Transactions on Information and Communications Technologies vol 11, © 1995 WIT Press, www.witpress.com, ISSN 1743-3517

Software quality through formal OO specification

J. Torres, J.A. Troyano, M. Toro

Dpto. de Lenguajes y Sistemas Informáticos, Universidad de Sevilla, Avd. Reina Mercedes s/n, Spain

Abstract

One way to guarantee software quality is to have a formal specification of the application that we are going to develop. Besides it is convenient to dispose of a design methodology that makes use of the system structure to describe the system model. In this sense object-oriented (OO) methodology is being very relevant nowadays, because it provides a natural way to represent the components of a system as objects, modelling the relationships among the components as messages among the objects. We try to combine formal aspects and OO concepts, in order to obtain a formal OO specification methodology.

1 Introduction

A natural way to understand a system is considering it as a set of cooperating objects working to reach a common goal. In this sense, there are development techniques, as object-oriented design [8]. With this methodology, we make use of the system's structure to describe a system's model. In this way we will have a software model (called object-oriented model) related to the problem's model.

Furthermore, we need a notation clear and concise enough that allows us to describe the system model without ambiguities. An effort to clearly describe the system model in the early phases of software development (analysis and design), will make the last stages of the software life cycle easier (implementation, proof and maintenance). As a result of this we can use a formal specification language as a tool in order to describe the system model. This formal language allows us to describe the model unambiguously and can help us to verify some properties of the model.

Objects are the fundamental constructs in object-oriented model. In our approach an object is characterized by its structure, its behaviour and its functionality. The structure is defined through a set of attributes, every a-ttribute has a type that is described with an algebraic specification language of abstract data types. The values of the attributes determine the state of an object in every moment. The behaviour is described through events. An event represents an atomic action in the life of an object and provides a mechanism to communicate and synchronize it with other objects. An object life is defined by a sequence of events (trace), we represent the set of valid traces of an object by means of a process description, using an algebraic model based on CSP. Finally, the functionality defines how to change the values of the attributes, this change is made up when an event occurs and it occasions a transition between states.

We have designed an OO specification language (called TESORO) to describe a system model without ambiguities. We can use a specification in TESORO as a formal document, result of analysis phase and useful in next stages of software life-cycle. In addition we can automatically obtain a prototype from the specification, useful to validate the characteristics of the system without implementing it.

Some works related to object-oriented specification languages are:

- CMSL [11] is a specification language of conceptual schemes that combines processes algebra with algebraic specification of data types to specify societies of abstract dynamic objects. The main difference with ower proposal is that CMSL has only contingent and essential classes and it does not make reference to mechanisms of complex classes definition.

- TROLL [4] is an object-oriented specification language based on sub-languages for: data term specification, first order logic, temporal logic and processes. The complexity and expresive capacity of this language does not permit us prototype it in all his extension.

- OASIS [7] is an object-oriented specification language based on ontological theory with a logical expressiveness. The main difference with ower proposal is found in description of object's behaviour. So in TESORO is allowed the description of dynamic constraints through an algebraic description of processes.

The organization of this paper is as follows. This introduction constitutes the first section. In second section are presented the features of the object-oriented model. Third section describes the general structure of a specification in TESORO. In fourth section simple classes are presented.

Fifth section presents algebraic abstract data types as a way for representing object attributes. In sixth section we describe the relationships among classes. Seventh section presents complex classes. In eighth section we show two distinct specification styles for the objects behaviour. In nineth section we extract conclussions and expound future work.

2 The object-oriented model

When we make a system model, we can get the benefit of the structure imposed by the system. The components of a system are interrelated and are interdependent; a set of independent components does not make up a system. The main task in modeling the system will be to identify the components and to determine the relationships among them. Every component can be represented by means of an object.

The object-oriented concept has its origins in the object-oriented programming, which sees the programs as a set of interacting objects that have a state and offer a functional interface by methods. This notion is used also in the analysis and design phases of a computer proyect.

Main features of the object-oriented model are [1]: (1) **abstraction**, that is a simplified description of the system only which insists on details which are outstanding, (2) **hiding information**, that is the process to hide the details of an object which do not contribute to its main features, (3) **classification**, that groups into classes objects which share common features, (4) **hierarchy**, that is an abstraction ordering provided by inheritance, (5) **concurrence**, that describes the execution of cooperating processes which synchronize and communicate among them, and (6) **identification**, that serves to reference an object uniquely during all its life.

2.1 Object-oriented model construction

The object-oriented model is described through a set of classes and relationships among classes specification. A class defined in a specification can be simple or complex.

- **Simple Classes**

  These classes are described without making reference to other classes, and they specify the structure and the behaviour which shares a set of objects.

  An object is compounded of a state, which is characterized by a set of attributes, a behaviour and an interaction with the environment, which are described by means of events and processes, and a set of transition rules that denotes the changes of states.

- **Relationships**
  In the model we can define relationships among classes. These relationships are based on the synchronization and communication of the objects of several classes, which is achieved by shared events.

- **Complex Classes**
  The complex classes are defined over other classes with the next constructors:

  1. **Inheritance**. One feature which is not defined with the simple classes and the relationships is the hierarchy of abstractions. This is achieved with the inheritance, where a new class is defined from one class (simple inheritance) or several classes (multiple inheritance). The new class is called son class, the existing classes are called father classes, then the son class inherits features from the father classes. Furthermore, we can append new features (called emergent features) to the new class.
  2. **Aggregation**. It defines a new class based on the relationships of existing classes and several emergent features.

2.2 The role of abstract data types

In order to describe the attributes and transitions we need some data types and operations over them. The classes are built on these data types, which serve to define the object identification and state domain.

With the idea of giving a formal definition for data types, we are going to use an algebraic specification sublanguage.

In next sections, we describe TESORO, an object-oriented language for systems specification.

3 Specification

The specification in TESORO is composed by three sections:

- **Library**
  In this section are enumerated the abstract data types that are used in the rest of specification.

- **Classes**
  Here we define the classes that will appear in the specification. These classes can be classified into simple or complex.

- **Relationships**
  As we have said above, the classes in a specification are not independent among them. So, in this section are described the relationships among classes which compound the model.

Specification syntax is the following:

```
Specification <specification name>
   Library <abstract data types used>
   <classes specification>
   <relationships specification>
End specification
```

4 Simple classes

For every class, we describe the structure and behaviour of the set of objects that it represents.

The class specification is composed by three sections:

- The attributes section describes the structural aspects of a class. Here are defined the attributes that we use for object identification, the constant attributes, whose values do not change during all the object life, and the variable attributes which make up the object state. Every attribute has a type. This type can be an abstract data type or even an object type, making possible to refer an object with its identification.

  Furthermore, we can impose a set of static constraints over the value attributes, so these constraints can never be broken.

- The events section describes the behavioural aspects of a class. The events can be internal to the system, or external if they denote an interaction with the environment. We can define parameters associated to an event. These parameters let us communicate data among objects when an event occurs. The parameters may be *send* or *receive* depending on communication way.

  There are two special events, one which denotes the object creation (*create*), this is, the way we have to introduce a new object in the system, and other which denotes the object destruction (*destroy*), this is, the way we have to eliminate an existing object of the system.

  The object behaviour is specified by means of permissions and triggers, which are boolean expressions. With permissions we say when an event can ocurr, and with triggers we represent the object responses when it is found in a certain state.

  The dynamic constraints impose an event order, which is described by means of processes specification. This specification is made up using a subset of process algebra constructs [6]. These constructs are the operator ; (sequential composition), the operator [] (choice composition), the operator ||| (interleaving composition) and the recursive processes description.

- The transitions section describes how to change the variable attributes values of the object in a class (and in consequence it state), by means of events occurrence or by means of changes of other attributes.

  Depending on the shape in which the attributes change their values, we can classify it in derived attributes, which are variable attributes whose values depend on others attributes, and not derived attributes, which whether are constant or identification attributes, or variable attributes, which value is modified when a certain event ocurrs.

Syntax of the simple classes specification is the following:

```
Class <class name>
  attributes
    identification
      <attribute name>:<type>; ...
    constant
      <attribute name>:<type>; ...
    variable
      <attribute name>:<type> {(<init>)}; ...
    static constraints
      <condition>; ...
  events
    external
      <event name>{(<formal parameters>)}; ...
    internal
      <event name>{(<formal parameters>)}; ...
    permissions
      [<condition>] <event>{(<parameters>)}; ...
    triggers
      [<condition>] <event>; ...
    dynamic constraints
      <processes descriptions>
  transitions
    from events
      <event>{(<formal parameters>)}
           -> <attribute> = <expression>; ...
    from attributes
      <attribute> = <expression>; ...
End class <class name>
```

5 Abstract data types

The classes (in particular the attributes) are defined over domains. These domains are, in fact, abstract data types (ADT), and they consists of a sets of data values and a set of operations over these values. We use algebraic data specification to describe these domains.

When we write a specification, we must define the ADT's necessary for the definition of object attributes. For example we can use generic types for group more basic ADT's with the well-known collection mechanisms (stacks, sequences, queues, sets, maps, etc.).

The language used for describe ADT's will be ACT ONE. In this language data specifications are collected into *type* constructions. A type consists of a set of *sorts* which represents the possible sets of values, a set of *operations* which describes the signature of the type functions, and a set of *equations* written as equalities of expressions of the type.

Provided that we use ACT ONE for the abstract data type specifications, we do not describe here the syntax of this language. The interested readers are refered to the bibliography [2].

The abstract data types used in a specification, are included into the *Library* section.

6 Relationships among classes

The relationships connect objects through the syncronization of their events. These relationships allow us to describe the bonds among the separate components of the system.

When we establish a relationship, we make possible that objects of related classes share the events involved in the relationship. We can designate this events with a different name for each class, but in fact this is only a syntactic facility, because all the events of objects of different classes related by a relationship represent the same event.

To specify the relationships among classes we are going to use the following syntax, on one hand we enumerate the variables and variable types used in the expressions for events parameter or objects identification, on the other hand we enumerate the bonds which establish the communication channels among the objects of related classes.

```
Relationship <relationship name>
             among <class1>, <class2> ...
  [for all
    <variable name>:<type>; ...]
  bonds
    <class1>.<event> = <class2>.<event> ...; ...
End relationship <relationship name>
```

7 Complex classes

Till now, the only available mechanims to describe a system model are the simple classes and the relationships among classes. At certain cases these mechanisms are not enough for describing all the features of a system. For this reason, we introduce the complex classes as a new resource to describe a system model. The complex classes, are defined over other classes with the inheritance and aggregation constructs.

7.1 Inheritance

The inheritance is a powerful abstraction that allows us to define a new class of objects as an extension of existing classes. The new class inherits the structural an behavioural aspects of the other classes. Besides the inherit features, we can define emergent characteristics for the new class.

Associated to the concept of inheritance, appears the modificability, this is, the capability that the son class has to alter the characteristics of the father classes. In this sense, and accepting the classification proposed in [10] the inheritance available in our language is at the same level that *behaviour compatibility*. In this manner we only can impose stronger constraints (through the sections *static constraints*, *dynamic constraints* and *permissions*) to make the behaviour of the son class compatible with the behaviour of the father class.

As we have already commented, the inheritance can be simple or multiple. In the simple inheritance we have a specialization of the father class. This specialization can be temporary or permanent. We have a temporary specialization if the events *create* and *destroy* of the son class are different of the father class ones. In the permanent specialization the events *create* and *destroy* are the same for the son and father classes, so the life of an object of the son class is always bound to the corresponding object of the father class.

Multiple inheritance appears when a son class has more than one father classes. In this case, the son class has his own events *create* and *destroy* and the lives of his objects are not bounded to the objects of fathers classes.

Specification syntax of the simple inheritance is the following:

```
Class <class name> inherits from
      <father class> [where <condition>]
  [attributes    ...]
  [events        ...]
  [transitions   ...]
End class <class name>
```

The *where* clause, which is a predicate over the constant attributes, indicates which class belong to the objects we create. In the *attributes*, *events* and *transitions* sections are described the emergent properties of the new class.

Specification syntax of the multiple inheritance is the following:

```
Class <class name> inherits from
      <father class1>, <father class2> ...
  [attributes    ...]
  [events        ...]
  [transitions   ...]
End class <class name>
```

Like simple inheritance, in the *attributes*, *events* and *transitions* sections we describe the emergent properties of the new class.

7.2 Aggregation

The aggregation of classes is based on a similar concept that we used in the relationships among classes, because establishes connections among objects by means of its synchronization through events. However, the aggregation gives class features to a relationship, so we can add attributes and behaviour to the aggregate class.

Every bond that is defined in the relationship over which is defined the aggregate class, is matched with an event of the new class. One of these events must be the *create* event and another must be the *destroy* event (if it exists) of the aggregate class.

Aggregation syntax is the following:

```
Class <class name> aggregates
      <class1>, <class2> ...
  [attributes    ...]
  [events        ...]
  [transitions   ...]
  relationships
    [for all
      <variable name>:<type>; ...]
    bonds
      <class1>.<event>=<class2>.<event> ...; ...
End class <class name>
```

The bonds among classes over which is defined the aggregate class are specified in the relationships section.

8 Specification styles

TESORO allow us two differents specifications styles for object's behaviour:

- **Constraint Oriented Style.**
  This style is characterized by the use of the process algebra operators to specify the object behaviour as the set of valid events traces in the object life, by means of dynamic constraints and without making explicit reference to the object internal state.

- **State Oriented Style.**
  In this style we define a set of variables which make explicit the object state all the time, describing the behaviour by means of a set of events ocurrence permissions. Then from a certain state and applying a set of transitions we can determine the state changes after an event ocurrence.

In TESORO, it is allowed to combine both specification styles, this let us extend the expressive capacity of the language.

The state oriented style will serve us to describe an operational semantic for our language. We can associate a state to each object in the system and then we describe the behaviour through a basic transition system similar to the proposed in [5]. In order to describe the semantic of our language, we need to identify the representation of each language construct in the basic transition system that must be defined.

9 Conclusions and future work

With TESORO we describe an object-oriented model whose principal constructs are the objects. We have a vision of an object that consists of three fundamental parts, the structure imposed by his attributes, the behaviour described by the possible sequence of events and his funcionality defined by a set of transition rules. All the objects that share the same characteristics are grouped into classes. We also allow to describe relationships among objects of distinct classes. With these features, we consider the system model as the parallel composition of objects. We also have presented two distinct specification styles for the objects behaviour, showing two approachs, one in a more declarative sense and another one in a more operational sense.

The future work is going to be organized in order to 1) specify an operational semantic for our language, based on a basic transition system [5], 2) generate a prototype from the specification, 3) verify properties of a model and choose a notation to specify these properties. A proposal in the generation of a prototype is in [9] where we present a relationship between an object-oriented language and the formal description technique LOTOS [3]. Actually we also are developing graphical tools that will constitute a work environment for the analysis and design phases in software development.

We pretend as final objective to link the formal techniques (specification and verification) with the real necesities in software development (prototyping and implementation).

References

[1] G. Booch. *Object-Oriented Design with Applications.* Benjamin Cummings. 1991.

[2] H. Ehrig and B. Mahr. *Fundamentals of Algebraic Specification, Part 1.* Springer Verlag. Berlin. 1985.

[3] ISO-Information Processing Systems - Open Systems Interconnection. *LOTOS, A Formal Description Technique based on the Temporal Ordering of Observational Behaviour.* ISO 8807. 1988.

[4] R. Jungclaus, G. Saake, T. Hartmann and C. Sernadas. *Object-Oriented Specification of Information Systems: The TROLL Language.* 1991.

[5] Z. Manna, A. Pnueli. *The Temporal Logic of Reactive and Concurrent Systems. Specification.* Springer-Verlag. 1992.

[6] R. Milner. *A Calculus of Communication Systems.* LNCS, Vol. 92. Springer-Verlag. 1980.

[7] O. Pastor. *Diseño y Desarrollo de un Entorno de Producción Automática de Software basado en el Modelo Orientado a Objetos.* Tesis Doctoral. Universidad Politécnica de Valencia. Abril 1992.

[8] J. Rumbaugh, M. Blaha, W. Premerlani, F. Eddy and W. Lorensen. *Object-Oriented Modelling and Design.* Prentice-Hall. 1991.

[9] Jesús Torres, José A. Troyano, Miguel Toro. *Desde el Lenguaje de Especificación Orientado a Objetos TESORO a LOTOS. Informática y Automática* journal. Vol. 27 number 2, pp. 22-31, Junio 1994.

[10] P. Wegner. *Concept and Paradigms of Object-Oriented Programming.* OOPS Messenger, ACM Press, Volume 1, Number 1. August 1990.

[11] R.J. Wieringa. *A Conceptual Model Specification Language (CMSL versión 2).* Technical Report, Dep. of Mathematics and Computer Science, Vrije Universiteit, Amsterdam. 1991.