Int (spec v5/S)

lec9

2024-11-08

(v4) + $\begin{cases} \text{IND} & \text{— Princípio da indução} \\ \text{PBO} & \text{— Princípio da Boa Ordem} \end{cases}$

Set Int
— sinônimo de —
Int → Prop

$$\dfrac{\varphi(1) \qquad (\forall k \geq 1)[\varphi(k) \Rightarrow \varphi(k+1)]}{(\forall n \geq 1)[\varphi(n)]}$$

$$\dfrac{1 \in W \qquad W_{>0} \text{ é } (+1)\text{-fechado}}{W \supseteq \text{Pos}}$$

$\text{IND}_\varphi \quad (\varphi : \text{Int} \to \text{Prop})$

$\text{IND}_W \quad (W : \text{Set Int})$

✓ Para todo inteiro $x \geqslant c$, $\varphi(x)$

Seja $\psi(x) \overset{\text{def}}{\iff} \varphi(x + (c-1))$

✓ Para todo inteiro negativo x, $\varphi(x)$.

Seja $\psi(x) \overset{\text{def}}{\iff} \varphi(-x)$

$(\forall k \geq 1)(\psi(k) \Rightarrow \psi(k+1))$

$\varphi(-k) \Rightarrow \varphi(-k-1)$

$(\forall t \leq -1)[\varphi(t) \Rightarrow \varphi(t-1)]$

Hacking

<body bgcolor = "red"
fg color = "green"
background = "http..... legal.jpg"
>
;
;

red

green

green" background="...jpg

$$\psi(1)$$
$$\Updownarrow$$
$$\varphi(-8)$$

$$(\forall k \geq 1)\,[\psi(k) \Rightarrow \psi(k+1)]$$

$$\varphi(k-9) \Rightarrow \varphi((k+1)-9)$$

$$(\forall t \geq -8)\,[\varphi(t) \Rightarrow \varphi(t+1)]$$

$$(\forall n \geq 1)\,[\psi(n)]$$

Mais que uma base

$$\text{fib} : \text{Int} \to \text{Int}$$

$$\text{fib}\ 0 = 0$$

$$\text{fib}\ 1 = 1$$

$$\text{fib}\ n = \begin{cases} \text{fib}(n-1) + \text{fib}(n-2), & n \geq 2 \\ 42, & n < 0 \end{cases}$$

$$\varphi(0) \qquad \varphi(1) \qquad (\forall k \geq 0)[\varphi(k)\ \&\ \varphi(k+1) \Rightarrow \varphi(k+2)]$$

Seja $k \geq 0$ t.q. $\varphi(k)^{H.I.1}$ & $\varphi(k+1)^{H.I.2}$.

DADOS	ALVO
$\varphi(k)$	$\varphi(k+2)$
$\varphi(k+1)$	
$k \geq 0$	

$$(\forall k \geq 2)[\varphi(k-2)\ \&\ \varphi(k-1) \Rightarrow \varphi(k)]$$

Seja $k \geq 2$ t.q. $\varphi(k-1)$ & $\varphi(k-2)$.

$k \geq 2$	$\varphi(k)$
$\varphi(k-1)$	
$\varphi(k-2)$	

$$\psi(n) \overset{\text{def}}{\iff} \varphi(n) \;\&\; \varphi(n+1)$$

$$\varphi(k) \,\&\, \varphi(k+1) \Longrightarrow \varphi(k+2)$$

$$\frac{\varphi(0) \qquad \varphi(1)}{\varphi(0) \,\&\, \varphi(1)} \qquad (\forall k \geq 0)\left[\varphi(k) \,\&\, \varphi(k+1) \Longrightarrow \varphi(k+1) \,\&\, \varphi(k+2)\right]$$

$$\Updownarrow \qquad\qquad \Updownarrow \qquad\qquad \Updownarrow$$

$$\frac{\psi(0) \qquad (\forall k \geq 0)\left[\psi(k) \Longrightarrow \psi(k+1)\right]}{(\forall n \geq 0)\left[\psi(n)\right]} \, \mathrm{Ind}_{\psi}$$

$$P \,\&\, Q \Longrightarrow Q \,\&\, R \quad \dashv\vdash \quad P \,\&\, Q \Longrightarrow R$$

Indução forte

$$(\forall i)[\, 0 \leq i < k \Rightarrow \varphi(i) \,]$$

$$\dfrac{(\forall k \geq 0)\left[\, \overbrace{(\forall 0 \leq i < k)[\, \varphi(i) \,]}^{\Updownarrow\ \text{sug}} \Rightarrow \varphi(k) \,\right]}{(\forall n \geq 0)[\, \varphi(n) \,]}\ \textsc{IndStrong}$$

PBO

lec10

2024-11-13

- ◦ Pos é bem-ordenado (pela $(\leq)$)

  (“$\mathbb{Z}_{>0}$”)

a ordem consultada é implícita pelo contexto

$\_\_$ é bem-ordenado : Set Int $\to$ Prop

$\_\_$ é $\_$-bem-ordenado : Set Int $\times$ $\underbrace{(\text{Int} \times \text{Int} \to \text{Prop})}_{\text{Order Int}}$ $\to$ Prop

+ axiomas de ordem

Sejam W : Set Int e $(\leq)$ uma ordem no Int.

subconjunto habitado

W é $(\leq)$-bem-ordenado $\overset{\text{def}}{\iff}$ $(\forall X \subseteq W)[X \text{ possui mínimo}]$

$(\forall X \subseteq W)[X \text{ hab} \Rightarrow X \text{ possui mínimo}]$

Θ. $\neg(\exists x)[0 < x < 1]$

ALVO

$\perp$

DADOS

$(\exists x)[0<x<1]$

$\left(\begin{array}{l} x : \mathrm{Int} \\ 0 < x < 1 \end{array}\right)$

$m : \mathrm{Int}$

$0 < m < 1$

$m = \min\{x \mid 0<x<1\}$

DEMONS.

Sup $\overbrace{(\exists x)[0 < x < 1]}^{C \text{ habitado}}$.

(Seja x t.q. $0 < x < 1$.)

Seja m o menor inteiro t.q. $0 < m < 1$.

Seja $m = \min \underbrace{\{x \mid 0 < x < 1\}}_{C}$. [PBO ($C \subseteq Pos$? C hab?)]

Vou demonstrar: $0 < m^2 < m < 1$

- $m^2 > 0$: $\dfrac{\dfrac{m > 0}{m \neq 0}\,\text{Tri}}{m^2 > 0}\,\Theta$.

- $m^2 < m$: $\dfrac{m > 0 \quad m < 1}{\underbrace{m \cdot m}_{m^2} < m \cdot 1}\,\Theta$

  $m^2 < m$

Contradição (pela escolha de m). ∎

Outras versões de PBO

original : $\mathbb{Z}_{>0}$ é bem-ordenado

- $\mathbb{Z}_{\geq -8}$ é bem-ordenado
- $\mathbb{Z}_{<0}$ ...
- $2\mathbb{Z}_{\geq 0}$ ...

$\vdots$

Wishlist

- PBO & Indução
- Θ. $\neg(\exists x)[0 < x < 1]$
- Θ. Divisão : $\text{Int} \times \text{Int} \to \underset{\text{quot}}{\text{Int}} \times \underset{\text{rem}}{\text{Int}}$

  : Prop

  $$(\forall a, b \neq 0)(\exists! q, r)[\ a = b \cdot \underset{\text{quot}}{q} + \underset{\text{rem}}{r} \ \ \& \ \ \underbrace{0 \leq r < |b|}_{\text{size}(r) < \text{size}(b)}\ ]$$

  $7 = 2 \cdot 3 + 1$

  $7 = 2 \cdot 20 + (-33)$

  $7 = 2 \cdot 0 + 7$

- Θ. Sistemas posicionais de numerais de inteiros

⋮

?

Sistemas posicionáis de numeráis

lec11
2024-11-18

base

$|\text{alfabeto}|$: 0 1 2 3 4 5 6 7 8 9 (A B C D E F ...)

dígitos ou algarismos

$\mathbb{Z}_{\geq 0}$ '0' "0"

"0"
1
2 ← numeráis
3
⋮
9
10
11
⋮
19
20
⋮
29
⋮
99
100

$$2403_{(10)} = 2 \cdot \underline{10}^3 + 4 \cdot \underline{10}^2 + 0 \cdot \underline{10}^1 + 3 \cdot \underline{10}^0$$

base

$|\text{alfabeto}|$ ← base = 7

0 1 2 3 4 5 6

$\mathbb{Z}_{\geq 0}$

'0'

"0"

1

2

3

⋮

6

1 0

1

⋮

1 6

2 0

⋮

2 6

⋮

6 6

1 0 0

0

. . .

$\underbrace{1111}_{F}$

785

$$2403_{(7)} = 2 \cdot 7^3 + 4 \cdot 7^2 + 0 \cdot 7^1 + 3 \cdot 7^0$$

Θ. Divisão (Euclides)

size(r) < size(b)

$$(\forall a^{\geq 0}, b \underset{\neq 0}{> 0})(\exists! q, r)\left[\, a = b q + r \quad \& \quad 0 \leq r < \genfrac{}{}{0pt}{}{b}{|b|} \,\right]$$

Tentativa: por indução no b.

Seja a : Int.

Seja b > 0.

Por indução (no b).

$\overset{a}{420}$ por $\overset{b}{7}$
$(\underset{q_b}{60}, \underset{r_b}{0})$

isso parece inútil

~~420 por 8~~
421 por 7

isso parece ajudar mesmo

BASE: $(\exists! q, r)[\; a = 1 \cdot q + r \quad \& \quad 0 \leq r < 1 \;]$

⋮

P.I.: Divida a por b. [H.I]

Logo sejam q_b, r_b os quot e rem da divisão de a por b.

Ou seja, temos $a = b \cdot q_b + r_b \;\&\; 0 \leq r_b < b$.

Procuro q, r t.q. $a = (b+1)q + r \quad \& \quad 0 \leq r < b+1$.

Tentativa: por indução no a.

Seja $b \neq 0$.

BASE: ...

P.I.:

Seja a t.q. sei dividir a por b. $\qquad r_a \in \{0, 1, \ldots, b-1\}$

Ou seja, sejam q_a, r_a t.q. $a = b \cdot q_a + r_a$ & $\underbrace{0 \leq r_a < b}$.

Quero dividir $a+1$ por b.

Ou seja, procuro q, r t.q. $a+1 = b \cdot q + r$ & $0 \leq r < b$.

Separo em casos a partir do r_a. ($\star$?)

CASO $r_a = b-1$:

Esc: $q := q_a + 1$

$r := 0$

CASO CONTRÁRIO $(0 \leq r_a < b-1)$:

Esc. $q := q_a$

$r := r_a + 1$

Defender que os testemunhas servem!

Demonstração usando o PBO (rascunho)

o conjunto de todos os contraexemplos
(queremos mostrar que não há nenhum)

Seja $b : \text{Int}$.

Seja $C = \{ c \geq 0 \mid$ não tem como dividir c por $b \}$

Basta demonstrar que C não é habitado.

Suponha C habitado.

Logo seja c o menor membro de C. [PBO]

(i) infira $c \not< b$; (ii) considere o $c - b$.

$0 \leq c < b$

0 1 2 3 ... 419 420 421 ...

c

o primeiro (menor) contraexemplo

mdc

$\underbrace{\text{m}}$dc → melhor

$(\leq)$ vs $(\mid)$

Sejam a, b : Int.

Seja m : Int.

m é um mdc dos $a, b \overset{\text{def}}{\iff}$

$$\left\{\begin{array}{l} \overbrace{m \text{ é um div com. dos } a, b}^{m \mid a \ \& \ m \mid b} \\ \& \\ \cancel{m = \max(\text{divcom}(a,b))} \\ \underbrace{m \text{ é o melhor deles}}_{(\forall d \text{ div. com. } a,b)[\, d \mid m \,]} \end{array}\right.$$

envolve uma ordem nada-a-ver com a $(\mid)$

Diagramas Hasse

$\mathbb{Z}_{\geq 0}$ $(\leq)$ $(|)$