On RT-Lotos and its application to the formal design of multimedia protocols *

Jean-Pierre COURTIAI **
Roberto C. DE OLIVEIRA **

Abstract
The paper is devoted to the presentation of a new formal description technique RT-Lotos (real-time Lotos) which is a temporal extension of the standard formal description technique Lotos. After a brief introduction to Lotos, the first part of the paper describes the main features of RT-Lotos both informally by means of simple examples and formally by detailing its operational semantics and stating some important properties of the model. The second part of the paper shows the applicability of RT-Lotos for the formal design of multimedia protocols. A design method based on generic and reusable specification building blocks is presented for formalizing an intra-stream synchronization mechanism designed and used within the Cesame project. Several simulation results obtained with RTL (RT-Lotos Laboratory), the tool environment supporting RT-Lotos, are presented for assessing the quality of service of the proposed mechanism.

Key words : Formal description technique, Real-time, Semantics, Transmission protocol, Multimedia service, Specification, System design, Programming aids.

I. INTRODUCTION

Formal description techniques are increasingly being recognized more and more important for the design of...
complex critical systems. This is particular true for large distributed systems, where, due to the level of concurrency involved, the interactions among the component parts of the system are difficult to be mastered. This has motivated the use of different formal methods for the design of communication protocols and distributed algorithms and several formal description techniques (FDT in short) have been studied and standardized at the international level (see Estelle and Lotos [ISO88] at ISO, and SDL at ITU-T). At the same time, several efforts, both in Europe with the support of the EEC and in North America, have been devoted to the elaboration of design methods and to the development of support tools for putting these formal methods to work in practice.

Standard FDT suffer however from a major shortcoming as they do not provide the required capabilities for expressing time-related behaviors, which appear to be mandatory in several application areas, like manufacturing, avionics and multimedia systems. The Lotos standard does not propose any feature at all, whereas Estelle and SDL present only limited capability (for instance, the Estelle delay clause for specifying a time-out).

The paper presents a new FDT, RT-Lotos (for real-time Lotos), and demonstrates its applicability for the design of multimedia protocols and systems. RT-Lotos, an upward compatible extension of Lotos, belongs to the so-called process algebras family [Mi189], which has gained a considerable attention over the past few years for the following two main reasons:

- they make it possible to express formal specifications at different levels of abstraction,
- a general theory of behavioral equivalences has been developed providing mathematical tools for comparing the behavior of different specifications.

The paper is organized as follows: Section II introduces briefly Lotos. Section III presents the main features of RT-Lotos and shows in particular what kind of temporal constraints may be expressed. Section IV develops the formal definition of RT-Lotos. Section V details RTL, the tool environment supporting RT-Lotos, emphasizing the currently operational simulation capabilities. A complete illustration of the use of RT-Lotos is given in Section VI with the formal specification and validation of a general purpose intra-stream synchronization mechanism. Finally, some conclusions are drawn and future research work is outlined in Section VII.

II. LOTOS

Lotos, language of temporal ordering specifications, is a formal description technique standardized at ISO (ISO 8807) based on both CCS [Mil89] (extended by a multiway synchronization mechanism inherited from CSP [Hoa85]) for the specification of the behavior part, and on act-one, an abstract data type formalism.

The basic idea behind Lotos is that systems can be specified by expressing the relations among the interactions that constitute their externally observable behavior. In Lotos, a distributed system is seen as a process, possibly consisting of several subprocesses. A subprocess is a process in itself, and a Lotos specification describes a system via a hierarchy of process definitions. A process is an entity able to perform internal, unobservable actions, and to interact with other processes which form its environment.

In that sense, Lotos implements a black box paradigm making it possible to develop high level, concise and abstract specifications of complex systems. At some abstraction level, it is possible to express the interactions of a process with its environment without having to describe the internal structure (or implementation) of that process.

Process definitions are expressed by the specification of behavior expressions which are constructed by means of a restricted set of powerful operators making it possible to express behaviors as complex as desired. Processes may in general be defined recursively, and the multi-way rendez-vous mechanism represents the basic communication facility between processes. Among the operators, action prefixing, choice, parallel composition and hiding play a fundamental role.

Let us call as usual basic Lotos the subset of Lotos where the processes interact with each other by pure synchronizations, without exchange of values. To provide some intuitive background on the use of basic Lotos operators, an informal composition statement is associated with each configuration depicted in Figure 1:

1. « P1[a, b] is independent from P2[c, d] ».
2. « P1[a, b] is independent from P2[c, d] ».
3. « P1[a, b] is independent from P2[b, c] for all gates (or actions) but gate b on which both processes should synchronize ».
4. « P1[a, b] is independent from P2[b, c] for all gates but gate b on which both processes should synchronize, gate b being furthermore not available for any potential synchronization with processes belonging to the environment of process P ».
5. « Either P1[a, b] or P2[c, d] depending on which action will occur first ».
6. « First P1[a, b] followed, when P1 terminated, by P2[c, d] ».
7. « P1[a, b] which may be interrupted at any time before its termination by P2[c, d] ».

II.1. Basic Lotos formal syntax.

Let PV be the set of process variables and X range over PV. Let GV be the set of the user-definable gates (i.e. the observable actions in basic Lotos). Let \( g_1, g_2, \ldots, g_n \in GV \), let also \( L \) be any (possibly empty) subset of GV noted \( L = g_1, \ldots, g_n \) and \( i \) the internal action. The formal syntax of basic Lotos is recursively given by: