PRESENTATIONS

LOTOSPHERE WORKSHOP

3 - 4 May 1990

PTT Research Neher

Laboratories

Leidschendam

The Netherlands

Reference : Lo/WP1/T1.2/IEI/N0012/V1

ESPRIT Project 2304[1]

Title : **Partial Correctness Preservation for Extensive Transformations**

Status : Public

Type : Foreground, Preliminary

Editor : A. Fantechi

Date : Wed, May 3, 1990

Distribution : PM, WP1M, T1.2

Owner :

Note : Copies of the transparencies presented at the LOTOSPHERE WORKSHOP

Leidschendam, The Netherlands, 3 May 1990

[1] The LOTOSPHERE consortium consists of the following companies/institutes/universities:

Alcatel Standard Electrica, Ascom Tech, British Telecommunications, C.N.R.-CNUCE, PTT-DNL, Consorzio Pisa Ricerche, Gesellschaft für Mathematik und Datenverarbeitung, C.N.R.- Istituto di Elaborazione della Informazione, Institut National de Recherche en Informatique et en Automatique, Laboratoire d'Automatique et d'Analyse des Systemes du CNRS, Océ Nederland, SYSECA Logiciel, TECSIEL, Technische Universität Berlin, Universidad Politécnica de Madrid, University of Stirling, University of Twente.

A page from the "Catalogue"

1.4.14 MULTI-WAY TO TWO-WAY SYNCHRONIZATION

Informal description

Starting from any process P, the transformation requirement imposes that each action of process Q be performed at most by two entities. That is, the degree of synchronization associated to Q should be at most 2 (the SyncDegree() view function is defined in Section 1.3.6). A variant of this problem imposes a bound on the synchronization degrees relative to a predefined subset of gates.

Motivation

In many concurrent programming languages it is not allowed to perform multi-way synchronization within a single communication construct, but only two-way communications with two-way. It is then likely that specifications developed in the latest phases of the design trajectory will contain only two-way communications.

Formal description

Auxiliary concepts SyncDegree().

Input PD: a process definition.

Output QD: a process definition.

Transformation requirements SyncDegree(QD) ≤ 2.

Correctness preservation requirements ----- *V O I D* -----

%

Example

```
process P[a] : noexit :=
  ...
  a !endtransaction; exit
  |[a]|
  ( SlaveTrans_1[a] |[a]| SlaveTrans_2[a] |[a]| SlaveTrans_3[a] )
  ...
where
  process SlaveTrans_1[a] : noexit :=
    ....
    a ?x : signal-sort ;
    ....
  endproc

  process SlaveTrans_2[a] : noexit :=
    ....
    a ?x : signal-sort ;
    ....
  endproc

  process SlaveTrans_3[a] : noexit :=
    ....
    a ?x : signal-sort ;
    ....
  endproc
endproc
```

PD

```
process Q[a] : noexit :=
  ...
  a !endtransaction; a !endtransaction; a !endtransaction; exit
  |[a]|
  ( SlaveTrans_1[a] ||| SlaveTrans_2[a] ||| SlaveTrans_3[a] )
  ...
where
...
endproc
```

QD

Solutions ----- *V O I D* -----

EXTENSIVE transformation
in the sense that it does not preserve any equivalence relation

need to define a "weaker" notion of correctness

An attempt to fill the "Correctness Preservation Requirement" field

Every time PD performs a broadcast communication on a,

every subprocess Q of QD should be ready

to perform a two-way synchronization on a.

TEMPORAL LOGIC expression:

$$PD \models a \quad \Leftrightarrow \quad \forall Q \in QD, \quad Q \models e\mathcal{U}a$$

and SyncDegree (QD) ≤ 2

- This "partial" property still does not characterize completely the transformation, but is preserved by it
- Non Constructive (Solutions field still VOID)
- Compositionality -> Formulae satisfied by processes as composition of formulae satisfied by subprocesses

FORMALISMS TO EXPRESS PARTIAL PROPERTIES

Temporal Logic

$$\Box (\text{query} \Rightarrow \Diamond \text{reply})$$

Partial Process specification

P := a; *unknown* ; P

"wild card"
"abstraction"

USES OF PARTIAL PROPERTIES

Definition of correctness requirements

Verification of Partial Properties on a specification

Analysis of a specification by Partial Properties
(seen as experiments)

Derivation of Partial Properties by a specification

Properties not expressible in LOTOS (e.g. *fairness*)

.....

THREE APPROACHES PURSUED

TEMPORAL SEMANTICS (IEI- CNR - PISA)

ANALYSIS BY REDUCTION (INRIA - SOPHIA ANTIPOLIS)

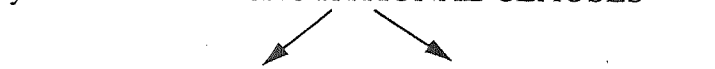
TEMPORAL LOGIC AND REDUCTION COMBINED
(LAAS - CNRS - TOULOUSE)

TEMPORAL SEMANTICS

Function $\mathcal{L}$: LOTOS ⟶ TL

associates a formula to a behaviour expression

Definition by means of DENOTATIONAL CLAUSES



- The formula obtained has a structure similar to that of the behaviour expression

(Limited) Treatment also of non finite-state cases

- Mainly aimed at establishing a correspondence between LOTOS processes and Temporal Logic formulae

- Verification of Partial Properties defined in Temporal Logic possible:

$$P \text{ satisfies } \phi \quad \text{iff} \quad \mathcal{L}(P) \Rightarrow \phi$$

Linear Temporal Semantics

$$\mathcal{L}(\text{stop}) = e\ \mathcal{W}\ \text{false} \qquad \mathcal{L}(a;B) = e\ \mathcal{W}\ (a \wedge \bigcirc \mathcal{L}(B))$$

$$\mathcal{L}(B1 \,[]\, B2) = \mathcal{L}(B1) \vee \mathcal{L}(B2) \qquad \mathcal{L}(B1 \,|||\, B2) = \mathcal{L}(B1) \wedge \mathcal{L}(B2)$$

$$\mathcal{L}(B1 \,|[\alpha]|\, B2) = \mathcal{L}(B1)[(e \vee \bigvee_{f \in \alpha(B2)} f)/e] \wedge \mathcal{L}(B2)[(e \vee \bigvee_{f \in \alpha(B1)} f)/e]$$

$$\mathcal{L}(\text{rec } x.B(x)) = \nu x.\, \mathcal{L}(B(x)) \qquad \mathcal{L}(x) = x$$

The compositional approach suggested by Barringer, Kuiper, Pnueli, is used to define the temporal semantics of this language in a denotational style (*use of "external" actions*)

Linear temporal semantics has been given for all Basic LOTOS processes

ANALYSIS BY REDUCTION

How can process specifications be "reduced"?

Abstraction

Set of concrete LOTOS action sequences

↓ *Abstraction criteria*

Abstract Action

Applying an Abstraction Criterion to a transition system, it provides an *Abstract Reduced* version.

-- Extends *Renaming* functionalities

Hiding as a special case

Language for defining abstract actions

-- e.g. (enter; exit)*

Context Filtering

Constraining a behaviour with contexts (regular expressions represented as abstract actions)

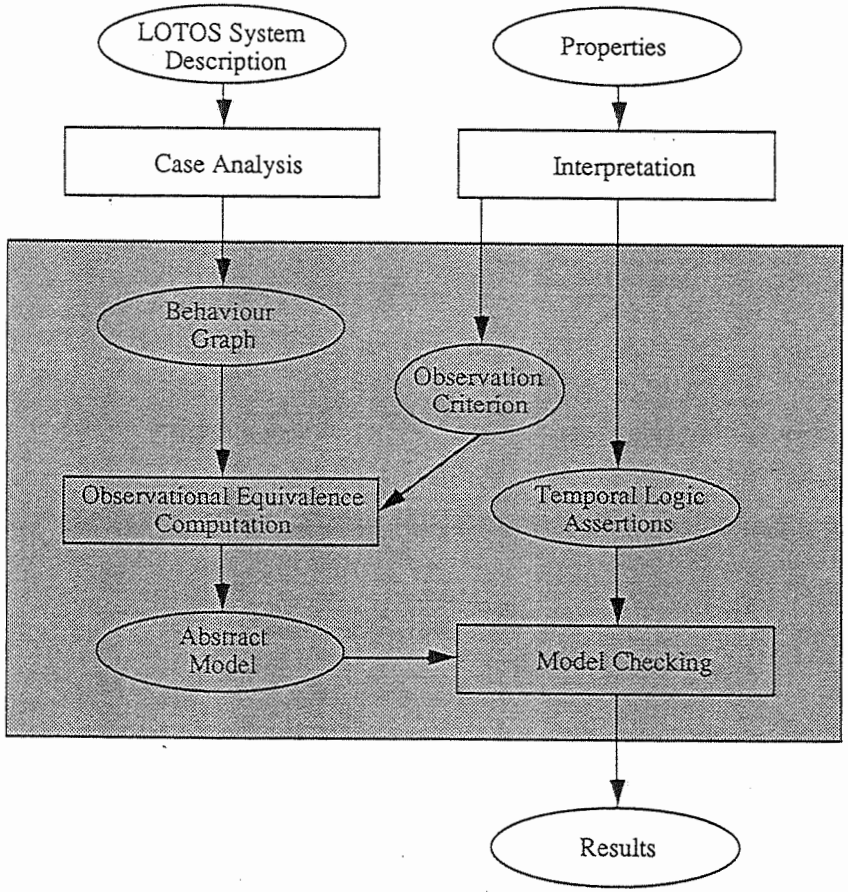
-- *similar to constraint-oriented style*

-- extends *Restriction* functionalities

Other algorithms to performs reductions

such as those employed in equivalence verification....

TEMPORAL LOGIC AND REDUCTION COMBINED



- *A simple case of reduction (hiding non-interesting gates)*
- *Definition of an observational equivalence which is sensitive to "livelocks"*
- *Model checking of the desired properties on a reduced model*

OPEN ISSUES

Use of Partial Properties and Application of the

Proposed Approaches to complete the Definitions

of "useful" Transformations

Theoretical Aspects

- Relations between the studied approaches
- Relations with different equivalences defined on LOTOS terms
- Decidability, Effectiveness, Complexity of verification problems and techniques on several language restrictions

  full LOTOS / basic LOTOS
  finite-state / non finite-state

Tool Support *(defining / experimenting prototypes)*

- Model Checking
- Temporal Semantics Translator
- Decision Procedures & Theorem Provers for the Logic
- Translator from LOTOS to Finite-State Automata
- Tools for combined approach