Ensuring Safety of Large-Scale Structures

Background

The application of cyber-physical systems in safety-critical environments requires formal verification techniques in order to ensure correct functionality. Reachability analysis is one of the main techniques to provide safety guarantees: A tight over-approximation of the reachable set of states of a dynamical system is computed and checked against a set of unsafe states, which is usually given by unwanted system behavior. If the reachable set and the unsafe set do not intersect, safety is formally guaranteed. In general, we can only compute over-approximations of the reachable sets to maintain soundness, but the computational effort increases with the system dimension, which recently led to the development of specialized methods for large-scale systems.

The *Olympiaturm* in Munich's *Olympiapark*. The verification of such a large-scale structure requires specialized methods. Image from `https://www.muenchen.de/sehenswuerdigkeiten`.

Description

In this thesis, the mechanical model of a tall building (see Figure above) is considered which gives rise to a large-scale linear system. These systems are usually described by sparse system matrices containing blocks (submatrices) of empty, diagonal, or tridiagonal matrices, which can be exploited to achieve a more efficient reachable set computation. This thesis is aimed at leveraging block decomposition methods [2], where the system matrix is decomposed into blocks in order to decrease the complexity of the operations of the reachability algorithm. Furthermore, the sparsity also allows to neglect dimensions which are irrelevant for the verification task. All programming will be done in MATLAB, and the final implementation should be integrated into the CORA toolbox [1].

Tasks

- Development and implementation of block-decomposition methods for reachability analysis of large-scale linear systems
- Evaluation of the performance on a provided scalable tall building benchmark
- Integration of the final implementation into the CORA toolbox

References

[1] M. Althoff. An introduction to CORA 2015. In *Proc. of the Workshop on Applied Verification for Continuous and Hybrid Systems*, pages 120–151, 2015.

[2] Sergiy Bogomolov and et al. Reachability analysis of linear hybrid systems via block decomposition. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 39(11):4018–4029, 2020.

Technische Universität München

Fakultät für Informatik

Lehrstuhl für Echtzeitsysteme und Robotik

Supervisor:
Prof. Dr.-Ing. Matthias Althoff

Advisor:
Mark Wetzlinger, M.Sc.

Research project:
ConVeY

Type:
MA

Research area:
Reachability Analysis

Programming language:
MATLAB

Required skills:
Good mathematical background (calculus), programming in MATLAB

Language:
English

Date of submission:
18. Juni 2021

For more information please contact us:

Phone: +49.89.289.18144
(currently not available)

E-Mail: m.wetzlinger@tum.de

Internet:
https://www.in.tum.de/i06