On the Design of a *Periodic* Table of VDM Specifications

J. N. Oliveira

Presented by Paulo Bernardes

Program Semantics, Verification and Construction - MAPi – Di – Uminho

Braga, 18 October 2010

Universidade do Minho

Motivation

- Formal modelling
  - ➢ Reliable software description
    - ❖ But... What is really innovative in new models?
      - ▪ Domain-specific terminology
- Algorithmics
  - ➢ Difficult to understand → very unstructed
  - ➢ Factorization Methods → algorithmic elements
    - ❖ Component-oriented programming and software reuse
- Factorization vs. Calculation
  - ➢ Fundamental Theorem of Arithmetics
  - ➢ Is there a *fundamental theorem* for software code factorization?

Universidade do Minho

Algorithm and Data Specification

- Data precede Algorithms
  - Visible data-structure
  - Invisible data-structure → rôle in algorithm factorization
- Divide-and-conquer

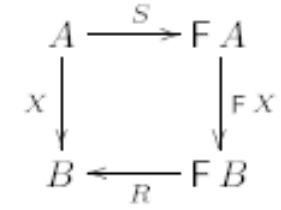
$$\begin{array}{ccc} A & \xrightarrow{\ divide\ } & \mathsf{F}A \\ {\scriptstyle solve}\uparrow & & \downarrow{\scriptstyle \mathsf{F}\ solve} \\ B & \xleftarrow[\ conquer\ ]{} & \mathsf{F}B \end{array}$$

- Binary Relations
  - Total/partial functions
  - Predicates; datatype invariants and loop-invariants
  - Orders and inductive structures
  - Nondeterminism
  - Vagueness or under-specification

Universidade do Minho

A relational approach to divide-and-conquer

- The divide-and-conquer scheme



- The *hylo equation*

$$X = R \cdot (\mathsf{F}\, X) \cdot S$$

- The meaning of **F**
  - **F** is a relator

$$\mathsf{F}\,(R \cdot S) = (\mathsf{F}\, R) \cdot (\mathsf{F}\, S)$$
$$\mathsf{F}\,(R^\circ) = (\mathsf{F}\, R)^\circ$$
$$\mathsf{F}\, id = id$$

Universidade do Minho

A relational approach to divide-and-conquer

- How to solve the previous hylo-equation?
  - Unique least solution $\mu X.R \cdot (\mathsf{F}\, X) \cdot S$
  - Suppose $X = X_2 \cdot X_1$
  - Then

$$C \xleftarrow{T} \mathsf{F}\, C$$

$$\begin{array}{ccc} A & \xrightarrow{S} & \mathsf{F}\, A \\ {\scriptstyle X_1}\downarrow & & \downarrow{\scriptstyle \mathsf{F}\, X_1} \\ C & \xleftarrow[T]{} & \mathsf{F}\, C \\ {\scriptstyle X_2}\downarrow & & \downarrow{\scriptstyle \mathsf{F}\, X_2} \\ B & \xleftarrow[R]{} & \mathsf{F}\, B \end{array}$$

Universidade do Minho

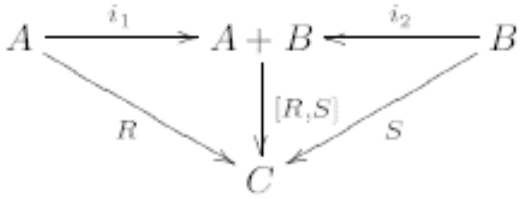
A relational approach to divide-and-conquer

- S must be "well-fouded" $\rightarrow$ sub-problem stricly smaller
- T must de bijective $\rightarrow$ C=μF
- And

$$\langle b, d\rangle (R \times S)\langle a, c\rangle \equiv (bRa) \wedge (dSc)$$

$$R + S = [i_1 \cdot R, i_2 \cdot S]$$

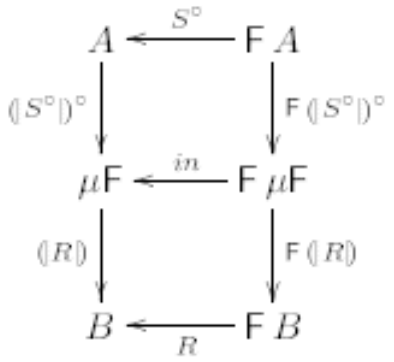
$$c[R, S](i_1\, a) \equiv cRa$$
$$c[R, S](i_2\, b) \equiv cSb$$



Universidade do Minho

A relational approach to divide-and-conquer

- Returning to the divide-and-conquer diagram



- The **hylo-factorization theorem**

$$\mu X.(R \cdot \mathsf{F}\ X \cdot S) = (\!|R|\!) \cdot (\!|S^\circ|\!)^\circ$$

$$\mu X.(R \cdot \mathsf{F}\ X \cdot S^\circ) = (\!|R|\!) \cdot (\!|S|\!)^\circ$$

A "*periodic*" Table of Algorithms

Table1 – Sample of a VDM-SL specification repository

$\mathsf{F}\,X$	$1+X$	$1+A\times X$	$A+X^2$	$1+A\times X^2$	$(B\times A+B\times X)^*$
$\mu\mathsf{F}$	nat	$\texttt{seq of}\ A$	$LTree$	$BTree$	$HTree$
$In\to Out$	**Specifications**				
$nat\to bool$	odd $even$				
$nat\to nat$		$square$ $factorial$	$fibonnaci$ $doubleFactorial$		
$nat\to\texttt{set of}\ nat1$		$inseg$			
$\texttt{seq of}\ A\to\texttt{seq of}\ A$		$insertSort$ $invSeq$	$mergeSort$	$quickSort$	
$\texttt{seq of}\ A\to bool$		$ordSeq$			
$\texttt{seq of}\ A\to\texttt{set of}\ A$		$elems$			
$\texttt{seq of}\ A\to\texttt{set of}\ nat1$		$inds$			
$\texttt{seq of}\ A\to\texttt{Bag of}\ A$		$seq2bag$			
$\texttt{seq of}\ A\to nat$		len			
$LTree\to bool$			$balLTree$		
$LTree\to nat$			$depthLTree$		
$LTree\to int$			$addLTree$ $countLTree$		
$LTree\to\texttt{seq of}\ A$			$tips$		
$LTree\to LTree$			$invLTree$		
$BTree\to bool$				$ordBTree$ $balBTree$	
$BTree\to nat$				$depthBTree$	
$BTree\to\texttt{seq of}\ A$				$preOrder$ $inOrder$ $postOrder$	
$BTree\to\texttt{seq of seq of}\ A$				$traces$	
$BTree\to BTree$				$invBTree$	
$\texttt{set of}\ A\to nat$		$card$			
$\texttt{set of}\ A\to\texttt{seq of}\ A$		$Set2seq$			
$\texttt{set of}\ bool\to bool$		$\forall$ $\exists$			
$\texttt{set of set of}\ A\to\texttt{set of}\ A$		$dunion$			
$\texttt{map}\ A\ \texttt{to}\ B\to\texttt{set of}\ A$		dom			
$\texttt{map}\ A\ \texttt{to}\ B\to\texttt{set of}\ B$		ran			
$\texttt{set of}\ (\texttt{map}\ A\ \texttt{to}\ B)\to\texttt{map}\ A\ \texttt{to}\ B$		$merge$			
$PTree\to\texttt{Bag of}\ A$					$explode$
$FS\to\texttt{map}\ String\ \texttt{to}\ A$					tar
$(Other)$				$hanoi$	

A "*periodic*" Table of Algorithms

Table2 – Sample of *Periodic* Table of VDM specifications elements

$\mathsf{F}\,X$	$1+X$	$1+A\times X$	$A+X^2$	$1+A\times X^2$	$(B\times A+B\times X)^*$
$\mu\mathsf{F}$	nat	$\texttt{seq of}\ A$	$LTree$	$BTree$	$HTree$
Carrier	**F-(co)algebras**				
$bool$	$[\underline{\mathtt{F}}, \neg]$ $[\underline{\mathtt{T}}, \neg]$	$[\underline{\mathtt{F}}, \vee]$ $[\underline{\mathtt{T}}, \wedge]$	$[\underline{\mathtt{F}}, \vee]$ $[\underline{\mathtt{T}}, \wedge]$		
nat	$[\underline{0}, suc]$	$[\underline{0}, +]$ $odds^\circ$ $[\underline{1}, *]$ $nats^\circ$	$[id, +]$ $[id, *]$ $[\underline{1}, +]$ $fibd^\circ$	$[\underline{1}, bmul]$ $[\underline{0}, badd]$	
$nat * nat$			$dfacd^\circ$		
$\texttt{seq of}\ A$		$[[\underline{\ }], cons]$ $[[\underline{\ }], rcons]$ $[[\underline{\ }], \hat{\ }]$	$[singl, \hat{\ }]$ $[singl, pconc]$ $[singl, lmerge]$	$[[\underline{\ }], inord]$ $[[\underline{\ }], pinord]$ $[[\underline{\ }], prord]$ $[[\underline{\ }], psord]$	
$LTree$			in $in\cdot(id+sw)$		
$BTree$				in $in\cdot(id+id\times sw)$	
$HTree$					in
$\texttt{set of}\ A$		ins $pins$ $[\underline{\emptyset}, \cup]$ $ins\cdot(id+\pi_1\times id)$ $ins\cdot(id+\pi_2\times id)$	$[\lambda x.\{x\}, \cup]$	$[\underline{\emptyset}, bputs]$	
$\texttt{map}\ A\ \texttt{to}\ B$		ins $pins$ $[\underline{\{\mapsto\}}, munion]$			
$PTree$					$exsplit^\circ$
$\texttt{Bag of}\ A$					$exjoin$
$FileS$					$tsplit^\circ$
$\texttt{map}\ String\ \texttt{to}\ A$					$tjoin$
$(Other)$				$hsplit^\circ$	

Universidade do Minho

Thank You! ☺