Widening and Interpolation

Kenneth L. McMillan

Microsoft Research

Abstract. Widening/narrowing and interpolation are two techniques for deriving a generalization about unbounded behaviors from an analysis of bounded behaviors. The purpose of both methods is to produce an inductive invariant that proves some property of a program or other discrete dynamic system. In the case of widening, we obtain a guess at an inductive invariant by extrapolating a sequence of approximations of the program behavior, either forward or backward. In the case of interpolation, we use the intermediate assertions in proofs of correctness of bounded behaviors.

To contrast these approaches, we will view widening/narrowing operators as deduction systems that have been weakened in some way in order to force generalization. From this point of view, we observe some important similarities and differences between the methods. Both methods are seen to derive candidate inductive invariants from proofs about bounded execution sequences. In the case of widening/narrowing, we produce the strongest k-step post-condition (or weakest k-step pre-condition) derivable in the weakened proof system. By contrast, using interpolation, we derive candidate inductive invariants from a *simple* proof of safety a k-step sequence. The intermediate assertions we infer are neither the strongest nor the weakest possible, but are merely sufficient to prove correctness of the bounded sequence. In widening/narrowing there is an asymmetry in the treatment of the initial and final conditions, since we widen either forward or backward. In interpolation, there is no preferred direction. The initial and final conditions of the sequence are dual.

The most salient distinction between the two approaches is in their *inductive bias*. Any kind of generalization requires some *a priori* preference for one form of statement over another. In the case of widening, this bias is explicit, and given as an *a priori* weakening of the deduction system. In interpolation, we do not weaken the deduction system, but rather bias in favor of parsimonious proofs in the given system. This can be viewed as an application of Occam's razor: proofs using fewer concepts are more likely to generalize. The inductive bias in interpolation is thus less direct than in widening/narrowing as it derives from the chosen logic, and some notion of cost associated to proofs.

E. Yahav (Ed.): SAS 2011, LNCS 6887, p. 1, 2011.