

# 2015 CAV Award

The 2015 CAV Award is given to

Edmund Clarke, Orna Grumberg, Ron Hardin, Zvi Harel, Somesh Jha, Robert Kurshan, Yuan Lu, and Helmut Veith

*For the development and implementation of the localization-reduction technique and the formulation of counterexample-guided abstraction refinement (CEGAR).*

Abstraction is a key technique in automated verification and program analysis, as it enables model checkers and many other kinds of analyses to scale to systems of significant size. It is, however, difficult to provide an abstraction that is "just right" for a given model and property. In case the property fails to verify on the abstraction, it is often not possible to conclude anything about the original model, as any counterexample may be spurious. The key idea of Counterexample-Guided Abstraction Refinement (CEGAR) is to put the counterexample to good use: CEGAR-based techniques attempt to discover a reason why the counterexample is spurious. This reason is then used to discover those parts of the abstraction that lack detail. The abstraction can then be refined automatically. The specific merit of CEGAR is its versatility: CEGAR applies to virtually any verification scenario, and has been implemented in a vast number of verification algorithms with great success, and is often the key enabler for scalability. CEGAR today is one of the central paradigms of model checking and automated verification, combining two well-established model checking techniques--counterexample generation and abstraction -- into a new adaptive model checking algorithm. The basic idea of CEGAR is general yet compelling. A choice of abstraction can be seen as a conjectured proof that the property holds. If this proof fails, the counterexample is used to learn from the failed attempt, resulting in a new and improved argument for correctness.

Localization Reduction, conceived and implemented in COSPAN in the early 1990s by Hardin, Harel, and Kurshan, is the first instance of this paradigm in model checking. In localization reduction, a particular abstraction is a choice of a subset of the state-holding elements of the model. The chosen elements are retained as visible, whereas all others are removed from the model, thereby greatly reducing its complexity. In this scenario, a spurious counterexample can point to those invisible state-holding elements that need to be made visible again. Localization reduction was generalized and formulated as CEGAR in the late 1990s by Clarke, Grumberg, Jha, Lu, and Veith, and published in the CAV Conference in 2000 and in J. ACM in 2003. This work by now has over 2,000 citations. CEGAR-based techniques have become so commonplace that they often do not warrant a separate publication, but are standard ingredients of state-of-the-art model checkers.