Combining Zonotope Abstraction and Constraint Programming for Finding an Invariant

Bibek Kabi, Eric Goubault, Sylvie Putot

Cosynus team, LIX, École Polytechnique, Palaiseau, France

bibek,goubault,putot(@lix.polytechnique.fr)

Abstract

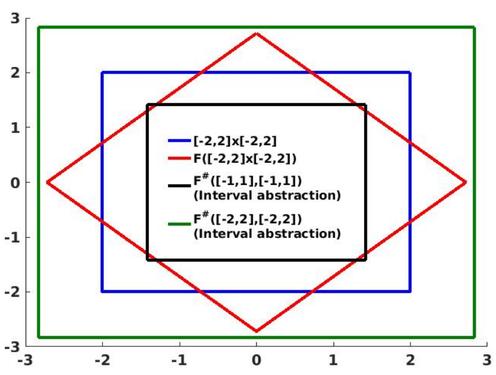
This work deals with the challenges associated while combining abstract interpretation (zonotopes) and constraint programming for infering inductive invariants.

1. Introduction

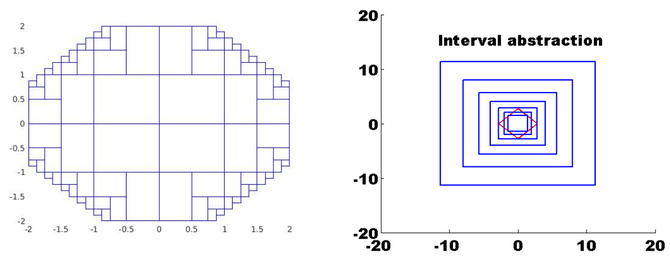
Example [1]

x := input $[-1,1]$ // $E := [-1,1]\times[-1,1]$(entry states)
y := input $[-1,1]$
while true do
// $F(Y) := \{(\frac{\sqrt{2}}{2}(x-y), \frac{\sqrt{2}}{2}(x+y))|(x,y) \in Y\}$(loop)
$x' := \frac{\sqrt{2}}{2} * (x-y)$
$y' := \frac{\sqrt{2}}{2} * (x+y)$
$x := x'$ $y := y'$
done

- The box $I := [-2,2] \times [-2,2]$ is an invariant



- I is not an inductive invariant because $F(I) \nsubseteq I$
- Invariants are not always inductive invariants
- No box is an inductive invariant for this example
- We would like to have a disjunction of boxes (left figure)
- This can be achievable by constraint solving based on propagation and splitting [1], [2]



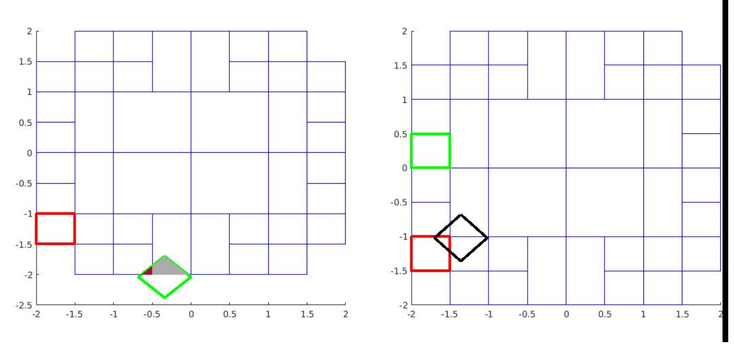
Why the kind of abstract domain to be chosen is very crucial (right figure) ?

Kleene iterations ($Y^0 = E, Y^1 = F(Y^0), \ldots, Y^{k+1} = Y^k \cup F(Y^k)$) on the example using interval abstract domain do converge but to $[-\infty,\infty] \times [-\infty,\infty]$

2. Algorithm [1]

- *doomed*, if $F^\sharp(S_k) \cap (\cup_i S_i) = \emptyset$
- *benign*, if $F^\sharp(S_k) \subseteq \cup_i S_i$

  coverage(S_k):= $\frac{\sum_i volume(F^\sharp(S_k) \cap S_i)}{volume(F^\sharp(S_k))}$ (left figure)
- *necessary*, if $S_k \cap E \neq \emptyset$
- *useful*, if $\exists i$: $S_k \cap F^\sharp(S_i) \neq \emptyset$ (right figure)

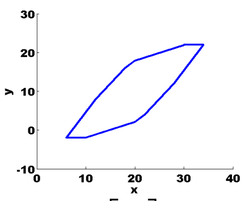


3. Zonotopes, but first why?

- To have a more precise $F^\sharp$
- To have less splitting

$\hat{x} = 20 - 3\varepsilon_1 + 5\varepsilon_2 + 2\varepsilon_3 + 1\varepsilon_4 + 3\varepsilon_5$,
$\hat{y} = 10 - 4\varepsilon_1 + 2\varepsilon_2 + 1\varepsilon_4 + 5\varepsilon_5$

Zonotope is the geometric concretization of sets of values taken by the affine forms [3]



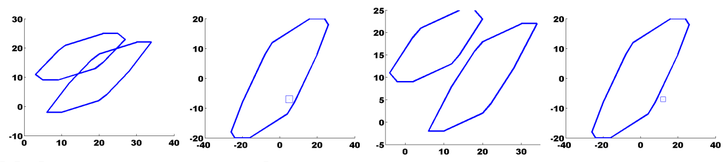
$\mathfrak{Z}$=$\{x \in \mathbb{R}^p | x = c + \sum_{i=1}^{n} \varepsilon_i g^i\}$

where c=$\begin{bmatrix}20\\10\end{bmatrix}$, $g^{(i)}$=$\begin{bmatrix}-3 & 5 & 2 & 1 & 3\\-4 & 2 & 0 & 1 & 5\end{bmatrix}$ and $\varepsilon_i \in [-1,1]$

4. Challenges

Checking for Intersection

- Let $\mathfrak{Z}_1$=$(c1, g_1, \cdots, g_k)$ and $\mathfrak{Z}_2$=$(c2, h_1, \cdots, h_m)$
- $\mathfrak{Z}_1 \cap \mathfrak{Z}_2 \neq \emptyset$ if $c1 - c2$ is entailed in $(0, g_1, \cdots, g_k, h_1, \cdots, h_m)$

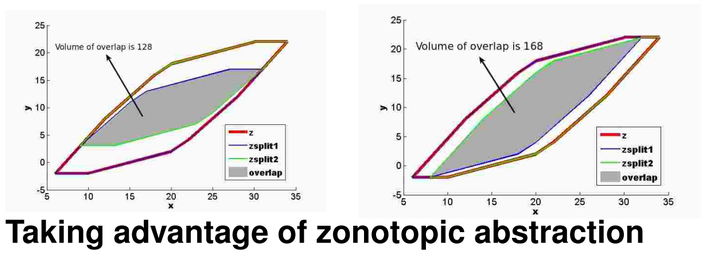


Volume computation

- volume($\mathfrak{Z}(v_1, \cdots, v_n)$) = $2^d \dot{\sum} |\det(v_{i_1}, \cdots, v_{i_d})|$
- Intersection volume from polytope [4]

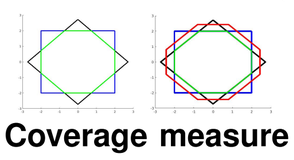
Splitting with overlap

- By splitting the j^{th} generator
- $c1$=$c - g(ind)/2$, $c2$=$c + g(ind)/2$



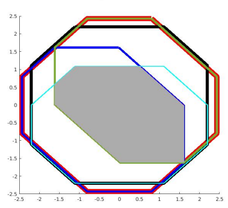
Taking advantage of zonotopic abstraction

- The initial box $(x,y) \in S_0$=$[-2,2]^2$ abstracted using zonotopes as S_0 = $\begin{bmatrix}2\varepsilon_1 & 2\varepsilon_2\end{bmatrix}^{\mathrm{T}}$ is still a box
- In order to use actual zonotopes we tighten S_0 as $S_0 \rightarrow (S_0 \cap F^\sharp(S_0)) \cup (S_0 \cap E)$ [1]



$\alpha \begin{bmatrix}2\varepsilon_1\\2\varepsilon_2\end{bmatrix} + (1-\alpha) \begin{bmatrix}\sqrt{2}(\varepsilon_3 - \varepsilon_4)\\\sqrt{2}(\varepsilon_3 + \varepsilon_4)\end{bmatrix}$

Coverage measure for overlapping zonotopes

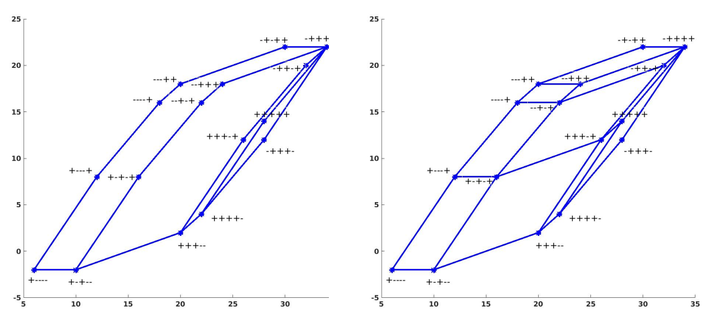


Inclusion-exclusion principle in combinatorics

Splitting via tilings (parallelotopes) [5],[6]

- No overlap and union is equal to $\mathfrak{Z}$
- $\mathfrak{Z}_X := \sum_{i \in X^0} [-v_i, +v_i] + \sum_{i \in X^+} v_i - \sum_{i \in X^-} v_i$

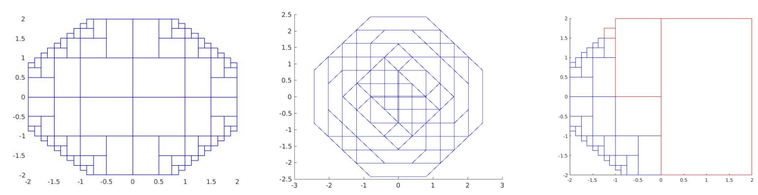
(Left figure (keep iterating until first tile), right figure (all tiles))



5. Experiments

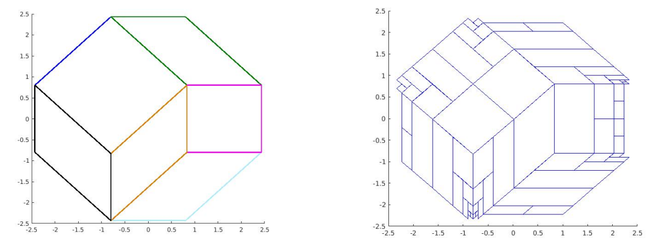
With boxes & actual zonotopes (split: overlap)

- **84** boxes with vol=13.1875 (leftmost figure), 207 iterations and 76.192s(vol=16 for initial box)
- With actual zonotopes, huge overlap & time consuming ($\sum_i vol(F^\sharp(S_k) \cap S_i)$)
- Stopping criteria: algorithm returns once the mean coverage $\geq$ 0.9944
- **12** actual zonotopes(middle figure, vol=18.3316 no change from initial)
- **36** boxes(rightmost figure, vol=14.6250)



With actual zonotopes (split: tilings)

- **6** tilings (left figure) via parallelotopes
- **61** actual zonotopes with vol=16.9398 (right figure), 135 iterations and 38.824 s
- Volume could be "$<$" if starting element (vol=18.3316 for initial) is more compact



6. Acknowledgement

This work is being supported by project ANR-15-CE25-0002-01 COVERIF.

References

[1] Miné, A., Breck, J., & Reps, T. (2016, April). An algorithm inspired by constraint solvers to infer inductive invariants in numeric programs. In European Symposium on Programming Languages and Systems (pp. 560-588). Springer, Berlin, Heidelberg.

[2] Pelleau, M., Miné, A., Truchet, C., & Benhamou, F. (2013, January). A constraint solver based on abstract domains. In Verification, Model Checking, and Abstract Interpretation (pp. 434-454). Springer Berlin Heidelberg.

[3] Goubault, E., & Putot, S. (2015). A zonotopic framework for functional abstractions. Formal Methods in System Design, 47(3), 302-360.

[4] Althoff, M. (2015). An introduction to CORA 2015. In Proc. of the Workshop on Applied Verification for Continuous and Hybrid Systems.

[5] Richter-Gebert, J., & Ziegler, G. M. (1994). Zonotopal tilings and the Bohne-Dress theorem. Contemporary Mathematics, 178, 211-211.

[6] Ferrez, J. A., Fukuda, K., & Liebling, T. M. (2005). Solving the fixed rank convex quadratic maximization in binary variables by a parallel zonotope construction algorithm. European Journal of Operational Research, 166(1), 35-50.