$ (+)-id $\Leftrightarrow (\forall x) [a + x = x = x + a]$

$hb : b$ (+)-id $\Leftrightarrow (\forall x) [b + x = x = x + b]$

$a = b$

(+)-cancelamento

$$\ominus. (+)\text{-canR} \iff (\forall c) (\forall x, y) [x + c = y + c \Rightarrow x = y]$$

Sejam $c, u, v : \text{Int}$ [c é (+)-cancelável pela direita]

$$\text{Sup } u + c = v + c.$$

$$\text{Logo } (u + c) + (-c) = (v + c) + (-c). \quad [(+ (-c))] \quad \begin{array}{c} \text{ALVO} \\ u = v \end{array}$$

⋮
?

↗
app esta função
nos dois lados
da equação usada.

« a função $f : \text{Int} \rightarrow \text{Int}$

definida pela

$$f\ x = x + (-c). \gg$$

$$(_ + (-c))$$

ou

$$(+ (-c))$$

↖ ninguém merece

"Aplicar a mesma função nos dois lados"

$$\vdash (\forall f : \alpha \rightarrow \beta) (\forall u, v : \alpha) [u = v \Rightarrow f u = f v]$$

$$\frac{u =_{\alpha} v}{f u =_{\beta} f v} \text{cong}[f]$$

qual é o tipo?

essa árvore serve

pois tem a mesma raiz (conclusão)
e depende das mesmas folhas abertas
(hipoteses)

$$\frac{u =_{\alpha} v \quad \frac{}{f u =_{\beta} f u} \text{refl}[f u]}{f u =_{\beta} f v} \text{subs}[2]$$

