

Cálculo de Programas

Trabalho Prático

MiEI+LCC — 2017/18

Departamento de Informática
Universidade do Minho

Junho de 2018

Grupo nr.	13
a81047	Catarina Machado
a82339	João Vilaça

1 Preâmbulo

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

Na sequência pedagógica dos planos de estudo dos dois cursos que têm esta disciplina, restringe-se a aplicação deste método à programação funcional em **Haskell**. 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 e a produzir textos técnico-científicos de qualidade.

2 Documentação

Para cumprir de forma integrada os objectivos enunciados acima vamos recorrer a uma técnica de programação dita “**literária**” [?], 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 `cp1718t.pdf` que está a ler é já um exemplo de **programação literária**: foi gerado a partir do texto fonte `cp1718t.lhs`¹ que encontrará no **material pedagógico** desta disciplina descompactando o ficheiro `cp1718t.zip` e executando

```
$ lhs2TeX cp1718t.lhs > cp1718t.tex
$ pdflatex cp1718t
```

em que **lhs2tex** é um pre-processor que faz “pretty printing” de código Haskell em **L^AT_EX** e que deve desde já instalar executando

```
$ cabal install lhs2tex
```

Por outro lado, o mesmo ficheiro `cp1718t.lhs` é executável e contém o “kit” básico, escrito em **Haskell**, para realizar o trabalho. Basta executar

```
$ ghci cp1718t.lhs
```

Abra o ficheiro `cp1718t.lhs` no seu editor de texto preferido e verifique que assim é: todo o texto que se encontra dentro do ambiente

¹O suffixo ‘lhs’ quer dizer *literate Haskell*.

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

vai ser seleccionado pelo **GHCI** para ser executado.

3 Como realizar o trabalho

Este trabalho teórico-prático deve ser realizado por grupos de três 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 de trabalho por forma a poderem responder às questões que serão colocadas 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 **C** 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 **BibTeX**) e o índice remissivo (com **makeindex**),

```
$ bibtex cp1718t.aux
$ makeindex cp1718t.idx
```

e recompilar o texto como acima se indicou. Dever-se-á ainda instalar o utilitário **QuickCheck**, que ajuda a validar programas em **Haskell**, a biblioteca **JuicyPixels** para processamento de imagens e a biblioteca **gloss** para geração de gráficos 2D:

```
$ cabal install QuickCheck JuicyPixels gloss
```

Para testar uma propriedade **QuickCheck** *prop*, basta invocá-la com o comando:

```
> quickCheck prop
+++ OK, passed 100 tests.
```

Problema 1

Segundo uma [notícia do Jornal de Notícias](#), referente ao dia 12 de abril, “*apenas numa hora, foram transacionadas 1.2 mil milhões de dólares em bitcoins. Nas últimas 24 horas, foram transacionados 8,5 mil milhões de dólares, num total de 24 mil milhões de dólares referentes às principais criptomoedas*”.

De facto, é inquestionável que as criptomoedas, e em particular as bitcoin, vieram para ficar. Várias moedas digitais, e em particular as bitcoin, usam a tecnologia de block chain para guardar e assegurar todas as transações relacionadas com a moeda. Uma **block chain** é uma coleção de blocos que registam os movimentos da moeda; a sua definição em Haskell é apresentada de seguida.

```
data Blockchain = Bc { bc :: Block } | Bcs { bcs :: (Block, Blockchain) } deriving Show
```

Cada **bloco** numa block chain regista um número (mágico) único, o momento da execução, e uma lista de transações, tal como no código seguinte:

```
type Block = (MagicNo, (Time, Transactions))
```

Cada **transação** define a entidade de origem da transferência, o valor a ser transacionado, e a entidade destino (por esta ordem), tal como se define de seguida.

```
type Transaction = (Entity, (Value, Entity))
type Transactions = [ Transaction]
```

A partir de uma block chain, é possível calcular o valor que cada entidade detém, tipicamente designado de ledger:

```
type Ledger = [(Entity, Value)]
```

Seguem as restantes definições Haskell para completar o código anterior. Note que *Time* representa o momento da transação, como o número de **milisegundos** que passaram desde 1970.

```
type MagicNo = String
type Time = Int -- em milisegundos
type Entity = String
type Value = Int
```

Neste contexto, implemente as seguintes funções:

1. Defina a função *allTransactions :: Blockchain → Transactions*, como um catamorfismo, que calcula a lista com todas as transações numa dada block chain.

Propriedade QuickCheck 1 *As transações de uma block chain são as mesmas da block chain revertida:*

$$prop1a = sort \cdot allTransactions \equiv sort \cdot allTransactions \cdot reverseChain$$

Note que a função sort é usada apenas para facilitar a comparação das listas.

2. Defina a função *ledger :: Blockchain → Ledger*, utilizando catamorfismos e/ou anamorfismos, que calcula o ledger (i.e., o valor disponível) de cada entidade numa dada block chain. Note que as entidades podem ter valores negativos; de facto isso acontecerá para a primeira transação que executarem.

Propriedade QuickCheck 2 *O tamanho do ledger é inferior ou igual a duas vezes o tamanho de todas as transações:*

$$prop1b = length \cdot ledger \leq (2*) \cdot length \cdot allTransactions$$

Propriedade QuickCheck 3 *O ledger de uma block chain é igual ao ledger da sua inversa:*

$$prop1c = sort \cdot ledger \equiv sort \cdot ledger \cdot reverseChain$$

3. Defina a função *isValidMagicNr :: Blockchain → Bool*, utilizando catamorfismos e/ou anamorfismos, que verifica se todos os números mágicos numa dada block chain são únicos.

Propriedade QuickCheck 4 *A concatenação de uma block chain com ela mesma nunca é válida em termos de números mágicos:*

$$prop1d = \neg \cdot isValidMagicNr \cdot concChain \cdot \langle id, id \rangle$$

Propriedade QuickCheck 5 *Se uma block chain é válida em termos de números mágicos, então a sua inversa também o é:*

$$prop1e = isValidMagicNr \Rightarrow isValidMagicNr \cdot reverseChain$$

Problema 2

Uma estrutura de dados frequentemente utilizada para representação e processamento de imagens de forma eficiente são as denominadas **quadrees**. Uma *quadtree* é uma árvore quaternária em que cada nodo tem quatro sub-árvores e cada folha representa um valor bi-dimensional.

```
data QTree a = Cell a Int Int | Block (QTree a) (QTree a) (QTree a) (QTree a)
deriving (Eq, Show)
```

```

( 0 0 0 0 0 0 0 0 )   Block
( 0 0 0 0 0 0 0 0 )   (Cell 0 4 4) (Block
( 0 0 0 0 1 1 1 0 )   (Cell 0 2 2) (Cell 0 2 2) (Cell 1 2 2) (Block
( 0 0 0 0 1 1 0 0 )   (Cell 1 1 1) (Cell 0 1 1) (Cell 0 1 1) (Cell 0 1 1)))
( 1 1 1 1 1 1 0 0 )   (Cell 1 4 4)
( 1 1 1 1 1 1 0 0 )   (Block
( 1 1 1 1 0 0 0 0 )   (Cell 1 2 2) (Cell 0 2 2) (Cell 0 2 2) (Block
( 1 1 1 1 0 0 0 1 )   (Cell 0 1 1) (Cell 0 1 1) (Cell 0 1 1) (Cell 1 1 1)))

```

(a) Matriz de exemplo *bm*.

(b) Quadtree de exemplo *qt*.

Figura 1: Exemplos de representações de bitmaps.

Uma imagem monocromática em formato bitmap pode ser representada como uma matriz de bits², tal como se exemplifica na Figura 1a.

O anamorfismo *bm2qt* converte um bitmap em forma matricial na sua codificação eficiente em quad-trees, e o catamorfismo *qt2bm* executa a operação inversa:

$$\begin{aligned}
bm2qt &:: (Eq\ a) \Rightarrow Matrix\ a \rightarrow QTree\ a & qt2bm &:: (Eq\ a) \Rightarrow QTree\ a \rightarrow Matrix\ a \\
bm2qt &= anaQTree\ f\ \textbf{where} & qt2bm &= cataQTree\ [f, g]\ \textbf{where} \\
f\ m &= \textbf{if}\ one\ \textbf{then}\ i_1\ u\ \textbf{else}\ i_2\ (a, (b, (c, d))) & f\ (k, (i, j)) &= matrix\ j\ i\ k \\
&\textbf{where}\ x = (nub \cdot toList)\ m & g\ (a, (b, (c, d))) &= (a \uparrow b) \leftrightarrow (c \uparrow d) \\
&\quad u = (head\ x, (ncols\ m, nrows\ m)) & & \\
&\quad one = (ncols\ m \equiv 1 \vee nrows\ m \equiv 1 \vee length\ x \equiv 1) & & \\
&\quad (a, b, c, d) = splitBlocks\ (nrows\ m \div 2)\ (ncols\ m \div 2)\ m & &
\end{aligned}$$

O algoritmo *bm2qt* particiona recursivamente a imagem em 4 blocos e termina produzindo folhas para matrizes unitárias ou quando todos os píxeis de um sub-bloco têm a mesma cor. Para a matriz *bm* de exemplo, a quadtree correspondente *qt* = *bm2qt* *bm* é ilustrada na Figura 1b.

Imagens a cores podem ser representadas como matrizes de píxeis segundo o código de cores *RGBA*, codificado no tipo *PixelRGBA8* em que cada pixel é um quádruplo de valores inteiros (*red*, *green*, *blue*, *alpha*) contidos entre 0 e 255. Atente em alguns exemplos de cores:

```

whitePx = PixelRGBA8 255 255 255 255
blackPx  = PixelRGBA8 0 0 0 255
redPx    = PixelRGBA8 255 0 0 255

```

O módulo *BMP*, disponibilizado juntamente com o enunciado, fornece funções para processar ficheiros de imagem bitmap como matrizes:

```

readBMP :: FilePath → IO (Matrix PixelRGBA8)
writeBMP :: FilePath → Matrix PixelRGBA8 → IO ()

```

Teste, por exemplo, no *GHCi*, carregar a Figura 2a:

```
> readBMP "cp1718t_media/person.bmp"
```

Esta questão aborda operações de processamento de imagens utilizando quadrees:

1. Defina as funções *rotateQTree* :: *QTree* *a* → *QTree* *a*, *scaleQTree* :: *Int* → *QTree* *a* → *QTree* *a* e *invertQTree* :: *QTree* *a* → *QTree* *a*, como catamorfismos e/ou anamorfismos, que rodam³, re-dimensionam⁴ e invertem as cores de uma quadtree⁵, respectivamente. Tente produzir imagens similares às Figuras 2b, 2c e 2d:

```

> rotateBMP "cp1718t_media/person.bmp" "person90.bmp"
> scaleBMP 2 "cp1718t_media/person.bmp" "personx2.bmp"
> invertBMP "cp1718t_media/person.bmp" "personinv.bmp"

```

²Cf. módulo *Data.Matrix*.

³Segundo um ângulo de 90° no sentido dos ponteiros do relógio.

⁴Multiplicando o seu tamanho pelo valor recebido.

⁵Um pixel pode ser invertido calculando 255 − *c* para cada componente *c* de cor RGB, exceptuando o componente alpha.



(a) Bitmap de exemplo.



(b) Rotação.



(c) Redimensionamento.



(d) Inversão de cores.



(e) Compressão de 1 nível.



(f) Compressão de 2 níveis.



(g) Compressão de 3 níveis.



(h) Compressão de 4 níveis.



(i) Bitmap de contorno.



(j) Bitmap com contorno.

Figura 2: Manipulação de uma figura bitmap utilizando quadrees.

Propriedade QuickCheck 6 Rodar uma quadtree é equivalente a rodar a matriz correspondente:

$$\text{prop2c} = \text{rotateMatrix} \cdot \text{qt2bm} \equiv \text{qt2bm} \cdot \text{rotateQTree}$$

Propriedade QuickCheck 7 Redimensionar uma imagem altera o seu tamanho na mesma proporção:

$$\text{prop2d} (\text{Nat } s) = \text{sizeQTree} \cdot \text{scaleQTree } s \equiv ((s*) \times (s*)) \cdot \text{sizeQTree}$$

Propriedade QuickCheck 8 Inverter as cores de uma quadtree preserva a sua estrutura:

$$\text{prop2e} = \text{shapeQTree} \cdot \text{invertQTree} \equiv \text{shapeQTree}$$

2. Defina a função $\text{compressQTree} :: \text{Int} \rightarrow \text{QTree } a \rightarrow \text{QTree } a$, utilizando catamorfismos e/ou anamorfismos, que comprime uma quadtree cortando folhas da árvore para reduzir a sua profundidade num dado número de níveis. Tente produzir imagens similares (mas não necessariamente iguais) às Figuras 2e, 2f, 2g e 2h:

```
> compressBMP 1 "cp1718t_media/person.bmp" "person1.bmp"
> compressBMP 2 "cp1718t_media/person.bmp" "person2.bmp"
> compressBMP 3 "cp1718t_media/person.bmp" "person3.bmp"
> compressBMP 4 "cp1718t_media/person.bmp" "person4.bmp"
```

Propriedade QuickCheck 9 A quadtree comprimida tem profundidade igual à da quadtree original menos a taxa de compressão:

$$\text{prop2f} (\text{Nat } n) = \text{depthQTree} \cdot \text{compressQTree } n \equiv (-n) \cdot \text{depthQTree}$$

3. Defina a função $\text{outlineQTree} :: (a \rightarrow \text{Bool}) \rightarrow \text{QTree } a \rightarrow \text{Matrix Bool}$, utilizando catamorfismos e/ou anamorfismos, que recebe uma função que determina quais os píxeis de fundo e converte uma quadtree numa matriz monocromática, de forma a desenhar o contorno de uma **malha poligonal** contida na imagem. Tente produzir imagens similares (mas não necessariamente iguais) às Figuras 2i e 2j:

```
> outlineBMP "cp1718t_media/person.bmp" "personOut1.bmp"
> addOutlineBMP "cp1718t_media/person.bmp" "personOut2.bmp"
```

Propriedade QuickCheck 10 A matriz de contorno tem dimensões iguais às da quadtree:

$$\text{prop2g} = \text{sizeQTree} \equiv \text{sizeMatrix} \cdot \text{outlineQTree} (<0)$$

Teste unitário 1 Contorno da quadtree de exemplo qt:

$$\text{teste2a} = \text{outlineQTree} (\equiv 0) \text{ qt} \equiv \text{qtOut}$$

Problema 3

O cálculo das combinações de n k -a- k ,

$$\binom{n}{k} = \frac{n!}{k! * (n - k)!} \quad (1)$$

envolve três factoriais. Recorrendo à **lei de recursividade múltipla** do cálculo de programas, é possível escrever o mesmo programa como um simples ciclo-for onde se fazem apenas multiplicações e somas. Para isso, começa-se por estruturar a definição dada da forma seguinte,

$$\binom{n}{k} = h \ k \ (n - k)$$



Figura 3: Passos de construção de uma árvore de Pitágoras de ordem 3.

onde

$$h \ k \ d = \frac{f \ k \ d}{g \ d}$$

$$f \ k \ d = \frac{(d+k)!}{k!}$$

$$g \ d = d!$$

assumindo-se $d = n - k \geq 0$. É fácil de ver que $f \ k$ e g se desdobram em 4 funções mutuamente recursivas, a saber

$$f \ k \ 0 = 1$$

$$f \ k \ (d+1) = \underbrace{(d+k+1)}_{l \ k \ d} * f \ k \ d$$

$$l \ k \ 0 = k+1$$

$$l \ k \ (d+1) = l \ k \ d + 1$$

e

$$g \ 0 = 1$$

$$g \ (d+1) = \underbrace{(d+1)}_{s \ d} * g \ d$$

$$s \ 0 = 1$$

$$s \ (d+1) = s \ d + 1$$

A partir daqui alguém derivou a seguinte implementação:

$$\binom{n}{k} = h \ k \ (n-k) \text{ where } h \ k \ n = \text{let } (a, -, b, -) = \text{for loop (base k) n in } a / b$$

Aplicando a lei da recursividade múltipla para $\langle f \ k, l \ k \rangle$ e para $\langle g, s \rangle$ e combinando os resultados com a [lei de banana-split](#), derive as funções *base k* e *loop* que são usadas como auxiliares acima.

Propriedade QuickCheck 11 Verificação que $\binom{n}{k}$ coincide com a sua especificação (1):

$$\text{prop3 } (\text{NonNegative } n) (\text{NonNegative } k) = k \leq n \Rightarrow \binom{n}{k} \equiv n! / (k! * (n-k)!)$$

Problema 4

Fractais são formas geométricas que podem ser construídas recursivamente de acordo com um conjunto de equações matemáticas. Um exemplo clássico de um fractal são as **árvores de Pitágoras**. A construção de uma árvore de Pitágoras começa com um quadrado, ao qual se unem dois quadrados redimensionados pela escala $\sqrt{2}/2$, de forma a que os cantos dos 3 quadrados coincidam e formem um triângulo rectângulo isósceles. Este procedimento é repetido recursivamente de acordo com uma dada ordem, definida como um número natural (Figura 3).

Uma árvore de Pitágoras pode ser codificada em Haskell como uma *full tree* contendo quadrados nos nodos e nas folhas, sendo um quadrado definido simplesmente pelo tamanho do seu lado:

```
data FTree a b = Unit b | Comp a (FTree a b) (FTree a b) deriving (Eq, Show)
type PTree = FTree Square Square
type Square = Float
```

1. Defina a função `generatePTree :: Int → PTree`, como um anamorfismo, que gera uma árvore de Pitágoras para uma dada ordem.

Propriedade QuickCheck 12 Uma árvore de Pitágoras tem profundidade igual à sua ordem:

$$\text{prop4a } (\text{SmallNat } n) = (\text{depthFTree} \cdot \text{generatePTree}) \, n \equiv n$$

Propriedade QuickCheck 13 Uma árvore de Pitágoras está sempre balanceada:

$$\text{prop4b } (\text{SmallNat } n) = (\text{isBalancedFTree} \cdot \text{generatePTree}) \, n$$

2. Defina a função `drawPTree :: PTree → [Picture]`, utilizando catamorfismos e/ou anamorfismos, que anima incrementalmente os passos de construção de uma árvore de Pitágoras recorrendo à biblioteca `gloss`. Anime a sua solução:

```
> animatePTree 3
```

Problema 5

Uma das áreas em maior expansão no campo da informática é a análise de dados e `machine learning`. Esta questão aborda um *mónade* que ajuda a fazer, de forma simples, as operações básicas dessas técnicas. Esse *mónade* é conhecido por *bag*, *saco* ou *multi-conjunto*, permitindo que os elementos de um conjunto tenham multiplicidades associadas. Por exemplo, seja

```
data Marble = Red | Pink | Green | Blue | White deriving (Read, Show, Eq, Ord)
```

um tipo dado.⁶ A lista `[Pink, Green, Red, Blue, Green, Red, Green, Pink, Blue, White]` tem elementos repetidos. Assumindo que a ordem não é importante, essa lista corresponde ao saco

```
{ Red |-> 2 , Pink |-> 2 , Green |-> 3 , Blue |-> 2 , White |-> 1 }
```

que habita o tipo genérico dos “bags”:

```
data Bag a = B [(a, Int)] deriving (Ord)
```

O *mónade* que vamos construir sobre este tipo de dados faz a gestão automática das multiplicidades. Por exemplo, seja dada a função que dá o peso de cada berlinde em gramas:

```
marbleWeight :: Marble → Int
marbleWeight Red   = 3
marbleWeight Pink  = 2
marbleWeight Green = 3
marbleWeight Blue  = 6
marbleWeight White = 2
```

Então, se quisermos saber quantos *berlindes* temos, de cada *peso*, não teremos que fazer contas: basta calcular

```
marbleWeights = fmap marbleWeight bagOfMarbles
```

onde `bagOfMarbles` é o saco de berlindes referido acima, obtendo-se:

```
{ 2 |-> 3 , 3 |-> 5 , 6 |-> 2 }.
```

⁶“Marble”traduz para “berlinde”em português.



Figura 4: Distribuição de berlindes num saco.

Mais ainda, se quisermos saber o total de berlindes em *bagOfMarbles* basta calcular `fmap (!) bagOfMarbles` obtendo-se `{ () | -> 10 }`; isto é, o saco tem 10 berlindes no total.

Finalmente, se quisermos saber a probabilidade da cor de um berlinde que tiremos do saco, basta converter o referido saco numa distribuição correndo:

```
marblesDist = dist bagOfMarbles
```

obtendo-se a distribuição (graças ao módulo **Probability**):

```
Green  30.0%
Red    20.0%
Pink   20.0%
Blue   20.0%
White  10.0%
```

cf. Figura 4.

Partindo da seguinte declaração de *Bag* como um functor e como um mónade,

```
instance Functor Bag where
  fmap f = B · map (f × id) · unB
instance Monad Bag where
  x >>= f = (μ · fmap f) x where
    return = singletonbag
```

1. Defina a função μ (multiplicação do mónade *Bag*) e a função auxiliar *singletonbag*.
2. Verifique-as com os seguintes testes unitários:

Teste unitário 2 *Lei* $\mu \cdot \text{return} = \text{id}$:

$$\text{test5a} = \text{bagOfMarbles} \equiv \mu (\text{return bagOfMarbles})$$

Teste unitário 3 *Lei* $\mu \cdot \mu = \mu \cdot \text{fmap } \mu$:

$$\text{test5b} = (\mu \cdot \mu) \text{ b3} \equiv (\mu \cdot \text{fmap } \mu) \text{ b3}$$

onde *b3* é um saco dado em anexo.

Anexos

A Mónade para probabilidades e estatística

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

$$\text{newtype Dist } a = D \{ \text{unD} :: [(a, \text{ProbRep})] \} \quad (2)$$

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 ,

A	■ 2%
B	■ 12%
C	■ 29%
D	■ 35%
E	■ 22%

será representada pela distribuição

$$\begin{aligned} d1 &:: \text{Dist Char} \\ d1 &= D [('A', 0.02), ('B', 0.12), ('C', 0.29), ('D', 0.35), ('E', 0.22)] \end{aligned}$$

que o **GHCI** mostrará assim:

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

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

B Definições auxiliares

Funções para mostrar *bags*:

```
instance (Show a, Ord a, Eq a) => Show (Bag a) where
  show = showbag . consol . unB where
    showbag = concat .
      (+[ " } " ]) . ( " { " : ) .
      (intersperse " , " ) .
      sort .
      (map f) where f (a, b) = (show a) ++ " | -> " ++ (show b)
    unB (B x) = x
```

Igualdade de *bags*:

```
instance (Eq a) => Eq (Bag a) where
  b == b' = (unB b) 'lequal' (unB b')
  where lequal a b = isempty (a ⊖ b)
        ominus a b = a ++ neg b
        neg x = [(k, -i) | (k, i) <- x]
```

Ainda sobre o mónade *Bag*:

```

instance Applicative Bag where
  pure = return
  (< * >) = aap

```

O exemplo do texto:

```

bagOfMarbles = B [(Pink, 2), (Green, 3), (Red, 2), (Blue, 2), (White, 1)]

```

Um valor para teste (bags de bags de bags):

```

b3 :: Bag (Bag (Bag Marble))
b3 = B [(B [(B [(Pink, 2), (Green, 3), (Red, 2), (Blue, 2), (White, 1)], 5)
  , (B [(Pink, 1), (Green, 2), (Red, 1), (Blue, 1)], 2)], 2)]

```

Outras funções auxiliares:

```

a ↦ b = (a, b)
consol :: (Eq b) ⇒ [(b, Int)] → [(b, Int)]
consol = filter nzero · map (id × sum) · col where nzero (_, x) = x ≠ 0
isempty :: Eq a ⇒ [(a, Int)] → Bool
isempty = all (≡ 0) · map π₂ · consol
col x = nub [k ↦ [d' | (k', d') ← x, k' ≡ k] | (k, d) ← x]
consolidate :: Eq a ⇒ Bag a → Bag a
consolidate = B · consol · unB

```

C Soluções dos alunos

Os alunos devem colocar neste anexo as suas soluções aos exercícios propostos, de acordo com o “layout” que se fornece. Não podem ser alterados os nomes ou tipos das funções dadas, mas pode ser adicionado texto e / ou outras funções auxiliares que sejam necessárias.

Problema 1

De modo a resolver este primeiro problema, antes de procedermos ao desenvolvimento das 3 alíneas do problema, tivemos que definir algumas funções que nos ajudarão a implementar as soluções requeridas.

```

inBlockchain = [Bc, Bcs]
outBlockchain (Bc a) = i₁ (a)
outBlockchain (Bcs (a, b)) = i₂ (a, b)
recBlockchain g = id + (id × g)
cataBlockchain g = g · (recBlockchain (cataBlockchain g)) · outBlockchain
anaBlockchain g = inBlockchain · (recBlockchain (anaBlockchain g)) · g
hyloBlockchain h g = cataBlockchain h · anaBlockchain g

```

Estas funções, nomeadamente *inBlockchain*, *outBlockchain*, *recBlockchain*, *cataBlockchain*, *anaBlockchain* e *hyloBlockchain*, podem ser deduzidas tendo em consideração o Tipo de Dados do problema, a matéria de Cálculo de Programas e com a ajuda de alguns diagramas.

Uma vez que o tipo de Blockchain é *Bc* { *bc* :: *Block* } ou *Bcs* { *bcs* :: (*Block*, *Blockchain*) }

Sabemos que o *inBlockchain* e o *outBlockchain* deverão “fechar” e “abrir” a Blockchain, respetivamente, logo, conseguimos representar os diagramas:

$$Blockchain \xleftarrow{\text{inBlockchain}} Block + (Block \times Blockchain)$$

$$Blockchain \xrightarrow{\text{outBlockchain}} Block + (Block \times Blockchain)$$

Assim, conseguimos perceber de imediato a definição de ambas as funções:

$$inBlockchain = [Bc, Bcs]$$

$$outBlockchain (Bc\ a) = i_1\ (a)$$

$$outBlockchain (Bcs\ (a, b)) = i_2\ (a, b)$$

Relativamente às funções *recBlockchain*, *cataBlockchain*, *anaBlockchain* e *hyloBlockchain*, os seus tipos já estavam presentes no enunciado e o significado e intuito de cada uma delas também já era sabido.

$$\begin{array}{ccc}
 A* & \xrightarrow{lsplitBGEne} & 1 + A* \times (A \times A\ above)\ above \\
 \downarrow \text{anaBlockchain } h & & \downarrow id + ((ana\ lsplitBGEne) \times map\ (id \times ana\ lsplitBGEne)) \\
 Blockchain & \xrightleftharpoons[inBlockchain]{outBlockchain} & Block + (Block \times Blockchain) \\
 \downarrow \text{cataBlockchain } g & & \downarrow id + ((cata\ inordBGEne) \times map\ (id \times cata\ inordBGEne)) \\
 Blockchain & \xleftarrow{g} & Block + (Block \times Blockchain)
 \end{array}$$

Na resolução das alíneas recorreremos a alguns diagramas onde também fica implícito o porquê da definição de cada uma destas funções.

TODOO

1. Função allTransactions

O objetivo da função *allTransactions* é calcular a lista com todas as transações numa dada block chain, utilizando um catamorfismo.

O diagrama desta função será:

$$\begin{array}{ccc}
 Blockchain & \xleftarrow{inBlockchain} & Block + (Block \times Blockchain) \\
 \downarrow \text{cataBlockchain } g & & \downarrow recBlockchain\ (cataBlockchain\ g) \\
 Transactions & \xleftarrow{g} & Block + (Block \times Transactions)
 \end{array}$$

O objetivo é descobrir o gene *g*, para assim termos a definição final de *allTransactions* = *cataBlockchain g*.

Assim, tendo em atenção o tipo de Block:

$$\text{type } Block = (MagicNo, (Time, Transactions))$$

E o tipo de Blockchain já apresentado, deduzimos que o *g* terá que ser um “either”, $g = [b0, joint]$, onde de um lado irá tratar o *Block* e do outro o $Block \times Transactions$.

(a) Descobrir b0

Para tratar o lado em que o domínio é *Block*, e sabendo que o resultado terá que ser *Transactions*, o objetivo desta função será “retirar” do *Block* as *Transactions*.

Assim, teremos que definir *b0* com projeções π_2 como podemos verificar no diagrama em seguida:

$$\begin{array}{c}
 MagicNo \times (Time \times Transactions) \\
 \downarrow \pi_2 \cdot \pi_2 \\
 Transactions
 \end{array}$$

Deste modo, fica definido *b0* como:

$$b0 = \pi_2 \cdot \pi_2$$

(b) Descobrir joint

Tendo em conta o domínio da função *joint*, isto é, $Block \times Transactions$, percebemos que o objetivo desta função será retirar de *Block* as suas *Transactions* e juntá-las às *Transactions* já acumuladas (passadas como parâmetro).

Assim, uma definição de *joint pointwise* é:

$$joint (block, transac) = (\pi_2 (\pi_2 block)) \uplus transac$$

Esta função cumpre os requisitos a que a propusemos.

Temos então a definição de *b0* e *joint*, pelo que ficamos a saber qual é o gene *g*:

$$\begin{aligned} g &= [b0, joint] \\ &\equiv \{ \text{Definição de } b0 ; \text{Definição de } joint \} \\ g &= [\pi_2 \cdot \pi_2, joint] \\ &\textbf{where } joint (x, y) = (\pi_2 (\pi_2 x)) \uplus y \end{aligned}$$

Deste modo, está definida a função *allTransactions* pedida:

$$\begin{aligned} allTransactions a &= cataBlockchain [\pi_2 \cdot \pi_2, joint] a \\ &\textbf{where } joint (x, y) = (\pi_2 (\pi_2 x)) \uplus y \end{aligned}$$

2. Função ledger

—

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

$$\begin{array}{ccc} A* & \xrightarrow{lsplitBGene} & 1 + A* \times (A \times A \text{ above}) \text{ above} \\ \downarrow \text{ana } lsplitBGene & & \downarrow id + ((\text{ana } lsplitBGene) \times \text{map } (id \times \text{ana } lsplitBGene)) \\ B & \xleftarrow[\text{in } B]{out B} & 1 + B \times (A \times B) \text{ above} \\ \downarrow \text{cata } inordBGene & & \downarrow id + ((\text{cata } inordBGene) \times \text{map } (id \times \text{cata } inordBGene)) \\ A \text{ above} & \xleftarrow{inordBGene} & 1 + A \text{ above} \times (A \times A \text{ above}) \text{ above} \end{array}$$

groupL :: *Ledger* → *Ledger*

```
groupL t = (sums · map (mapFst head · unzip) · groupBy (λx y → π1 x ≡ π1 y) · sort) t
  where mapFst f (a, b) = (f a, b)
        sums [] = []
        sums ((a, b) : t) = (a, sum b) : sums t
```

ledger a = *groupL* (*cataList* [*nil*, *insert*] (*allTransactions* a))

 where *insert* (x, y) = (π₁ x, −π₁ (π₂ x)) : (π₂ (π₂ x), π₁ (π₂ x)) : y

isValidMagicNr a = *all* ((≡) 1 · length) · *group* · *sort* \$ *cataBlockchain* [*list*, *insert*] a

 where *list* x = [π₁ x]

insert (x, y) = (π₁ x) : y

Problema 2

```

inQTree = [uncurryCell Cell, uncurryBlock Block]
  where uncurryCell f (e, (n1, n2)) = f e n1 n2
        uncurryBlock f (q1, (q2, (q3, q4))) = f q1 q2 q3 q4
outQTree (Cell e n1 n2) = i1 (e, (n1, n2))
outQTree (Block q1 q2 q3 q4) = i2 (q1, (q2, (q3, q4)))
baseQTree f g = (f × id) + (g × (g × (g × g)))
recQTree g = baseQTree id g
cataQTree g = g · (recQTree (cataQTree g)) · outQTree
anaQTree g = inQTree · (recQTree (anaQTree g)) · g
hyloQTree h g = cataQTree h · anaQTree g
instance Functor QTree where
  fmap f = cataQTree (inQTree · baseQTree f id)
rotateQTree = ⊥
scaleQTree = ⊥
invertQTree = ⊥
compressQTree = ⊥
outlineQTree = ⊥

```

Problema 3

O objetivo deste problema é derivar as funções *base k* e *loop* de modo a podermos calcular as combinações de *n k-a-k*,

$$\binom{n}{k} = \frac{n!}{k! * (n - k)!}$$

recorrendo a um ciclo-for onde apenas se fazem multiplicações e somas:

$$\binom{n}{k} = h \ k \ (n - k) \text{ where } h \ k \ n = \text{let } (a, -, b, -) = \text{for loop } (base \ k) \ n \text{ in } a / b$$

Tendo em conta o **where** *h k n* e o **in** *a / b* da função acima apresentada e comparando com a definição de *h k* do enunciado,

$$\begin{aligned}
 h \ k \ n &= \frac{f \ k \ n}{g \ n} \\
 f \ k \ n &= \frac{(n + k)!}{k!} \\
 g \ n &= n!
 \end{aligned}$$

constatamos que o nosso **a** em **in** *a / b* terá que ser a função *f k* e o **b** será a função *g*.

Assim, para podermos descobrir a definição das funções pedidas (*base k* e *loop*) teremos que, a partir da definição de *f k* (e consequentemente de *l k*) e da definição de *g* (e consequentemente de *s*), descobriremos a definição de $\langle f \ k, l \ k \rangle$ e de $\langle g, s \rangle$ (com recurso à lei da recursividade múltipla) e posteriormente combinarmos os seus resultados com a lei de banana-split.

Para tal, dividimos o nosso problema em diferentes partes:

1. Determinar $\langle f \ k, l \ k \rangle$

Para isso, tirando partido da indicação do enunciado, ou seja, com o intuito de aplicar a lei da recursividade múltipla, temos:

$$\begin{aligned}
 &\begin{cases} f \ k \cdot \text{in} = o \cdot F \ \langle f \ k, l \ k \rangle \\ l \ k \cdot \text{in} = p \cdot F \ \langle f \ k, l \ k \rangle \end{cases} \\
 &\equiv \quad \{ \text{Fokkinga: (50)} \} \\
 &\langle f \ k, l \ k \rangle = \langle \langle o, p \rangle \rangle
 \end{aligned}$$

O objetivo será então determinar o e p e, para isso, teremos que olhar individualmente para cada uma das funções f , k e l , apresentadas no enunciado:

(a) Descobrir o (com a ajuda da função f , k)

$$\begin{aligned}
& \begin{cases} f \ k \ 0 = 1 \\ f \ k \ (d + 1) = (l \ k \ d) * (f \ k \ d) \end{cases} \\
\equiv & \quad \{ \text{Def comp: (74)} ; (*) \text{ escrita como função prefixo} \} \\
& \begin{cases} f \ k \cdot 0 = 1 \\ f \ k \cdot (d + 1) = (*) \ (l \ k \ d) \ (f \ k \ d) \end{cases} \\
\equiv & \quad \{ \text{Igualdade extencional: (73)} ; \text{Def const: (76)} \} \\
& \begin{cases} f \ k \cdot \underline{0} = \underline{1} \\ f \ k \cdot (d + 1) = (*) \ (l \ k \ d) \ (f \ k \ d) \end{cases} \\
\equiv & \quad \{ \text{Definição de mul: mul (a, b) = (*) a b ; } \} \\
& \begin{cases} f \ k \cdot \underline{0} = \underline{1} \\ f \ k \cdot (d + 1) = mul \ (f \ k \ d, l \ k \ d) \end{cases} \\
\equiv & \quad \{ \text{Def split: (78)} ; \text{Def comp: (74)} ; \text{Definição de succ: succ d = d + 1 ; Igualdade extencional: (73)} \} \\
& \begin{cases} f \ k \cdot \underline{0} = \underline{1} \\ f \ k \cdot (\text{succ}) = mul \cdot \langle f \ k, l \ k \rangle \end{cases} \\
\equiv & \quad \{ \text{Eq + : (27)} ; \text{Natural id : (1)} \} \\
& [f \ k \cdot \underline{0}, f \ k \cdot (\text{succ})] = [\underline{1} \cdot id, mul \cdot \langle f \ k, l \ k \rangle] \\
\equiv & \quad \{ \text{Fusão + : (20)} ; \text{Absorção x : (11)} \} \\
& f \ k \cdot [\underline{0}, (\text{succ})] = [\underline{1}, mul] \cdot (id + \langle f \ k, l \ k \rangle) \\
\equiv & \quad \{ \text{Definição de in e functor (dos naturais): in} = [\underline{0}, (\text{succ})] , F \ \langle f \ k, l \ k \rangle = (id + \langle f \ k, l \ k \rangle) \} \\
& f \ k \cdot \mathbf{in} = [\underline{1}, mul] \cdot F \ \langle f \ k, l \ k \rangle
\end{aligned}$$

Logo, $o = [\underline{1}, mul]$.

(b) Descobrir p (com a ajuda da função l , k)

$$\begin{aligned}
& \begin{cases} l \ k \ 0 = k + 1 \\ l \ k \ (d + 1) = l \ k \ d + 1 \end{cases} \\
\equiv & \quad \{ \text{Def comp: (74)} \} \\
& \begin{cases} l \ k \cdot 0 = k + 1 \\ l \ k \cdot (d + 1) = l \ k \ d + 1 \end{cases} \\
\equiv & \quad \{ \text{Definição de succ: succ d = d + 1 ; Def const: (76)} ; \text{Igualdade extencional: (73)} \} \\
& \begin{cases} l \ k \cdot \underline{0} = \underline{(\text{succ } k)} \\ l \ k \cdot (\text{succ}) = \text{succ} \cdot (l \ k) \end{cases} \\
\equiv & \quad \{ \text{Eq + : (27)} ; \text{Natural id : (1)} \} \\
& [l \ k \cdot \underline{0}, l \ k \cdot (\text{succ})] = [\underline{(\text{succ } k)}, \text{succ} \cdot l \ k] \\
\equiv & \quad \{ \text{Natural id : (1)} ; \text{Cancelamento x : (7)} \} \\
& [l \ k \cdot \underline{0}, l \ k \cdot (\text{succ})] = [\underline{(\text{succ } k)} \cdot id, \text{succ} \cdot \pi_2 \cdot \langle f \ k, l \ k \rangle] \\
\equiv & \quad \{ \text{Fusão + : (20)} ; \text{Absorção x : (11)} \} \\
& l \ k \cdot [\underline{0}, (\text{succ})] = [\underline{(\text{succ } k)}, \text{succ} \cdot \pi_2] \cdot (id + \langle f \ k, l \ k \rangle) \\
\equiv & \quad \{ \text{Definição de in e functor (dos naturais): in} = [\underline{0}, (\text{succ})] , F \ \langle f \ k, l \ k \rangle = (id + \langle f \ k, l \ k \rangle) \} \\
& l \ k \cdot \mathbf{in} = [\underline{(\text{succ } k)}, \text{succ} \cdot \pi_2] \cdot F \ \langle f \ k, l \ k \rangle
\end{aligned}$$

Logo, $p = [(\text{succ } k), \text{succ} \cdot \pi_2]$.

Deste modo, após encontrarmos a definição de o e de p conseguimos determinar a definição de $\langle f \ k, l \ k \rangle$ uma vez que já havíamos concluído que $\langle f \ k, l \ k \rangle = \langle \langle o, p \rangle \rangle$.

Logo, $\langle f \ k, l \ k \rangle = \langle \langle [1, \text{mul}], [(\text{succ } k), \text{succ} \cdot \pi_2] \rangle \rangle$.

2. Determinar $\langle g, s \rangle$

Para descobrir $\langle g, s \rangle$ seguimos o mesmo raciocínio, isto é, tentamos descobrir um v e um j de modo a podermos aplicar a lei da recursividade múltipla:

$$\begin{aligned} & \begin{cases} g \cdot \text{in} = v \cdot F \langle g, s \rangle \\ s \cdot \text{in} = j \cdot F \langle g, s \rangle \end{cases} \\ \equiv & \quad \{ \text{Fokkinga: (50)} \} \\ & \langle g, s \rangle = \langle \langle v, j \rangle \rangle \end{aligned}$$

(a) Descobrir v (com a ajuda da função g)

$$\begin{aligned} & \begin{cases} g \ 0 = 1 \\ g \ (d + 1) = (g \ d) * (s \ d) \end{cases} \\ \equiv & \quad \{ \text{Def comp: (74)} ; (*) \text{ escrita como função prefixo} \} \\ & \begin{cases} g \cdot 0 = 1 \\ g \cdot (d + 1) = (*) \ (g \ d) \ (s \ d) \end{cases} \\ \equiv & \quad \{ \text{Igualdade extencional: (73)} ; \text{Def const: (76)} \} \\ & \begin{cases} g \cdot \underline{0} = \underline{1} \\ g \cdot (d + 1) = (*) \ (g \ d) \ (s \ d) \end{cases} \\ \equiv & \quad \{ \text{Definição de mul: mul (a, b) = (*) a b ; } \} \\ & \begin{cases} g \cdot \underline{0} = \underline{1} \\ g \cdot (d + 1) = \text{mul} \ (g \ d, s \ d) \end{cases} \\ \equiv & \quad \{ \text{Def split: (78)} ; \text{Def comp: (74)} ; \text{Definição de succ: succ d = d + 1 ; Igualdade extencional: (73)} \} \\ & \begin{cases} g \cdot \underline{0} = \underline{1} \\ g \cdot (\text{succ}) = \text{mul} \cdot \langle g, s \rangle \end{cases} \\ \equiv & \quad \{ \text{Eq + : (27)} ; \text{Natural id : (1)} \} \\ & [g \cdot \underline{0}, g \cdot (\text{succ})] = [\underline{1} \cdot \text{id}, \text{mul} \cdot \langle g, s \rangle] \\ \equiv & \quad \{ \text{Fusão + : (20)} ; \text{Absorção x : (11)} \} \\ & g \cdot [\underline{0}, (\text{succ})] = [\underline{1}, \text{mul}] \cdot (\text{id} + \langle g, s \rangle) \\ \equiv & \quad \{ \text{Definição de in e functor (dos naturais): in} = [\underline{0}, (\text{succ})] , F \langle g, s \rangle = (\text{id} + \langle g, s \rangle) \} \\ & g \cdot \text{in} = [\underline{1}, \text{mul}] \cdot F \langle g, s \rangle \end{aligned}$$

Logo, $v = [\underline{1}, \text{mul}]$.

(b) Descobrir j (com a ajuda da função s)

$$\begin{aligned} & \begin{cases} s \ 0 = 1 \\ s \ (d + 1) = s \ d + 1 \end{cases} \\ \equiv & \quad \{ \text{Def comp: (74)} \} \\ & \begin{cases} s \cdot 0 = 1 \\ s \cdot (d + 1) = s \ d + 1 \end{cases} \end{aligned}$$

$$\begin{aligned}
&\equiv \{ \text{Definição de succ: } \text{succ } d = d + 1 ; \text{Def const: (76) ; Igualdade extencional: (73) } \} \\
&\quad \left\{ \begin{array}{l} s \cdot \underline{0} = \underline{1} \\ s \cdot (\text{succ}) = \text{succ} \cdot s \end{array} \right. \\
&\equiv \{ \text{Eq } + : (27) ; \text{Natural id : (1) } \} \\
&\quad [s \cdot \underline{0}, s \cdot (\text{succ})] = [\underline{1}, \text{succ} \cdot s] \\
&\equiv \{ \text{Natural id : (1) ; Cancelamento x : (7) } \} \\
&\quad [s \cdot \underline{0}, s \cdot (\text{succ})] = [\underline{1} \cdot id, \text{succ} \cdot \pi_2 \cdot \langle g, s \rangle] \\
&\equiv \{ \text{Fusão } + : (20) ; \text{Absorção x : (11) } \} \\
&\quad s \cdot [\underline{0}, (\text{succ})] = [\underline{1}, \text{succ} \cdot \pi_2] \cdot (id + \langle s, g \rangle) \\
&\equiv \{ \text{Definição de in e functor (dos naturais): } \mathbf{in} = [\underline{0}, (\text{succ})], F \langle \langle s, g \rangle = (id + \langle s, g \rangle) \rangle \} \\
&\quad s \cdot \mathbf{in} = [\underline{1}, \text{succ} \cdot \pi_2] \cdot F \langle s, g \rangle
\end{aligned}$$

Logo, $j = [\underline{1}, \text{succ} \cdot \pi_2]$.

Deste modo, após encontrarmos a definição de v e de j conseguimos determinar a definição de $\langle g, s \rangle$ uma vez que já havíamos constatado que $\langle g, s \rangle = \langle \langle v, j \rangle \rangle$.

Logo, $\langle g, s \rangle = \langle \langle [\underline{1}, mul], [\underline{1}, \text{succ} \cdot \pi_2] \rangle \rangle$.

3. Aplicar a lei de banana split à definição de $\langle f \ k, l \ k \rangle$ e $\langle g, s \rangle$

A lei de banana split (51) é a seguinte:

$$\begin{aligned}
&\langle \langle i \rangle, \langle j \rangle \rangle \\
&\equiv \{ \text{Banana-split : (51) } \} \\
&\quad \langle (i \times j) \cdot \langle F \pi_1, F \pi_2 \rangle \rangle
\end{aligned}$$

Assim, podemos constatar que, no nosso caso:

$$\langle i \rangle = \langle \langle [\underline{1}, mul], [\underline{1}, \text{succ} \cdot \pi_2] \rangle \rangle$$

e

$$\langle j \rangle = \langle \langle [\underline{1}, mul], [\underline{1}, \text{succ} \cdot \pi_2] \rangle \rangle$$

Assim, retomando o resultado anterior e aplicando a lei temos:

$$\begin{aligned}
&\langle \langle \langle [\underline{1}, mul], [\underline{1}, \text{succ} \cdot \pi_2] \rangle, \langle [\underline{1}, mul], [\underline{1}, \text{succ} \cdot \pi_2] \rangle \rangle \rangle \\
&\equiv \{ \text{Banana-split : (51) } \} \\
&\quad \langle \langle \langle [\underline{1}, mul], [\underline{1}, \text{succ} \cdot \pi_2] \rangle \rangle \times \langle \langle [\underline{1}, mul], [\underline{1}, \text{succ} \cdot \pi_2] \rangle \rangle \rangle \cdot \langle F \pi_1, F \pi_2 \rangle
\end{aligned}$$

Agora podemos então continuar a resolver o problema, sempre com o intuito de chegar a um $\langle [b, i] \rangle$ para podermos aplicar a definição de ciclo for:

$$\text{for } b \ \underline{i} = \langle [i, b] \rangle$$

Retomando o resultado anterior e continuando a aplicar as leis do cálculo de programas, temos:

$$\begin{aligned}
&\langle \langle \langle [\underline{1}, mul], [\underline{1}, \text{succ} \cdot \pi_2] \rangle \rangle \times \langle [\underline{1}, mul], [\underline{1}, \text{succ} \cdot \pi_2] \rangle \rangle \cdot \langle F \pi_1, F \pi_2 \rangle \\
&\equiv \{ \text{Absorção x : (11) ; Lei da troca : (28) } \}
\end{aligned}$$

$$\begin{aligned}
& \langle \langle \langle \underline{1}, (\text{succ } k) \rangle, \langle \text{mul}, \text{succ} \cdot \pi_2 \rangle \rangle \cdot F \pi_1, [\langle \underline{1}, \underline{1} \rangle, \langle \text{mul}, \text{succ} \cdot \pi_2 \rangle] \cdot F \pi_2 \rangle \rangle \\
\equiv & \quad \{ \text{Definição do Functor (dos naturais): } F \pi_1 = id + \pi_1, F \pi_2 = id + \pi_2 \} \\
& \langle \langle \langle \underline{1}, (\text{succ } k) \rangle, \langle \text{mul}, \text{succ} \cdot \pi_2 \rangle \rangle \cdot (id + \pi_1), [\langle \underline{1}, \underline{1} \rangle, \langle \text{mul}, \text{succ} \cdot \pi_2 \rangle] \cdot (id + \pi_2) \rangle \rangle \\
\equiv & \quad \{ \text{Absorção } + : (22) \times 2 ; \text{Fusão } \times : (10) \times 2 ; \text{Natural id} : (1) \times 2 \} \\
& \langle \langle \langle \underline{1}, (\text{succ } k) \rangle, \langle \text{mul} \cdot \pi_1, \text{succ} \cdot \pi_2 \cdot \pi_1 \rangle \rangle, [\langle \underline{1}, \underline{1} \rangle, \langle \text{mul} \cdot \pi_2, \text{succ} \cdot \pi_2 \cdot \pi_2 \rangle] \rangle \rangle \\
\equiv & \quad \{ \text{Lei da troca : (28)} \} \\
& \langle \langle \langle \underline{1}, (\text{succ } k) \rangle, \langle \underline{1}, \underline{1} \rangle \rangle, \langle \langle \text{mul} \cdot \pi_1, \text{succ} \cdot \pi_2 \cdot \pi_1 \rangle, \langle \text{mul} \cdot \pi_2, \text{succ} \cdot \pi_2 \cdot \pi_2 \rangle \rangle \rangle \rangle \\
\equiv & \quad \{ \text{Definição de for: for } b \ i = \langle [i, b] \rangle \} \\
& \text{for } \langle \langle \text{mul} \cdot \pi_1, \text{succ} \cdot \pi_2 \cdot \pi_1 \rangle, \langle \text{mul} \cdot \pi_2, \text{succ} \cdot \pi_2 \cdot \pi_2 \rangle \rangle \langle \langle \underline{1}, (\text{succ } k) \rangle, \langle \underline{1}, \underline{1} \rangle \rangle
\end{aligned}$$

Assim, tendo em conta a definição do enunciado:

$$\text{for loop (base } k)$$

E comparando com o nosso resultado:

$$\text{for } \langle \langle \text{mul} \cdot \pi_1, \text{succ} \cdot \pi_2 \cdot \pi_1 \rangle, \langle \text{mul} \cdot \pi_2, \text{succ} \cdot \pi_2 \cdot \pi_2 \rangle \rangle \langle \langle \underline{1}, (\text{succ } k) \rangle, \langle \underline{1}, \underline{1} \rangle \rangle$$

Temos que:

$$\begin{aligned}
\text{loop} &= \langle \langle \text{mul} \cdot \pi_1, \text{succ} \cdot \pi_2 \cdot \pi_1 \rangle, \langle \text{mul} \cdot \pi_2, \text{succ} \cdot \pi_2 \cdot \pi_2 \rangle \rangle \\
\text{base } k &= \langle \langle \underline{1}, (\text{succ } k) \rangle, \langle \underline{1}, \underline{1} \rangle \rangle
\end{aligned}$$

4. Derivar a definição de base k

Focando em *base k*:

$$\text{base } k = \langle \langle \underline{1}, (\text{succ } k) \rangle, \langle \underline{1}, \underline{1} \rangle \rangle$$

Vamos agora introduzir variáveis à definição *pointfree* para podermos ter o resultado da função *base k* em *haskell*.

Uma vez que o tipo de *split*, por exemplo, $\langle id, id \rangle$ é:

$$\begin{array}{c}
A \\
\downarrow \langle id, id \rangle \\
A \times A
\end{array}$$

O tipo de $\langle \langle id, id \rangle, \langle id, id \rangle \rangle$ será:

$$\begin{array}{c}
A \\
\downarrow \langle \langle id, id \rangle, \langle id, id \rangle \rangle \\
(A \times A) \times (A \times A)
\end{array}$$

Assim, conseguimos perceber qual é o tipo da variável que temos que adicionar uma vez que no nosso caso também se trata de um *split* de *split*.

Logo, continuando a derivação:

$$\begin{aligned}
& \text{base } k = \langle \langle \underline{1}, (\text{succ } k) \rangle, \langle \underline{1}, \underline{1} \rangle \rangle \\
\equiv & \quad \{ \text{Igualdade extensional : (73)} \} \\
& \text{base } k = \langle \langle \underline{1}, (\text{succ } k) \rangle, \langle \underline{1}, \underline{1} \rangle \rangle a
\end{aligned}$$

$$\begin{aligned}
&\equiv \{ \text{Def split : (78)} \} \\
&\quad \text{base } k = (\langle \underline{1}, \underline{\text{succ } k} \rangle a, \langle \underline{1}, \underline{1} \rangle a) \\
&\equiv \{ \text{Def split : (78) x2} \} \\
&\quad \text{base } k = ((\underline{1} a, \underline{\text{succ } k} a), (\underline{1} a, \underline{1} a)) \\
&\equiv \{ \text{Def const : (76) x4 ; Definição de succ: succ } k = k + 1 \} \\
&\quad \text{base } k = ((1, k + 1), (1, 1))
\end{aligned}$$

Porém, tendo em consideração a implementação desejada:

$$\binom{n}{k} = h \ k \ (n - k) \text{ where } h \ k \ n = \text{let } (a, -, b, -) = \text{for loop } (base \ k) \ n \text{ in } a / b$$

Vemos que em $\text{let } (a, -, b, -)$ o tipo de dados é um quádruplo o que implica que os tipos de loop e $\text{base } k$, mais especificamente o tipo de retorno, terão que ser também um quádruplo (o $\text{for loop } (base \ k) \ n$, por sua vez, também deverá retornar um quádruplo).

Deste modo, através da aplicação de uma simples função que nos altere o tipo de dados, por exemplo:

$$\begin{aligned}
\text{altera} &:: ((a, b), (c, d)) \rightarrow (a, b, c, d) \\
\text{altera} &((a, b), (c, d)) = (a, b, c, d)
\end{aligned}$$

Conseguimos ter a derivação desejada da função $\text{base } k$:

$$\text{base } k = (1, k + 1, 1, 1)$$

5. Derivar a definição de loop

Por último, para derivar a definição de loop teremos que pensar da mesma forma, ou seja, inserir variáveis. Porém, ao contrário da função $\text{base } k$, as variáveis a inserir terão que ser do tipo $((a, b), (c, d))$ uma vez que temos um split com projeções π_1 e π_2 . Nos diagramas abaixo pode-se verificar o motivo desta diferença de domínio:

Tendo em conta o primeiro split do split maior, temos:

$$\begin{array}{c}
(A \times B) \times (C \times D) \\
\downarrow \langle \text{mul} \cdot \pi_1, \text{succ} \cdot \pi_2 \cdot \pi_1 \rangle \\
Z \times B
\end{array}$$

É de salientar que o tipo $\text{mul } (a, b) = a * b$, ou seja, o tipo desta função é:

$$\begin{array}{c}
(A \times B) \\
\downarrow \text{mul} \\
Z
\end{array}$$

Tendo agora em consideração o segundo split do split maior, temos:

$$\begin{array}{c}
(A \times B) \times (C \times D) \\
\downarrow \langle \text{mul} \cdot \pi_2, \text{succ} \cdot \pi_2 \cdot \pi_2 \rangle \\
(Z \times D)
\end{array}$$

Temos então,

$$\begin{aligned}
&\text{loop} = \langle \langle \text{mul} \cdot \pi_1, \text{succ} \cdot \pi_2 \cdot \pi_1 \rangle, \langle \text{mul} \cdot \pi_2, \text{succ} \cdot \pi_2 \cdot \pi_2 \rangle \rangle \\
&\equiv \{ \text{Igualdade extensional : (73)} \}
\end{aligned}$$

$$\begin{aligned}
& loop = \langle \langle mul \cdot \pi_1, succ \cdot \pi_2 \cdot \pi_1 \rangle, \langle mul \cdot \pi_2, succ \cdot \pi_2 \cdot \pi_2 \rangle \rangle ((a, b), (c, d)) \\
\equiv & \quad \{ \text{Def split : (78)} \} \\
& loop = (\langle mul \cdot \pi_1, succ \cdot \pi_2 \cdot \pi_1 \rangle ((a, b), (c, d)), \langle mul \cdot \pi_2, succ \cdot \pi_2 \cdot \pi_2 \rangle ((a, b), (c, d))) \\
\equiv & \quad \{ \text{Def split : (78) x2 ; Def comp : (74) x6 ; Def proj : (81) x6 } \} \\
& loop = ((mul (a, b), succ b), (mul (c, d), succ d)) \\
\equiv & \quad \{ \text{Definição de succ : succ k = k + 1 x2 ; Definição de mul : mul (m,n) = m * n x2 } \} \\
& loop = ((a * b, b + 1), (c * d, d + 1))
\end{aligned}$$

Deparámo-nos com o mesmo problema da função *base k* e por isso vamos aplicar novamente a função *altera* para reparar o tipo de dados de retorno. Temos então:

$$loop (a, b, c, d) = (a * b, b + 1, c * d, d + 1)$$

Deste modo, obtemos os dois resultados pretendidos:

$$base\ k = (1, k + 1, 1, 1)$$

$$loop (a, b, c, d) = (a * b, b + 1, c * d, d + 1)$$

Problema 4

```

inFTree = ⊥
outFTree = ⊥
baseFTree = ⊥
recFTree = ⊥
cataFTree = ⊥
anaFTree = ⊥
hyloFTree = ⊥
instance Bifunctor FTree where
  bimap = ⊥
  generatePTree = ⊥
  drawPTree = ⊥

```

Problema 5

```

singletonbag = ⊥
μ = ⊥
dist = ⊥

```

D Como exprimir cálculos e diagramas em LaTeX/lhs2tex

Estudar o texto fonte deste trabalho para obter o efeito:⁷

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

□

⁷Exemplos tirados de [?].

Os diagramas podem ser produzidos recorrendo à *package* \LaTeX `xymatrix`, por exemplo:

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