**Contemporary algebraic and geometric techniques**
**in coding theory and cryptography**
Summer school — July 18-22, 2022
Università degli Studi della Campania "Luigi Vanvitelli"

# Group Theoretic Model Repair of Kripke Structures

**William Cocke**

Affiliation: School of Computer and Cyber Sciences, Augusta University
USA

## Abstract

The model checking problem for a finite-state program $P$ with respect to a temporal logic formula $f$ is to verify that the Kripke structure $\mathscr{M}$ that is generated by the execution of $P$ satisfies $f$ [3]. Large Kripke structures are more expensive to model check, and given a concurrent program, many such structures suffer from state explosion.

The symmetry of a Kripke structure $\mathscr{M}$ has been exploited to replace a model check of $\mathscr{M}$ by a model check of the potentially smaller structure $\mathscr{N}$ obtained as the quotient of $\mathscr{M}$ by a group of symmetries $G$ [5, 6, 4]. For model checking, we restrict to symmetries of $\mathscr{M}$ that are guaranteed to preserve the evaluation of $f$. This means the valuation of $f$ is the same in $\mathscr{M}$ and its quotient $\mathscr{N}$. We extend this work to model repair: identifying a substructure of $\mathscr{M}$ that satisfies $f$ [2, 1]. We show that the substructures of $\mathscr{M}$ that are preserved by $G$ form a lattice that maps to the substructure lattice of $\mathscr{N}$. Moreover, the evaluation of $f$ on a substructure of $\mathscr{M}$ can be determined by its evaluation on the corresponding substructure of $\mathscr{N}$. This gives rise to a monotone Galois connection between the lattice of substructures of $\mathscr{N}$ and the lattice of substructures of $\mathscr{M}$ that are "maximal" with respect to an appropriately defined group action of $G$ on $\mathscr{M}$.

These results enable us to repair $\mathscr{N}$ and then to lift the repair to $\mathscr{M}$. Concurrent programs often present a high degree of symmetry between processes. We can repair such programs by repairing the corresponding $\mathscr{N}$, thereby effecting program repair while avoiding state-explosion in many cases.

**Keywords**: CTL, Model checking, symmetry reduction

# References


[1] Paul C. Attie, Kinan Dak-Al-Bab, and Mouhammad Sakr. Model and program repair via SAT solving. *ACM Trans. Embed. Comput. Syst.*, 17(2):32:1–32:25, 2018.

[2] F. Buccafurri, T. Eiter, G. Gottlob, and N. Leone. Enhancing model checking in verification by AI techniques. *Artif. Intell.*, 112:57–104, 1999.

[3] Edmund M Clarke. Model checking. In *International Conference on Foundations of Software Technology and Theoretical Computer Science*, pages 54–56. Springer, 1997.

[4] Edmund M. Clarke, E. Allen Emerson, Somesh Jha, and A. Prasad Sistla. Symmetry reductions in model checking. In *CAV*, volume 1427 of *Lecture Notes in Computer Science*, pages 147–158. Springer, 1998.

[5] E. Allen Emerson and A. Prasad Sistla. Symmetry and model checking. *Formal Methods Syst. Des.*, 9(1/2):105–131, 1996.

[6] E. Allen Emerson and A. Prasad Sistla. Utilizing symmetry when model-checking under fairness assumptions: An automata-theoretic approach. *ACM Trans. Program. Lang. Syst.*, 19(4):617–638, 1997.