Enseñando Métodos Formales con Coq

Carlos Daniel Luna[1]
[1] Instituto de Computación, Facultad de Ingeniería, Universidad de la República, Montevideo, Uruguay

Resumen

En este trabajo presentamos una propuesta para apoyar la enseñanza de métodos formales en una currícula de grado, y postgrado, usando el asistente de pruebas *Coq* y conceptos del área de Teoría de Tipos. Proponemos un taller de especificación, construcción y verificación de sistemas en los paradigmas de programación funcional e imperativo, que también abarca el análisis de sistemas críticos: sistemas reactivos y de tiempo real. Describimos algunas experiencias en el desarrollo del taller y planteamos cambios y extensiones.

Palabras clave: Enseñanza de la Programación, Métodos Formales, Teoría de Tipos, Coq, Especificación y Verificación de Corrección.

1. Introducción

Los profesionales de computación deben estar capacitados para estudiar los fundamentos de su disciplina. El núcleo central de las Ciencias de la Computación está constituido en buena parte por la matemática discreta y la lógica matemática. En consecuencia, un especialista en computación debe estar en condiciones de usar las herramientas básicas y las técnicas de dichas áreas. Esto le permitirá una adecuación rápida y eficaz a los acelerados cambios tecnológicos, que son una constante en la disciplina.

En este trabajo proponemos un taller que tiene como meta la adquisición de destreza en el uso de herramientas de razonamiento fundamentales: la inducción matemática y la deducción lógica aplicadas a la construcción y verificación de programas. Los objetivos centrales que se persiguen pueden resumirse en la frase “programar rigurosamente sobre la base de argumentos matemáticos”. Esto es, fortalecer la noción de que junto con la construcción de los algoritmos existe la obligación de la verificación rigurosa (formal) de su corrección y que los programas son objetos matemáticos plausibles de ser tratados con argumentos lógico-matemáticos [13].

Para lograr estos objetivos presentamos un taller para apoyar la enseñanza de métodos formales en una currícula de grado, usando el asistente de pruebas *Coq* [1] y conceptos del área de Teoría de Tipos. El taller abarca la especificación, construcción y verificación de sistemas en los paradigmas de programación funcional e imperativo y, el análisis de sistemas críticos: programas reactivos y de tiempo real.

La estructura del artículo es como sigue. En la sección 2 describimos sucintamente las metodologías más usadas para desarrollar programas correctos y verificar corrección. En la sección 3 destacamos las principales características del asistente de pruebas *Coq* y en la sección 4 desarrollamos algunas de estas características para ilustrar la utilidad de *Coq* como asistente para programadores. En la sección 5 presenta-mos nuestra propuesta, un taller de construcción de programas certificados usando *Coq*. En la sección 6 exhibimos algunas experiencias en el desarrollo del taller y finalmente, en la sección 7, incluimos las conclusiones de este artículo. Una versión inicial de este trabajo fue presentada en la Conferencia Latinoamérica-na de Informática: CLEI'2002 – CIESC’2002 [25] y la versión más reciente en el primer Congreso de Tecnología en Educación y Educación en Tecnología: TE&ET’2006 [24].

2. Demostración y Verificación de Corrección

Es indiscutible hoy la influencia que tiene en la industria y en casi todos los ámbitos el uso del software. La cantidad de aplicaciones reales y potenciales de la computación ha alcanzado cotas inimaginables apenas veinte años atrás. A pesar de su uso extensivo, uno de los costos más alto no se da en la producción del software, sino en la corrección de errores que son detectados posteriormente al desarrollo del sistema. En la actualidad, el método más usado para validar software es el “testing”, que consiste en la simulación sobre casos de prueba representativos. No obstante, este método no garantiza la corrección del software analizado, por ser incompleto en la mayoría de los casos [28]. En las aplicaciones críticas, que tratan con vidas humanas y/o grandes inversiones económicas, la certeza de corrección es, en general, un criterio indispensable. De un software correcto se espera que resuelva un problema determinado por una especificación y que exista una justificación formal –matemática– de que el programa la satisface.

En los últimos años un gran esfuerzo de investigación se ha invertido en el desarrollo de métodos y herramientas para la especificación y el análisis de la corrección de sistemas. Sin embargo no hay un formalismo, una metodología o una herramienta claramente preferibles a otras en todas circunstancias. Para el análisis de la corrección formal de sistemas se destacan dos importantes enfoques:

- **Verificación de corrección**. En este enfoque un sistema es considerado correcto cuando se prueba que toda ejecución posible satisface la especificación. Existen algunas técnicas bien conocidas que permiten recorrer, en ciertos casos, de manera exhaustiva el espacio de ejecuciones posibles y herramientas que las implementan.

- **Demostración de corrección**. En este caso se construye o deriva una prueba matemática de que el sistema satisface su especificación. Aquí las herramientas asisten al programador en el proceso de construcción de la prueba. Algunas de estas herramientas están basadas en teorías constructivas de tipos [7, 8, 9], las cuales han sido formuladas como fundamento de la Matemática Constructiva. Ejemplos de estos sistemas son ALF [27], *Coq* [1] y LEGO [26]. Una de las principales características de los mismos es el carácter unificador de la teoría que implementan, en la cual pueden ser expresados programas, teoremas y pruebas de éstos. Otro punto destacable es que el usuario es guiado en forma interactiva por el sistema en el proceso de construcción de un programa o una prueba, siendo verificada inmediatamente la validez de cada paso del desarrollo. El principal objetivo de estos sistemas es convertirse en sofisticadas herramientas que asistan en la tarea del desarrollo incremental de programas correctos. Sin embargo, el marco conceptual necesario para desarrollar software verificado es de una muy alta complejidad y requiere cubrir muchos aspectos que en realidad escapan a la construcción de un asistente de pruebas. Estos sistemas disponen de un lenguaje de especificación de orden superior, permiten hacer pruebas en lógica de alto orden y proveen definiciones de tipos inductivos y co-inductivos.

En este artículo usaremos los términos verificación y demostración de corrección indistintamente de aquí en adelante, salvo expresa acotación, refiriéndonos conceptualmente siempre a este último tipo de análisis de corrección.

3. Acerca de Coq

El asistente de pruebas *Coq* es una implementación del cálculo de construcciones inductivas, una lógica intuicionista de alto orden con tipos dependientes y tipos inductivos como objetos primitivos [8, 32]. El usuario introduce definiciones y hace demostraciones en un estilo de deducción natural, las cuales son chequeadas mecánicamente por el sistema.

Dicho formalismo permite especificar y probar en lógica intuicionista de alto orden. Esta lógica asocia una interpretación computacional a las pruebas, la noción de veracidad de una proposición corresponde a la existencia de una prueba. Curry y Howard demostraron que los siguientes juicios son equivalentes:

- "t es una demostración de la proposición A".
- "el término t tiene tipo A".
- "t es un programa de la especificación A".

Esto es, probar una proposición A es equivalente a construir un término de tipo A. Esta equivalencia es conocida como isomorfismo de Curry-Howard [21] y está basada en que las pruebas en deducción natural pueden ser representadas como términos de un cálculo lambda tipado [21], o de la misma manera, de un lenguaje de programación funcional (por ejemplo, Caml [33]). Consecuentemente *Coq* puede ser considerado, rigurosamente hablando, un chequeador de tipos ("type-checker").

A los efectos de diferenciar objetos computacio-nales de información lógica, distinguimos dos clases de tipos importantes en *Coq*: Prop para los tipos que contienen términos lógicos (las proposiciones) y Set que agrupa a los tipos que contienen información computacional (los conjuntos). Por ejemplo, los números naturales se definen en Set y las relaciones $\leq$ y la conjunción $\wedge$ en Prop. Set y Prop pertenecen a Type, que es en realidad una familia infinita de tipos notada de esta forma. Un procedimiento de extracción de programas puede ser usado para remover las partes lógicas de los términos, manteniendo sólo las partes de información computacional [30, 31].

Además de los habituales tipos inductivos (o sea, conjuntos definidos inductivamente, como por ejemplo los números naturales o las listas finitas), *Coq* permite también la definición de tipos co-inductivos. Estos son tipos recursivos que pueden contener objetos infinitos, no bien fundados. Un ejemplo de tipos co-inductivos es el de las secuencias infinitas, usualmente llamadas streams, de elementos de un tipo dado.

En el proceso de prueba de un teorema, *Coq* entra en un ciclo interactivo donde el usuario completa la demostración usando tácticas, las cuales implementan reglas de inferencia o de tipado (esquemas de prueba). El conjunto de tácticas puede ser incrementado por el usuario, a partir de un lenguaje diseñado para tal fin.

Entre las funcionalidades que incluye *Coq* como asistente de programación, podemos citar:

- *Definición de tipos inductivos*. Es posible definir relaciones y tipos de datos inductivos, los cuales especifican la existencia de construcciones matemáticas concretas, como por ejemplo: desi-gualdades, predicados de pertenencia (relaciones) y, listas, árboles, números enteros (tipos de datos).
- Una vez definidos los tipos se pueden definir funciones, recursivas o no, y especificar propie-dades sobre estos tipos, como así también probar las propiedades (eventualmente por inducción).
- *Construcción y verificación de programas funcio-nales*. Es posible especificar sistemas y extraer pro-gramas funcionales a partir de pruebas. Asimismo probar la corrección de programas con respecto a una especificación dada.
- *Definición y verificación de programas impera-tivos*. Se puede probar la corrección de programas imperativos razonando en lógica de Hoare. Sin embargo este asistente no permite, a la actualidad, derivar un programa imperativo en base a una especificación [12].
- *Definición de tipos con objetos infinitos*. *Coq* permite definir tipos de datos que pueden contener objetos no bien fundados, como por ejemplo las secuencias infinitas o streams, y modelar a través de estos tipos sistemas complejos, tales como: sistemas reactivos (que se comportan como una secuencia de estímulos-respuestas) y de tiempo real (sistemas reactivos cuya corrección depende de la magnitud de los retardos temporales).

En este trabajo no estamos interesados en dar una descripción completa del cálculo de construcciones inductivas y co-inductivas, ni del sistema *Coq*, en general. Por aspectos teóricos el lector puede referirse a [7, 8, 9] por el cálculo puro de construcciones, a [32] por tipos inductivos y a [2, 3, 4, 6, 10, 14, 15, 17, 22, 29, 23] por tipos co-inductivos y aplicaciones de éstos. Acerca de *Coq*, una buena introducción son los tutoriales [16, 20] y detalles adicionales pueden encontrarse en el manual de referencia [1].

4. Descripción del asistente Coq

A continuación desarrollamos algunas de las principales características de *Coq*, referidas en la sección previa, para ilustrar la utilidad que este asistente presenta a programadores y, en el marco de este artículo, a estudiantes de grado y de postgrado interesados en aprender construcción y análisis de corrección de programas funcionales e imperativos. La sintaxis de *Coq* utilizada en esta sección corresponde a la versión 7.4 [1]. Actualmente estamos terminando de adaptar el curso/taller para la nueva versión de *Coq* (la 8.0) que cambia ligeramente la sintaxis, en algunos casos, pero no los conceptos fundamentales presentados a continuación.

4.1. Definición de tipos inductivos

Coq permite definir tipos inductivos. Cada definición establece la introducción de un nuevo conjunto, junto con la manera de construir sus objetos, que además es única. Por ejemplo, podemos definir el conjunto de los números naturales como sigue:

```
Inductive nat : Set := Co : nat | Sg : nat -> nat.
```

nat es el conjunto definido, en el cual sus constructores son *Co* y *Sg*. El primero representa la constante 0 del tipo *nat*, y el segundo la operación sucesor de los naturales, que dado un número n, representa el número natural n+1.

También es posible hacer definiciones inductivas paramétricas, para manejar la abstracción sobre objetos de diversos tipos. Por ejemplo, podemos definir árboles binarios genéricos de elementos de un tipo arbitrario de la siguiente manera:

```
Inductive bintree [A:Set] : Set :=
    emptyb : (bintree A) |
    consb : A -> (bintree A) -> (bintree A) ->
            (bintree A).
```

bintree representa al tipo de todos los posibles árboles binarios de elementos de un tipo genérico *A*. Sus constructores son *emptyb* y *consb*, los cuales construyen el árbol vacío y un árbol binario a partir de otros dos y un elemento de tipo *A*, respectivamente.

Cuando se define un tipo inductivo, *Coq* genera tres constantes correspondientes a los principios de inducción y recursión. Las mismas implementan el principio de inducción estructural, permiten hacer definiciones recursivas y definir familias recursivas de tipos.

4.2. Definición de funciones recursivas

En *Coq* es posible definir funciones por recursión primitiva y recursión general. Un ejemplo de las primeras es la función que retorna el espejo de un árbol binario de elementos de un tipo genérico.

```
Fixpoint reverse [A:Set; b:(bintree A)] : (bintree A)
```

```
:= Cases b of
     emptyb => (emptyb A)
   | (consb x b1 b2) =>
     (consb A x (reverse A b2) (reverse A b1))
   end.
```

En esta definición, dado cualquier árbol binario *b* de tipo *A*, si *b* es el árbol vacío su espejo es él mismo, y si es un árbol no vacío, el espejo es el que se construye con *consb* aplicado al elemento raíz del árbol original y el espejo de sus dos subárboles permutados.

Las funciones recursivas primitivas quedan perfectamente definidas a partir de su especificación. También es posible definir en *Coq* funciones por recursión general, especificando un orden bien fundado que asegure la terminación.

4.3. Definición y prueba de propiedades

Coq permite definir propiedades sobre los tipos y los programas, y demostrarlas luego utilizando *tácticas* de prueba, en particular inducción. Una propiedad sobre los árboles binarios anteriormente definidos es: "el espejo del espejo de un árbol binario es el mismo árbol".

```
Lemma rev_rev : (∀A∈Set) (∀b∈(bintree A))
  reverse A (reverse A b)  =  b.
```

Notación. La cuantificación universal sobre un tipo S se escribe en *Coq* "(x:S) P". Sin embargo, usaremos la notación "(∀x∈S) P" en este trabajo para dar más claridad a las especificaciones. Asimismo, denotaremos "(∃x∈S) P" la cuantificación existencial sobre un tipo S, que en *Coq* es {x:S | P}.

Para probar propiedades sobre un tipo inductivo *Coq* provee una táctica llamada *Induction.* Esta táctica permite usar el principio de inducción primitiva, el cual genera los casos según la definición del tipo sobre el que se establece la propiedad.

Una prueba del lema *rev_rev* en el Asistente *Coq* es la siguiente:

Proof.	Comienzo de la prueba
Intros.	Asume las hipótesis en el contexto
Induction b.	Aplica el principio de inducción estructural sobre el árbol
Simpl.	Aplica la definición de reverse al caso base
Trivial.	Se cierra la demostración del caso base
Simpl.	Aplica la definición de reverse al caso inductivo
Rewrite Hrecb1.	Aplica una hipótesis inductiva
Rewrite Hrecb0.	Aplica la otra hipótesis inductiva
Trivial.	Se cierra la demostración del caso inductivo
Qed.	Culmina la demostración y salva la prueba

Por razones de espacio omitimos el árbol de deriva-ción para esta prueba.

4.4. Derivación y verificación de programas funcionales

Coq permite construir funciones a partir de la demostración de un lema que establece una propiedad existencial sobre una relación. Esta relación especifica el comportamiento deseado del programa a construir. Por ejemplo, el siguiente lema especifica que para todo árbol binario existe otro que es su espejo:

```
Lemma mirrorInverse: (∀A∈Set)(∀b∈(bintree A))
  (∃t'∈(bintree A)) (mirror A t t').
```

Donde el predicado inductivo *mirror* sobre árboles binarios genéricos se define como sigue:

```
Inductive mirror [A: Set]: (bintree A) ->
  (bintree A) -> Prop:=
    vacio: (mirror A (emptyb A) (emptyb A))
  | no_vacio: ∀x∈A , ∀t1,t2,t3,t4∈(bintree A)
    (mirror A t1 t2) -> (mirror A t3 t4) ->
    (mirror A (consb A x t1 t3)
              (consb A x t4 t2)).
```

vacio es una prueba de que *(emptyb A)* es el espejo de si mismo y *no_vacio* es una prueba de que *(consb A x t4 t2)* es el espejo de *(consb A x t1 t3)* si se tiene una prueba de que *t2* es el espejo de *t1* y de que *t4* es el espejo de *t3*.

Una vez demostrado el lema, a través de dos tácticas simplemente, podemos "derivar" (extraer) un programa en Haskell u otro lenguaje funcional, utilizando el comando *Write* disponible en la biblioteca *Extraction* de *Coq*. Para el ejemplo anterior el programa Haskell extraído es:

```
Coq > Write Haskell File "mirror_function"
  [ mirror_inverse].
```

```
data Tree a = Nil | Cons a (Tree a) (Tree a)
    inverse t =  case t of
        Nil -> Nil
        Cons a0 t1 t2 ->
            Cons a0 (inverse t2) (inverse t1)
    mirror_inverse = inverse
```

También es posible "verificar" que un programa funcional satisface una especificación usando las tácticas *Realizer* y *Program* (o *Program_all*) en la prueba de un lema que establece una propiedad existencial sobre una relación que especifica el comportamiento deseado del programa a construir.

4.5. Especificación y verificación de programas imperativos

También es posible especificar y verificar programas imperativos en *Coq*. Por ejemplo, podemos dar el siguiente predicado inductivo binario sobre los enteros (*Z*):

```
Inductive RFact : Z -> Z -> Prop :=
    f0: (RFact `0` `1`)
    | fs: ∀z,f∈Z (RFact z f) ->
        (RFact `z+1` `f*(z+1)`).
```

Este predicado es válido cuando el segundo argumento es el factorial del primero. Aquí *f0* es una prueba de que `1` es el factorial de `0` y *fs* es una prueba de que `f*(z+1)` es el factorial de `z+1`, si se tiene una prueba de que *f* es el factorial de *z*. A partir del predicado *RFact* podemos especificar un programa que calcule el factorial de un número entero de la siguiente manera:

```
Global Variable f,i,n:Z ref.
    (* definición de f, i y z, variables enteras *)
Correctness imperative_program
    (* cláusula para verificar programas *)
{`n>=0`}
    (* precondición del programa *)
begin
    (* inicio del programa *)
    f:=1;
    i:=1;
        (* asignaciones *)
        while (!i < !n+1) do
            (* comando iterativo *)
            { invariant  (RFact `(i-1)` f) /\ `i<= n+1`
            variant `n-i+1` }
                (* invariante: f tiene el factorial de i-1,
                cota de terminación del ciclo: `n-i+1` *)
                f:=!f*!i;
                i:=!i+1
        done
        (* fin de la iteración *)
end {(RFact n@0 f)}.

(* postcondición del programa: el factorial del
valor inicial de n (n@0) es f  *)
```

Sintaxis: *!x* indica el valor almacenado en la variable *x*. Cabe aclarar que en especificaciones como la anterior es posible escribir funciones y relaciones utilizando notación infija (por ejemplo: `(i-1)`), al incluir una biblioteca especial de *Coq* llamada *Arith*.

Una vez definido el programa y especificado su comportamiento deseado, podemos verificar si el programa satisface la especificación, mediante la táctica *Correctness*. Esto es, si a partir de un estado de las variables que satisfacen la precondición se cumple la postcondición luego de ejecutar el programa. La demostración de fórmulas de corrección corresponde a la construcción de árboles de prueba al estilo de deducción natural. Estos árboles están construidos en términos de:

- Reglas de inferencia de Floyd-Hoare para probar los objetivos. Por ejemplo, en el caso de un ciclo, que: el invariante del ciclo vale al comienzo; la cota es positiva y estrictamente decreciente dentro del ciclo; el invariante se restablece luego de la ejecución un comando del ciclo; al finalizar el ciclo vale la postcondición del programa [11, 19].
- Reglas del cálculo de predicados para demostrar las fórmulas lógicas que expresan el comportamiento del programa.

4.6. Especificación y verificación de sistemas críticos: sistemas reactivos y de tiempo real

La experimentación desarrollada en el uso de asistentes de pruebas basados en teoría de tipos se ha enfocado principalmente en demostrar la corrección de programas secuenciales, pero dado su poder expresivo considera-mos que pueden ser también adecuados para razonar sobre sistemas críticos, y en particular sobre sistemas

reactivos y de tiempo real. Algunas experiencias llevadas a cabo en esta dirección y particularmente en *Coq* son [2, 3, 4, 6, 14, 16, 17, 22, 23].

La formalización de estas clases de sistemas hace uso, generalmente, de tipos co-inductivos y el análisis sobre los mismos requiere por lo tanto el empleo de co-inducción como mecanismo de prueba.

Un ejemplo de tipos co-inductivos es el de las secuencias infinitas, usualmente llamadas *streams*, de elementos de un tipo dado. El tipo *streams* puede ser introducido a través de la siguiente definición:

```
Variable A: Set..
CoInductive Stream: Set :=
    Cons : A -> Stream ->Stream.
```

La inducción estructural es la manera de expresar que los tipos inductivos sólo contienen objetos bien fundados. Aquí el principio de eliminación no es válido para tipos co-inductivos y la única regla de eliminación para *streams* es el análisis de casos. Este principio puede ser usado, por ejemplo, para definir los destructores *head* y *tail*.

```
Definition head : Stream -> A :=
    [x:Stream] Cases x of (Cons a s) => a  end.
Definition tail: Stream -> Stream :=
    [x:Stream] Cases x of (Cons a s) => s  end.
```

Los objetos infinitos son definidos por medio de métodos (infinitos) de construcción, semejantes a los presentes en los lenguajes de programación funcional perezosos. Estos métodos pueden ser definidos usando el comando *CoFixpoint*. Por ejemplo la siguiente definición introduce la lista infinita [a,a,a,…]:

```
CoFixpoint repeat: A -> Stream A :=
    [a:A] (Cons a (repeat a)).
```

El comportamiento de sistemas reactivos y de tiempo real puede ser expresado en término de trazas de ejecución infinitas (*streams*) de estados, donde el paso de un estado al próximo en una traza está dado por una operación (transición) válida del sistema. Por más detalles y aplicaciones ver [2, 3, 4, 6, 10, 14, 15, 16, 17, 22, 23, 29, 34], entre otros.

5. Taller de construcción de programas certificados usando Coq

En esta sección presentamos un taller para apoyar la enseñanza de métodos formales en una currícula de grado (y de postgrado), usando el asistente de pruebas *Coq* y conceptos del área de *Teoría de Tipos*. El taller abarca fundamentalmente la especificación, derivación y verificación de sistemas en diferentes paradigmas de programación. Debido a la característica de taller, el enfoque seguido es eminentemente práctico, orientado al análisis de aplicaciones, con un fundamente teórico mínimo. Esta característica sumada a la utilización de herramientas de apoyo permiten una introducción al estudio formal de los temas abracados por el taller a estudiantes de distintas disciplinas de la informática e incluso de otras áreas, como la matemática.

Nombre del taller: *Construcción formal de programas en teoría de tipos*, también llamado, *taller de producción de programas sin fallas*.

Carácter: Grado-Postgrado.

Institución responsable: Instituto de Computación, Facultad de Ingeniería, Universidad de la República, Montevideo, Uruguay.

Objetivos

- Presentar a la Teoría de Tipos como lógica de programación y familiarizar al estudiante con ambientes de desarrollo de programas basados en este formalismo.
- Iniciar al estudiante en el uso de métodos formales para la especificación, producción, derivación y verificación de software correcto por construcción en los paradigmas de programación funcional e imperativo.
- Iniciar al alumno en el uso de métodos formales para la especificación y verificación de otras clases de sistemas. En particular, sistemas críticos (sistemas reactivos y de tiempo real).
- Mostrar la utilidad de editores de pruebas basados en teoría de tipos para la especificación y verificación de aplicaciones industriales y académi-cas.

Temario

- Presentación formal de la lógica proposicional, de primer orden y uso de orden superior en el asistente de pruebas *Coq*.
- Pruebas y programas: especificaciones y tipos, su vinculación.
- Identificación de pruebas y programas. Extracción de programas a partir de pruebas: derivación. Construcción de pruebas a partir de programas: verificación.
- Recursión: definiciones inductivas, principios de inducción y esquemas de recursión.
- Definición de tipos de datos de lenguajes de programación (lineales, arborescentes, entre otros), definición de programas sobre éstos tipos y prueba de propiedades de corrección de los programas.
- Construcción de programas certificados usando *Coq*: programas funcionales y programas imperati-

vos.
- Extensiones: una introducción al desarrollo de programas y pruebas con tipos recursivos que pueden contener objetos infinitos. Sistemas reactivos y de tiempo real.
- Aplicaciones: desarrollo y análisis de trabajos industriales y académicos, usando *Coq*.

Metodología de enseñanza: Se desarrollarán clases teórico-prácticas y se trabajará en base a tareas obligatorias que los estudiantes deberán realizar en máquina. Se utilizará como asistente de pruebas el sistema *Coq*.

Conocimientos previos recomendados: El taller presupone conocimientos previos de lógica de primer orden y de algún lenguaje de programación funcional o lógica. Asimismo, se recomienda tener conocimientos básicos de verificación de programas.

Contexto en el plan de estudio de las carreras de computación del Instituto de Computación: El taller es desarrollado como asignatura electiva en los últimos semestres de la carrera de Ingeniería en Computación y como asignatura de postgrado en el marco de la Maestría y el Doctorado en Computación.

Modalidad de evaluación: Se seguirá un régimen de taller con tareas evaluables a lo largo del semestre. Los alumnos deberán presentar, semanal o quincenalmente, un trabajo práctico resuelto en grupos de a lo sumo dos personas. Esto le permitirá al docente evaluar gradualmente el aprendizaje de los distintos temas. Asimismo, se desarrollará un proyecto final de carácter individual para integrar los temas abarcados en el taller y se llevarán a cabo pruebas parciales a lo largo del dictado.

Plantel docente: Un docente responsable de los contenidos teóricos, un docente responsable del taller y un ayudante por comisión en el taller.

Duración y carga horaria: El taller tendrá duración de un cuatrimestre y una carga total de 192 horas, distribuidas en horas de aula y horas de trabajo del estudiante.

Cupo: La cantidad de alumnos por comisión queda supeditada a la disponibilidad de computadoras. Estimamos conveniente un cupo máximo de 30 alumnos por comisión distribuidos en a lo sumo dos personas por computadora.

Infraestructura e insumos: Sala con 15 computadoras conectadas en red, donde se tenga instalado el software *Coq* y un PC con monocañón.

La bibliografía usada incluye artículos del área de teoría de tipos y, fundamentalmente, manuales y tutoriales de la herramienta *Coq* [1, 16, 20], como así también el libro “Interactive Theorem Proving and Program Development. Coq'Art: The Calculus of Inductive Constructions” [5]. Información adicional sobre el curso y los materiales usados pueden consultarse en el sitio web "http://www.fing.edu.uy/inco/grupos/mf/TPPSF/". Asimismo, información acerca del proyecto *Coq* puede obtenerse en "http://coq.inria.fr/".

En el desarrollo del taller se usan distintas interfaces (*IDEs*) del asistente *Coq* para facilitar la especificación de sistemas y propiedades, y la construcción de pruebas sobre éstos. Existen interfaces de *Coq* para distintas plataformas (*linux*, *windows* y *unix*). Estas herramientas poseen ambientes gráficos, con ventanas, que hacen más amigables los procesos de trabajo con *Coq*, que fueron parcialmente descriptos en la sección 4. Actualmente estamos usando en los laboratorios de clase una *IDE windows* para *Coq*, disponible de forma gratuita en "http://coq.inria.fr/".

6. Experiencias en el desarrollo del taller

El taller presentado viene desarrollándose regularmente en el Instituto de Computación de la Facultad de Ingeniería de la Universidad de la República (Montevideo, Uruguay) desde el año 2000, en versiones ligeramente diferentes, tanto como curso de grado para la carrera de Ingeniería en Computación, como curso de postgrado para la Maestría o el Doctorado en Computación. Las primeras ediciones no abarcaban el estudio de sistemas críticos ni el análisis de aplicaciones industriales y académicas realizadas con *Coq*. Posteriores versiones fueron incorporando estas características y recientemene anexamos al taller el módulo: análisis de aplicaciones industriales y académicas realizadas con *Coq*. De esta manera logramos captar el interés por estos temas en estudiantes de áreas no necesariamente vinculadas directamente con métodos formales.

En el año 2001 desarrollamos el taller en el Departamento de Computación de la Facultad de Ingeniería de la Universidad de Río Cuarto (Argentina), y en los años 2000, 2001 y 2005 en la Universidad Nacional de Rosario (Argentina). Asimismo, versiones cortas del taller se llevaron a cabo en las siguientes escuelas de ciencias informáticas: Rio'2000, séptima escuela de verano de ciencias informáticas, desarrollada del 14 al 19 de Febrero de 2000, UNRC, Río IV, Argentina; y, ECI'2001, escuela de ciencias informáticas, desarrollada del 23 al 28 de Julio de 2001, UBA, Bs. As., Argentina. Finalmente en Febrero de 2004 presentamos una versión del taller orientada a aplicaciones computacionales –industriales– de la demostración asistida de teoremas usando *Coq* en el marco de la Rio'2004: décima primera escuela de verano de ciencias informáticas, UNRC, Río IV, Argentina. Aplicaciones de este tipo son por ejemplo: protocolos de comunica-

ción, protocolos de comercio electrónico, compiladores, sistemas operativos y desarrollo de aplicaciones seguras para tarjetas inteligentes y dispositivos móviles, entre otras.

En total, más de 300 estudiantes participaron de alguna edición del taller; tanto estudiantes del área de métodos formales como estudiantes de otras áreas de informática o de matemáticas, de grado y de postgrado. Los intereses en cada caso han sido diferentes y en este sentido los proyectos finales que se propusieron. A partir de estas experiencias surgieron cuatro tesis de maestría y varias tesinas (proyectos) de grado. Desde el año 2000 a la actualidad tres proyectos de investigación han sido llevados a cabo. Asimismo, dos proyectos adicionales están en curso en el Instituto de Computación de la Facultad de Ingeniería de la Universidad de la República (Montevideo, Uruguay) en temas relacionados y varias colaboraciones con instituciones regionales e internacionales han sido establecidas. El taller ha oficiado como punto de encuentro entre distintas áreas y nos ha permitido acercar a estudiantes con diferentes perfiles en una introducción "práctica" a los métodos formales, focalizándonos en la especificación, construcción y verificación de sistemas en diferentes paradigmas de programación.

Luego de las múltiples experiencias en el desarrollo del taller evaluamos altamente positivos los logros alcanzados. En particular, consideramos que los estudiantes de grado de una carrera de informática ven complementada su formación, dentro del área de los métodos formales, con el taller propuesto. El taller les permite profundizar en la aplicación de técnicas de inducción-recursión y deducción en la definición y verificación de sistemas, como así también en la formulación y el análisis de especificaciones. Estos conceptos, que son centrales en la formación de profesionales universitarios en el área, consideramos que, al margen del aporte técnico que les representa, los entrena y capacita para una adecuación rápida y eficaz a los acelerados cambios tecnológicos, que son una constante en la disciplina.

Conclusiones

En este trabajo presentamos una propuesta para apoyar la enseñanza de métodos formales en una currícula de grado, y de postgrado, usando el asistente de pruebas *Coq* y conceptos del área de *Teoría de Tipos*. El taller abarca contenidos esenciales en la formación de un profesional en Ciencias de la Computación: la especificación, construcción y verificación de sistemas en diferentes paradigmas de programación. El taller permite fortalecer la noción de que junto con la construcción de los algoritmos existe la obligación de la verificación rigurosa (formal) de su corrección y que los programas son objetos matemáticos plausibles de ser tratados con argumentos lógico-matemáticos. *Coq* ha demostrado ser una herramienta adecuada para asistir a los estudiantes en este proceso de aprendizaje. El uso de IDEs para *Coq* facilita y a la vez hace más amigables los procesos de trabajo con *Coq*, que fueron parcial-mente descriptos en la sección 4.

Según describimos en la sección previa, numerosas experiencias se han desarrollado en relación al taller en el país y en la región. El taller ha sido continuamente actualizado en virtud de estas experiencias aunque su núcleo central se ha mantenido estable. El mismo corresponde a la especificación, construcción y verificación de sistemas usando una lógica de alto orden en el contexto de los paradigmas de programación funcional e imperativo.

El desarrollo de un taller de estas características permite también integrar a docentes y estudiantes interesados en trabajar en la construcción formal y la verificación de sistemas de software en diversos para-digmas de programación, desde los clásicos (imperativo y funcional) hasta otros, tales como los correspondientes a sistemas reactivos y de tiempo real. Asimismo, el taller ofrece un marco adecuado para la realización de trabajos de investigación, trabajos finales en carreras de grado y trabajos de postgrados en el área de métodos formales o en áreas interdisciplinarias afines. Varias experiencias en esta dirección han sido y están siendo llevadas a cabo en Uruguay y Argentina.

Actualmente se están desarrollando en el Instituto de Computación de la Facultad de Ingeniería de la Universidad de la República (Montevideo, Uruguay) un par de trabajos –tesis de maestría– sobre el análisis de sistemas orientados a objetos usando *Coq*, y la especificación y verificación de lenguajes de bajo nivel para la programación de sistemas embebidos (empotrados). Un trabajo futuro es extender el taller con un módulo para la especificación y verificación de sistemas orientados a objetos en el cálculo de construcciones (co)inductivas de *Coq* y ampliar el análisis de sistemas críticos (sistemas reactivos y de tiempo real) en este formalis-mo. Una segunda línea a seguir se relaciona con trabajos actuales del grupo de métodos formales en el área de seguridad. En particular, estamos interesados en el análisis de políticas de seguridad para dispositivos móviles usando *Coq* [33]. En el año 2005 los proyectos finales del curso y un trabajo de grado se desarrollaron en esta temática.

Agradecimientos

A las Dras. Cristina Cornes y Nora Szasz que participaron en las primeras versiones del taller. Al Dr. Gustavo Betarte, responsable actual. A los estudiantes

de grado y postgrado que formaron o forman parte del taller y de sus proyectos relacionados.

Referencias

[1] B. Barras, S. Boutin, C. Cornes, J. Courant, Y. Coscoy, D. Delahaye, D. de Rauglaudre, J-C. Filliâtre, E. Giménez, H. Herbelin, G. Huet, H. Laulhère, C. Muñoz, Ch. Murthy, C. Parent-Vigouroux, P. Loiseleur, Ch. Paulin-Mohring, A. Saïbi, and B. Werner. “The Coq Proof Assistant. Reference Manual, Versión 7.4”. INRIA, 2003.

[2] G. Barthe, J. Cederquist, and S. Tarento. "A Machine-Checked Formalization of the Generic Model and the Random Oracle Model". In D. Basin and M. Rusinowitch, editors, Proceedings of IJCAR'04, volume 3097 of Lecture Notes in Computer Science, pages 385-399, Cork, Ireland, 2004.

[3] G. Barthe and G. Dufay. "A Tool-Assisted Framework for Certified Bytecode Verification". In M. Wermelinger and T. Margaria-Steffen, editors, Proceedings of FASE'04, volume 2984 of Lecture Notes in Computer Science, pages 99-113, Barcelona, Spain, 2004.

[4] G. Barthe and S. Stratulat. "Validation of the JavaCard Platform with Implicit Induction Techniques". In R. Nieuwenhuis, editor, Proceedings of RTA'03, LNCS, 2003.

[5] Y. Bertot and P. Castéran. “Interactive Theorem Proving and Program Development. Coq'Art: The Calculus of Inductive Constructions”. Series: Texts in Theoretical Computer Science. An EATCS Series, ISBN: 3-540-20854-2, 2004.

[6] C. Breunesse, N. Cataño, M. Huisman, and B. Jacobs. "Formal methods for smart cards: an experience report". Science of Computer Programming, 55(1-3):53-80, 2005.

[7] T. Coquand and G. Huet. “Constructions: A higher order proof system for mechanizing mathematics”. In EUROCALL´85, LNCS 203, Linz, 1985, Springer-Verlag, 1985.

[8] T. Coquand and G. Huet. “The calculus of constructions”. Information and Computation, 76(2/3), 1988.

[9] T. Coquand. “Metamathematical investigations of a calculus of constructions”. INRIA and Cambridge, University, 1986.

[10] T. Coquand. “Infinite objects in type theory”. In H. Barendregt and T. Nipkow, editors, Workshop on Types for Proofs and Programs, number 806 in LNCS, pages 62-78. Springer-Verlag, 1993.

[11] E. Dijkstra, “A Discipline of Programming”. Prentice-Hall, Englewood Cliffs, NJ, 1976.

[12] J.C. Filliatre. “Proof of imperative programs”. In Chapter 18 of The Coq Proof Assistant Reference Manual, Version 7.0, 2001.

[13] A. Ferreira, C. Luna y R. Medel. “Manual-Guía de Aprendizaje de Programación Avanzada”, publicado por la Editorial de la Fundación de la Universidad Nacional de Río Cuarto –miembro de la Red de Editoriales Universitarias Argentinas– en Marzo de 1998.

[14] E. Giménez. “An application of Co-inductive Types in Coq: Verification of the Alternating Bit Protocol”. In BRA Workshop on Types for Proofs and Programs (TYPES’95), LNCS 1158, pages 135-152, Springer-Verlag, 1995.

[15] E. Giménez. A Calculus of Infinite Constructions and its application to the verification of communicating systems. PhD thesis, Ecole Normale Supérieure de Lyon, 1996, Unité de Recherche Associée au CNRS No. 1398, 1996.

[16] E. Gimenez and P. Casteran. A Tutorial on [Co-]Inductive Types in Coq, Technical Report, INRIA (accesible en http://coq.inria.fr/), 2005.

[17] E. Giménez. “Two Approaches to the Verification of Concurrent Programs in Coq”, 1999.

[18] M. Gordon. Introduction to HOL: a theorem proving environment based for higher order logic. Cambridge University, Press, 1993.

[19] D. Gries. The science of programming, Springer-Verlag New York Inc., 1981.

[20] G. Huet, G. Kahn and C. Paulin-Mohring. The Coq Proof Assistant: A Tutorial (accesible desde el sitio web http://coq.inria.fr/), 2004.

[21] W. Howard. “The formulae-as-types notion of construction”. In J. Seldin and J. Hindley, editors, To H. Curry: Essays on combinatory logic, lambda calculus and formalism. Academic Press, 1980. A reprint of an unpublished manuscript from 1969.

[22] C. Luna. “Verificación de Sistemas de Tiempo Real en Teoría de Tipos. Un Caso de Estudio: The RailRoad Crossing example in Coq”. En proceedings de la Conferencia Latinoamericana de Informática: CLEI'2002, Montevideo, Noviembre de 2002.

[23] C. Luna. "Especificación y análisis de sistemas de tiempo real en teoría de tipos". Vol VIII No. 1, Julio-Setiembre de 2004, Revista Iberoamericana Computación y Sistemas, ISSN 1405-5546. Centro de Investigación en Computación, Instituto Politécnico Nacional, México, D.F., 2004.

[24] C. Luna. "Enseñando Métodos Formales con COQ". I Congreso de Tecnología en Educación y Educación en Tecnología (TE&ET’06), La Plata, Argentina, Agosto de 2006.

[25] C. Luna, P. Martellotto, M. M. Novaira. “Teoría de Tipos y Coq en la Enseñanza de Programación Funcional e Imperativa. Taller de Construcción Formal de Programas”. En proceedings de la Conferencia Latinoamericana de Informática: CLEI'2002 – CIESC’2002. Montevideo, Uruguay, 2002.

[26] Z. Luo and R. Pollack. “Lego proof development system: User’s manual”. Technical Report ECS-LFCS-92-211, LFCS, 1992.

[27] L. Magnusson. The implementation of ALF – a proof editor based on Matin Löf’s Monomorphic Type Theory

with Explicit Substitution. PhD thesis, Chalmers University of Göteborg, 1994.

[28] D. Mandrioli, Carlo Ghezzi, and Mehdi Jazayeri. Fundamentals of Software Engineering. Prentice Hall, 1991.

[29] L. Paulson. “Co-induction and Co-recursion in Higher-order Logic”. Technical Report 304, Computer Laboratory, University of Cambridge, 1993.

[30] C. Paulin-Mohring. “Extracting Fω’s programs from proofs in the calculus of constructions”. In Sixteenth Annual ACM Symposium on Principles of Programming Languages, Austin, ACM, 1989.

[31] C. Paulin-Mohring. Extraction de programmes dans le calcul des constructions. Thèse de doctorat, Université de Paris VII, 1989.

[32] C. Paulin-Mohring. “Inductive definitions in the system Coq – rules and properties”. In M. Bezem and J. Groote, editors, Proceeedings of the conference Typed Lambda Calculi and Aplications, LNCS 664, 1993.

[33] P. Weis et X. Leroy. “Le Langage CAML”. Second edition, Dunod, Paris, 1999. First edition, InterEditions, Paris, 1993.

[34] S. Zanella Béguelin, G. Betarte, and C. Luna. “A formal specification of the MIDP 2.0 security model”. In Proc. 4th International Workshop on Formal Aspects in Security and Trust, FAST 2006, Hamilton, Canada, August 26-27 2006, Lectures Notes in Computer Science. Springer 2006. To appear.

Dirección de Contacto del Autor:

Carlos Daniel Luna
Yerbalito 3821 (personal)
Julio Herrera y Reissig, piso 5 (laboral)
Montevideo
Uruguay
e-mail: cluna@fing.edu.uy
sitio web: http://www.fing.edu.uy/~cluna

Carlos Luna ha participado en 8 proyectos regionales e internacionales en temas relacionados con la enseñanza, desarrollo y aplicación de métodos formales. Posee más de 40 publicaciones en congresos y revistas arbitrados. Por información adicional consultar el curriculum vitae accesible desde su página web.