Available online at www.sciencedirect.com
SCIENCE DIRECT®
Electronic Notes in Theoretical Computer Science
ELSEVIER Electronic Notes in Theoretical Computer Science 130 (2005) 151–167
www.elsevier.com/locate/entcs

Architectural Prototyping: From CCS to .Net

Nuno F. Rodrigues[1]

Departamento de Informática
Universidade do Minho
Braga, Portugal

Luís S. Barbosa[2]

Departamento de Informática
Universidade do Minho
Braga, Portugal

Abstract

Over the last decade, software architecture emerged as a critical issue in Software Engineering. This encompassed a shift from traditional programming towards software development based on the deployment and assembly of independent components. The specification of both the overall systems structure and the interaction patterns between their components became a major concern for the working developer. Although a number of formalisms to express behaviour and to supply the indispensable calculational power to reason about designs, are available, the task of deriving architectural designs on top of popular component platforms has remained largely informal.
This paper introduces a systematic approach to derive, from CCS behavioural specifications the corresponding architectural skeletons in the Microsoft .NET framework, in the form of executable $C^\sharp$ and $C\omega$ code. The prototyping process is fully supported by a specific tool developed in HASKELL.

Keywords: Software architecture, prototyping, CCS, .NET.

1 Introduction

1.1 Motivation

In recent years the specification of software architectures [8,7] has been recognized as a critical design step in software engineering. Its role is to make

[1] Email: nfr@di.uminho.pt
[2] Email: lsb@di.uminho.pt

doi:10.1016/j.entcs.2005.03.009

explicit the underlying structure of a software system, identifying its components and the interaction dynamics among them. I.e., the *behavioural patterns* which characterise their *interactions*.

Classical process algebras (like, *e.g.*, CCS [14] or CSP [10]) on the other hand, emerged over the last thirty years as calculi to understand and reason about systems in which interaction and concurrency play a significant, even dominant, role. It is not surprising that such calculi, which embodied precise notions of behaviour and observational equivalence, as well as specific proof techniques, were often integrated in the design of generic *architectural description languages* (ADL). Typical examples are WRIGHT [1], based on CSP, and DARWIN [12] or PICCOLA [11], which integrate a number of constructions borrowed from the π-calculus [16,15].

It is not the purpose of this paper to introduce a new description language for software architectures, not even to suggest additional features to existing languages. Our motivation is essentially *pragmatic*: supposing behavioural requirements for a given system are supplied as a collection of process algebra expressions, how can such requirements be incorporated on the design of a particular system? In other words, how can such requirements be animated and, which is even more important, how can they guide the overall design of the application architecture?

Our implementation target is the .NET framework [9] for component-based, distributed application design. Behavioural specifications, on the other hand, are written in the CCS [14] notation. The contribution of the paper is basically a strategy to implement such CCS specifications on top of both $C^\sharp$ [9] and $C\omega$ [13]. Rather than relying on a specific ADL, we resort to behavioural specifications written in a popular process algebra to identify its active components, the interaction vocabulary and the, often distributed, execution control. Such elements guide the (automatic) generation of an application skeleton in the .NET framework.

The strategy proposed for prototyping behavioural specifications in $C^\sharp$ is described in section 2 and its application to a small example — the specification of a control architecture for a road/railway crossing — is discussed in section 4. This is further extended to $C\omega$ in section 5. The systematic character of the approach proposed is tested by the possibility of rendering it automatic: section 3 describes a small tool for the derivation of $C^\sharp$ prototypes from CCS specifications. For quick reference, the next subsection provides a (rather terse) introduction to CCS.

1.2 CCS: An Overview

The CCS notation [14] describes labelled transition structures interacting via a particular synchronisation discipline imposed on the labels. Such synchronisation discipline assumes the existence of *actions* of dual polarity (called *complementary* and represented as, *e.g.*, α and $\overline{\alpha}$), whose simultaneous occurrence is understood as a synchronous handshaking, externally represented by a non observable action τ.

Sequential, non deterministic behaviours are built by what in CCS are called *dynamic* combinators: *prefix*, represented by $\alpha.P$, where α denotes an action, for action sequencing, and *sum*, $P + Q$ for non deterministic choice. The *inert* behaviour is represented by $\mathbf{0}$. Their formal semantics is given operationally by the following transition rules:

$$\frac{}{\alpha.E \xrightarrow{\alpha} E} \qquad \frac{E \xrightarrow{\alpha} E'}{E + F \longrightarrow E'} \qquad \frac{F \xrightarrow{\alpha} F'}{E + F \xrightarrow{\alpha} F'}$$

As shown by the rules above, dynamic combinators are sensible to transitions and disappear upon completion. Differently, *static* combinators persist along transitions, therefore establishing the system's architecture. This group includes *parallel* composition, $P \mid Q$, and *restriction* $\mathbf{new}\, K\ P$, where K is a set of actions declared internal to process P, i.e., not accessible from the process environment. Their operational semantics is as follows:

$$\frac{E \xrightarrow{\alpha} E' \quad F \xrightarrow{\overline{\alpha}} F'}{E \mid F \xrightarrow{\tau} E' \mid F'} \qquad \frac{E \xrightarrow{\alpha} E'}{E \mid F \xrightarrow{\alpha} E' \mid F} \qquad \frac{F \xrightarrow{\alpha} F'}{E \mid F \xrightarrow{\alpha} E \mid F'}$$

$$\frac{E \xrightarrow{\alpha} E'}{\mathbf{new}\,\{\beta\}\ E \xrightarrow{\alpha} \mathbf{new}\,\{\beta\}\ E'}\ (\text{if } \alpha \notin \{\beta, \overline{\beta}\})$$

On top of process terms a number of notions of observational equivalence are defined based on the capacity of processes to simulate each other behaviour (or an observable subset thereof). This entails a number of equational laws which form the basis of a rich calculus to reason and transform behavioural specifications. Such laws range, for example, from asserting the fact that both *sum* and *parallel* are abelian monoids, idempotent in the first case, to the powerful *expansion law* which equates the unfolding of a process with the sum of all of its derivatives computed by the transition relation.

Typically, the architecture of a system composed of several processes running in parallel and interacting with each other is described by what is known in CCS as a *concurrent normal form*

$$\mathbf{new}\, K\ (P_1 \mid P_2 \mid ... \mid P_n)$$

where K is the subset of local (*i.e.*, internal) actions (or communication ports)

and each process P_i has the shape of a non empty non deterministic choice between alternative execution threads.

Such a specification format seems to match reasonably well with the informal description of a software architecture as a collection of computational components (represented by processes P_1 to P_n) together with a description of the interactions between them (represented by actions whose scope is constrained by the scope of the **new** operator). While this abstraction ignores some other fundamental aspects of architectural descriptions (namely non functional features such as performance measures or resource allocation), it provides a useful starting point for the software engineer.

In such a context, the following sections discuss how such behaviour expressions can be prototyped in $C^\sharp$ to set the overall architectural structure of a software system. Interestingly enough, as the specification notation supports a well-studied calculus, one becomes equipped with the right tools to transform architectural designs at very early phases of the design process.

2 Prototyping Behaviour in the .Net Framework

This section focus on the prototyping process, starting from arbitrary CCS specifications of a system behaviour to derive its skeleton architecture in .NET. The qualificative *skeleton* is a keyword here. Actually, we do not aim to derive the whole system, but just to resort to the behavioural requirements, as expressed by the CCS specifications, to automatically derive the bare structures of implementations, i.e., their building blocks and corresponding interaction and synchronization restrictions.

Thus, one is not particularly concerned with the flow of actual values as arguments of methods or constructors, nor with how some eventually critical algorithms, specific to individual components, will perform. What interests us at this level are issues like the ways processes communicate, what kind of messages do they pass to each others, what are their internal states at some point, how control flow is performed, how processes evolve in time and the implications of such evolutions in the other processes that also compose the system. Bearing this in mind, the prototyping process is described in the sequel.

2.1 Actions

An action in a CCS specification corresponds to a method whose name is equal to the action's label in the corresponding implementation. Since such methods typically implement *input ports* in the system, they have invariably data type `void` as the domain of their return values. On the other hand,

complementary actions specifying *output ports*, denoted in CCS by an overline annotation, correspond to methods which may return values of any valid data type.

Accessibility restrictions on methods will be addressed later. For the moment, let us consider all these methods to be public. As an example, consider the following CCS specification of a simple vending machine which receives a coin, performs an internal computation, retrieves a coffee and finally returns to the initial state:

$$M \equiv coin.\tau.\overline{coffee}.M$$

In $C^\sharp$ the *coin* port will be implemented as

```
public void coin() { }
```

Later, in the method body, one will define the corresponding computation to process coin reception.

On the other hand, the $\overline{coffee}$ port, which specifies an output port, will be translated as

```
public cof coffee() { }
```

declaring a method able to return a value of type `cof`. Of course, in this example, the choice of returning some value is rather optional, since the action of returning a coffee could be achieved inside the definition of the coffee method, by some internal computation, instead of returning the desired output.

2.2 Processes

Processes in CCS correspond in $C^\sharp$ to *classes* with the same identifier. Such classes encapsulate all the methods derived from the process ports specification. Therefore, in the previous example, one would get the following $C^\sharp$ class:

```
public class M {
    public void coin() { ... }
    public cof coffee() { ... }
}
```

Note that `class M` implements the *context* for process M, by declaring and grouping its two actions, but still, it does not capture its behaviour. In fact, there is no method invocation order subjacent to `class M`, whereas in process M one can only perform method `coffee()` after method `coin()` has been activated. Even more, in process M the execution of method `coin()` is immediately followed by a single execution of method `coffee()`. The specification does not allow, for example, that several calls to `coin()` precede the `coffee()` call or that several calls to `coffee()` follow a `coin()` insertion.

Addressing such issues, concerning the process execution order, requires some additional control flow code on the implementation side. Such is the topic of the following subsection.

2.3 Reactions

Prototyping sequential port activation, as typically specified in a CCS expression, requires the introduction of an additional variable for state control. This auxiliary variable, denoted by `state` and simply declared of type string, contains the current state, captured by the name of the last executed method. Operationally, every method must inspect this variable to check whether its value is exactly the identifier of the port that precedes the current one.

For ports corresponding to initial actions on the CCS specification, a slightly different approach is adopted. In such cases, the corresponding methods must check whether variable `state` is either null or contains one of the port identifiers from the set of ports that precede a (re-)execution of the current process.

The implementation of this flow control mechanism requires the introduction of three basic functions to analyse the specification: `initialPorts(P)`, `precPorts(P)`, `finalPorts(P)`. Their purpose is to identify the initial, preceding and final actions on a CCS expression, respectively. Once these functions evaluate, the rest of the implementation process falls into pretty-printing and class accessibility control routines.

Nevertheless, one still has to prevent that no sequential ports execute simultaneously. To accomplish this, a method must first set the state variable to a particular temporary execution value (in the example the "`processing`" value is used), and release it at the end of its execution, a scheme similar to what is called a semaphore in classical concurrency control. This way, one not only guarantees that no sequential ports execute simultaneously, but also gets a way to inspect the current state of a particular port. Note that any port in the system is either performing some computation (revealed by the value "`processing`" in the `state` variable) or prepared to be called. Applying the above translation scheme to the example at hands results in the following $C^\sharp$ code:

```
public class M {
    private string value;
    public void coin()
    {
        if(state != null || state.Equals("coffee"))
        {
            state = "processing";
             "code from the coin computations"
            state = "coin";
```

```
    }
    else { throw new Exception("Process sequence violation."); }
}

public cof coffee()
{
    if(state.Equals("coin"))
    {
        state = "processing";
         "code from the coffee computations"
        state = "coffee";
    }
    else { throw new Exception("Process sequence violation."); }
} }
```

Example

2.4 Alternative Reactions

Alternative reactions in a behavioural specification are achieved by the CCS non deterministic choice combinator. At the implementation level this combinator is regarded as a special sequence control. This is implemented on the analysis phase by means of functions `initialPorts(P)`, `precPorts(P)` and `finalPorts(P)`, which deal as expected with the choice combinator + while evaluating over the inspected processes.

2.5 Restriction

Interaction restrictions within a process are handled in CCS by the **new** combinator. Its implementation at the prototype level resorts to the accessibility mechanisms of the .NET platform. Thus, for every variable in the scope of a CCS restriction, the corresponding method is set to an `internal` method, rather than to a `public` one, as used so far in our toy example.

With this additional step, methods declared `internal` become only available for classes inside the same aggregation, isolating them from possible direct interactions with other classes.

Through accessibility control, one may regard a .NET prototyping structure as a process execution domain, where every identifier lies within a precise execution scope. Again, a question remains: where should the boundaries of the system be set?

At a first glance one might think that processes are themselves good candidates for the boundary definition of the corresponding classes. This approach, however, would easily lead to a great amount of aggregations (one per process) without taking any direct advantage out of it, even because there can be no bounded variables at the level of the entire system. Thus, a minimalist approach is preferred, where one starts with a single aggregation for the entire system, and then relies on each **new** occurrence in the CCS expres-

sion to define process scopes and the corresponding bounded variables. Such scopes are created at implementation time leading to the construction of fresh aggregations with their methods correctly addressed in terms of accessibility.

By adopting such a methodology for prototyping CCS restrictions, one not only obtains a correct isolation of process ports, but also specific process space domains within a system, which can be regarded as smaller (sub)systems of the overall architecture.

With the introduction of subsystems, another characteristic of typical architectural reasoning becomes explicit at the prototyping level: the ability to reason safely on simpler and isolated parts of the entire system.

2.6 The Parallel Architecture

The previous sections have shown how sequential CCS processes can be correctly implemented in $C^\sharp$ [3], but one is still missing the entire picture of a system composed of several interacting processes, as specified by a CCS parallel expression.

To address this last issue two techniques are presented. In the first one the execution of the system is totally controlled by a system's analyser. In the second alternative, which is closer to the execution model of CCS, processes evolve in time by internally reacting to each other until the system reaches a point where it requires interaction with the outside world.

Both ways provide an encapsulation of the entire system and a simple way to test it. They rely on the introduction of an additional class, called the *system interaction class*. This class encapsulates the entire system, exposing only its free variables and ensuring a correct execution order for all the assembled processes.

The first technique relies on a single class with a single method which is able to deal with all the assembled processes. This requires that the state of all processes is kept and, that on every action occurrence, all possible interactions are checked.

The second technique builds a system interaction class in a similar way, but for the fact that, for each action occurrence (and corresponding execution call), all the internal reactions are performed until the system stops for communication (on an external input or output port) or faces a non deterministic control choice.

At this point, one might think that some of the previous presented strategies, addressing process restriction and correct process order reaction, were

[3] Actually such a prototyping methodology can be tuned to any object-oriented language, or with some modifications, even to classical imperative ones.

unnecessary since the system interaction class already addresses all this issues. However, the system interaction class should be regarded as a simpler way of interacting with the entire system, and not as the only way of interaction. At the prototyping level it is always possible, and even desirable, to make use of single processes or process's domains for interaction in order to test individual parts of the system or, in general, any of its sub-architectures.

3 Prototype Derivation

To automate the application of this methodology to derive $C\sharp$ architectural skeletons out of CCS specifications, a specific tool was developed in HASKELL.

The translator is based on a two phase procedure. The first phase consists of a parser for the CCS notation which converts the processes' specifications into a suitable HASKELL data type. Its implementation is achieved by the `CCSParser` HASKELL module, which resorts to the PARSEC libraries. Therefore, after the parsing stage, all CCS specifications are encoded in the following data type:

```
data Process a = Port a (Process a)
               | CompPort a (Process a)
               | Sum (Process a) (Process a)
               | Conc (Process a) (Process a)
               | New [a] (Process a)
               | RCall
               | PCall (ProcDef a)
               | ProcessEnd deriving Show

data ProcDef a = PDef (String, Process a) deriving Show
```

Type Process a

The `PDef` type constructor receives a pair with a process identifier and the process definition itself. The former is used to define the class for the process currently under implementation as well as for cross reference calls between processes, specified by the type constructor `PCall` or by complementary port calls.

Data type `Process a` captures a CCS process definition, as presented in section 1, with a minor difference: recursive calls (`RCall`) are explicitly distinguished from non recursive ones (`PCall`). Of course the latter require that the identifier and definition of the process being called are supplied, in order to correctly define inter-class calls at the implementation level.

The second phase of the translator performs the calculation of the $C\sharp$ implementation out of instances of data type `ProcDef a`. This second phase is implemented by the `CCS2DotNet` module, which includes the `buildSystem` function, responsible for the generation of the corresponding $C\sharp$ code.

Function `buildSystem` receives an instance of data type `ProcDef a`, capturing a CCS system definition, and produces a series of files, each containing a $C^\sharp$ class definition for each process in the CCS specification.

The `buildSystem` function relies on several auxiliary functions, but three of them really constitute the building blocks where the entire Automatic Translator stands upon. These functions analyse the CCS specification and were already mentioned above as central functions for an automatic implementation. They are, respectively, `getFinalPorts`, which computes all the final ports of a given process, `getInitialPorts`, which computes all the available initial ports when a process executes and finally `portPreds`, which finds all the possible preceding ports of a given port in a given system.

4 An Example

As a small case study, consider the specification of a control system governing a crossing between a road and a railway. Notice this example, in despite of its small size, has a number of characteristics which are paradigmatic of the sort of systems this prototyping approach may be useful for. First of all it is a simple and effective system, concerned with a real world situation which embodies safety-critical requirements. Avoidance of deadlock and safe control flow are certainly properties which are required to be formally proved. This can be done within the CCS calculus. Once proved, our prototyping approach allows the software architect to derive an architectural skeleton of the final implementation which is, therefore, correct by construction.
We start with the following CCS specification, due to C. Stirling [19]:

$$\begin{aligned} Road &\equiv car.up.\overline{ccross}.\overline{dw}.Road \\ Rail &\equiv train.green.\overline{tcross}.\overline{red}.Rail \\ Signal &\equiv \overline{green}.red.Signal + \overline{up}.dw.Signal \end{aligned}$$

$$C \equiv new\{green, red, up, dw\}(Road|Rail|Signal)$$

The specification is self-explanatory: basically note that process *Signal* ensures the mutual exclusion of control access to both the (physical) semaphore controlling the railway and the gate governing the road traffic. The overall system is specified by process C which, presented in the concurrent normal form, exposes the overall system's architecture.

To use the prototype generator to automatically derive process C as a

skeleton architecture in .NET, one has to perform the two-phase procedure described in the previous section. For illustration purposes, we shall consider here process *Signal* in some detail, and abstract a little of the entire system, though some calls to other processes which interact with *Signal* will appear in the implementation. A similar procedure applies to the other processes.

In a first step function `parseCCS`, from module `CCSParser`, is called on the original specification:

```
Signal = /green.red.Signal + /up.dw.Signal
```

This returns the correspondent process as a value of data type `ProcDef a`:

```
signal = Sum (CompPort "green" (Port "red" RCall))
             (CompPort "up" (Port "dw" RCall))

psignal = PDef ("Signal", signal)
```

Once the CCS system is defined as a value of the `ProcDef a` data type, one just has to apply function `buildSystem` to that value. Function

```
buildSystem :: ProcDef String -> IO ()
```

is responsible for creating all the files containing the $C^\sharp$ classes which implement the original process.

Function `buidSystem` relies on many other functions, many of them working exhaustively with strings and string manipulation. To improve this sort of operations a new type `ShowS = String -> String` was introduced. The advantage of resorting to `ShowS` values, instead of directly working with `String`, is that functional composition with `ShowS` maintains linear complexity in functions dealing with many string concatenations.

The resulting implementation of the process specification must then be stimulated with the initial action string (in this case the empty string), and the result written to a `.cs` file or passed to other function. The result of applying function `buildSystem` is the different `.cs` files implementing each process defined in the CCS specification. For example, `Signal.cs` contents is as follows:

```
using System;

namespace CCS {
    public class Signal
    {
        private static string state;

        public static void greenComp(bool b)
        {
            if(state == null || state.Equals("red") || state.Equals("dw") )
            {
```

```
                if(!b) { Rail.green(true); }
                state = "processing";
                //(computational details to be supplied)
                state = "green";
            }
            else { throw new Exception("Process sequence violation."); }
        }

        public static void red(bool b)
        {
            if( state.Equals("green") )
            {
                if(!b) { Signal.red(true); }
                state = "processing";
                //(computational details to be supplied)
                state = "red";
            }
            else { throw new Exception("Process sequence violation."); }
        }

        public static void upComp(bool b)
        {
            if(state == null || state.Equals("red") || state.Equals("dw") )
            {
                if(!b) { Road.up(true); }
                state = "processing";
                //(computational details to be supplied)
                state = "up";
            }
            else { throw new Exception("Process sequence violation."); }
        }

        public static void dw(bool b)
        {
            if( state.Equals("up") )
            {
                if(!b) { Signal.dw(true); }
                state = "processing";
                //(computational details to be supplied)
                state = "dw";
            }
            else { throw new Exception("Process sequence violation."); }
        }
    }
}
```

Signal.cs

Note that every method receives a boolean value. This has to do with cross reference calls when treating calls to complementary actions. Its objective is to prevent the system to get into an infinite loop when complementary actions are called. This is achieved by forcing `false` as an argument in every user call to a method. Only internal calls use the value `true` to call other complementary actions. This protocol guarantees that each method can inspect if it is being called by an internal call and therefore not needing to call the method that called him again from users calls that do need to check if there are complementary actions to be called.

Also notice that the definition of specific computations inside each method implementing process ports is simply signalised by the

```
//(computational details to be supplied)
```

annotation, making explicit the skeleton character of the derived code. In any case, however, the underlying architecture specified in the CCS expression has been translated to the .NET framework in a way which is both executable and guarantees, by construction, all the relevant safety-critical properties.

5 Prototyping in $C\omega$

$C\omega$ [13] is an extension to the $C^\sharp$ language at two different levels: data type support for XML and table manipulation, on the one hand, and new asynchronous concurrency abstractions, based on the join calculus [6], on the other. The language brings to life a model of concurrency rich enough to be applicable both to multithreaded applications running on a single machine and to the orchestration of asynchronous, event-based components interacting over a (wide area) network.

The major contribution of $C\omega$ to concurrent programming is the introduction of *chords*. In contrast to normal methods where for each method declaration corresponds a body containing the code of its implementation, in a chord a method implementation can be associated to a set of methods. The code corresponding to a chord only executes when all the methods in the head of the chord are called. This structure, combined with the notion of *asynchronous methods*, already present in $C^\sharp$, is extremely powerful. Note, *en passant*, that a chord may have at most a synchronous method in its definition.

This section reports on the use of $C\omega$ as a target language for prototyping behavioural specifications. Experience shows that translations become closer to the corresponding CCS specification and smaller (in terms of the amount of code written). Some aspects of this approach are outlined below; the reader is referred to [18] for a detailed introduction.

5.1 From CCS to $C\omega$

The process of prototyping CCS specifications in $C\omega$ is similar to the corresponding translation to $C^\sharp$. The main differences are pointed out below.

5.1.1 Actions

Ports are implemented either by methods, as before, or by *chords* to reflect cases of dependence on other ports or to maintain strict sequencing control in process execution. The distinction between the use of chords and methods and when to use one or the other will be made clear below.

Output ports, with corresponding complementary ports that need to be executed simultaneously, wait to be called from the latter. They must therefore be guarded by a semaphore insuring the sequential evolution of the process. This semaphore is implemented by an asynchronous method which is then bounded to the port as in the following implementation of port $\overline{fork_1}$, from process P_{12}, taken from the *dining philosophers problem* mentioned below.

```
public async allow_c_fork1();
    public void c_fork1(object obj) & allow_c_fork1() {
        Console.WriteLine("Phil_12 releases fork 1");
        if(obj is Fork1) {
            ((Fork1) obj).obs_fork1();
        }
        allow_c_fork2();
    }
```

A Port Implementation

5.1.2 Reactions

The way reactions are implemented as already been partially revealed in the previous section. As mentioned above output ports with corresponding complementary ports in the specification wait to be called by them. Input ports, on the other hand, are always called by their predecessors and, therefore, are not required to be bounded to semaphores to ensure their correct sequential execution. Nevertheless, input ports with corresponding complementary ports, which need to be executed simultaneously, are also implemented as chords to force simultaneity of action occurrence[4] This way, a port in this conditions Such a port must perform a previous call to the asynchronous method `request_obs_Port()` in the process(es) holding its corresponding output port. This call acts like a request activation, signalising the beginning of an active waiting state.

5.1.3 Alternative Reactions

Alternative reactions are implemented by defining their initial ports as chords bounded to a semaphore (`alternative()`). This is a private asynchronous method which becomes available whenever the choice for the alternative reaction is also available. Notice that non determinism in choice was not treated in the $C\sharp$ approach. With $C\omega$, however, it can be prototyped by performing random choices in the actions previous to the alternative reaction.

[4] understood here as atomicity in the sense that both actions occur in an atomic way, that is, without being interleaved by other events.

5.1.4 The Parallel Architecture

Every process prototype is equipped with an asynchronous `start()` method which wakes the process and starts its execution. The parallel composition in the CCS specification is then implemented by calling the `start()` method of each process composed in a parallel context.

5.2 Dining Philosophers Example

To illustrate how CCS behavioural specifications can be prototyped in $C\omega$, a solution to the dining philosophers problem[4] was developed. This example, which by space limitations can not be discussed in this paper, is detailed in [18] [5] .

It is interesting to compare the prototype obtained with the approach discussed in this paper, starting from a CCS specification, with the direct implementation of the same problem supplied in the $C\omega$ documentation [13]. In the latter the boundaries of each entity in the system are not clear nor are the means by which they interact or how resource sharing is accomplished. The $C\omega$ prototype in [18], on the other hand, follows very closely the original CCS specification, which entails a concise description of the solution, a clear definition of the intervening entities and a precise notion of the behaviour of each of them. Moreover all the interaction vocabulary is established in function `main`, which also deals with the activation of processes' instances. Therefore, the resulting $C\omega$ code is easier to understand and analyse.

6 Conclusions and Future Work

This paper, an extended version of [17], proposed a simple, yet powerful, approach to the automatic derivation of $C^\sharp$ and $C\omega$ prototypes of behavioural specifications written in CCS. The resulting code can be used in a number of different contexts. For example, applications developed under stateless environments which abound in the internet, with particular relevance to Web-Services. Targeting this last paradigm, one can easily distribute processes in an (inter/intra)net and make use of SOAP to manage all external method calls.

The motivation is exactly the one typically invoked on the use of formal methods: first resort to a formal notation to enable precise expression of requirements and calculation power to discuss correctness and refinement. Then, derive executable prototypes in suitable implementation frameworks closer to the working programmer concerns.

[5] the corresponding $C\omega$ code is available from `wiki.di.uminho.pt/wiki/bin/view/Nuno`.

We believe that the working programmer is more and more becoming the working software architect, whose job is essentially to look for suitable software components and plugging them in order to guarantee some desirable behaviour. If CCS seems to be a sound and relatively well-known calculational formalism, .NET is becoming an almost *de facto* standard for implementing component based applications. The approach, however, is largely independent of the interaction discipline of CCS: for example, CSP-like synchronization, as used in some popular ADLs, or broadcast communication, can easily be incorporated as well. In any case the emphasis is shifted from stand-alone programming to architectural design and, in such a sense, we believe the approach sketched in this paper may be found useful in practice. It should be mentioned that this ideas have been used in the context of a project on architectural reconstruction of legacy systems as well as in an undergraduate course on software architecture taught to third-year students of a Computer Science degree at Minho University.

Current work includes

- The generation of test classes and the derivation of a web-based interface for prototype testing.
- The extension of the prototyping approach to *mobile* applications, starting from behavioural specifications in the π-calculus [15].
- The integration of this approach in a methodology for formal specification of software architectures. This basically requires the construction of a library of specifications of typical *software connectors*, and corresponding .NET skeletons, able to be re-used in architectural design. Recall that a *software connector* [7,5,2] is an abstraction intended to represent the interaction patterns among components, the latter regarded as primary computational elements or information repositories. The aim of connectors is to mediate the communication and coordination activities among components, acting as a sort of gluing code between them. Examples range from simple channels or pipes, to event broadcasters, synchronization barriers or even more complex structures encoding client-server protocols or hubs between databases and applications. All of them can be specified in a process algebra notation (as in, *e.g.*, [1,12]) and, therefore translated to .NET skeletons.

Finally, it should be mentioned that $C^\sharp$ itself is also evolving towards the integration of primitive distribution and concurrency control primitives at the language level [3]. As sketched in section 5, this provides a richer environment for architectural prototyping.

Acknowledgements. This research was carried on in the context of the PURE Project (*Program Understanding and Re-engineering*) supported by

FCT under contract POSI/ICHS/44304/2002.

References

[1] R. Allen and D. Garlan. A formal basis for architectural connection. *ACM TOSEM*, 6(3):213–249, 1997.

[2] M. Barbosa and L. Barbosa. Specifying Software Connectors. In K. Araki and Z. Liu, editors, *Proc. First International Colloquim on Theoretical Aspects of Computing (ICTAC'04), Guiyang, China*, pages 53–68. Springer Lect. Notes Comp. Sci. (3407), 2004.

[3] N. Benton, L. Cardelli, and C. Fournet. Modern concurrency abstractions for $C^\sharp$. In *Proc. ECOOP 2002*. Springer Lect. Notes Comp. Sci. (2374), 2002.

[4] E. W. Dijkstra. Cooperating sequential processes. Technical report, Technische Universiteit Eindhoven, The Netherlands (reprinted in *Programming Languages*, F. Genuys (ed.), Academic Press, New York, 1968, 43-112), September 1965.

[5] J. Fiadeiro and A. Lopes. Semantics of architectural connectors. In *Proc. of TAPSOFT'97*, pages 505–519. Springer Lect. Notes Comp. Sci. (1214), 1997.

[6] C. Fournet, G. Gonthier, J.-J. Lévy, L. Maranget, and D. Rémy. A calculus of mobile agents. In *Proc. CONCUR' 96*. Springer Lect. Notes Comp. Sci. (1119), 1996.

[7] D. Garlan. Formal modeling and analysis of software architecture: Components, connectors and events. In M. Bernardo and P. Inverardi, editors, *Third International Summer School on Formal Methods for the Design of Computer, Communication and Software Systems: Software Architectures (SFM 2003)*. Springer Lect. Notes Comp. Sci, Tutorial, (2804), Bertinoro, Italy, September 2003.

[8] D. Garlan and M. Shaw. An introduction to software architecture. In V. Ambriola and G. Tortora, editors, *Advances in Software Engineering and Knowledge Engineering (volume I)*. World Scientific Publishing Co., 1993.

[9] E. Gunnerson. *A Programmer's Introduction to* $C^\sharp$. Apress, 2000.

[10] C. A. R. Hoare. *Communicating Sequential Processes*. Series in Computer Science. Prentice-Hall International, 1985.

[11] M. Lumpe. *A* π*-calculus Based Approach to Software Composition*. PhD thesis, University of Bern, January 1999.

[12] J. Magee, N. Dulay, S. Eisenbach, and J. Kramer. Specifying distributed software architectures. In *5th European Software Engineering Conference*, 1995.

[13] Microsoft Research. *C*ω *Documentation*, 2004.

[14] R. Milner. *Communication and Concurrency*. Series in Computer Science. Prentice-Hall International, 1989.

[15] R. Milner. *Communicating and Mobile Processes: the* π*-Calculus*. Cambridge University Press, 1999.

[16] R. Milner, J. Parrow, and D. Walker. A calculus of mobile processes (parts I and II). *Information and Computation*, 100(1):1–77, 1992.

[17] N. Rodrigues and L. S. Barbosa. Prototyping behavioural specifications in the .Net framework. In A. Mota and A. Moura, editors, *Proc. 7th Brazilian Symposium on Formal Methods (SBMF'2004)*, pages 108–118. UFP, November 2004.

[18] N. Rodrigues and L. S. Barbosa. Prototyping concurrent systems in $c\omega$. Technical report, Universidade do Minho, Portugal, February 2005.

[19] C. Stirling. Modal and temporal logics for processes. *Springer Lect. Notes Comp. Sci. (715)*, pages 149–237, 1995.