# Performance and Formal Design: A Process Algebraic Perspective

Ed Brinksma
Department of Computer Science
Tele-informatics and Open Systems Group
University of Twente, The Netherlands
brinksma@cs.utwente.nl

## Abstract

Sofar most research in the area of formal methods has been focussed on the development of theories, methods, and tools for the design and analysis of functional, or qualitative, aspects of information-processing systems. Performance analysis, on the other hand, has always been concerned with the quantitative analysis of such systems. As a result each community has been doing its research mostly independently of the other, although a number of formal models of system behaviour have made their way into the world of performance analysis. First of all, there is the now established field of stochastic Petri nets and its application to performance modelling. More recently, there is a growing interest in the application of process algebraic techniques to performance modelling, and a number of proposals for timed, probabilistic, and stochastic process algebras have been put forward.

At the same time we observe that the once clear distinction between the functional and performance properties of systems is getting blurred. With the technological means and the economical drive in place to offer a host of high-performance services to end-users there is a clear need to treat the quantitative *quality-of-service* parameters as requirements in functional specifications. The rapidly growing importance and proliferation of such systems not only implies a conceptual merging of functionality and performance, but also calls for the integration of qualitative and quantitative aspects in their design and realization.

In our presentation we will analyse to what extent the use of process algebraic techniques can contribute to an increased collaboration between the performance analysis and formal methods communities. Ideally, such collaboration should not only lead to further progress in performance analysis, but also contribute to the incorporation of performance analysis in an integrated discipline of *formal design*. Some of the more specific topics that we will address are:

**Design by transformation:** Process algebras have contributed significantly to the theory of design by transformation. Process algebraic laws allow us to rewrite one description of a system into another whilst preserving the notion of correctness that is captured by the equivalence (or pre-order) that is used in the underlying semantic model. Such transformation laws can be used to model the application of actual design principles in a strategy of stepwise refinement to obtain concrete descriptions of implementations from abstract system specifications. It would be interesting to study how this approach extends to refinement in performance-oriented design.

**Derivation of performance models:** In performance models one can often abstract from many functional aspects of the system that have a negligible effect on its performance characteristics, leading to substantially simpler models. To what extent can such abstractions be captured by the application of formal transformations on specifications of the complete system?

**Compositionality:** A particular strong point of process algebras resides in their support of compositional reasoning. This enables the construction of complex systems as the combination of conceptually simpler systems. As many process algebraic operators have been chosen to represent intuitive composition principles of distributed systems, the principle allows one to structure process algebraic specifications by following the compositional layout of potential implementations. Decompositions can also be analytically motivated, viz. by decomposing the system in such a way that a given property of the composition can be understood as a well-understood function of properties of the components. In functional specification this has given rise to a *conjunction* operator allowing so-called *constraint-oriented specification* in addition to ordinary parallel composition. It would be interesting to find out what forms of system decomposition would be useful for the compositional validation of performance properties, and whether this would require new (de)composition principles.

**Liveness and fairness:** Liveness properties are properties that guarantee that the system will eventually reach some (desirable) state. They define the progress of computational behaviour in an abstract



1063-6714/95 $4.00 © 1995 IEEE

way. Fairness is an abstract assumption on scheduling mechanisms that can be used to show liveness. Both properties can be interpreted as a sort of non-quantitative performance properties. The link between these abstract notions of performance and quantitative performance is of considerable potential interest. To what extent do these concepts allow for some sort of abstract performance analysis? On the other hand, liveness properties are often difficult to prove, and it may in many cases be sufficient, easier, and even more relevant to work with a more quantitative notion of *bounded* or *stochastic* liveness. This would call for design transformations in which qualitative properties are refined into quantitative properties that can be validated by subsequent performance analytical methods.

**True concurrency:** Most process algebraic as well as performance models deal with concurrency using the so-called *interleaving* interpretation of parallel composition. In this approach the number of states of a parallel system grows with the product of the numbers of states of the components. This leads to the well-known problem of *state-space explosion* in the analysis of distributed systems. In stochastic process algebras it also leads to severe restrictions on the distributions that can be assigned to transitions, effectively limiting them to memoryless distributions. True concurrency models limit the growth of the state space to that of the sum of the state spaces of the component processes. They also make it easier to consider more general families of distributions to be associated with transitions.