Comparison of the Galois Connexion and Widening/Narrowing Approaches to Abstract Interpretation (extended abstract)

Patrick Cousot & Radhia Cousot

LIX, URA CNRS 1439
École Polytechnique, F-91128 Palaiseau Cedex, France
email: cousot@polytechnique.fr

1 The Galois Connexion Approach to Abstract Interpretation

Following [2], [3] and [4], the abstract interpretation of a program can be formalized as the effective computation of an approximation A of the least fixed point $lfp(F)$ of a monotone operator $F \in L \stackrel{mon}{\longmapsto} L$ on a complete poset $L(\sqsubseteq, \bot, \sqcup)$ specifying the *collecting semantics* of the program. The upper approximation must be *correct* in the sense that $lfp(F) \sqsubseteq A$.

The Galois connexion approach to abstract interpretation formalizes the idea that the system of equations $X = F(X)$ can be first simplified into $\overline{X} = \overline{F}(\overline{X})$, where $\overline{F} \in \overline{L} \stackrel{mon}{\longmapsto} \overline{L}$, and then solved iteratively starting from the infimum $\bot$. The connexion between the semantic domain L and its abstract version $\overline{L}$ can be formalized by a Galois connexion (also called *pair of adjoined functions*) $L \underset{\gamma}{\overset{\alpha}{\leftrightarrows}} \overline{L}$ where $\alpha \in L \stackrel{mon}{\longmapsto} \overline{L}$ and $\gamma \in \overline{L} \stackrel{mon}{\longmapsto} L$ are monotone functions such that:

$$\forall x \in L, y \in \overline{L} : (\alpha(x) \sqsubseteq y) \Longleftrightarrow (x \sqsubseteq \gamma(y))$$

If $\alpha \circ F \circ \gamma \sqsubseteq \overline{F}$ then $lfp(\overline{F})$ is a correct upper approximation of $lfp(F)$ in the sense that $lfp(F) \sqsubseteq \gamma(lfp(\overline{F}))$.

2 The Widening/Narrowing Approach to Abstract Interpretation

Another method [2], [3] consists in using a *widening* operator $\triangledown \in L \times L \longmapsto L$ such that:

$$\forall x, y \in L : x \sqsubseteq x \triangledown y$$

$$\forall x, y \in L : y \sqsubseteq x \triangledown y$$

and for all increasing chains $x^0 \sqsubseteq x^1 \sqsubseteq \ldots$, the chain defined by $y^0 = x^0, \ldots, y^{i+1} = y^i \triangledown x^{i+1}, \ldots$ is not strictly inscreasing. It follows that the approximate iteration sequence $\underline{X}^0 = \bot$, ..., if $F(\underline{X}^i) \sqsubseteq \underline{X}^i$ then $\underline{X}^{i+1} = \underline{X}^i$ else $\underline{X}^{i+1} = \underline{X}^i \triangledown F(\underline{X}^i)$, ... is ultimately stationary and its limit $\underline{A}$ is a correct upper approximation of $lfp(F)$.

This approximation can then be improved using a *narrowing* operator $\triangle \in L \times L \longmapsto L$ such that:

$$\forall x, y \in L : x \sqcap y \sqsubseteq x \triangle y \sqsubseteq x$$

and for all decreasing chains $x^0 \sqsupseteq x^1 \sqsupseteq \ldots$, the chain defined by $y^0 = x^0, \ldots, y^{i+1} = y^i \triangle x^{i+1}, \ldots$ is not strictly descreasing. It follows that the approximate iteration sequence $\overline{X}^0 = \underline{A}$, ..., if $F(\overline{X}^i) = \overline{X}^i$ then $\overline{X}^{i+1} = \overline{X}^i$ else $\overline{X}^{i+1} = \overline{X}^i \triangle F(\overline{X}^i)$, ... is ultimately stationary and its limit $\overline{A}$ as well as each term $\overline{X}^i$ of the decreasing sequence is a correct upper approximation of $lfp(F)$.

In practice both methods are combined. First a Galois connexion is used to obtain approximate equations $\overline{X} = \overline{F}(\overline{X})$ on an infinite domain $\overline{L}$ not satisfying the ascending chain condition. These fixpoint equations are then solved iteratively using a widening and a narrowing to enforce convergence or to accelerate it for finite but very large abstract domains.

3 Unappreciated conjectures about the two approaches

The widening/narrowing approach to abstract interpretation is not so well understood as the Galois connexion approach, as exemplified by [1] where no paper refers to the convergence acceleration method.

An often used argument for 'proving' the uselessness of the widening/narrowing approach is that given an infinite abstract domain together with specific widening and narrowing operators, it is possible to find a finite lattice which will give the same results. For example [6] claims that "One may wonder whether or not it is necessary to choose a finite domain for abstract

interpretation, since apparently more information can be obtained from an interpretation over an infinite domain. The answer is that if uniform termination of the abstract interpretation is required, no more information can be obtained by choosing an infinite domain").

4 Comparing the two approaches

The purpose of this short paper is to analyze carefully the above statement claiming that finite lattices can be used instead of widening/narrowing operators.

First we show that no finite abstract domain (or domain satisfying the ascending chain condition) can be used instead of widening/narrowing operators on infinite domains, since :

1. For each program there exists such a finite lattice;
2. No such finite lattice will do for all programs;
3. For all programs, infinitely many abstract values are necessary;
4. For a particular program it is not possible to infer the set of needed abstract values by a simple inspection of the text of the program (so that the finite subset which is used for analyzing a given program cannot be directly derived from its text).

Second we show that given an infinite abstract domain, it is always possible to find widening/narrowing operators giving results similar (in precision and speed of convergence) to the ones that could be obtained by further approximations of the domain based upon Galois connexions.

Third we show how Galois connexions can help in the design of widening operators.

All these points are also illustrated by means of examples. Various widening operators are suggested for solving non-convergence problems left opened in the literature (such as [5] who resorts to human interaction where a widening operator would do).

References

[1] Abramsky, S. & Hankin, C. (eds). "Abstract interpretation of declarative languages". Ellis Horwood, 1987.

[2] Cousot, P. & Cousot, R. "Static determination of dynamic properties of programs". Proc. 2$^{\mathtt{nd}}$ Int. Symp. on Programming, Dunod, Paris, 1976, pp. 106–130.

[3] Cousot, P. & Cousot, R. "Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints". Conference Record of the 4$^{\mathtt{th}}$ ACM Symposium on Principles of Programming Languages, Los Angeles, California, U.S.A., 1977, pp. 238–252.

[4] Cousot, P. & Cousot, R. "Systematic design of program analysis frameworks". Conference Record of the 6$^{\mathtt{th}}$ ACM Symposium on Principles of Programming Languages, San Antonio, Texas, U.S.A., 1979, pp. 269–282.

[5] Van Gelder, A. "Deriving Constraints Among Arguments Sizes in Logic Programs". Proceedings of the 9$^{\mathtt{th}}$ ACM Symposium on Principles of Database Systems, Nashville, Tennesse, U.S.A., 1990, pp. 47–60.

[6] Kieburtz, R.B. & von Neumann, N.W. "Abstract semantics". In [1], pp. 143–180.