Métodos Formais em Engenharia de Software

1.º Ano de Mestrado de Informática da Universidade do Minho
Ano Lectivo de 2008/09

Exame de recurso — 23 de Julho de 2009
09h00
Sala DI 1.08

NB*: Esta prova consta de **8** alíneas todas com as mesma cotação.*

PROVA COM CONSULTA (2 horas)

Questão 1 Suponha que M e N são relações simples e que pretende exprimir os invariantes seguintes sobre essas relações:

(a) Os domínios de M e N são disjuntos

(b) Para valores comuns aos seus domínios, M e N dão o mesmo valor

(c) O domínio de M é fechado por N, isto é $\langle \forall\ x\ :\ x \in dom\ M :\ x \in dom\ N \Rightarrow (N\ x) \in dom\ M \rangle$

Escolha (justificando) que expressões seguintes do cálculo relacional exprimem os invariantes indicados:

$$M \subseteq M \cdot \delta\, N \tag{1}$$
$$N \cdot M^\circ \subseteq id \tag{2}$$
$$M \cdot N^\circ \subseteq \bot \tag{3}$$
$$M \cdot N^\circ \subseteq \top \cdot M \tag{4}$$

Questão 2 Vamos escrever $R \xleftarrow{f} S$ sempre que $f(R \leftarrow S)f$ se verifica, isto é, sempre que o diagrama

$$\begin{array}{ccc} A & \xleftarrow{S} & B \\ {\scriptstyle f}\downarrow & \subseteq & \downarrow{\scriptstyle f} \\ C & \xleftarrow[R]{} & D \end{array} \tag{5}$$

comuta.

Seja agora s um *stream* representado como uma função de $\mathbb{N}_0$ (índices ou posições no *stream*) para A, o tipo de elementos que estão a ser *streamed*. Seja ainda $\sqsubseteq$ uma ordem total em A. Se escrevermos

$$\sqsubseteq \xleftarrow{s} \leq \tag{6}$$

que propriedade de s está a ser declarada? Justifique convenientemente a sua resposta.

Questão 3 A conecção de Galois

$$\rho\,(f \cdot \Phi) \subseteq \Psi \quad \Leftrightarrow \quad \Phi \subseteq \delta\,(\Psi \cdot f) \tag{7}$$

decorre facilmente das leis the *shunting* de funções e outras propriedades do cálculo relacional que conhece. Prove-o.

Questão 4 Uma das funções básicas do *Prelude* do Haskell é a função

```
zipWith :: (a -> b -> c) -> [a] -> [b] -> [c]
```

Se invocar o calculador de teoremas grátis disponibilizado por Janis Voigtlaender em

```
http://linux.tcs.inf.tu-dresden.de/~voigt/ft
```

(restrito a funções) obterá o seguinte resultado:

```
forall g :: t1 -> t2.
 forall h :: t3 -> t4.
  forall k :: t5 -> t6.
   forall p :: t1 -> t3 -> t5.
    forall q :: t2 -> t4 -> t6.
     (forall x :: t1. forall y :: t3. k (p x y) = q (g x) (h y))
     ==> (forall z :: [t1].
           forall v :: [t3]. map k (zipWith p z v) = zipWith q (map g z) (map h v))
```

Calcule o teorema grátis associado ao tipo de $zipWith$ por forma a validar o corolário que acima obteve automaticamente, completando o cálculo relacional *pointfree* que se segue:

$$
\begin{array}{cl}
& zipWith\ (R_{c^\star \leftarrow b^\star \leftarrow a^\star \leftarrow ((c \leftarrow b) \leftarrow a)})\ zipWith \\
\Leftrightarrow & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& zipWith\ (R_{c^\star \leftarrow b^\star \leftarrow a^\star} \leftarrow R_{(c \leftarrow b) \leftarrow a})\ zipWith \\
\Leftrightarrow & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& zipWith \cdot R_{(c \leftarrow b) \leftarrow a} \subseteq R_{c^\star \leftarrow b^\star \leftarrow a^\star} \cdot zipWith \\
\Leftrightarrow & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& \vdots
\end{array}
$$

Questão 5 A sobreposição $R \dagger S$ de duas relações R e S é a relação que se comporta como S sempre que esta está definida e que, quando isso não acontece, se comporta como R. A definição que se segue é sugestiva desse comportamento,

$$R \dagger S \quad \triangleq \quad S \rightarrow S, R \tag{8}$$

em que se recorre à seguinte variante do condicional de McCarthy,

$$R \rightarrow S, U \quad \stackrel{\mathrm{def}}{=} \quad (S \cdot \delta\, R) \cup (U \cdot \neg\delta\, R)$$

onde o operador de *negação* de coreflexivas satisfaz a propriedade

$$\neg\Phi \cdot (\neg\Psi) \quad = \quad \neg(\Phi \cup \Psi) \tag{9}$$

(Lei de de Morgan).

1. Sendo fácil de mostrar que a definição (8) acima é equivalente a

$$R \dagger S \quad = \quad S \cup R \cdot (\neg\delta\, S) \tag{10}$$

complete o cálculo seguinte da propriedade associativa de †:

$$
\begin{array}{cl}
& (R \dagger S) \dagger P \\
= & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& P \rightarrow P, (S \rightarrow S, R) \\
= & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& P \cup (S \cup R \cdot (\neg\delta\, S)) \cdot (\neg\delta\, P) \\
= & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& P \cup S \cdot (\neg\delta\, P) \cup R \cdot (\neg(\delta\, S \cup \delta\, P)) \\
= & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& (S \dagger P) \cup R \cdot (\neg\delta\, (S \dagger P)) \\
= & \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \quad \} \\
& R \dagger (S \dagger P)
\end{array}
$$

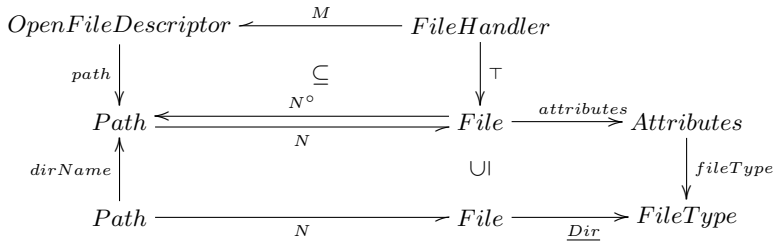
2. Demonstre a propriedade distributiva

$$\Phi \cdot (R \dagger S) = (\Phi \cdot R) \dagger (\Phi \cdot S) \quad \Leftarrow \quad S \preceq \Phi \cdot S \tag{11}$$

onde a ordem $\preceq$ é a ordem de definição de relações:

$$M \preceq N \quad = \quad \delta\, M \subseteq \delta\, N \tag{12}$$

Questão 6 O modelo abstracto de um sistema de ficheiros tipo POSIX estudado nas aulas consta (recorda-se) de duas relações simples: a tabela dos ficheiros em uso (M) e a relação *path*/ficheiro propriamente dita (N). Recorda-se ainda que N está condicionada por um invariante que nas aulas designámos por pc ('prefix-closed') e que corresponde ao rectângulo inferior do diagrama seguinte:



Por outras palavras, N é a relação simples que representa o armazenamento de ficheiros propriamente dito (*file store*), de tipo

$$FStore = Path \rightharpoonup File$$
$$\textbf{inv}\ \ store \triangleq pc\, store$$

Seja

$$unzip(Z : FStore)$$
$$\textbf{wr}\ N : FStore$$
$$\textbf{pre}\ \ldots$$
$$\textbf{post}\ \ N' = N \dagger Z$$

a especificação da semântica formal (muito simplificada!) do comando `unzip`, escrita em estilo VDM, cuja pós-condição recorre ao operador de sobreposição que é assunto da questão 5 desta prova.

1. Complete o processo de cálculo que se segue de uma pre-condição suficiente para que a operação em causa não viole o invariante pc (onde dn abrevia $dirName$ e $ft = fileType \cdot attributes$):

$$\begin{array}{ll}
 & pc(N \dagger Z) \\
\Leftrightarrow & \quad \{\ \ldots\ \} \\
 & \underline{Dir} \cdot (N \dagger Z) \subseteq ft \cdot (N \dagger Z) \cdot dn \\
\Leftrightarrow & \quad \{\ \ldots\ \} \\
 & \quad \left\{ \begin{array}{l} \underline{Dir} \cdot Z \subseteq ft \cdot (N \dagger Z) \cdot dn \\ \underline{Dir} \cdot (N \cdot \neg\delta\, Z) \cdot dn^\circ \subseteq ft \cdot (N \dagger Z) \end{array} \right. \\
\Leftarrow & \quad \{\ \ldots\ \} \\
 & \quad \left\{ \begin{array}{l} \underline{Dir} \cdot Z \subseteq ft \cdot Z \cdot dn \\ \underline{Dir} \cdot (N \cdot \neg\delta\, Z) \cdot dn^\circ \subseteq ft \cdot (N \dagger Z) \end{array} \right. \\
\Leftrightarrow & \quad \{\ \ldots\ \} \\
 & \quad \left\{ \begin{array}{l} pc\, Z \\ \underline{Dir} \cdot (N \cdot \neg\delta\, Z) \cdot dn^\circ \subseteq ft \cdot Z \cup ft \cdot N \cdot \neg\delta\, Z \end{array} \right. \\
\Leftrightarrow & \quad \{\ \ldots\ \} \\
 & \quad \left\{ \begin{array}{l} Z \in FStore \\ \underline{Dir} \cdot (N \cdot \neg\delta\, Z) \cdot dn^\circ \cdot (\delta\, Z) \subseteq ft \cdot Z \cup ft \cdot N \cdot \neg\delta\, Z \\ \underline{Dir} \cdot (N \cdot \neg\delta\, Z) \cdot dn^\circ \cdot (\neg\delta\, Z) \subseteq ft \cdot Z \cup ft \cdot N \cdot \neg\delta\, Z \end{array} \right.
\end{array}$$

$$\Leftarrow \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \}$$

$$\left\{ \begin{array}{l} \underline{Dir} \cdot (N \cdot \neg\delta\, Z) \cdot dn^\circ \cdot (\delta\, Z) \subseteq ft \cdot Z \\ \underline{Dir} \cdot (N \cdot \neg\delta\, Z) \cdot dn^\circ \cdot (\neg\delta\, Z) \subseteq ft \cdot N \cdot \neg\delta\, Z \end{array} \right.$$

$$\Leftrightarrow \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \}$$

$$\left\{ \begin{array}{l} \underline{Dir} \cdot (N \cdot \neg\delta\, Z) \cdot dn^\circ \cdot (\delta\, Z) \subseteq ft \cdot Z \\ \underline{Dir} \cdot (N \cdot \neg\delta\, Z) \cdot dn^\circ \cdot (\neg\delta\, Z) \subseteq ft \cdot N \end{array} \right.$$

$$\Leftarrow \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \}$$

$$\left\{ \begin{array}{l} \underline{Dir} \cdot (N \cdot \neg\delta\, Z) \cdot dn^\circ \cdot (\delta\, Z) \subseteq ft \cdot Z \\ \underline{Dir} \cdot N \cdot dn^\circ \subseteq ft \cdot N \end{array} \right.$$

$$\Leftrightarrow \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \}$$

$$\left\{ \begin{array}{l} \underline{Dir} \cdot (N \cdot \neg\delta\, Z) \cdot dn^\circ \cdot (\delta\, Z) \subseteq ft \cdot Z \\ pc\, N \end{array} \right.$$

$$\Leftrightarrow \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \}$$

$$\left\{ \begin{array}{l} \underline{Dir} \cdot (N \cdot \neg\delta\, Z) \cdot dn^\circ \cdot (\delta\, Z) \subseteq ft \cdot Z \\ N \in FSTore \end{array} \right.$$

$$\Leftrightarrow \quad \{ \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \}$$

$$\underline{Dir} \cdot (N \cdot \neg\delta\, Z) \cdot (Z \cdot dn)^\circ \subseteq ft$$

2. Introduza variáveis na pré-condição calculada e escreva-a em notação VDM ou Alloy. Apoie a sua resposta com um diagrama relacional explicativo dos tipos involvidos.
Sugestão: recorra a leis de *shunting* que desloquem material da esquerda para a direita da inclusão antes da tradução para notação *pointwise*, por forma a minimizar o número de quantificadores existenciais.