Widening Polyhedra with Landmarks

Axel Simon and Andy King

Computing Laboratory, University of Kent, Canterbury, UK
{a.simon, a.m.king}@kent.ac.uk

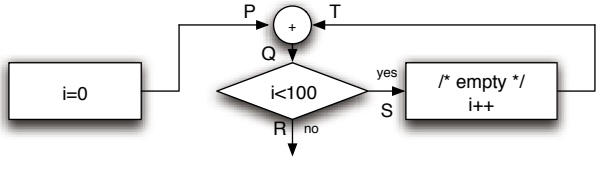
Abstract. The abstract domain of polyhedra is sufficiently expressive to be deployed in verification. One consequence of the richness of this domain is that long, possibly infinite, sequences of polyhedra can arise in the analysis of loops. Widening and narrowing have been proposed to infer a single polyhedron that summarises such a sequence of polyhedra. Motivated by precision losses encountered in verification, we explain how the classic widening/narrowing approach can be refined by an improved extrapolation strategy. The insight is to record inequalities that are thus far found to be unsatisfiable in the analysis of a loop. These so-called landmarks hint at the amount of widening necessary to reach stability. This extrapolation strategy, which refines widening with thresholds, can infer post-fixpoints that are precise enough not to require narrowing. Unlike previous techniques, our approach interacts well with other domains, is fully automatic, conceptually simple and precise on complex loops.

1 Introduction

In the last decade, the focus of static analysis has shifted from program optimisations towards program verification [5]. In this context, the abstract domain of polyhedra [2,10] has attracted much interest due to its expressiveness, as have sub-classes of polyhedra [18,19,21,22] that solve specific analysis tasks more efficiently. However, an inherent problem in polyhedral analysis is the ability to finitely reason about loops. Since the values of variables may differ in each iteration, each iterate may well be described by a different polyhedron. In order to quickly analyse a large or potentially infinite number of iterations, special acceleration techniques are required. One such acceleration framework is provided by the widening/narrowing approach to abstract interpretation [9,10].

1.1 A Primer on Widening/Narrowing

In order to illustrate the widening/narrowing approach on the domain of polyhedra and to discuss the implications of applying narrowing in an actual analyser, consider the control flow graph of `for (i=0; i<100; i++) {/*empty*/}`:



N. Kobayashi (Ed.): APLAS 2006, LNCS 4279, pp. 166–182, 2006.

The analysis amounts to characterising the values that can arise on the edges of the control flow graph. To this end, each edge is decorated with a polyhedron describing the relationships between the values of the variables on that edge. Given that the program contains only a single variable i, the polyhedra P, Q, R, S, T coincide with intervals over the reals. In the example, the polyhedron $P = \{i \in \mathbb{R} \mid 0 \leq i \leq 0\}$ describes the value of i at the beginning of the program. The +-node joins the polyhedra P and T to obtain $Q = P \sqcup T$. This join corresponds to the smallest convex polyhedron that includes the set of points $P \cup T$. Due to the integrality of i, the polyhedra that characterise the two outcomes of the test $i < 100$ are $R = Q \sqcap \{i \in \mathbb{R} \mid i \geq 100\}$ and $S = Q \sqcap \{i \in \mathbb{R} \mid i \leq 99\}$ where $\sqcap = \cap$ denotes the intersection of two polyhedra. The last polyhedron T is characterised by the affine map $T = \{i + 1 \mid i \in S\}$.

A solution of these equations can be found by applying Jacobi iteration [8], which calculates new polyhedra $P_{j+1}, Q_{j+1}, R_{j+1}, S_{j+1}, T_{j+1}$ from the polyhedra of the previous iteration P_j, Q_j, R_j, S_j, T_j. To ensure rapid convergence, a widening point must be inserted into the Q, S, T cycle. Widening at Q amounts to replacing the equation for Q with $Q_{j+1} = Q_j \nabla (P_j \sqcup T_j)$ where ∇ is a widening operator that removes unstable bounds [9]. The possible values of `i` are given below where $\perp$ denotes the empty set; the updated entries are shown in bold:

j	P_j	Q_j	R_j	S_j	T_j
1	$[\mathbf{0}, \mathbf{0}]$	$\perp$	$\perp$	$\perp$	$\perp$
2	$[0, 0]$	$[\mathbf{0}, \mathbf{0}]$	$\perp$	$\perp$	$\perp$
3	$[0, 0]$	$[0, 0]$	$\perp$	$[\mathbf{0}, \mathbf{0}]$	$\perp$
4	$[0, 0]$	$[0, 0]$	$\perp$	$[0, 0]$	$[\mathbf{1}, \mathbf{1}]$
5	$[0, 0]$	$[\mathbf{0}, \infty]$	$\perp$	$[0, 0]$	$[1, 1]$

j	P_j	Q_j	R_j	S_j	T_j
6	$[0, 0]$	$[0, \infty]$	$[\mathbf{100}, \infty]$	$[\mathbf{0}, \mathbf{99}]$	$[1, 1]$
7	$[0, 0]$	$[0, \infty]$	$[100, \infty]$	$[0, 99]$	$[\mathbf{1}, \mathbf{100}]$
8	$[0, 0]$	$[0, \infty]$	$[100, \infty]$	$[0, 99]$	$[1, 100]$
1'	$[0, 0]$	$[\mathbf{0}, \mathbf{100}]$	$[100, \infty]$	$[0, 99]$	$[1, 100]$
2'	$[0, 0]$	$[0, 100]$	$[\mathbf{100}, \mathbf{100}]$	$[0, 99]$	$[1, 100]$

In iteration 5, the output of the +-node is $P_4 \sqcup T_4 = [0, 1]$. The widening operator compares $P_4 \sqcup T_4$ against $Q_4 = [0, 0]$ and removes the unstable upper bound, yielding $Q_5 = [0, \infty]$. Stability is reached in iteration 8. The calculated post-fixpoint is now refined. This is realised by replacing widening with narrowing, i.e. $Q_{j+1} = Q_j \triangle (P_j \sqcup T_j)$. For polyhedra, it is sufficient to put $\triangle = \sqcap$ and to bound the number of iterations [9, page 290]. Hence, let $Q_{j+1} = Q_j \sqcap (P_j \sqcup T_j)$ which yields a refined state 1' and a further refinement $2'$ which, in this case, coincides with the least fixpoint of the original equations.

1.2 The Limitations of Narrowing

To illustrate one drawback of narrowing, consider a re-analysis of the above example where the widening is applied on S rather than on Q. In particular, let $S_{j+1} = S_j \nabla (Q_i \sqcap \{i \in \mathbb{R} \mid i \leq 99\})$. The analyses differ after the first 4 iterations:

j	P_j	Q_j	R_j	S_j	T_j
5	$[0, 0]$	$[0, 1]$	$\perp$	$[0, 0]$	$[1, 1]$
6	$[0, 0]$	$[0, 1]$	$\perp$	$[\mathbf{0}, \infty]$	$[1, 1]$
7	$[0, 0]$	$[0, 1]$	$\perp$	$[0, \infty]$	$[\mathbf{1}, \infty]$
8	$[0, 0]$	$[\mathbf{0}, \infty]$	$\perp$	$[0, \infty]$	$[\mathbf{1}, \infty]$
9	$[0, 0]$	$[0, \infty]$	$[\mathbf{100}, \infty]$	$[0, \infty]$	$[1, \infty]$

j	P_j	Q_j	R_j	S_j	T_j
10	$[0, 0]$	$[0, \infty]$	$[100, \infty]$	$[0, \infty]$	$[1, \infty]$
1'	$[0, 0]$	$[0, \infty]$	$[100, \infty]$	$[\mathbf{0}, \mathbf{99}]$	$[1, \infty]$
2'	$[0, 0]$	$[0, \infty]$	$[100, \infty]$	$[0, 99]$	$[\mathbf{1}, \mathbf{100}]$
3'	$[0, 0]$	$[\mathbf{0}, \mathbf{100}]$	$[100, \infty]$	$[0, 99]$	$[1, 100]$
4'	$[0, 0]$	$[0, 100]$	$[\mathbf{100}, \mathbf{100}]$	$[0, 99]$	$[1, 100]$