40 years of convex polyhedra, and what's more to say?

David Monniaux*[1]

[1]VERIMAG – Centre National de la Recherche Scientifique : UMR5104, Université Grenoble Alpes, Institut polytechnique de Grenoble (Grenoble INP) – France

Résumé

Convex polyhedra - solution sets of systems of linear inequalities and equalities - have been used for the static analysis of programs since Cousot & Halbwachs' seminal 1978 article.

The classical algorithmic approach to convex polyhedra is to describe them both using the system of constraints, and as the convex hull of generators (vertices, rays, and lines). Unfortunately, the generator representation is exponential in the number of dimensions on cases very common in static analysis. Another difficulty is the use of the "widening" operator for extrapolating iterations into candidate inductive invariants.

Instead of this double description, we have implemented in our library, VPL (https://github.com/VERIMAG-Polyhedra/VPL) a constraint-only representation, first with variants of the Fourier-Motzkin projection algorithm, then with parametric linear programming.

Because of this high algorithmic cost of general convex polyhedra, various subclasses of convex polyhedra have been proposed in the last twenty years: octagons, templates, etc. In some of these domains, it is possible to do away completely with the widening operator: the least inductive invariant in the domain can be directly computed.

One may thus wonder whether the widening operator is needed at all for general polyhedra - could there be an algorithm that would answer whether a program has polyhedral inductive invariants establishing a safety property? We have shown that, if there are non-linear polynomial transitions, this problem is undecidable. The question remains open for linear transitions only.

*Intervenant