

Propuesta de Trabajo Final

Licenciatura en Ciencias de la Computación

Una versión del algoritmo Wave Propagation sensible al flujo

Alumno: Giovanni Buchieri
Docente Responsable: Francisco Bavera
Co-Director: Marcelo Arroyo

Departamento de Computación
Facultad de Ciencias Exactas, Físico-Químicas y Naturales
Universidad Nacional de Río Cuarto
Río Cuarto, Argentina

1 Resumen

El análisis de alias es una técnica fundamental dentro del análisis estático de programas, ya que permite determinar si dos punteros pueden referirse a la misma ubicación en memoria. *Wave Propagation* [2] (WP) es un algoritmo de análisis de alias, *insensitivo al flujo*, basado en *inclusion-based points-to analysis*. El método WP ha demostrado mejorar la precisión y eficiencia respecto de enfoques tradicionales, pero aún presenta limitaciones que motivan su extensión. En este proyecto se propone analizar dichas limitaciones, diseñar y desarrollar una extensión *sensitiva al flujo* del algoritmo WP, e implementar un prototipo que permita comparar experimentalmente su desempeño frente a su versión original.

2 Introducción

El análisis estático de programas es un área de la ciencia de la computación orientada a inferir propiedades sobre el comportamiento de un programa sin necesidad de ejecutarlo. Dentro de este campo, *alias analysis* cumple un rol clave en optimización de compiladores, verificación formal y herramientas de ingeniería de software. El presente trabajo se centra en el estudio y la extensión del algoritmo WP un *inclusion-based points-to analysis*, con el fin de obtener una versión sensitiva al flujo.

Los métodos tradicionales de análisis de alias basados en *inclusion constraints* (como el algoritmo de Andersen [1]) son precisos pero costosos en términos computacionales. En respuesta a estas limitaciones, se han propuesto algoritmos más eficientes como el de Steensgaard [3] (basado en el enfoque *unification-based*) y *Wave Propagation* [2], que busca un equilibrio entre precisión y eficiencia. Investigaciones recientes han demostrado que WP reduce la complejidad en casos comunes, pero aún presenta limitaciones en ciertos patrones de programas.

La hipótesis de este trabajo es que la extensión del algoritmo de *Wave Propagation* para que sea sensitivo al flujo permitirá mejorar la precisión del análisis, manteniendo un costo computacional razonable.

El estudio del análisis de alias no solo es un área activa en investigación, sino también de aplicación directa en optimización de compiladores modernos, verificación de seguridad y análisis de vulnerabilidades. La extensión del algoritmo WP contribuirá tanto a la formación académica del estudiante como a la práctica profesional en herramientas de análisis estático.

La investigación se sitúa en el área de análisis de programas, más específicamente en análisis estático de alias. Este tema es relevante porque:

- Contribuye a mejorar compiladores y entornos de desarrollo.

- Aporta a la detección temprana de errores y vulnerabilidades en software.
- Se conecta con problemas actuales en verificación de programas, seguridad informática y optimización de alto rendimiento.

3 Objetivos

Objetivo General

Desarrollar una extensión al algoritmo *Wave Propagation* para mejorar su precisión y eficiencia en el análisis de alias en programas, evaluando experimentalmente sus resultados frente a enfoques existentes.

Objetivos Específicos

- Realizar un estudio comparativo de métodos de análisis de alias (*inclusion-based* y *unification-based*).
- Analizar en detalle el algoritmo WP, identificando sus fortalezas y limitaciones.
- Diseñar una extensión insensitiva al flujo del método WP que mejore su precisión.
- Implementar un prototipo experimental que integre la extensión propuesta.
- Evaluar empíricamente el desempeño del prototipo en benchmarks conocidos, comparándolo con la versión base del WP y otros algoritmos de referencia.
- Redactar y presentar el informe final con los resultados obtenidos.

4 Cronograma de Actividades a Realizar

Meses	Actividad
1-2	Estudio de análisis de alias, métodos <i>points-to analysis</i> y algoritmos relacionados. Análisis del algoritmo WP: Estudio de la implementación base. Identificación de limitaciones y posibles mejoras.
2	Diseño de la extensión propuesta. Formalización de la extensión. Definición de casos de prueba preliminares.
2-4	Selección de las herramientas para la implementación. Diseño e Implementación de la herramienta.
4-5	Experimentación, testing y depuración. Detectar y documentar deficiencias y limitaciones. Comparar con técnicas y herramientas existentes.
5-6	Redacción del informe.

Fecha de Inicio: 1 de Septiembre de 2025.
Fecha estimada de finalización: 15 de febrero de 2026.
Duración total estimada en meses: 6 meses.

Bibliografía

- [1] L. O. Andersen. (1994). Program Analysis and Specialization for the C Programming Language. PhD thesis, DIKU, University of Copenhagen, 1994
- [2] Pereira, F. and Berlin, D. (2009). Wave Propagation and Deep Propagation for Pointer Analysis. CGO, pp 126-135.
- [3] B. Steensgaard. (1996). Points-to analysis in almost linear time. In POPL, pages 32–41, 1996
- [4] Zyrianov, Vlas; Newman, Christian D.; Guarnera, Drew T.; Collard, Michael L.; Maletic, Jonathan I. (2019). srcPtr: A Framework for Implementing Static Pointer Analysis Approaches. ICPC '19: Proceedings of the 27th IEEE International Conference on Program Comprehension. Montreal, Canada: IEEE.
- [5] Thiessen, Rei; Lhoták, Ondřej. (2017). Context transformations for pointer analysis. ACM SIGPLAN Notices. 52 (6): 263–277. doi:10.1145/3140587.3062359. ISSN 0362-1340.