Informe Intermediario de Proyecto
Action ECOS-Sud U00E02
Especificaciones y Programas:
Modelos de Cálculo, Tipos, Implementaciones

Maribel Fernández
Maître de conférences, École Normale Supérieure

Giuseppe Longo (Responsable francés del proyecto)
Directeur de recherche, CNRS et École Normale Supérieure

Ian Mackie
Chargé de recherche, CNRS et École Polytechnique

Paula Severi
Profesor Grado 3, Centro de Matemática
Facultad de Ciencias, Universidad de la República

Nora Szasz (Responsable uruguayo del proyecto)
Profesor Grado 4, Instituto de Computación
Facultad de Ingeniería, Universidad de la República

1 Introducción

Este informe intermediario de la Action Ecos-Sud U00E02 cubre el período noviembre 2000-noviembre 2002. Debido a cambios circunstanciales en la situación de Paula Severi, sólo Maribel Fernández, Ian Mackie y Nora Szasz continuarán con el proyecto en 2003, finalizando el proyecto en diciembre 2003.

2 Justificación de gastos

Primer Año: Noviembre 2000-Noviembre 2001

De las 3 misiones otorgadas en este año, una misión le correspondió a la parte uruguaya y las otras dos a la parte francesa. A continuación se detallan los períodos de las misiones en orden cronológico:

1. **Misión Uruguay-Francia: Paula Severi.** El período de esta misión fue del 18 de noviembre al 18 de diciembre de 2000.
2. **Misión Francia-Uruguay: Maribel Fernández.** El período de esta misión fue del 22 de agosto al 17 de setiembre de 2001.
3. **Misión Francia-Uruguay: Ian Mackie.** El período de esta misión fue del 22 de agosto al 17 de setiembre de 2001.

Segundo Año: Noviembre 2001-Noviembre 2002

Como en el año anterior, se realizaron tres misiones, una uruguaya y las otras dos francesas. A continuación se detallan los períodos de las misiones en orden cronológico:

1. **Misión Uruguay-Francia: Paula Severi.** Esta misión fue desglosada en dos partes: a) La estadía en Francia fue financiada por ECOS desde el 4 de junio al 30 de junio de 2002. El pasaje de Uruguay a Francia no fue utilizado en esta oportunidad ya que Paula Severi se encontraba en Europa, siendo éste empleado en agosto 2002.
2. **Misión Francia-Uruguay: Maribel Fernández.** El período de esta misión fue del 16 de agosto al 8 de setiembre de 2002.
3. **Misión Francia-Uruguay: Ian Mackie.** El período de esta misión fue del 16 de agosto al 8 de setiembre de 2002.

3 Trabajo Científico Realizado

Como estaba establecido originalmente en el plan de investigación de este proyecto, estudiamos las propiedades de confluencia y terminación de los cálculos tipados que permiten el desarrollo de programas correctos (certificados) a partir de especificaciones formales.

En los últimos años se han definido varios métodos de extracción de programas certificados a partir de especificaciones usando Teorías de Tipos. Una especificación de un problema, como por ejemplo el de ordenar una lista, pude especificarse del siguiente modo: *dada una lista de naturales arbitraria, existe una permutación ordenada de la misma*, y es en general una fórmula de la forma: $\forall x.\exists y.P(x,y)$. En Teoría de Tipos, esta fórmula se representa con un tipo $\Pi x{:}A.\Sigma y{:}B.P(x,y)$. La extracción de programas consiste en extraer a partir de un habitante t de este tipo, una función $f : A \to B$ tal que $P(x, f(x))$ es válido para todo $x : A$. El problema es que en general el programa extraído contiene información superflua proveniente de la prueba de corrección.

La Teoría de Especificaciones fue introducida en [Sza97] basada en la Teoría de Tipos de Martin Löf. En [SS01] se reformuló dicha teoría internalizando el procesos de extracción de programas por medio de una reducción llamada $\to_\sigma$. Intuitivamente, las reglas de reducción σ borran las partes que no tienen contenido computacional, y que son por lo tanto inútiles en el programa extraído.

En la primera etapa del proyecto, el objetivo fijado era el estudio de las propiedades de normalización fuerte de la Teoría de Especificaciones. En [SS01] se formalizó la semántica de esta teoría y también se probaron propiedades como confluencia, normalización y correctitud.

En [SS02], Nora Szasz y Paula Severi formularon la teoría en el contexto del Cálculo de Construcciones Inductivas con una jerarquía infinita de tipos y extendieron la reducción $\to_\sigma$ a tipos inductivos. En este trabajo también se probaron propiedades de confluencia y normalización. Sin embargo, no se estudiaron las propiedades de Subject Reduction y Normalización Fuerte, que son más delicadas. En [RS02] Femke van Raamsdonk y Paula Severi mostraron que estas propiedades no se cumplen en general. En [RS02] se muestra un contraejemplo para Subject Reduction y Normalización Fuerte para dicha teoría. Las autoras definen un subconjunto de la Teoría de Especificaciones donde sólo se consideran las reglas de reducción σ que corresponden a la eliminación de partes lógicas de un programa. De esta forma se pudo aislar el problema y recuperar Subject Reduction y Normalización Fuerte para esta subteoría.

En [FS02] Maribel Fernández y Paula Severi presentan una versión de la teoría que finalmente tiene las propiedades de Subject Reduction y Normalización Fuerte. La idea en este trabajo es restringir la β-reducción a formas normales de la σ-reducción. Es decir que se da prioridad a las reglas σ (que realizan el borrado de las partes del término que no tienen contenido computacional) sobre las reglas β. Esta es una restricción fuerte, natural desde el punto de vista de la extracción de programas, pero resta por estudiar su impacto en la práctica cuando se desarrollen ejemplos reales de derivación de programas. En la versión de la teoría definida en [FS02] se cumplen todas las propiedades deseadas (Subject Reduction, Confluencia, Terminación), por lo cual consideramos que con este trabajo se termina la primera etapa del proyecto (se ha cumplido el primer objetivo del plan de trabajo inicial).

Continuando esta línea de investigación, en [FMSS] Maribel Fernández, Ian Mackie, Paula Severi y Nora Szasz presentan una extensión de los Sistemas de Tipos Puros con tipos Ultra-Σ, que generaliza los trabajos previos sobre extracción de programas en Teoría de Tipos. Este marco general incluye los trabajos de Paulin basados en interpretaciones de realización, la Teoría de Especificaciones y Librables de Burstall y McKinna, la Lógica de Programación de Poll, y la Teoría de Especificaciones de Severi y Szasz. Se muestra como expresar todas estas teorías como casos particulares de Sistemas de Tipos Puros con tipos Ultra-Σ. Esta presentación general permite una mejor comprensión y comparación de los diferentes enfoques existentes de la extracción de programas. Una conclusión importante de este trabajo es que las reglas de reducción σ dan una semántica operacional de la extracción de programas que es independiente del cálculo λ tipado que se utilice.

La segunda parte del proyecto, según se estableció en el plan de investigación presentado en la propuesta del proyecto, consiste en el estudio de estrategias de reducción eficaces y la definición de un algoritmo de chequeo de tipos, con vistas a la implementación de la Teoría de Especificaciones. Para el estudio de estrategias de reducción, la herramienta elegida es la lógica lineal, y en particular las redes de interacción y los cálculos textuales derivados de las redes de prueba de la lógica lineal. En [FM01a] Maribel Fernández e Ian Mackie estudian la codificación de estrategias de evaluación del λ-cálculo en redes de interacción. Para estudiar la corrección de estos codajes y la simulación del λ-calculo, se definió en [FM01b] un cálculo con substituciones explícitas y manejo de recursos explícito basado en el uso de *director strings*. Este cálculo fue utilizado por François-Régis Sinot (en su tesis de Master (DEA) bajo la supervisión de Maribel Fernández) para definir una familia de máquinas abstractas que implementan la reducción débil en el λ-cálculo (weak head normal form reduction). Posteriormente, Maribel Fernández e Ian Mackie definieron una traducción del Cálculo de Construcciones en redes de interacción (trabajo aún no publicado), y en colaboración con François-Régis Sinot (actualmente en primer año de doctorado, École Polytechnique, dirigido por Maribel Fernández), están estudiando la modelización del Cálculo de Construcciones usando director strings, para lo cual se necesita modelizar la reducción a forma normal (no basta con weak-head-normal form). Con esto se abren dos caminos para la implementación de la Teoría de Especificaciones, una implementación basada en redes de interacción (reescritura de grafos) y otra basada en una máquina abstracta con manejo de ambientes. El objetivo para el año 2003 es definir y comparar estas dos implementaciones para el Cálculo de Construcciones. Dependiendo de los resultados obtenidos, el paso siguiente es la incorporación de la reducción σ en uno de los prototipos.

4 Producción de Conocimiento Original

Presentación de Trabajos en Congresos

Los trabajos presentados en congresos en temas relativos al proyecto se listan a continuación:

1. El 8 de diciembre de 2000 Paula Severi presentó *Internal Program Extraction in the Calculus of Inductive Constructions* (trabajo en conjunto con Nora Szasz) en el encuentro del *Types Working Group* que se realizó del 8 al 12 de diciembre en Durham, Reino Unido.

2. El 10 de setiembre de 2001 Ian Mackie presentó el artículo titulado *Packing Interaction Nets: Applications to Linear Logic and the λ-calculus,* realizado en conjunto con Maribel Fernández, en el Argentinian Workshop on Theoretical Computer Science, WAIT 2001, que se realizó en Buenos Aires, Argentina. Este workshop forma parte de las 30 JAIIO (Jornadas Argentinas de Informática e Investigación Operativa).

3. El 10 de setiembre de 2002, Nora Szasz presentó el artículo *Internal Program Extraction in the Calculus of Inductive Constructions* (trabajo en conjunto con Paula Severi) en el Argentine Workshop on Theoretical Computer Science WAIT 2002 que se realizó del 9 al 13 de setiembre en Santa Fé, Argentina. Este workshop forma parte de las 31 JAIIO (Jornadas Argentinas de Informática e Investigación Operativa).

4. El 21 de setiembre de 2002, Paula Severi presentó el artículo *An operational approach to program extraction in the Calculus of Constructions* (trabajo en conjunto con Maribel Fernández) en el International Workshop on Logic Based Program Development and

Transformation (LOPSTR 2002) que se realizó del 20 al 23 de setiembre en Madrid, España.

5. El 25 de noviembre de 2002, Nora Szasz presentó el artículo *Pure Type Systems with Ultra-Σ types* (trabajo en conjunto con Maribel Fernández, Ian Mackie y Paula Severi) en el CLEI 2002 que se realizó del 25 al 29 de noviembre en Montevideo, Uruguay.

Presentación de Trabajos en Seminarios

Los trabajos presentados en seminarios en torno a temas del proyecto o durante las misiones se listan a continuación:

1. El 22 de noviembre de 2000 Paula Severi presentó *Internal Program Extraction in the Calculus of Inductive Constructions* (trabajo en conjunto con Nora Szasz) en el seminario del Laboratorio de Informática de la École Polytechnique (LIX).

2. El 22 de octubre de 2001 Paula Severi presentó en el seminario de la Universidad de Leicester (Reino Unido) el artículo *Elimination proofs from programs* (trabajo en conjunto con Femke van Raamsdonk).

3. El 6 de junio de 2002, Paula Severi presentó en el seminario regular de Computación de Paris VII el artículo titulado *An Extensional Böhm Model.* Este es un trabajo que realizó en conjunto con Fer-Jan de Vries [SV02b, SV02a].

4. El 2 de julio de 2002, Paula Severi presentó un seminario en la Universidad de Leicester basado en los artículos sobre la Teoria de Especificaciones [SS01, SS02, RS02, FS02].

5. El 29 de agosto de 2002, Paula Severi dió una charla en el seminario regular de Métodos Formales de la Facultad de Ingeniería titulada *Una extension de la Lógica de Hoare para demostrar correctitud de programas imperativos de bajo nivel.* Esta charla estuvo basada en el artículo: *Separation Logic: A Logic for shared Mutable Data Structures* por John Reynolds [Rey02].

6. El 11 de abril de 2002, Maribel Fernández dio un seminario en el Laboratorio de Informática de la Universidad d'Evry, basado en los trabajos del proyecto.

7. El 19 de abril de 2002, Maribel Fernández e Ian Mackie dieron una charla en el Departamento de Computación de King's College London, basada en los trabajos del proyecto.

8. En agosto de 2002, Nora Szasz presentó *Internal Program Extraction in the Calculus of Inductive Constructions* (trabajo en conjunto con Paula Severi) en el seminario de Computación de la Facultad de Ingeniería.

Publicaciones

Los trabajos científicos publicados durante los años 2001 y 2002 en torno a temas del proyecto se listan a continuación:

1. *Studies of a Theory of Specifications with Built-in Program Extraction.* Paula Severi and Nora Szasz. Journal of Automated Reasoning, Vol. 27(1), July 2001.

2. *Packing Interaction Nets: Applications to Linear Logic and the λ-calculus,* Maribel Fernández, Ian Mackie. Actas del WAIT'01, 30 JAIIO (Jornadas Argentinas de Informática e Investigación Operativa), Argentina, 2001.

3. *Internal Program Extraction in the Calculus of Inductive Constructions.* Paula Severi y Nora Szasz. Proceedings of WAIT 2002 (Argentine workshop in Theoretical Computer Science), 31 JAIIO (Jornadas Argentinas de Informática e Investigación Operativa), Argentina, 2002.

4. *An operational approach to program extraction in the Calculus of Constructions.* Maribel Fernández y Paula Severi. Proceeding of Logic Based Program Development and Transformation 2002 (LOPSTR'02), *Lecture Notes in Computer Science*, Springer.

5. *Eliminating proofs from programs.* Femke van Raamsdonk y Paula Severi. Third International Workshop on Logical Frameworks and Meta-Languages (LFM'02). Volumen 70.2 de *Electronic Notes in Theoretical Computer Science.*

6. *A uniform approach to program extraction: Pure Type Systems with Ultra Σ-types.* Maribel Fernández, Ian Mackie, Paula Severi y Nora Szasz. Proceedings of CLEI 2002.

5 Actividades de formación

Como estaba establecido en la propuesta del proyecto, Maribel Fernández e Ian Mackie realizaron cursos de introducción a la Lógica Lineal en Uruguay en 2001 y 2002. También participaron en otras actividades relacionadas con la organización de la investigación. A continuación se detallan las actividades realizadas.

1. Agosto 2001:

   - Curso de especialización de 18 horas de clase teórica, para estudiantes de la Facultad de Ingeniería de la Universidad de la República. En este curso se presentaron las bases de la Lógica Lineal (definida por Jean-Yves Girard en 1987), y se describieron las aplicaciones principales de esta lógica para la implementación de lenguajes de programación funcional. El examen consistió en un trabajo obligatorio de 40 horas.
   - Participación en el jurado de evaluación de candidatos a promoción del Conicyt.

2. Agosto 2002:

   - Curso de 18 horas de clase teórica, para estudiantes de la Facultad de Ciencias de la Universidad de la Republica. En la primera parte del curso se presentaron las bases la Lógica Lineal (definida por Jean-Yves Girard en 1987) y en la segunda parte se discutieron los modelos de reducción derivados de esta lógica: redes de prueba, redes de interacción, geometria de la interacción.

     Estos temas fueron abordados en el curso que dimos en 2001 en la Facultad de Ingeniería, pero esta vez el enfoque fue diferente habida cuenta de los intereses y la formación de los estudiantes de Ciencias (la mayor parte de los estudiantes eran matemáticos, no informáticos).

     Los estudiantes fueron evaluados mediante un trabajo obligatorio de 40 horas.

Se establecieron vínculos que permitirán colaboraciones futuras con la Facultad de Ciencias. En particular, Ian Mackie co-dirigirá con Walter Ferrer, director del Centro de Matematicas de la Facultad de Ciencias, la tesis de Maestría de Octavio Malherbe (estudiante de Matematicas de la Facultad de Ciencias).

- Presentación de la estructura de estudios de postgrado y becas francesas a los estudiantes interesados en continuar sus estudios en Francia.

References

[FMSS] M. Fernández, I. Mackie, P. Severi, and N. Szasz. A uniform approach to program extraction: Pure Type Systems with ultra-Σ types. In *Proceedings of CLEI 2002.*

[FM01a] M. Fernández and I. Mackie. Packing Interaction Nets: Applications to Linear Logic and the λ-calculus. In *Argentinian Workshop on Theoretical Computer Science (WAIT'01)*, Actas de 30 JAIIO, Buenos Aires, 2001.

[FM01b] M. Fernández and I. Mackie. Director Strings and Explicit Substitutions. In *Workshop on Explicit Substitutions and Applications, WESTAPP'01*, Utrecht, 2001.

[FS02] M. Fernández and P. Severi. An operational approach to program extraction in the Calculus of Constructions. In *Proceedings of the International Workshop on Logic Based Program Development and Transformation*, 2002. Lecture Notes in Computer Science, Springer.

[Rey02] M. Reynolds. Separation Logic: A Logic for Shared Mutable Data Structures. In *Proceedings of the Seventeenth Annual IEEE Symposium on Logic in Computer Science*, 2002.

[RS02] F. van Raamsdonk and P. Severi. Eliminating proofs from programs. In *Proceedings of Third International Workshop on Logical Frameworks and Meta-Languages*, volume 70.2 of *Electronic Notes in Theoretical Computer Science*, 2002.

[SV02a] P. Severi and F.-J. de Vries. A lambda calculus for D_∞. In *Proceedings of Domain 2002.* Abstract. Workshop in honour of Dana Scott's 70'th birthday.

[SV02b] P. Severi and F.-J. de Vries. An Infinitary Extensional Lambda Calculus. In *Proceedings of Rewriting Techniques and Applications 2002*, Lectures Notes in Computer Science, Springer.

[SS01] P. Severi and N. Szasz. Studies of a Theory of Specifications with built-in program extraction. *Journal of Automated Reasoning*, 2001.

[SS02] P. Severi and N. Szasz. Internal Program Extraction in the Inductive Calculus of Constructions. In *Argentine Workshop on Theoretical Computer Science (Wait'02)*, 31 JAIIO, 2002.

[Sza97] N. Szasz. *A Theory of Specifications, Programs and Proofs.* PhD thesis, Department of Computing Science, Chalmers University of Technology, S-412 96 Göteborg, Sweden, June 1997.