Project Proposal: Pointer Analysis
15-745: Optimizing Compilers
Spring, 2005

Deepak Garg   Himanshu Jain

July 9, 2005

Project URL: http://www.cs.cmu.edu/∼hjain/compliers.html

Project Description

In this project we plan to implement Andersen's points-to-analysis [1] for the Pegasus IR. This is a flow and context insensitive analysis that is reported to be fast and scalable. It works by generating constraints which can be solved to obtain the points-to sets.

BANSHEE [2] is a constraint solver that simplifies the task of building constraint-based program analyses. To use BANSHEE, the analysis designer provides a short specification file describing the kinds of constraints used in the analysis. From this specification, BANSHEE builds a customized constraint resolution engine which solves those constraints efficiently.

An implementation of Andersen's points-to analysis using BANSHEE as the constraint solver is reported to be very fast [3]. We plan to implement a similar analysis for Pegasus. If we get time we would like to experiment with other pointer analysis.

In order to evaluate our implementation, we will identify a set of benchmarks and measure the performance in terms of time taken, memory requirements, accuracy of the points-to sets. We believe there is an existing pointer analysis implemented for Pegasus. We will compare our implementation against it also.

Logistics

Plan of Attack and Schedule. We plan to do this project in the following phases.

1. Studying BANSHEE: Download and install BANSHEE and learn how to use it. (0.5 week)
2. Read about Andersen's analysis and study its implementation in BANSHEE. We will also learn about the Pegasus IR. (1 week)
3. Implement Andersen's analysis on Pegasus IR using BANSHEE as a constraint solver. (1.5–2 weeks)
4. Find appropriate benchmarks and evaluate the performance of our implementation. (1 week)
5. If we have additional time left, we will use it to implement other pointer analysis, like Steensgaard's algorithm [4]. (Variable time)

Milestone. We expect to be in the middle of implementation phase at the project milestone (04/07).

Literature search. We have started reading Andersen's pointer analysis and the BANSHEE user's manual.

Resources needed. We do not need any special hardware resources for this project. The software resources are publicly available.

References

[1] L. Andersen. Program Analysis and Specification for the C Programming Language. Technical Report Ph.D. thesis, DIKU, University of Copenhagen, 1994.

[2] http://banshee.sourceforge.net/.

[3] Jeffrey S. Foster, Manuel Fähndrich, and Alexander Aiken. Flow-Insensitive Points-to Analysis with Term and Set Constraints. Technical Report CSD-97-964, University of California, Berkeley, 1997.

[4] B. Steensgaard. Points-to Analysis in Almost Linear Time. In *ACM SIGACT-SIGPLAN Symposium on Principles of Programming Languages*, pages 32–41, 1995.