Contribution ID: **211**   Type: **not specified**

Link-Time Points-To Analysis Implementation in GCC with Souffle

Monday, 20 September 2021 07:30 (30 minutes)

Points-to analysis is a static code analysis that calculates the pointer-pointee relationship between expressions and static memory locations. The results of the points-to analysis may be used by multiple optimizations and analyses. Of particular interest a precise points-to analysis is necessary to perform data-layout optimizations at the level of alias sets. We use the high level, declarative, logic language Souffle to encode the semantics of a points-to analysis in few lines of code. The Souffle compiler allows us to synthesize a parallel C++ representation of the points-to analysis from the Souffle representation. In this talk we will go over the implementation of an intra-procedural, inclusion-based, field-insensitive, flow-insensitive, context-insensitive, points-to analysis which works with the existing link-time optimization (LTO) framework in GCC. While the current prototype is less precise than the existing points-to analysis our plan is to increase the level of precision of this implementation and use its results to enable future link-time data-layout optimizations.

I agree to abide by the anti-harassment policy

I agree

Primary authors: OCHOA, Erick (SBA Research); MÜLLNER, Christoph (SBA Research); TOMSICH, Philipp (VRULL)

Presenters: OCHOA, Erick (SBA Research); MÜLLNER, Christoph (SBA Research); TOMSICH, Philipp (VRULL)

Session Classification: GNU Tools Track

Track Classification: GNU Tools Track