Constrained Dynamic Partial Order Reduction (Abstract)*

Elvira Albert, Miguel Gómez-Zamalloa, Miguel Isabel
Complutense University of Madrid, Spain
elvira,mzamalloa@fdi.ucm.es, miguelis@ucm.es

Albert Rubio
Universitat Politècnica de Catalunya, Spain
albert@cs.upc.edu

Dynamic Partial Order Reduction (DPOR) is one of the most successful techniques to alleviate the state explosion problem in the context of verification and testing of concurrent programs. The cornerstone of DPOR is the notion of *independence* that is used to decide whether each pair of concurrent events p and t are in a race and thus both $p \cdot t$ and $t \cdot p$ must be explored. We present *constrained* dynamic partial order reduction (CDPOR), an extension of the DPOR framework which is able to avoid redundant explorations based on the notion of *conditional independence* —the execution of p and t commutes only when certain *independence constraint*s (ICs) are satisfied. ICs can be declared by the programmer, but importantly, we present a novel SMT-based approach to automatically synthesize ICs in a static pre-analysis. A unique feature of our approach is that we have succeeded to exploit ICs within the state-of-the-art DPOR algorithm, achieving *exponential* reductions over existing implementations.

The full paper has been presented at the 30th International Conference on Computer Aided Verification (CAV 2018), which was held in the period 14-17 July 2018 in Oxford, United Kingdom, and is available at www.cs.upc.edu/~albert/papers/cav18.pdf.

*This work was funded partially by the Spanish MECD Salvador de Madariaga Mobility Grants PRX17/00297 and PRX17/00303, the Spanish MECD FPU Grant FPU15/04313, the Spanish MINECO projects TIN2015-69175-C4-2-R and TIN2015-69175-C4-3-R, and by the CM project S2013/ICE-3006.

Submitted to:
PROLE 2018