

Cálculo de Programas

Trabalho Prático

LCC — 2021/22 (2º semestre)

Departamento de Informática
Universidade do Minho

Junho de 2022

Grupo nr. 51

a91640	Beatriz Fernandes Oliveira
a87973	João Ricardo Rodrigues Nogueira
a90416	Miguel André Carvalho Gonçalves

1 Preâmbulo

Cálculo de Programas tem como objectivo principal ensinar a programação de computadores como uma disciplina científica. Para isso, baseia-se num repertório de *combinadores* que formam uma álgebra da programação (conjunto de leis universais e seus corolários) e usa esses combinadores para construir programas *composicionalmente*, isto é, agregando programas já existentes.

Na sequência pedagógica dos planos de estudo dos cursos que têm esta disciplina, opta-se pela aplicação deste método à programação em **Haskell** (sem prejuízo da sua aplicação a outras linguagens funcionais). Assim, o presente trabalho prático coloca os alunos perante problemas concretos que deverão ser implementados em **Haskell**. Há ainda um outro objectivo: o de ensinar a documentar programas, a validá-los e a produzir textos técnico-científicos de qualidade.

Antes de abordarem os problemas propostos no trabalho, os grupos devem ler com atenção o anexo [A](#) onde encontrarão as instruções relativas ao software a instalar, etc.

Problema 1

O algoritmo da *divisão Euclidiana*,

$$\begin{aligned}ed\ (n, 0) &= \text{Nothing} \\ed\ (n, d + 1) &= (\text{Just} \cdot \pi_1)\ (aux\ d\ n)\end{aligned}$$

dá erro quando o denominador d é zero, recorrendo à função auxiliar seguinte nos outros casos, paramétrica em d :

$$aux\ d = \langle q\ d, \langle r\ d, c\ d \rangle \rangle$$

Esta, por sua vez, é o emparelhamento das seguintes funções mutuamente recursivas,

$$\begin{aligned}q\ d\ 0 &= 0 \\q\ d\ (n + 1) &= q\ d\ n + (\text{if } x \equiv 0 \text{ then } 1 \text{ else } 0) \text{ where } x = c\ d\ n \\r\ d\ 0 &= 0 \\r\ d\ (n + 1) &= \text{if } x \equiv 0 \text{ then } 0 \text{ else } 1 + r\ d\ n \text{ where } x = c\ d\ n \\c\ d\ 0 &= d \\c\ d\ (n + 1) &= \text{if } x \equiv 0 \text{ then } d \text{ else } x - 1 \text{ where } x = c\ d\ n\end{aligned}$$

onde q colabora na produção do quociente, r na produção do resto, e c é uma função de controlo — todas paramétricas no denominador d .

Mostre, por aplicação da lei de recursividade mútua, que *aux d* é a mesma função que o ciclo-for seguinte:

```
loop d = for (g d) (0, (0, d)) where
  g d (q, (r, 0)) = (q + 1, (0, d))
  g d (q, (r, c + 1)) = (q, (r + 1, c))
```

Sugestão: consultar o anexo [B](#).

Problema 2

Considere o seguinte desafio, extraído de [O Bebras - Castor Informático](#) (edição 2020):

11 — Robôs e Pedras Preciosas A Alice e o Bob estão a controlar um robô num labirinto com pedras preciosas. O robô começa na localização indicada na figura abaixo [Fig. 1]. O robô segue um caminho até encontrar uma bifurcação. Um dos jogadores decide qual dos caminhos (esquerda ou direita) o robô deve tomar. Depois, o robô segue esse caminho até encontrar outra bifurcação, e assim consecutivamente (o robô nunca volta para trás no seu caminho).

A Alice e o Bob decidem à vez qual a direção a seguir, com a Alice a começar, o Bob decidindo a 2ª bifurcação, a Alice a 3ª e por aí adiante. O jogo termina quando o robô chegar ao final de um caminho sem saída, com o robô a recolher todas as pedras preciosas que aí encontrar. A Alice quer que o robô acabe o jogo com o maior número possível de pedras preciosas, enquanto que o Bob quer que o robô acabe o jogo com o menor número possível de pedras preciosas.

A Alice e o Bob sabem que cada um vai tentar ser mais esperto que o outro. Por isso se, por exemplo, o Bob redirecionar o robô para uma bifurcação onde é possível recolher 3 ou 7 pedras preciosas, ele sabe que a Alice vai comandar o robô escolhendo o caminho que leva às 7 pedras preciosas.

O labirinto deste desafio (Fig. 1) configura uma árvore binária de tipo *LTree* cujas folhas têm o número de pedras preciosas do correspondente caminho:¹

```
t = Fork (
  Fork (
    Fork (Leaf 2, Leaf 7),
    Fork (Leaf 5, Leaf 4)),
  Fork (
    Fork (Leaf 8, Leaf 6),
    Fork (Leaf 1, Leaf 3))
)
```

1. Defina como catamorfismo de *LTree*'s a função $\text{both} :: \text{LTree Int} \rightarrow \text{Int} \times \text{Int}$ tal que

$$(a, b) = \text{both } t$$

dê,

- em *a*: o resultado mais favorável à Alice, quando esta é a primeira a jogar, tendo em conta as jogadas do Bob e as suas;
- em *b*: o resultado mais favorável ao Bob, quando este é o primeiro a jogar, tendo em conta as jogadas da Alice e as suas.

2. De seguida, extraia (por recursividade mútua) as funções (recursivas) *alice* e *bob* tais que

$$\text{both} = \langle \text{alice}, \text{bob} \rangle$$

(Alternativamente, poderá codificar *alice* e *bob* em primeiro lugar e depois juntá-las num catamorfismo recorrendo às leis da recursividade mútua.)

¹Abstracção: as diferentes pedras preciosas são irrelevantes, basta o seu número.



Figure 1: Labirinto de “Robôs e Pedras Preciosas”.

Problema 3

O **triângulo de Sierpinski** (Fig. 2) é uma figura geométrica **fractal** em que um triângulo se subdivide recursivamente em sub-triângulos, da seguinte forma: considere-se um triângulo rectângulo e isósceles A cujos catetos têm comprimento s . A estrutura **fractal** é criada desenhando-se três triângulos no interior de A , todos eles rectângulos e isósceles e com catetos de comprimento $s \div 2$. Este passo é depois repetido para cada um dos triângulos desenhados e assim sucessivamente (Fig. 3).



Figure 2: Um triângulo de Sierpinski com profundidade 4.

Um triângulo de Sierpinski é gerado repetindo-se infinitamente o processo acima descrito; no entanto para efeitos de visualização é conveniente parar o processo recursivo a um determinado nível.

A figura a desenhar é constituída por triângulos todos da mesma dimensão (por exemplo, no quarto triângulo da Fig. 3 desenharam-se 27 triângulos). Seja cada triângulo geometricamente descrito pelas coordenadas do seu vértice inferior esquerdo e o comprimento dos seus catetos:

type $Tri = (Point, Side)$

onde

type $Side = Int$

type $Point = (Int, Int)$



Figure 3: Construção de um triângulo de Sierpinski

A estrutura recursiva que suporta a criação de **triângulos de Sierpinski** é captada por uma árvore ternária,

```
data LTree3 a = Tri a | Nodo (LTree3 a) (LTree3 a) (LTree3 a) deriving (Eq, Show)
```

em cujas folhas se irão encontrar os triângulos mais pequenos, todos da mesma dimensão, que deverão ser desenhados. Apenas estes conterão informação de carácter geométrico, tendo os nós da árvore um papel exclusivamente estrutural. Portanto, a informação geométrica guardada em cada folha consiste nas coordenadas do vértice inferior esquerdo e no cateto do respectivo triângulo. A função

```
sierpinski :: (Tri, Int) → [Tri]
sierpinski = folhasSierp · geraSierp
```

recebe a informação do triângulo exterior e a profundidade pretendida, que funciona como critério de paragem do processo de construção do fractal. O seu resultado é a lista de triângulos a desenhar.

Esta função é um hilomorfismo do tipo LTree3, i.e. a composição de duas funções: uma que gera LTree3s,

```
geraSierp :: (Tri, Int) → LTree3 Tri
geraSierp = anaLTree3 g2
```

e outra que as consome:

```
folhasSierp :: LTree3 Tri → [Tri]
folhasSierp = cataLTree3 g1
```

Trabalho a realizar:

1. Desenvolver a biblioteca *pointfree* para o tipo LTree3 de forma análoga a outras bibliotecas que conhece (eg. **BTree**, **LTree**, etc).
2. Definir os genes g_1 e g_2 do hilomorfismo *sierpinski*.
3. Correr

```
teste = desenha (sierpinski (base, 3))
```

para verificar a correcta geração de triângulos de Sierpinski em [SVG](#)², onde *desenha* é uma função dada no anexo [D](#) que, para o argumento *sierpinski* (*base*, 3), deverá produzir o triângulo colorido da Fig. 2.³

Problema 4

Os computadores digitais baseiam-se na representação Booleana da informação, isto é, sob a forma de *bits* que podem ter dois valores, vulg. 0 e 1. Um problema muito frequente é o de os bits se alterarem, devido a ruído ao nível electrónico. Essas alterações espúrias designam-se *bit-flips* e podem acontecer a qualquer nível: na transmissão de informação, na gravação em disco, etc, etc.

Em contraste com essas perturbações, o utilizador de serviços informáticos raramente dá pela sua presença. Porquê? Porque existe muito trabalho teórico em correcção dos erros gerados por *bit-flips*, que os permite esconder do utilizador.

O objectivo desta questão é conseguirmos avaliar experimentalmente o funcionamento de uma dessas técnicas de correcção de erros, a mais elementar de todas, chamada *código de repetição*, escrevendo tão pouco código ([Haskell](#)) quanto possível. Para isso vamos recorrer ao mónade das *distribuições probabilísticas* (detalhes no apêndice [C](#)).

Vamos supor que queremos medir a eficácia de um tal código na situação seguinte: queremos transmitir mensagens que constam exclusivamente de letras maiúsculas, representadas por 5 bits cada uma segundo o esquema seguinte de codificação,

```
enc :: Char → Bin
enc c = tobin (ord c - ord 'A')
```

e decodificação,

```
dec :: Bin → Char
dec b = chr (frombin b + ord 'A')
```

onde *tobin* e *frombin* são funções dadas no anexo [D](#). Por exemplo,

```
enc 'A' = [0,0,0,0,0]
enc 'B' = [0,0,0,0,1]
⋮
enc 'Z' = [1,1,0,0,1]
```

Embora *dec* e *enc* sejam inversas uma da outra, para o intervalo de 'A' a 'Z', deixam de o ser quando, a meio da transmissão, acontecem bit-flips:



Vejam os quantificar "os estragos". Sabendo-se, por exemplo e por observação estatística, que a probabilidade de um 0 virar 1 é de 4% e a de 1 virar 0 é de 10%⁴, simula-se essa informação sobre a forma de uma função probabilística, em Haskell:

```
bflip :: Bit → Dist Bit
bflip 0 = D [(0, 0.96), (1, 0.04)]
bflip 1 = D [(1, 0.90), (0, 0.10)]
```

Agora vamos simular o envio de caracteres. O que devia ser *transmit* = *dec* · *enc* vai ter agora que prever a existência de possíveis bit-flips no meio da transmissão:

```
transmit = dec' · propagate bflip · enc
```

Por exemplo, *transmit* 'H' irá dar a seguinte distribuição:

²[SVG](#), abreviatura de *Scalable Vector Graphics*, é um dialecto de [XML](#) para computação gráfica. A biblioteca *Svg.hs* (fornecida) faz uma interface rudimentar entre [Haskell](#) e [SVG](#).

³O resultado é gravado no ficheiro `_ .html`, que pode ser visualizado num browser. Poderão ser feitos testes com outros níveis de profundidade.

⁴Estas probabilidades, na prática muito mais baixas, estão inflacionadas para mais fácil observação.

'H'	67.2%
'D'	7.5%
'F'	7.5%
'G'	7.5%
'P'	2.8%
'X'	2.8%
'E'	0.8%
'B'	0.8%
'C'	0.8%
'L'	0.3%
'N'	0.3%
'O'	0.3%
'T'	0.3%
'V'	0.3%
'W'	0.3%
' '	0.1%
'A'	0.1%

A saída 'H', que se esperava com 100% de certeza, agora só ocorrerá, estatisticamente, com a probabilidade de 67.2%, consequência dos bit-flips, havendo um âmbito bastante grande de respostas erradas, mas com probabilidades mais baixas.

1. Trabalho a fazer: completar a definição do catamorfismo de listas *propagate*.

O que se pode fazer quanto a estes erros de transmissão? Os chamados códigos de repetição enviam cada bit um número ímpar de vezes, tipicamente 3 vezes. Cada um desses três bits (que na origem são todos iguais) está sujeito a bit-flips. O que se faz é *votar* no mais frequente — ver função v_3 no anexo. Se agora a transmissão do 'H' for feita em triplicado, usando

$$transmit3 = dec' \cdot propagate3 \cdot bflip3 \cdot enc$$

ter-se-á:

```
Main> transmit3 'H'
'H' 91.0%
'F' 2.6%
'G' 2.6%
'D' 2.6%
'P' 0.4%
'X' 0.4%
'B' 0.1%
'C' 0.1%
'E' 0.1%
```

Vê-se que a probabilidade da resposta certa aumentou muito, para 91%, com redução também do espectro de respostas erradas.

2. Trabalho a fazer: completar a definição do catamorfismo de listas *propagate3* e da função *bflip3*.

Apesar da sua eficácia, esta técnica de correcção de erros é dispendiosa, obrigando o envio do triplo dos bits. Isso levou a comunidade científica a encontrar formas mais sofisticadas para resolver o mesmo problema sem tal “overhead”. Quem estiver interessado em saber mais sobre este fascinante tópico poderá começar por visualizar este [vídeo](#) no YouTube.

Anexos

A Documentação para realizar o trabalho

Para cumprir de forma integrada os objectivos do trabalho vamos recorrer a uma técnica de programação dita “*literária*” [2], cujo princípio base é o seguinte:

Um programa e a sua documentação devem coincidir.

Por outras palavras, o código fonte e a documentação de um programa deverão estar no mesmo ficheiro.

O ficheiro `cp2122t.pdf` que está a ler é já um exemplo de **programação literária**: foi gerado a partir do texto fonte `cp2122t.lhs`⁵ que encontrará no **material pedagógico** desta disciplina descompactando o ficheiro `cp2122t.zip` e executando:

```
$ lhs2TeX cp2122t.lhs > cp2122t.tex
$ pdflatex cp2122t
```

em que `lhs2tex` é um pre-processor que faz “pretty printing” de código Haskell em **L^AT_EX** e que deve desde já instalar utilizando o utilitário **cabal** disponível em haskell.org.

Por outro lado, o mesmo ficheiro `cp2122t.lhs` é executável e contém o “kit” básico, escrito em **Haskell**, para realizar o trabalho. Basta executar

```
$ ghci cp2122t.lhs
```

Abra o ficheiro `cp2122t.lhs` no seu editor de texto preferido e verifique que assim é: todo o texto que se encontra dentro do ambiente

```
\begin{code}
...
\end{code}
```

é seleccionado pelo **GHCi** para ser executado.

A.1 Como realizar o trabalho

Este trabalho teórico-prático deve ser realizado por grupos de 3 (ou 4) alunos. Os detalhes da avaliação (datas para submissão do relatório e sua defesa oral) são os que forem publicados na **página da disciplina** na *internet*.

Recomenda-se uma abordagem participativa dos membros do grupo em todos os exercícios do trabalho, para assim poderem responder a qualquer questão colocada na *defesa oral* do relatório.

Em que consiste, então, o *relatório* a que se refere o parágrafo anterior? É a edição do texto que está a ser lido, preenchendo o anexo **E** com as respostas. O relatório deverá conter ainda a identificação dos membros do grupo de trabalho, no local respectivo da folha de rosto.

Para gerar o PDF integral do relatório deve-se ainda correr os comando seguintes, que actualizam a bibliografia (com **BibT_EX**) e o índice remissivo (com **makeindex**),

```
$ bibtex cp2122t.aux
$ makeindex cp2122t.idx
```

e recompilar o texto como acima se indicou.

No anexo **D** disponibiliza-se algum código **Haskell** relativo aos problemas que se seguem. Esse anexo deverá ser consultado e analisado à medida que isso for necessário.

A.2 Como exprimir cálculos e diagramas em LaTeX/lhs2tex

Como primeiro exemplo, estudar o texto fonte deste trabalho para obter o efeito:⁶

$$\begin{aligned} id &= \langle f, g \rangle \\ \equiv & \quad \{ \text{universal property} \} \\ & \left\{ \begin{array}{l} \pi_1 \cdot id = f \\ \pi_2 \cdot id = g \end{array} \right. \\ \equiv & \quad \{ \text{identity} \} \\ & \left\{ \begin{array}{l} \pi_1 = f \\ \pi_2 = g \end{array} \right. \\ & \square \end{aligned}$$

⁵O sufixo ‘lhs’ quer dizer *literate Haskell*.

⁶Exemplos tirados de [3].

Os diagramas podem ser produzidos recorrendo à *package* L^AT_EX *xymatrix*, por exemplo:

$$\begin{array}{ccc} \mathbb{N}_0 & \xleftarrow{\text{in}} & 1 + \mathbb{N}_0 \\ \downarrow \langle g \rangle & & \downarrow id + \langle g \rangle \\ B & \xleftarrow{g} & 1 + B \end{array}$$

B Regra prática para a recursividade mútua em \mathbb{N}_0

Nesta disciplina estudou-se como fazer **programação dinâmica** por cálculo, recorrendo à lei de recursividade mútua.⁷

Para o caso de funções sobre os números naturais (\mathbb{N}_0 , com functor $F X = 1 + X$) é fácil derivar-se da lei que foi estudada uma *regra de algibeira* que se pode ensinar a programadores que não tenham estudado **Cálculo de Programas**. Apresenta-se de seguida essa regra, tomando como exemplo o cálculo do ciclo-for que implementa a função de Fibonacci, recordar o sistema:

$$\begin{aligned} fib\ 0 &= 1 \\ fib\ (n + 1) &= f\ n \\ f\ 0 &= 1 \\ f\ (n + 1) &= fib\ n + f\ n \end{aligned}$$

Obter-se-á de imediato

$$\begin{aligned} fib' &= \pi_1 \cdot \text{for loop init where} \\ &\quad \text{loop } (fib, f) = (f, fib + f) \\ &\quad \text{init} = (1, 1) \end{aligned}$$

usando as regras seguintes:

- O corpo do ciclo *loop* terá tantos argumentos quanto o número de funções mutuamente recursivas.
- Para as variáveis escolhem-se os próprios nomes das funções, pela ordem que se achar conveniente.⁸
- Para os resultados vão-se buscar as expressões respectivas, retirando a variável n .
- Em *init* colecionam-se os resultados dos casos de base das funções, pela mesma ordem.

Mais um exemplo, envolvendo polinómios do segundo grau $ax^2 + bx + c$ em \mathbb{N}_0 . Seguindo o método estudado nas aulas⁹, de $f\ x = ax^2 + bx + c$ derivam-se duas funções mutuamente recursivas:

$$\begin{aligned} f\ 0 &= c \\ f\ (n + 1) &= f\ n + k\ n \\ k\ 0 &= a + b \\ k\ (n + 1) &= k\ n + 2\ a \end{aligned}$$

Seguindo a regra acima, calcula-se de imediato a seguinte implementação, em Haskell:

$$\begin{aligned} f'\ a\ b\ c &= \pi_1 \cdot \text{for loop init where} \\ &\quad \text{loop } (f, k) = (f + k, k + 2 * a) \\ &\quad \text{init} = (c, a + b) \end{aligned}$$

⁷Lei (3.93) em [3], página 110.

⁸Podem obviamente usar-se outros símbolos, mas numa primeira leitura dá jeito usarem-se tais nomes.

⁹Secção 3.17 de [3] e tópico **Recursividade mútua** nos vídeos de apoio às aulas teóricas.

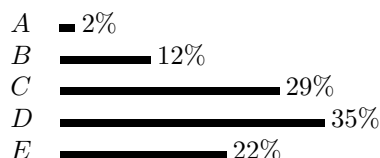
C O mónade das distribuições probabilísticas

Mónades são funtores com propriedades adicionais que nos permitem obter efeitos especiais em programação. Por exemplo, a biblioteca **Probability** oferece um mónade para abordar problemas de probabilidades. Nesta biblioteca, o conceito de distribuição estatística é captado pelo tipo

$$\text{newtype Dist } a = D \{ unD :: [(a, ProbRep)] \} \quad (1)$$

em que $ProbRep$ é um real de 0 a 1, equivalente a uma escala de 0 a 100%.

Cada par (a, p) numa distribuição $d :: \text{Dist } a$ indica que a probabilidade de a é p , devendo ser garantida a propriedade de que todas as probabilidades de d somam 100%. Por exemplo, a seguinte distribuição de classificações por escalões de A a E ,



será representada pela distribuição

$$d_1 :: \text{Dist Char}$$

$$d_1 = D [('A', 0.02), ('B', 0.12), ('C', 0.29), ('D', 0.35), ('E', 0.22)]$$

que o **GHCi** mostrará assim:

'D'	35.0%
'C'	29.0%
'E'	22.0%
'B'	12.0%
'A'	2.0%

É possível definir geradores de distribuições, por exemplo distribuições *uniformes*,

$$d_2 = \text{uniform}(\text{words "Uma frase de cinco palavras"})$$

isto é

"Uma"	20.0%
"cinco"	20.0%
"de"	20.0%
"frase"	20.0%
"palavras"	20.0%

distribuição *normais*, eg.

$$d_3 = normal [10..20]$$

etc.¹⁰ Dist forma um **mónade** cuja unidade é $\text{return } a = D [(a, 1)]$ e cuja composição de Kleisli é (simplificando a notação)

$$(f \bullet g) \ a = [(y, q * p) \mid (x, p) \leftarrow g \ a, (y, q) \leftarrow f \ x]$$

em que $g:A \rightarrow \text{Dist } B$ e $f:B \rightarrow \text{Dist } C$ são funções **monádicas** que representam *computações probabilísticas*.

Este mónade é adequado à resolução de problemas de *probabilidades e estatística* usando programação funcional, de forma elegante e como caso particular da programação monádica.

¹⁰Para mais detalhes ver o código fonte de **Probability**, que é uma adaptação da biblioteca **PHP** (“Probabilistic Functional Programming”). Para quem quiser saber mais recomenda-se a leitura do artigo [1].

D Código fornecido

Problema 3

Triângulo de base:

$$base = ((0, 0), 32)$$

Desenho de triângulos em SVG:

$$desenha\ x = picd''\ [scale\ 0.44\ (0, 0)\ (x \gg tri2svg)]$$

Função que representa cada triângulo em SVG:

$$\begin{aligned} tri2svg &:: Tri \rightarrow Svg \\ tri2svg\ (p, c) &= (red \cdot polyg)\ [p, p \cdot + (0, c), p \cdot + (c, 0)] \end{aligned}$$

NB: o tipo *Svg* é sinónimo de *String*:

$$type\ Svg = String$$

Problema 4

Funções básicas:

$$\begin{aligned} type\ Bit &= Int \\ type\ Bin &= [Bit] \\ type\ Bit3 &= (Bit, Bit, Bit) \\ tobin &= rtrim\ 5 \cdot pad\ 5 \cdot dec2bin \\ frombin &= bin2dec \cdot rtrim\ 5 \\ bin2dec &:: Bin \rightarrow Int \\ bin2dec\ [a] &= a \\ bin2dec\ b &= bin2dec\ (init\ b) * 2 + last\ b \\ rtrim\ n\ a &= drop\ (length\ a - n)\ a \\ dec2bin\ 0 &= [] \\ dec2bin\ n &= dec2bin\ m ++ [b]\ \textbf{where}\ (m, b) = (n \div 2, mod\ n\ 2) \\ pad\ n\ x &= take\ m\ zeros ++ x\ \textbf{where} \\ &\quad m = n - length\ x \\ &\quad zeros = 0 : zeros \\ bflips &= propagate\ bflip \end{aligned}$$

Função que vota no bit mais frequente:

$$\begin{aligned} v_3\ (0, 0, 0) &= 0 \\ v_3\ (0, 0, 1) &= 0 \\ v_3\ (0, 1, 0) &= 0 \\ v_3\ (0, 1, 1) &= 1 \\ v_3\ (1, 0, 0) &= 0 \\ v_3\ (1, 0, 1) &= 1 \\ v_3\ (1, 1, 0) &= 1 \\ v_3\ (1, 1, 1) &= 1 \end{aligned}$$

Descodificação monádica:

$$dec' = fmap\ dec$$

Para visualização abreviada de distribuições:

$$\begin{aligned} consolidate &:: Eq\ a \Rightarrow Dist\ a \rightarrow Dist\ a \\ consolidate &= D \cdot filter\ q \cdot map\ (id \times sum) \cdot collect \cdot unD\ \textbf{where}\ q\ (a, p) = p > 0.001 \\ collect\ x &= nub\ [k \mapsto nub\ [d' \mid (k', d') \leftarrow x, k' \equiv k] \mid (k, d) \leftarrow x] \end{aligned}$$

E Soluções dos alunos

Problema 1

Para resolver este problema, é necessário definir-mos as funções dadas no enunciado em pointfree. Começemos, então, pela função $q\ d$.

$$\begin{aligned}
& \begin{cases} (q\ d)\ 0 = 0 \\ (q\ d)\ n + 1 = (q\ d)\ n + (\text{if } x \equiv 0 \text{ then } 1 \text{ else } 0) \text{ where } x = (c\ d)\ n \end{cases} \\
\equiv & \quad \{ \text{Def succ dada nas aulas} \} \\
& \begin{cases} (q\ d)\ 0 = 0 \\ (q\ d)\ (\text{succ } n) = (q\ d)\ n + \text{if } (c\ d)\ n \equiv 0 \text{ then } 1 \text{ else } 0 \end{cases} \\
\equiv & \quad \{ \text{Def-const (74)}, \forall x\ (c\ d)\ x \equiv 0 \equiv \forall x\ (c\ d)\ x\ (\equiv 0) \equiv \forall x\ (0 \equiv) \cdot (c\ d)\ x \equiv \forall x\ ((0 \equiv) \cdot (c\ d)) \} \\
& \begin{cases} (q\ d)\ (\underline{0}\ n) = \underline{0}\ n \\ (q\ d)\ (\text{succ } n) = (q\ d)\ n + \text{if } (((0 \equiv) \cdot (c\ d)))\ n \text{ then } \underline{1}\ n \text{ else } \underline{0}\ n \end{cases} \\
\equiv & \quad \{ \text{Def-comp (72), Def-cond (78)} \} \\
& \begin{cases} (q\ d) \cdot \underline{0}\ n = \underline{0}\ n \\ ((q\ d) \cdot \text{succ})\ n = (q\ d)\ n + ((0 \equiv) \cdot (cd) \Rightarrow \underline{1}, \underline{0})\ n \end{cases} \\
\equiv & \quad \{ \text{Uncurry (84)} \} \\
& \begin{cases} (q\ d) \cdot \underline{0}\ n = \underline{0}\ n \\ ((q\ d) \cdot \text{succ})\ n = \widehat{(+)}\ ((q\ d)\ n, ((0 \equiv) \cdot (cd) \Rightarrow \underline{1}, \underline{0})\ n) \end{cases} \\
\equiv & \quad \{ \text{Def-split (76)} \} \\
& \begin{cases} (q\ d) \cdot \underline{0}\ n = \underline{0}\ n \\ ((q\ d) \cdot \text{succ})\ n = \widehat{(+)} \cdot \langle q\ d, (0 \equiv) \cdot (cd) \Rightarrow \underline{1}, \underline{0} \rangle\ n \end{cases} \\
\equiv & \quad \{ \text{Igualdade extensional (71)} \} \\
& \begin{cases} (q\ d) \cdot \underline{0} = \underline{0} \\ (q\ d) \cdot \text{succ} = \widehat{(+)} \cdot \langle q\ d, (0 \equiv) \cdot (cd) \Rightarrow \underline{1}, \underline{0} \rangle \end{cases} \\
\equiv & \quad \{ \text{Def condicional de McCarthy (30)} \} \\
& \begin{cases} (q\ d) \cdot \underline{0} = \underline{0} \\ (q\ d) \cdot \text{succ} = \widehat{(+)} \cdot \langle q\ d, [\underline{1}, \underline{0}] \cdot ((0 \equiv) \cdot (cd))?\rangle \end{cases} \\
\equiv & \quad \{ \text{Eq-+ (27)} \} \\
& [(q\ d) \cdot \underline{0}, (q\ d) \cdot \text{succ}] = [\underline{0}, \widehat{(+)} \cdot \langle q\ d, [\underline{1}, \underline{0}] \cdot ((0 \equiv) \cdot (cd))?\rangle] \\
\equiv & \quad \{ \text{Fusão -+ (20)} \} \\
& (q\ d) \cdot [\underline{0}, \text{succ}] = [\underline{0}, \widehat{(+)} \cdot \langle q\ d, [\underline{1}, \underline{0}] \cdot ((0 \equiv) \cdot (cd))?\rangle] \\
& \square
\end{aligned}$$

Procederemos à obtenção de uma definição alternativa da função $(r\ d)$.

$$\begin{aligned}
& \begin{cases} (r\ d)\ 0 = 0 \\ (r\ d)\ (n + 1) = \text{if } x \equiv 0 \text{ then } 0 \text{ else } 1 + (r\ d)\ n \text{ where } x = (c\ d)\ n \end{cases} \\
\equiv & \quad \{ \text{Def succ dada nas aulas} \} \\
& \begin{cases} (r\ d)\ 0 = 0 \\ (r\ d)\ (\text{succ } n) = \text{if } (c\ d)\ n \equiv 0 \text{ then } 0 \text{ else } 1 + (r\ d)\ n \end{cases} \\
\equiv & \quad \{ \text{Def-const (74)}, \forall x\ (c\ d)\ x \equiv 0 \equiv \forall x\ (c\ d)\ x\ (\equiv 0) \equiv \forall x\ (0 \equiv) \cdot (c\ d)\ x \equiv \forall x\ ((0 \equiv) \cdot (c\ d)) \}
\end{aligned}$$

$$\begin{aligned}
& \begin{cases} (r\ d)\ (\underline{0}\ n) = \underline{0}\ n \\ (r\ d)\ (\text{succ}\ n) = \text{if } ((0 \equiv) \cdot (c\ d))\ n \text{ then } \underline{0}\ n \text{ else } \underline{1}\ n + (r\ d)\ n \end{cases} \\
\equiv & \quad \{ \text{Uncurry (84), Def-comp (72)} \} \\
& \begin{cases} (r\ d) \cdot \underline{0}\ n = \underline{0}\ n \\ ((r\ d) \cdot \text{succ})\ n = \text{if } ((0 \equiv) \cdot (c\ d))\ n \text{ then } \underline{0}\ n \text{ else } \widehat{(+)} (\underline{1}\ n, (r\ d)\ n) \end{cases} \\
\equiv & \quad \{ \text{Def-split (76)} \} \\
& \begin{cases} (r\ d) \cdot \underline{0}\ n = \underline{0}\ n \\ ((r\ d) \cdot \text{succ})\ n = \text{if } ((0 \equiv) \cdot (c\ d))\ n \text{ then } \underline{0}\ n \text{ else } \widehat{(+)} \cdot \langle \underline{1}, r\ d \rangle\ n \end{cases} \\
\equiv & \quad \{ \text{Def-cond (78)} \} \\
& \begin{cases} (r\ d) \cdot \underline{0}\ n = \underline{0}\ n \\ ((r\ d) \cdot \text{succ})\ n = (((0 \equiv) \cdot (c\ d)) \Rightarrow \underline{0}, \widehat{(+)} \cdot \langle \underline{1}, r\ d \rangle)\ n \end{cases} \\
\equiv & \quad \{ \text{Igualdade extensional (71)} \} \\
& \begin{cases} (r\ d) \cdot \underline{0} = \underline{0} \\ (r\ d) \cdot \text{succ} = (((0 \equiv) \cdot (c\ d)) \Rightarrow \underline{0}, \widehat{(+)} \cdot \langle \underline{1}, r\ d \rangle) \end{cases} \\
\equiv & \quad \{ \text{Def condicional de McCarthy (30)} \} \\
& \begin{cases} (r\ d) \cdot \underline{0} = \underline{0} \\ (r\ d) \cdot \text{succ} = [\underline{0}, \widehat{(+)} \cdot \langle \underline{1}, r\ d \rangle] \cdot ((0 \equiv) \cdot (c\ d))? \end{cases} \\
\equiv & \quad \{ \text{Eq - + (27)} \} \\
& [(r\ d) \cdot \underline{0}, (r\ d) \cdot \text{succ}] = [\underline{0}, [\underline{0}, \widehat{(+)} \cdot \langle \underline{1}, r\ d \rangle] \cdot ((0 \equiv) \cdot (c\ d))?] \\
\equiv & \quad \{ \text{Fusão - + (20)} \} \\
& (r\ d) \cdot [\underline{0}, \text{succ}] = [\underline{0}, [\underline{0}, \widehat{(+)} \cdot \langle \underline{1}, r\ d \rangle] \cdot ((0 \equiv) \cdot (c\ d))?] \\
& \square
\end{aligned}$$

Finalmente, aplicaremos o mesmo processo para a função (c d).

$$\begin{aligned}
& \begin{cases} (c\ d)\ 0 = d \\ (c\ d)\ (n + 1) = \text{if } x \equiv 0 \text{ then } d \text{ else } x - 1 \text{ where } x = (c\ d)\ n \end{cases} \\
\equiv & \quad \{ \text{Def succ dada nas aulas} \} \\
& \begin{cases} (c\ d)\ 0 = d \\ (c\ d)\ (\text{succ}\ n) = \text{if } (c\ d)\ n \equiv 0 \text{ then } d \text{ else } (c\ d)\ n - 1 \end{cases} \\
\equiv & \quad \{ \text{Def-const (74), } \forall x\ (c\ d)\ x \equiv 0 \equiv \forall x\ (c\ d)\ x\ (x \equiv 0) \equiv \forall x\ (0 \equiv) \cdot (c\ d)\ x \equiv \forall x\ ((0 \equiv) \cdot (c\ d)) \} \\
& \begin{cases} (c\ d)\ (\underline{0}\ n) = \underline{d}\ n \\ (c\ d)\ (\text{succ}\ n) = \text{if } ((0 \equiv) \cdot (c\ d))\ n \text{ then } \underline{d}\ n \text{ else } (c\ d)\ n - (\underline{1}\ n) \end{cases} \\
\equiv & \quad \{ \text{Uncurry (84), Def-comp (72)} \} \\
& \begin{cases} (c\ d) \cdot \underline{0}\ n = \underline{d}\ n \\ ((c\ d) \cdot \text{succ})\ n = \text{if } ((0 \equiv) \cdot (c\ d))\ n \text{ then } \underline{d}\ n \text{ else } \widehat{(-)} ((c\ d)\ n, \underline{1}\ n) \end{cases} \\
\equiv & \quad \{ \text{Def-split (76)} \} \\
& \begin{cases} (c\ d) \cdot \underline{0}\ n = \underline{d}\ n \\ ((c\ d) \cdot \text{succ})\ n = \text{if } ((0 \equiv) \cdot (c\ d))\ n \text{ then } \underline{d}\ n \text{ else } \widehat{(-)} \cdot \langle (c\ d), \underline{1} \rangle\ n \end{cases} \\
\equiv & \quad \{ \text{Def-cond (78)} \} \\
& \begin{cases} (c\ d) \cdot \underline{0}\ n = \underline{d}\ n \\ ((c\ d) \cdot \text{succ})\ n = (((0 \equiv) \cdot (c\ d)) \Rightarrow \underline{d}, \widehat{(-)} \cdot \langle (c\ d), \underline{1} \rangle)\ n \end{cases}
\end{aligned}$$

$$\begin{aligned}
&\equiv \{ \text{Igualdade extensional (71)} \} \\
&\quad \left\{ \begin{array}{l} (c \ d) \cdot \underline{0} = \underline{d} \\ (c \ d) \cdot \text{succ} = (((0 \equiv) \cdot (c \ d)) \Rightarrow \underline{d}, \widehat{(-)} \cdot \langle (c \ d), \underline{1} \rangle) \end{array} \right. \\
&\equiv \{ \text{Def condicional de McCarthy (30)} \} \\
&\quad \left\{ \begin{array}{l} (c \ d) \cdot \underline{0} = \underline{d} \\ (c \ d) \cdot \text{succ} = [\underline{d}, \widehat{(-)} \cdot \langle (c \ d), \underline{1} \rangle] \cdot ((0 \equiv) \cdot (c \ d))? \end{array} \right. \\
&\equiv \{ \text{Eq - + (27)} \} \\
&\quad [(c \ d) \cdot \underline{0}, (c \ d) \cdot \text{succ}] = [\underline{d}, [\underline{d}, \widehat{(-)} \cdot \langle (c \ d), \underline{1} \rangle] \cdot ((0 \equiv) \cdot (c \ d))]? \\
&\equiv \{ \text{Fusão - + (20)} \} \\
&\quad (c \ d) \cdot [\underline{0}, \text{succ}] = [\underline{d}, [\underline{d}, \widehat{(-)} \cdot \langle (c \ d), \underline{1} \rangle] \cdot ((0 \equiv) \cdot (c \ d))]? \\
&\square
\end{aligned}$$

Por aplicação da lei de recursividade mútua em aux temos:

$$\begin{aligned}
&\equiv \{ \text{Fokkinga (52)} \} \\
&\quad \left\{ \begin{array}{l} (q \ d) \cdot \text{in} = h \cdot F \langle q \ d, \langle r \ d, c \ d \rangle \rangle \\ (r \ d) \cdot \text{in} = k \cdot F \langle q \ d, \langle r \ d, c \ d \rangle \rangle \\ (c \ d) \cdot \text{in} = l \cdot F \langle q \ d, \langle r \ d, c \ d \rangle \rangle \end{array} \right. \\
&\equiv \{ \text{Def in, } F \langle (q \ d), \langle (r \ d), (c \ d) \rangle \rangle \} \\
&\quad \left\{ \begin{array}{l} (q \ d) \cdot [\underline{0}, \text{succ}] = h \cdot (id + \langle q \ d, \langle r \ d, c \ d \rangle \rangle) \\ (r \ d) \cdot [\underline{0}, \text{succ}] = k \cdot (id + \langle q \ d, \langle r \ d, c \ d \rangle \rangle) \\ (c \ d) \cdot [\underline{0}, \text{succ}] = l \cdot (id + \langle q \ d, \langle r \ d, c \ d \rangle \rangle) \end{array} \right. \\
&\equiv \{ \text{Fusão-+ (20), como o } F \langle (q \ d), \langle (r \ d), (c \ d) \rangle \rangle \text{ mapeia para uma soma, temos que h, k e l são eithers.} \} \\
&\quad \left\{ \begin{array}{l} [(q \ d) \cdot \underline{0}, (q \ d) \cdot \text{succ}] = [h_1, h_2] \cdot (id + \langle (q \ d), \langle (r \ d), (c \ d) \rangle \rangle) \\ [(r \ d) \cdot \underline{0}, (r \ d) \cdot \text{succ}] = [k_1, k_2] \cdot (id + \langle (q \ d), \langle (r \ d), (c \ d) \rangle \rangle) \\ [(c \ d) \cdot \underline{0}, (c \ d) \cdot \text{succ}] = [l_1, l_2] \cdot (id + \langle (q \ d), \langle (r \ d), (c \ d) \rangle \rangle) \end{array} \right. \\
&\equiv \{ \text{Absorção-+ (22), Natural-id (1)} \} \\
&\quad \left\{ \begin{array}{l} [(q \ d) \cdot \underline{0}, (q \ d) \cdot \text{succ}] = [h_1, h_2 \cdot \langle (q \ d), \langle (r \ d), (c \ d) \rangle \rangle] \\ [(r \ d) \cdot \underline{0}, (r \ d) \cdot \text{succ}] = [k_1, k_2 \cdot \langle (q \ d), \langle (r \ d), (c \ d) \rangle \rangle] \\ [(c \ d) \cdot \underline{0}, (c \ d) \cdot \text{succ}] = [l_1, l_2 \cdot \langle (q \ d), \langle (r \ d), (c \ d) \rangle \rangle] \end{array} \right. \\
&\square
\end{aligned}$$

Consideremos apenas um ramo do sistema de cada vez, com o intuito de facilitar a resolução da questão. Assim sendo, no primeiro ramo temos que:

$$\begin{aligned}
&[(q \ d) \cdot \underline{0}, (q \ d) \cdot \text{succ}] = [h_1, h_2 \cdot \langle (q \ d), \langle (r \ d), (c \ d) \rangle \rangle] \\
&\equiv \{ \text{Eq - + (27)} \} \\
&\quad \left\{ \begin{array}{l} (q \ d) \cdot \underline{0} = h_1 \\ (q \ d) \cdot \text{succ} = h_2 \cdot \langle q \ d, \langle r \ d, c \ d \rangle \rangle \end{array} \right. \\
&\equiv \{ \text{Como foi provado em cima, } (q \ d) \cdot \underline{0} = \underline{0}, \text{ Igualdade extensional (71), Def-comp (72), Def-split (76)} \} \\
&\quad \left\{ \begin{array}{l} \underline{0} = h_1 \\ (q \ d) (\text{succ } x) = h_2 (q \ d \ x, (r \ d \ x, c \ d \ x)) \end{array} \right. \\
&\equiv \{ \text{Como foi provado em cima, } (q \ d) \cdot \text{succ} = \widehat{(+)} \cdot \langle q \ d, [\underline{1}, \underline{0}] \cdot ((0 \equiv) \cdot (cd))? \} \\
&\quad \left\{ \begin{array}{l} \underline{0} = h_1 \\ \widehat{(+)} \cdot \langle q \ d, [\underline{1}, \underline{0}] \cdot ((0 \equiv) \cdot (cd))? = h_2 (q \ d \ x, (r \ d \ x, c \ d \ x)) \end{array} \right.
\end{aligned}$$

$$\begin{aligned}
&\equiv \{ \text{Eq} - + (27), \text{Fusao} - + (20) \} \\
&h \cdot [\underline{0}, \text{succ}] = [\underline{0}, \widehat{(+)} \cdot \langle q \ d, [\underline{1}, \underline{0}] \cdot ((0 \equiv) \cdot (cd)) \rangle] \\
&\square
\end{aligned}$$

Para o segundo ramo temos que:

$$\begin{aligned}
&[(r \ d) \cdot \underline{0}, (r \ d) \cdot \text{succ}] = [k_1, k_2 \cdot \langle (q \ d), \langle (r \ d), (c \ d) \rangle \rangle] \\
&\equiv \{ \text{Eq} - + (27) \} \\
&\begin{cases} (r \ d) \cdot \underline{0} = k_1 \\ (r \ d) \cdot \text{succ} = k_2 \cdot \langle q \ d, \langle r \ d, c \ d \rangle \rangle \end{cases} \\
&\equiv \{ \text{Como foi provado em cima, } (r \ d) \cdot \underline{0} = \underline{0}, \text{ Igualdade extensional (71), Def-comp (72), Def-split (76)} \} \\
&\begin{cases} \underline{0} = k_1 \\ (r \ d) (\text{succ } x) = k_2 (q \ d \ x, (r \ d \ x, c \ d \ x)) \end{cases} \\
&\equiv \{ \text{Como foi provado em cima, } (r \ d) \cdot \text{succ} = [\underline{0}, \widehat{(+)} \cdot \langle \underline{1}, r \ d \rangle] \cdot ((0 \equiv) \cdot (c \ d)) \} \\
&\begin{cases} \underline{0} = k_1 \\ [\underline{0}, \widehat{(+)} \cdot \langle \underline{1}, r \ d \rangle] \cdot ((0 \equiv) \cdot (c \ d)) = k_2 (q \ d \ x, (r \ d \ x, c \ d \ x)) \end{cases} \\
&\equiv \{ \text{Eq} - + (27), \text{Fusao} - + (20) \} \\
&k \cdot [\underline{0}, \text{succ}] = [\underline{0}, [\underline{0}, \widehat{(+)} \cdot \langle \underline{1}, r \ d \rangle] \cdot ((0 \equiv) \cdot (c \ d)) \cdot] \\
&\square
\end{aligned}$$

Finalmente, para o terceiro ramo:

$$\begin{aligned}
&[(c \ d) \cdot \underline{0}, (c \ d) \cdot \text{succ}] = [l_1, l_2 \cdot \langle (q \ d), \langle (r \ d), (c \ d) \rangle \rangle] \\
&\equiv \{ \text{Eq} - + (27) \} \\
&\begin{cases} (c \ d) \cdot \underline{0} = l_1 \\ (c \ d) \cdot \text{succ} = l_2 \cdot \langle q \ d, \langle r \ d, c \ d \rangle \rangle \end{cases} \\
&\equiv \{ \text{Como foi provado em cima, } (c \ d) \cdot \underline{0} = \underline{d}, \text{ Igualdade extensional (71), Def-comp (72), Def-split (76)} \} \\
&\begin{cases} \underline{d} = l_1 \\ (r \ d) (\text{succ } x) = l_2 (q \ d \ x, (r \ d \ x, c \ d \ x)) \end{cases} \\
&\equiv \{ \text{Como foi provado em cima, } (c \ d) \cdot \text{succ} = [\underline{d}, \widehat{(-)} \cdot \langle (c \ d), \underline{1} \rangle] \cdot ((0 \equiv) \cdot (c \ d)) \} \\
&\begin{cases} \underline{d} = l_1 \\ [\underline{d}, \widehat{(-)} \cdot \langle (c \ d), \underline{1} \rangle] \cdot ((0 \equiv) \cdot (c \ d)) = l_2 (q \ d \ x, (r \ d \ x, c \ d \ x)) \end{cases} \\
&\equiv \{ \text{Eq} - + (27), \text{Fusao} - + (20) \} \\
&l \cdot [\underline{0}, \text{succ}] = [\underline{d}, [\underline{d}, \widehat{(-)} \cdot \langle (c \ d), \underline{1} \rangle] \cdot ((0 \equiv) \cdot (c \ d)) \cdot] \\
&\square
\end{aligned}$$

Logo,

$$\begin{aligned}
&\equiv \{ \text{Fokkinga (52)} \} \\
&\langle (q \ d), \langle (r \ d), (c \ d) \rangle \rangle = \langle \langle h, \langle k, l \rangle \rangle \rangle \\
&\equiv \{ \text{Lei da troca (28)} \} \\
&\langle (q \ d), \langle (r \ d), (c \ d) \rangle \rangle = \langle \langle h, [(\langle \underline{0}, (\underline{d}) \rangle \langle k_2, l_2 \rangle), \cdot] \rangle \rangle \\
&\equiv \{ \text{Lei da troca (28)} \}
\end{aligned}$$

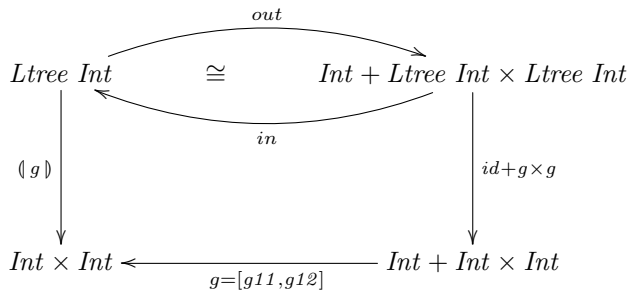
$$\begin{aligned}
& \langle (q \ d), \langle (r \ d), (c \ d) \rangle \rangle = \langle \langle \langle \underline{0}, \langle \underline{0}, \underline{d} \rangle \rangle, \langle \langle h_2, \langle k_2, l_2 \rangle \rangle \rangle \rangle \rangle \\
& \equiv \{ \text{for } \mathbf{b} \ \mathbf{i} = \langle [\underline{i}, b] \rangle \} \\
& \text{for } (h_2, (k_2, l_2)) \ (0, (0, d)) \\
& \square
\end{aligned}$$

Obter-se-á:

$$\text{for } g \ d \ 0, (0, d) \ \mathbf{where} \ (g \ d) \ (q, (r, 0)) = (g \ d) \ (q, (r, c + 1)) =$$

□

Problema 2



Assim sendo, pelo diagrama anterior podemos retirar a seguinte definição de g.

$$\begin{aligned}
& both :: Ord \ d \Rightarrow \textcolor{red}{LTree} \ d \rightarrow (d, d) \\
& both = \langle g \rangle \\
& g = [g11, g12] \\
& g11 \ x = (x, x) \\
& g12 \ ((a, b), (c, d)) = (a + c, b + d)
\end{aligned}$$

Para obtermos a definição das funções alice e bob, é necessário resolvermos a equação $\langle g \rangle = \langle alice, bob \rangle$ aplicando a lei da Recursividade Mútua. No entanto, primeiramente, é necessário transformar a nossa definição de g num split. Ora,

$$\begin{aligned}
& g \\
& \equiv \{ \text{Natural - id (1)} \} \\
& id \cdot g \\
& \equiv \{ \text{Reflexão - } \times \text{ (8)} \} \\
& \langle \pi_1, \pi_2 \rangle \cdot g \\
& \equiv \{ \text{Fusão - } \times \text{ (9)} \} \\
& \langle \pi_1 \cdot g, \pi_2 \cdot g \rangle
\end{aligned}$$

Assim sendo,

$$\begin{aligned}
& \langle g \rangle = \langle alice, bob \rangle \\
& \equiv \{ \text{Fokkinga (52)} \} \\
& \left\{ \begin{array}{l} alice = (\pi_1 \cdot g) \cdot F \ \langle alice, bob \rangle \\ bob = (\pi_2 \cdot g) \cdot F \ \langle alice, bob \rangle \end{array} \right. \\
& \equiv \{ \text{Base - Cata (49)} \} \\
& \left\{ \begin{array}{l} alice = (\pi_1 \cdot g) \cdot B \ (id, \langle alice, bob \rangle) \\ bob = (\pi_2 \cdot g) \cdot B \ (id, \langle alice, bob \rangle) \end{array} \right.
\end{aligned}$$

$$\begin{aligned}
&\equiv \{ B(id, \langle alice, bob \rangle) = id + \langle alice, bob \rangle \times \langle alice, bob \rangle \} \\
&\quad \left\{ \begin{array}{l} alice = (\pi_1 \cdot g) \cdot (id + \langle alice, bob \rangle \times \langle alice, bob \rangle) \\ bob = (\pi_2 \cdot g) \cdot (id + \langle alice, bob \rangle \times \langle alice, bob \rangle) \end{array} \right\} \\
&\equiv \{ \text{Def - + (21), Natural - id (1)} \} \\
&\quad \left\{ \begin{array}{l} alice = (\pi_1 \cdot g) \cdot [i_1, i_2 \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle)] \\ bob = (\pi_2 \cdot g) \cdot [i_1, i_2 \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle)] \end{array} \right\} \\
&\equiv \{ \text{Fusão - + (20)} \} \\
&\quad \left\{ \begin{array}{l} alice = [(\pi_1 \cdot g) \cdot i_1, (\pi_1 \cdot g) \cdot (i_2 \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle))] \\ bob = [(\pi_2 \cdot g) \cdot i_1, (\pi_2 \cdot g) \cdot (i_2 \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle))] \end{array} \right\} \\
&\equiv \{ \text{Assoc - comp (2)} \} \\
&\quad \left\{ \begin{array}{l} alice = [\pi_1 \cdot (g \cdot i_1), (\pi_1 \cdot g) \cdot (i_2 \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle))] \\ bob = [\pi_2 \cdot (g \cdot i_1), (\pi_2 \cdot g) \cdot (i_2 \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle))] \end{array} \right\} \\
&\equiv \{ \text{Universal - + (17)} \} \\
&\quad \left\{ \begin{array}{l} \left\{ \begin{array}{l} alice \cdot i_1 = \pi_1 \cdot (g \cdot i_1) \\ alice \cdot i_2 = (\pi_1 \cdot g) \cdot (i_2 \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle)) \\ bob \cdot i_1 = \pi_2 \cdot (g \cdot i_1) \\ bob \cdot i_2 = (\pi_2 \cdot g) \cdot (i_2 \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle)) \end{array} \right\} \end{array} \right\} \\
&\equiv \{ \text{Assoc - comp (2)} \} \\
&\quad \left\{ \begin{array}{l} \left\{ \begin{array}{l} alice \cdot i_1 = \pi_1 \cdot (g \cdot i_1) \\ alice \cdot i_2 = \pi_1 \cdot (g \cdot (i_2 \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle))) \\ bob \cdot i_1 = \pi_2 \cdot (g \cdot i_1) \\ bob \cdot i_2 = \pi_2 \cdot (g \cdot (i_2 \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle))) \end{array} \right\} \end{array} \right\} \\
&\equiv \{ \text{Assoc - comp (2)} \} \\
&\quad \left\{ \begin{array}{l} \left\{ \begin{array}{l} alice \cdot i_1 = \pi_1 \cdot (g \cdot i_1) \\ alice \cdot i_2 = \pi_1 \cdot ((g \cdot i_2) \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle)) \\ bob \cdot i_1 = \pi_2 \cdot (g \cdot i_1) \\ bob \cdot i_2 = \pi_2 \cdot ((g \cdot i_2) \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle)) \end{array} \right\} \end{array} \right\} \\
&\equiv \{ \text{Definição de } g : g = [g11, g12], \text{Cancelamento - + (18)} \} \\
&\quad \left\{ \begin{array}{l} \left\{ \begin{array}{l} alice \cdot i_1 = \pi_1 \cdot g11 \\ alice \cdot i_2 = \pi_1 \cdot (g12 \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle)) \\ bob \cdot i_1 = \pi_2 \cdot g11 \\ bob \cdot i_2 = \pi_2 \cdot (g12 \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle)) \end{array} \right\} \end{array} \right\} \\
&\equiv \{ \text{Igualdade Extensional (71)} \} \\
&\quad \left\{ \begin{array}{l} \left\{ \begin{array}{l} (alice \cdot i_1) z = (\pi_1 \cdot g11) z \\ (alice \cdot i_2) w = (\pi_1 \cdot (g12 \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle))) w \\ (bob \cdot i_1) z = (\pi_2 \cdot g11) z \\ (bob \cdot i_2) w = (\pi_2 \cdot (g12 \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle))) w \end{array} \right\} \end{array} \right\} \\
&\equiv \{ \text{Def-comp (72)} \} \\
&\quad \left\{ \begin{array}{l} \left\{ \begin{array}{l} alice (i_1 z) = \pi_1 (g11 z) \\ alice (i_2 w) = (\pi_1 (g12 \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle))) w \\ bob (i_1 z) = \pi_2 (g11 z) \\ bob (i_2 w) = (\pi_2 (g12 \cdot (\langle alice, bob \rangle \times \langle alice, bob \rangle))) w \end{array} \right\} \end{array} \right\} \\
&\equiv \{ \text{Def-comp (72)} \}
\end{aligned}$$

$$\begin{aligned}
& \left\{ \begin{array}{l} \{ \text{alice } (i_1 z) = \pi_1 (g11 z) \\ \text{alice } (i_2 w) = \pi_1 (g12 ((\langle \text{alice}, \text{bob} \rangle \times \langle \text{alice}, \text{bob} \rangle) w)) \\ \text{bob } (i_1 z) = \pi_2 (g11 z) \\ \text{bob } (i_2 w) = \pi_2 (g12 ((\langle \text{alice}, \text{bob} \rangle \times \langle \text{alice}, \text{bob} \rangle) w)) \end{array} \right\} \\
\equiv & \quad \{ \text{Mudança de variável } w : = (x,y), \text{Def-} \times (72) \} \\
& \left\{ \begin{array}{l} \{ \text{alice } (i_1 z) = \pi_1 (g11 z) \\ \text{alice } (i_2 (x, y)) = \pi_1 (g12 (\langle \text{alice}, \text{bob} \rangle x, \langle \text{alice}, \text{bob} \rangle y)) \\ \text{bob } (i_1 z) = \pi_2 (g11 z) \\ \text{bob } (i_2 (x, y)) = \pi_2 (g12 (\langle \text{alice}, \text{bob} \rangle x, \langle \text{alice}, \text{bob} \rangle y)) \end{array} \right\} \\
\equiv & \quad \{ \text{Def-split (77)} \} \\
& \left\{ \begin{array}{l} \{ \text{alice } (i_1 z) = \pi_1 (g11 z) \\ \text{alice } (i_2 (x, y)) = \pi_1 (g12 ((\text{alice } x, \text{bob } x), (\text{alice } y, \text{bob } y))) \\ \text{bob } (i_1 z) = \pi_2 (g11 z) \\ \text{bob } (i_2 (x, y)) = \pi_2 (g12 ((\text{alice } x, \text{bob } x), (\text{alice } y, \text{bob } y))) \end{array} \right\} \\
\equiv & \quad \{ \text{Definição de } g11 : g11 x = (x, x), \text{Definição de } g12 : g12 ((a, b), (c, d)) = (a + c, b + d) \} \\
& \left\{ \begin{array}{l} \{ \text{alice } (i_1 z) = \pi_1 (z, z) \\ \text{alice } (i_2 (x, y)) = \pi_1 ((\text{alice } x) + (\text{alice } y), (\text{bob } x) + (\text{bob } y)) \\ \text{bob } (i_1 z) = \pi_2 (z, z) \\ \text{bob } (i_2 (x, y)) = \pi_2 ((\text{alice } x) + (\text{alice } y), (\text{bob } x) + (\text{bob } y)) \end{array} \right\} \\
\equiv & \quad \{ \text{Def-proj (79)} \} \\
& \left\{ \begin{array}{l} \{ \text{alice } (i_1 z) = z \\ \text{alice } (i_2 (x, y)) = (\text{alice } x) + (\text{alice } y) \\ \text{bob } (i_1 z) = z \\ \text{bob } (i_2 (x, y)) = (\text{bob } x) + (\text{bob } y) \end{array} \right\} \\
\equiv & \quad \square
\end{aligned}$$

$\text{alice} :: \text{Ord } c \Rightarrow \text{LTree } c \rightarrow c$
 $\text{alice} = \perp$
 $\text{bob} :: \text{Ord } c \Rightarrow \text{LTree } c \rightarrow c$
 $\text{bob} = \perp$

Problema 3

Biblioteca LTree3:

$\text{inLTree3} = [\text{Tri}, \text{Nodo}]$

Ora, sabendo que outLTree3 é o isomorfismo de inLTree3 , temos então que $\text{outLTree3} \cdot \text{inLTree3} = \text{id}$. Ou seja, a partir desta equação, conseguimos obter a definição de outLTree3 .

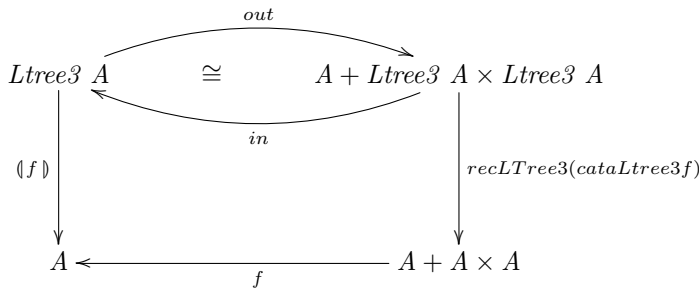
$$\begin{aligned}
& \text{outLTree3} \cdot \text{inLTree3} = \text{id} \\
\equiv & \quad \{ \text{Definição de } \text{inLTree3} : [\text{Tri}, \text{Nodo}] \} \\
& \text{outLTree3} \cdot [\text{Tri}, \text{Nodo}] = \text{id} \\
\equiv & \quad \{ \text{Fusão-+ (20)} \} \\
& [\text{outLTree3} \cdot \text{Tri}, \text{outLTree3} \cdot \text{Nodo}] = \text{id} \\
\equiv & \quad \{ \text{Universal-+ (17)} \} \\
& \left\{ \begin{array}{l} \text{outLTree3} \cdot \text{Tri} = \text{id} \cdot i_1 \\ \text{outLTree3} \cdot \text{Nodo} = \text{id} \cdot i_2 \end{array} \right\} \\
\equiv & \quad \{ \text{Natural-id (1), Igualdade extensional (71) considerando que } x, t, y, z \text{ são LTree3} \}
\end{aligned}$$

$$\begin{aligned}
& \left\{ \begin{array}{l} (outLTree3 \cdot Tri) x = i_1 x \\ (outLTree3 \cdot Nodo) t y z = i_2 t y z \end{array} \right. \\
& \equiv \quad \{ \text{Def-comp (72)} \} \\
& \left\{ \begin{array}{l} outLTree3 (Tri x) = i_1 x \\ outLTree3 (Nodo t y z) = i_2 t y z \end{array} \right. \\
& \square
\end{aligned}$$

$$\begin{aligned}
outLTree3 (Tri x) &= i_1 x \\
outLTree3 (Nodo t y z) &= i_2 t y z \\
baseLTree3 f g &= g + f * (f * f)
\end{aligned}$$

Pela propriedade de Base-cata, temos que $recLTree3 f = baseLTree3 id f = id + f * (f * f)$.

$$recLTree3 f = id + f * (f * f)$$



$$\begin{aligned}
cataLTree3 f &= f \Delta (recLTree3 (cataLTree3 f)) \Delta outLTree3 \\
anaLTree3 f &= inLTree3 \Delta (recLTree3 (anaLTree3 f)) \Delta f \\
hyloLTree3 f g &= cataLTree3 f \Delta anaLTree3 g
\end{aligned}$$

Genes do hilomorfismo *sierpinski*:

$$\begin{aligned}
g_1 &= (singl [\cdot, \cdot] (\text{conc} \Delta (id * \text{conc}))) \textbf{ where } \text{conc} (l_1, (l_2, l_3)) = l_1 \uparrow l_2 \uparrow l_3 \\
g_2 (t, 0) &= i_1 t \\
g_2 (((x, y), s), n + 1) &= i_2 ((t1, t2), t3) \textbf{ where} \\
t1 &= (((x, y), s / 2), n) \\
t2 &= (((x + s / 2, y), s / 2), n) \\
t3 &= (((x, y + s / 2), s / 2), n)
\end{aligned}$$

Problema 4

$$\begin{aligned}
propagate &:: Monad m \Rightarrow (t \rightarrow m a) \rightarrow [t] \rightarrow m [a] \\
propagate f &= \llbracket g f \rrbracket \textbf{ where} \\
g f &= [return \cdot nil, g_2 f] \\
g_2 f (a, b) &= \textbf{do} \{ h \leftarrow f a; t \leftarrow b; return (cons (h, t)) \}
\end{aligned}$$

$$\begin{aligned}
propagate3 &:: (Monad m) \Rightarrow (Bit3 \rightarrow m Bit3) \rightarrow [Bit] \rightarrow m [Bit] \\
propagate3 f &= \llbracket g f \rrbracket \textbf{ where} \\
g f &= [\perp, g_2 f] \\
g_2 f (a, b) &= \perp
\end{aligned}$$

A função *bflip3*, a programar a seguir, deverá estender *bflip* aos três bits da entrada:

$$\begin{aligned}
bflip3 &:: Bit3 \rightarrow Dist Bit3 \\
bflip3 (a, b, c) &= \textbf{do} \{ \perp \}
\end{aligned}$$

Index

- LaTeX, [7](#)
 - `bibtex`, [7](#)
 - `lhs2TeX`, [7](#)
 - `makeindex`, [7](#)
- Cálculo de Programas, [1](#), [7](#), [8](#)
 - Material Pedagógico, [7](#)
 - `BTree.hs`, [4](#)
 - `LTree.hs`, [2](#), [4](#), [11](#)
- Combinador “pointfree”
 - cata*
 - Listas, [11](#)
 - Naturais, [8](#)
 - either*, [11](#), [12](#)
- Fractal, [3](#)
 - Triângulo de Sierpinski, [3](#), [4](#)
- Função
 - for*, [2](#), [8](#)
 - length*, [10](#)
 - map*, [10](#)
 - Projecção
 - π_1 , [1](#), [7](#), [8](#)
 - π_2 , [7](#)
- Functor, [5](#), [8–10](#), [12](#)
- Haskell, [1](#), [5](#), [7](#)
 - Biblioteca
 - PFP, [9](#)
 - Probability, [9](#)
 - interpretador
 - GHCi, [7](#), [9](#)
 - Literate Haskell, [7](#)
- Números naturais (\mathbb{N}), [8](#)
- Programação
 - dinâmica, [8](#)
 - literária, [6](#), [7](#)
- SVG (Scalable Vector Graphics), [5](#), [10](#)
- U.Minho
 - Departamento de Informática, [1](#)
- XML (Extensible Markup Language), [5](#)

References

- [1] M. Erwig and S. Kollmansberger. Functional pearls: Probabilistic functional programming in Haskell. *J. Funct. Program.*, 16:21–34, January 2006.
- [2] D.E. Knuth. *Literate Programming*. CSLI Lecture Notes Number 27. Stanford University Center for the Study of Language and Information, Stanford, CA, USA, 1992.
- [3] J.N. Oliveira. *Program Design by Calculation*, 2018. Draft of textbook in preparation. viii+297 pages. Informatics Department, University of Minho.