CPAchecker 2.3 with Strategy Selection (Competition Contribution)

Daniel Baier
Dirk Beyer, Po-Chun Chien, Marek Jankola, Matthias Kettl, Nian-Ze Lee,
Thomas Lemberger, Marian Lingsch-Rosenfeld, Martin Spiessl,
Henrik Wachowitz, and Philipp Wendler

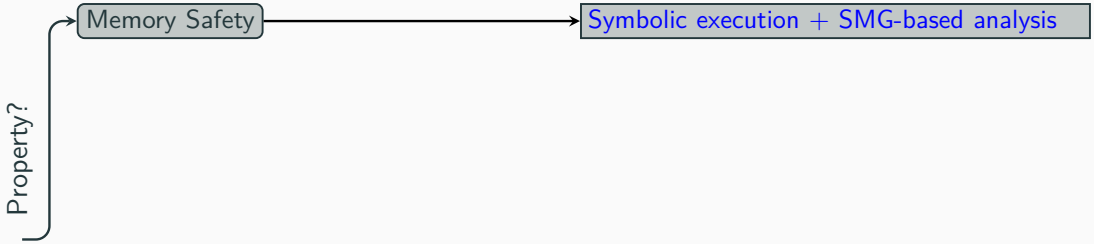
April 7, 2024
LMU Munich, SoSy-Lab

Competition Contribution

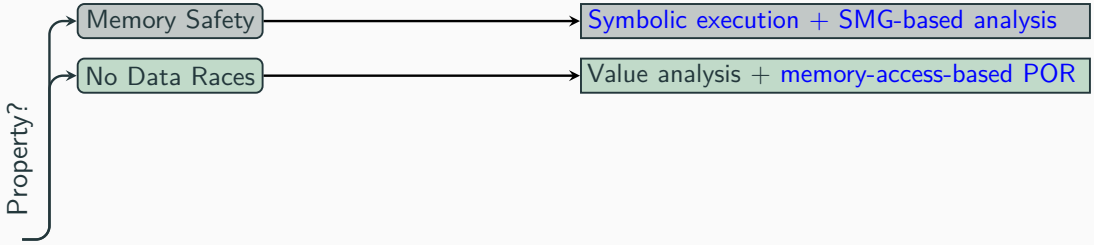
CPAchecker is a modern and versatile framework for building software-verification analyses from well-known concepts that match the user's requirements.

- Support for all properties and categories of C programs
- Utilizes strategy selection to predict a sequential portfolio of analyses that is suitable for a given verification task
- New and improved analyses for:
  - Reachability
  - Memory safety
  - Termination
  - Overflows
  - Data races

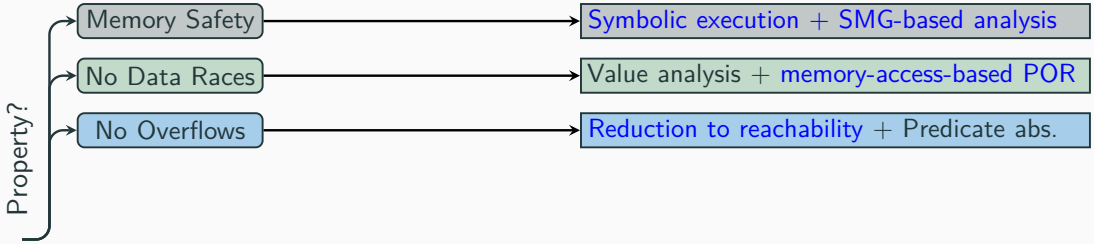
Verification Strategy for SV-COMP 2024



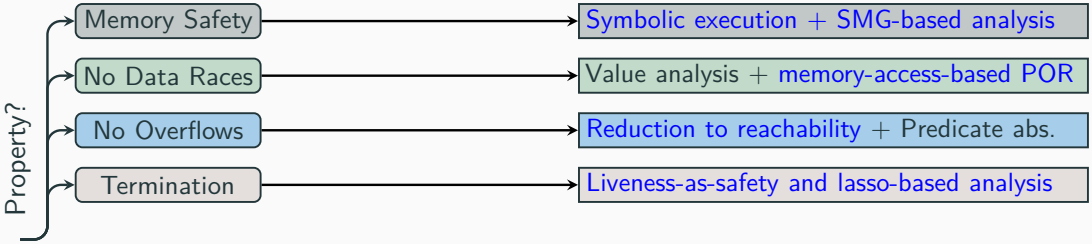
Verification Strategy for SV-COMP 2024



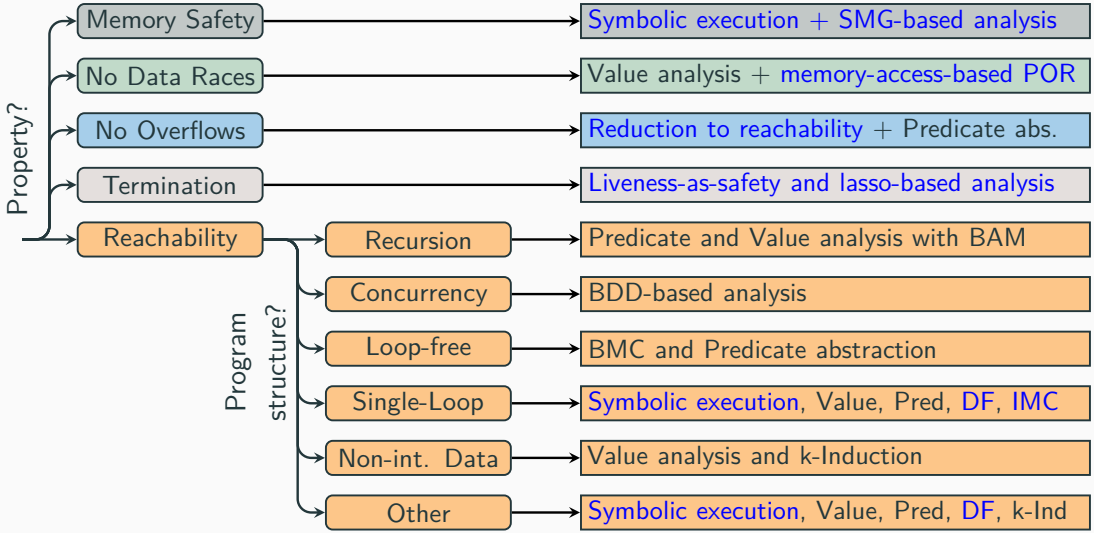
Verification Strategy for SV-COMP 2024



Verification Strategy for SV-COMP 2024



Verification Strategy for SV-COMP 2024



Competition Results

- 1st place in category *FalsificationOverall*
- 2nd place in category *Overall*
- 3rd place in category *ReachSafety*
- 17968 validated results in total (the most among all participants)
- Only 17 wrong results (0.06 % of all tasks)

cpachecker.
sosy-lab.org

Paper available here

References i

[1] Beyer, D., Chien, P.C., Lee, N.Z.: CPA-DF: A tool for configurable interval analysis to boost program verification. In: Proc. ASE. pp. 2050–2053. IEEE (2023). https://doi.org/10.1109/ASE56229.2023.00213

[2] Beyer, D., Dangl, M., Wendler, P.: Boosting k-induction with continuously-refined invariants. In: Proc. CAV. pp. 622–640. LNCS 9206, Springer (2015). https://doi.org/10.1007/978-3-319-21690-4_42

[3] Beyer, D., Dangl, M., Wendler, P.: A unifying view on SMT-based software verification. J. Autom. Reasoning **60**(3), 299–335 (2018). https://doi.org/10.1007/s10817-017-9432-6

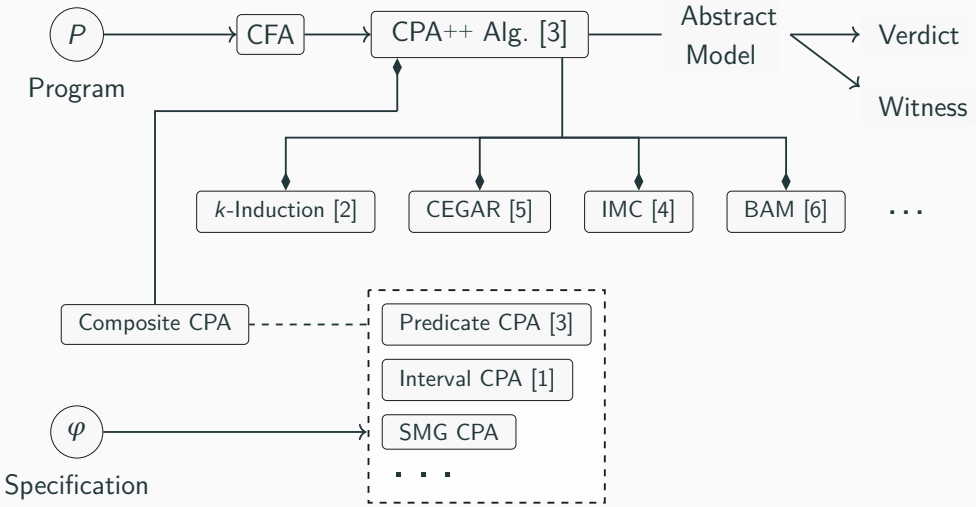
References ii

[4] Beyer, D., Lee, N.Z., Wendler, P.: Interpolation and SAT-based model checking revisited: Adoption to software verification. arXiv/CoRR **2208**(05046) (July 2022). https://doi.org/10.48550/arXiv.2208.05046

[5] Clarke, E.M., Grumberg, O., Jha, S., Lu, Y., Veith, H.: Counterexample-guided abstraction refinement for symbolic model checking. J. ACM **50**(5), 752–794 (2003). https://doi.org/10.1145/876638.876643

[6] Friedberger, K.: CPA-BAM: Block-abstraction memoization with value analysis and predicate analysis (competition contribution). In: Proc. TACAS. pp. 912–915. LNCS 9636, Springer (2016). https://doi.org/10.1007/978-3-662-49674-9_58

Overview


P
Program
CFA
CPA++ Alg. [3]
Abstract Model
Verdict
Witness
k-Induction [2]
CEGAR [5]
IMC [4]
BAM [6]
...
Composite CPA
Predicate CPA [3]
Interval CPA [1]
SMG CPA
...
φ
Specification