

VYPE abstract

Foundations of Data Flow Analysis & Constant Propagation

Jan Chaloupka (xchalo08)
David Chaloupka (xchalo09)

November 3, 2012

Abstract:

Data flow analysis is a method of static code analysis. Inspected code is transformed to corresponding Control Flow Graph (CFG) and abstract information is iteratively computed over this CFG. Computation can be made locally (in basic blocks), globally (within procedures or functions) or inter-procedurally. Based on information needed, we can use backward (from CFG's end points to start) or forward (from start to end points) analysis. Data Flow analysis can be used in fields such as compilers (dead variables elimination, common subexpression elimination, copy propagation, induction variables elimination etc.), formal verification, program debugging, etc. Iterative computation is based on the notion of complete lattices and flow functions defined over them. Flow functions describe transformation of one lattice into another whilst gathering more and more precise solution with every iteration. Based on lattices and flow functions, data flow analysis can be generalized. To compute the best result, we need to find the maximum fix-point of flow functions. Since computation of maximum fix-point is very hard in general, meet over paths is computed instead.