ESCOLA POLITÉCNICA

CURSO DE ENGENHARIA DE SOFTWARE

T1 MÉTODOS FORMAIS

ALUNOS: FELIPE R. TASONIERO, LUCAS S. WOLSCHICK

23 de Abril de 2025

1) Prova formal por indução de uma função recursiva sobre números naturais para o cálculo da potência:

Definição Recursiva	
Eq1	$pot(X, 0) = 1$
Eq2	$pot(X, Y+1) = X \cdot pot(X, Y)$

Lema: $\forall X, M, N \in \mathbb{N}\ (pot(X, M+N) = pot(X, M) \cdot pot(X, N))$

$P(M) \equiv \forall X, N \in \mathbb{N}\ (pot(X, M+N) = pot(X, M) \cdot pot(X, N))$

Caso base P(M)

Provar: $\forall X, N \in \mathbb{N}\ (pot(X, 0+N) = pot(X, 0) \cdot pot(X, N))$

$pot(X, 0+N) = pot(X, N)$ ⟶ por propriedades algébricas

$= 1 \cdot pot(X, N)$ ⟶ por propriedades algébricas

$= pot(X, 0) \cdot pot(X, N)$ ⟶ por Eq1

q.e.d

Caso indutivo $P(M) \rightarrow P(M+1)$

Provar: $\forall X, N \in \mathbb{N}$ (pot(X, (M + 1) + N) = pot(X, M + 1) . pot(X, N))

Assumir HI: pot(X, M + N) = pot(X, M) . pot(X, N)

pot(X , (M + 1) + N) = pot(X , M + 1 + N) $\rightarrow$ associatividade da soma

= X . pot(X , M + N) $\rightarrow$ pela definição recursiva de pot

= X . (pot(X , M). pot(X , N)) $\rightarrow$ HI

= pot(X , M + 1). pot(X , N) $\rightarrow$ por Eq2

q.e.d

Teorema: $\forall X, M, N \in \mathbb{N}$ (pot(X , M . N) = pot(pot(X , M) , N))

$P(N) \equiv \forall X, M \in \mathbb{N}$ (pot(X , M . N) = pot(pot(X , M) , N))

Caso base P(0)

Provar: $\forall X, M \in \mathbb{N}$ (pot(X , M . 0) = pot(pot(X , M) , 0))

pot(X , M . 0) = pot(X , 0) $\rightarrow$ por propriedades algébricas

= 1 $\rightarrow$ por Eq1

= pot(pot(X , M) , 0) $\rightarrow$ por propriedades algébricas, para qualquer pot(X , M) elevado a 0 vai dar 1

q.e.d

Caso indutivo $P(N) \rightarrow P(N+1)$

Provar: $\forall X, M \in \mathbb{N}\ (pot(X, M \cdot (N+1)) = pot(pot(X, M), N+1))$

Assumir HI: $pot(X, M \cdot N) = pot(pot(X, M), N)$

$pot(X, M \cdot (N+1)) = pot(X, M \cdot N + M)$	$\longrightarrow$ por propriedades algébricas
$= pot(X, M \cdot N) \cdot pot(X, M)$	$\longrightarrow$ por Lema
$= pot(pot(X, M), N) \cdot pot(X, M)$	$\longrightarrow$ HI
$= pot(pot(X, M), N+1)$	$\longrightarrow$ por Eq2

q.e.d

2) Prova formal por indução de funções recursivas sobre listas:

Definição Recursiva para Cat

Cat_Eq1	cat([ ], Ys) = Ys
Cat_Eq2	cat(X : Xs, Ys) = X : cat(Xs, Ys)

Definição Recursiva para reverso

Rev_Eq1	reverso([ ]) = [ ]
Rev_Eq2	reverso(X : Xs)= cat(reverso(Xs), [X])

Definição Recursiva para somatorio	
Som_Eq1	somatorio([ ]) = 0
Som_Eq2	somatorio(X : Xs) = X + somatorio(Xs)

Lema: $\forall Xs, Ys \in List(\mathbb{N})$ (somatorio(cat(Xs, Ys)) = somatorio(Xs) + somatorio(Ys))

P(xs) $\equiv \forall Ys \in List(\mathbb{N})$ (somatorio(cat(Xs, Ys)) = somatorio(Xs) + somatorio(Ys))

Caso base P([ ])

Provar: $\forall Ys \in List(\mathbb{N})$ (somatorio(cat([ ] , Ys)) = somatorio([ ]) + somatorio(Ys))

somatorio(cat([ ] , Ys)) = somatorio(Ys) $\longrightarrow$ por Cat_Eq1
= 0 + somatorio(Ys) $\longrightarrow$ por Som_Eq1
= somatorio([ ]) + somatorio(Ys) $\longrightarrow$ por Som_Eq1

q.e.d

Caso indutivo P(Xs) $\rightarrow$ P(x : Xs)

Provar: $\forall Ys \in List(\mathbb{N})$ (somatorio(cat(x : Xs, Ys)) = somatorio(x : Xs) + somatorio(Ys))

Assumir HI: somatorio(cat(Xs, Ys)) = somatorio(Xs) + somatorio(Ys)

somatorio(cat(x : Xs, Ys)) = somatorio(x : cat(Xs, Ys)) $\longrightarrow$ por Cat_Eq2
= x + somatorio(cat(Xs, Ys)) $\longrightarrow$ por Som_Eq2
= x + (somatorio(Xs) + somatorio(Ys)) $\longrightarrow$ pela HI
= (x + somatorio(Xs)) + somatorio(Ys) $\longrightarrow$ por associatividade da soma
= somatorio(x : Xs) + somatorio(Ys) $\longrightarrow$ por Som_Eq2

q.e.d

Teorema: $\forall Xs \in List(\mathbb{N})$ (somatorio(reverso(Xs)) = somatorio(Xs))

$P(Xs) \equiv \forall Xs \in List(\mathbb{N})$ (somatorio(reverso(Xs)) = somatorio(Xs))

Caso base P([ ])
Provar: somatorio(reverso([ ])) = somatorio([ ])
somatorio(reverso([ ]))= somatorio([]) $\longrightarrow$ por Rev_Eq1 q.e.d

Caso indutivo P(Xs) → P(x : Xs)
Provar: $\forall Xs \in List(\mathbb{N})$ (somatorio(reverso(x : Xs)) = somatorio(x : Xs)) Assumir HI: somatorio(reverso(Xs)) = somatorio(Xs)
somatorio(reverso(x : Xs)) = somatorio(cat(reverso(Xs), [x])) $\longrightarrow$ por Rev_Eq2 = somatorio(reverso(Xs)) + somatorio([x]) $\longrightarrow$ por lema = somatorio(Xs) + somatorio([x]) $\longrightarrow$ pela HI = somatorio(Xs) + x $\longrightarrow$ por propriedades algébricas = somatorio(x : Xs) $\longrightarrow$ por Som_Eq2 q.e.d