Static Analyses of Congruence Properties on Rational Numbers (extended abstract)*

Philippe Granger

ENSTA, 32, boulevard Victor, 75739 Paris Cedex 15, France
granger@ensta.fr

Abstract. We present several new static analysis frameworks applying to rational numbers, and more precisely, designed for discovering congruence properties satisfied by rational (or real) variables of programs. Two of them deal with additive congruence properties and generalize linear equation analysis [12] and congruence analyses on integer numbers [8, 9]. The others are based on multiplicative congruence properties in the set of positive rational numbers. Among other potential applications, we exemplify the interest of all these analyses for optimizing the representation of rational or real valued variables.

1 Introduction

Static (or semantic) analysis of programs covers a wide range of techniques conceived to discover dynamic properties of programs at compile-time. It has been given a unified formal framework by P. and R. Cousot [3, 4] in terms of the classical lattice-theoretic model for *abstract interpretation*. Applications are numerous and various and include program verification (e.g., type checking), program optimization (e.g., dead code elimination, static array bound checking [2], strictness analysis for lazy languages [18]) and program transformation (e.g., automatic vectorization [1, 14]).

Among the different types of analyses which have been proposed in the literature, those dedicated to the discovery of properties of numbers are certainly of major importance, because they provide a general multi-purpose tool usable in numerous application domains. First, they obviously apply directly to numerical variables of programs, which constitutes by itself an important application area (as suggested by the examples mentioned above). Secondly, they can be used also for many other purposes as a second stage abstraction process. More precisely, a large number of analyses are designed as the composition of two or more abstractions, the last one applying on numbers—for instance, consider the abstraction of the length of a list or of the height of a stack. N. Mercouroff's communication detection in parallel programs (by means of communication counters) [17] and A. Deutsch's alias analysis [6] are more complex examples of such analyses.

* This research was initiated when the author was with the Laboratoire d'Informatique, École Polytechnique, Palaiseau, France.

1.1 Contribution and Related Work

Let us briefly survey the most significant analyses on numbers currently available (i.e., apart from the finite ones, such as parity or sign analysis); variables are hereafter denoted by x or x_i, and constants by a, b, c, a_i:

- *Constant propagation* [13], designed for discovering properties of the type: $x = a$.
- *Interval analysis* [2], generalizing the previous one by properties of the type: $x \in [a, b]$ (including also unbounded intervals, such as: $x \in [a, +\infty)$).
- *Arithmetical congruence analysis* on integer numbers [8], dedicated to the discovery of properties of the form:

$$x \equiv a \pmod{b} \ ,$$

  and which extends constant propagation (when $b = 0$).
- *Linear equation analysis* [12], which is a relational[2] generalization of constant propagation on real (or rational) numbers, and which corresponds to systems of linear equations, such as:

$$\sum_{i=1}^{n} a_i x_i = b \ .$$

- *Linear restraint analysis* [5], which extends the preceding one to systems of linear restraints (in $\mathbb{R}$ or $\mathbb{Q}$), such as:

$$\sum_{i=1}^{n} a_i x_i \leq b \ .$$

- *Linear congruence analysis* [9], which also generalizes linear equation analysis, but in the set $\mathbb{Z}$ of integer numbers, and corresponds to systems of linear congruence equations, such as:

$$\sum_{i=1}^{n} a_i x_i \equiv b \pmod{c} \ . \tag{1}$$

In this paper, we first present the extensions of both congruence analyses to rational numbers, which correspond to the same kind of properties with the following definition of the congruence relation in the set $\mathbb{Q}$ of rational numbers:

$$\forall x, y, z \in \mathbb{Q}, (x \equiv y \pmod{z}) \Leftrightarrow (\exists \lambda \in \mathbb{Z}, x = y + \lambda z) \ . \tag{2}$$

One must be aware that these extensions are not straightforward, and that they are by nature very different from the equivalent analyses in $\mathbb{Z}$: for instance, they correspond to complete lattices which do not satisfy the *ascending chain property* (contrarily to their equivalents in $\mathbb{Z}$—see [8, 9]), i.e., complete lattices containing infinite ascending chains.

[2] By definition, a *relational* analysis infers properties relating several variables.