Software Verification

Bounded Box

Mattia Bottaro - Mauro Carlin
May, 2018

Università degli Studi di Padova

Outline

Project - Domain

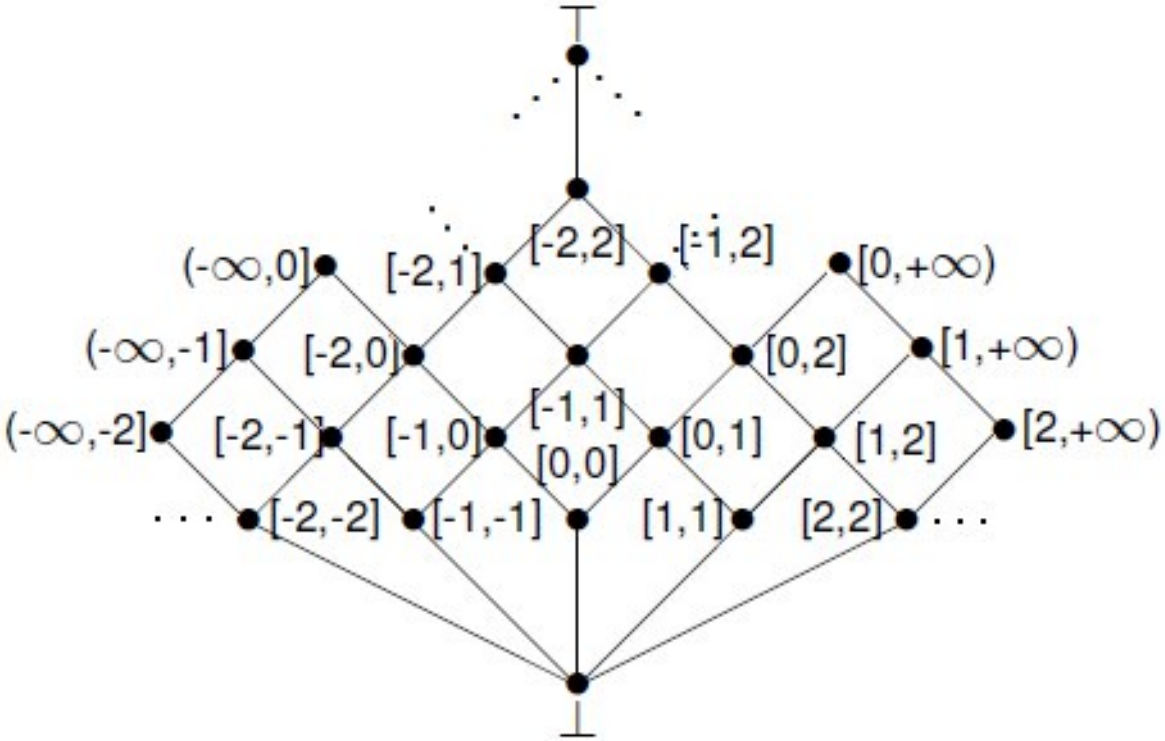
We have chosen the **Bounded Box Domain**, which is a parametric restriction of the interval abstract domain *Int*:

Given $m, n \in \mathbb{Z} \cup \{-\infty, +\infty\}$, then

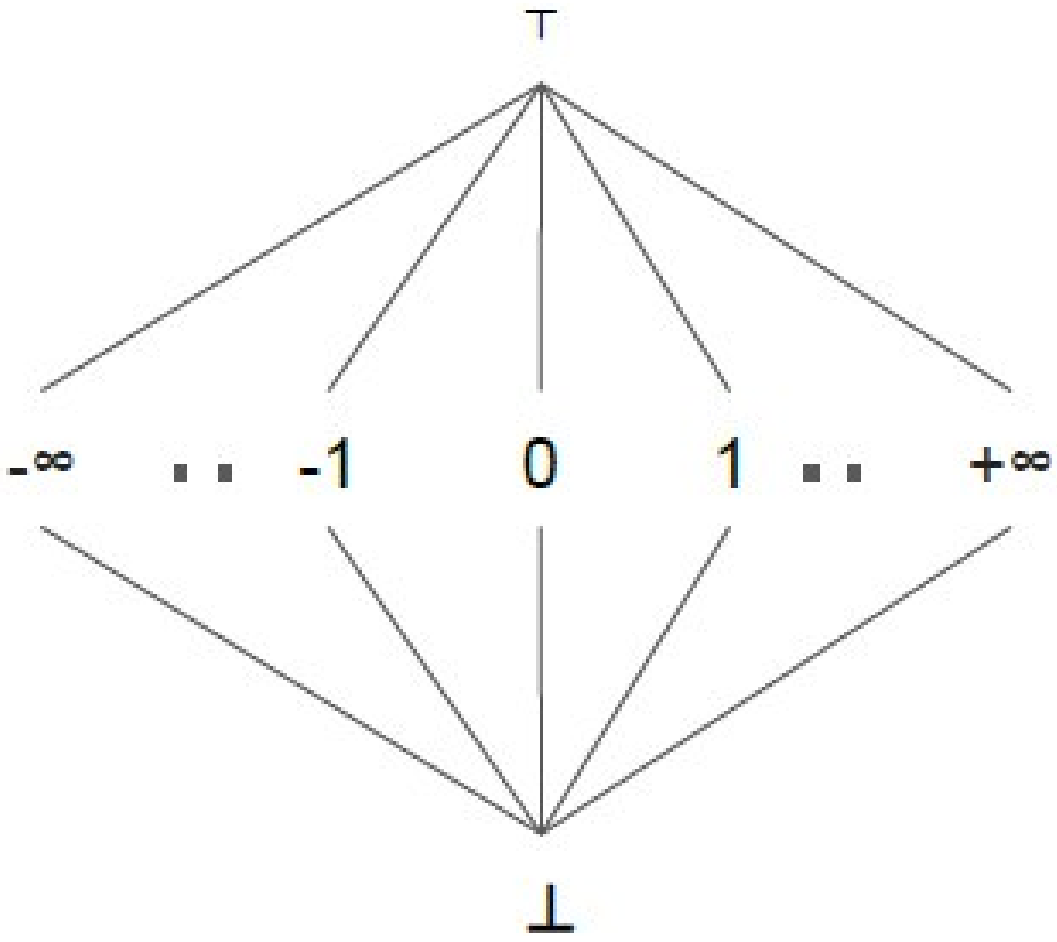
$$\mathbf{Int}_{m,n} := \{\varnothing, \mathbb{Z}\} \cup \{[k,k] \mid k \in \mathbb{Z}\} \cup \{[a,b] \mid a < b,\ [a,b] \subseteq [m,n]\} \cup \{(-\infty, k] \mid k \in [m,n]\} \cup \{[k, +\infty) \mid k \in [m,n]\}$$

Project - Domain

Bounded Box with m = -2, n = 2



Bounded Box with m > n

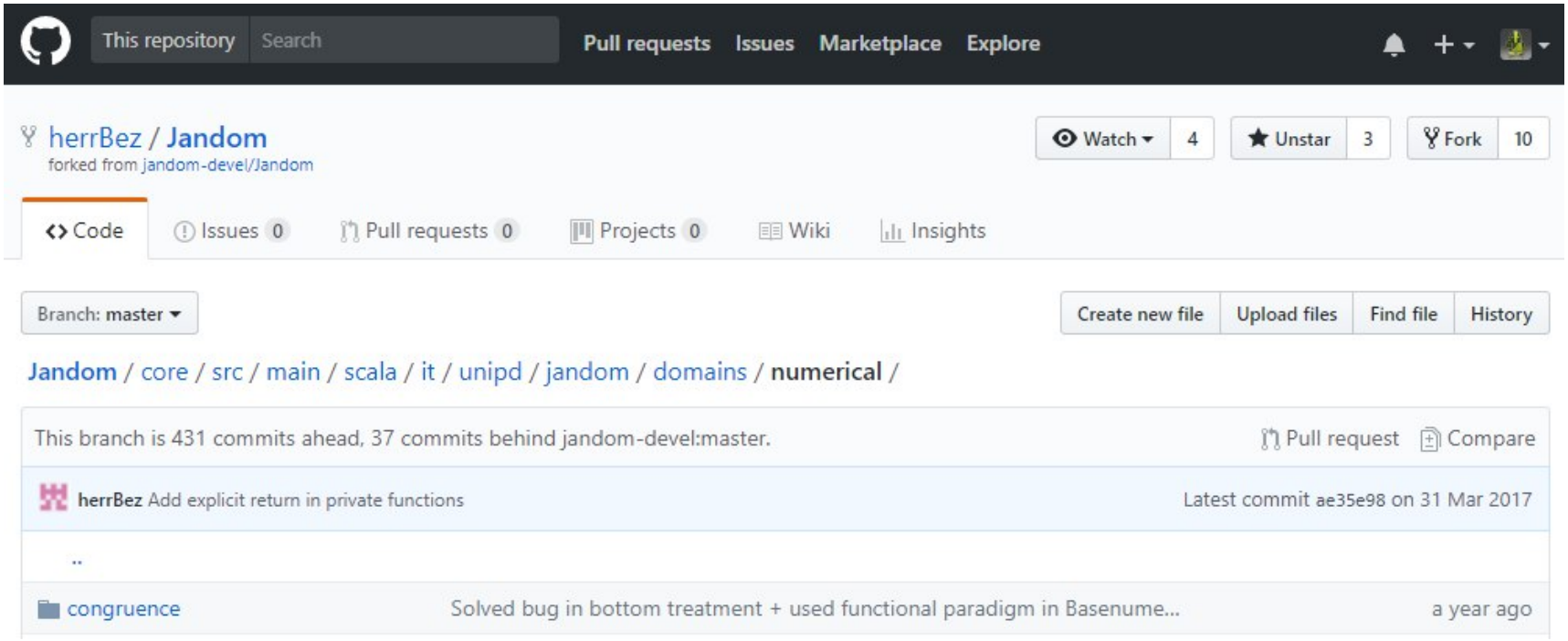


Project - Jandom

- Static Analyzer for **Numerical** and Object Domains (forse togliere object)
- Jandom was created at the University of Chieti-Pescara
- It's a buildup of **RANDOM**, which analyzes **R** code
- Jandon is written in **Scala**
- Jandom analyzes JVM bytecode using **Soot**

Project - Jandom

We've extended Jandom from this repository created by University of Padua' students



Our Contribution

We have:

1. Implemented the Integer Interval Domain
2. Implemented Bounded Box Domain specializing the previous domain, because abstract operators of both domains are very similar

Our Contribution

Abstract **sum** operator algorithm in Bounded Box Domain.

1. Execute sum operator of Interval Domain.
   $[a, b] +^{\#} [c, d] = [a + c, b + d] = [e, f]$
2. $[e, f]$ must be represented as an element of Bounded Box Domain

$$[e, f] = \begin{cases} \top & e < m \wedge f > n \\ [n, +\infty) & e \geq n \wedge e \neq f \\ [e, +\infty) & e < n \wedge f > n \\ (-\infty, m] & f \leq m \wedge e \neq f \\ (-\infty, f] & f > m \wedge e < m \\ [e, f] & \textit{otherwise} \end{cases}$$

Our contribution

Normal block

Fusce luctus venenatis felis quis semper

Alert block

$$E = (x_1 \vee \neg x_2 \vee \neg x_3) \wedge (x_1 \vee x_2 \vee x_4)$$

Example block

Proin tincidunt, neque at tincidunt mollis