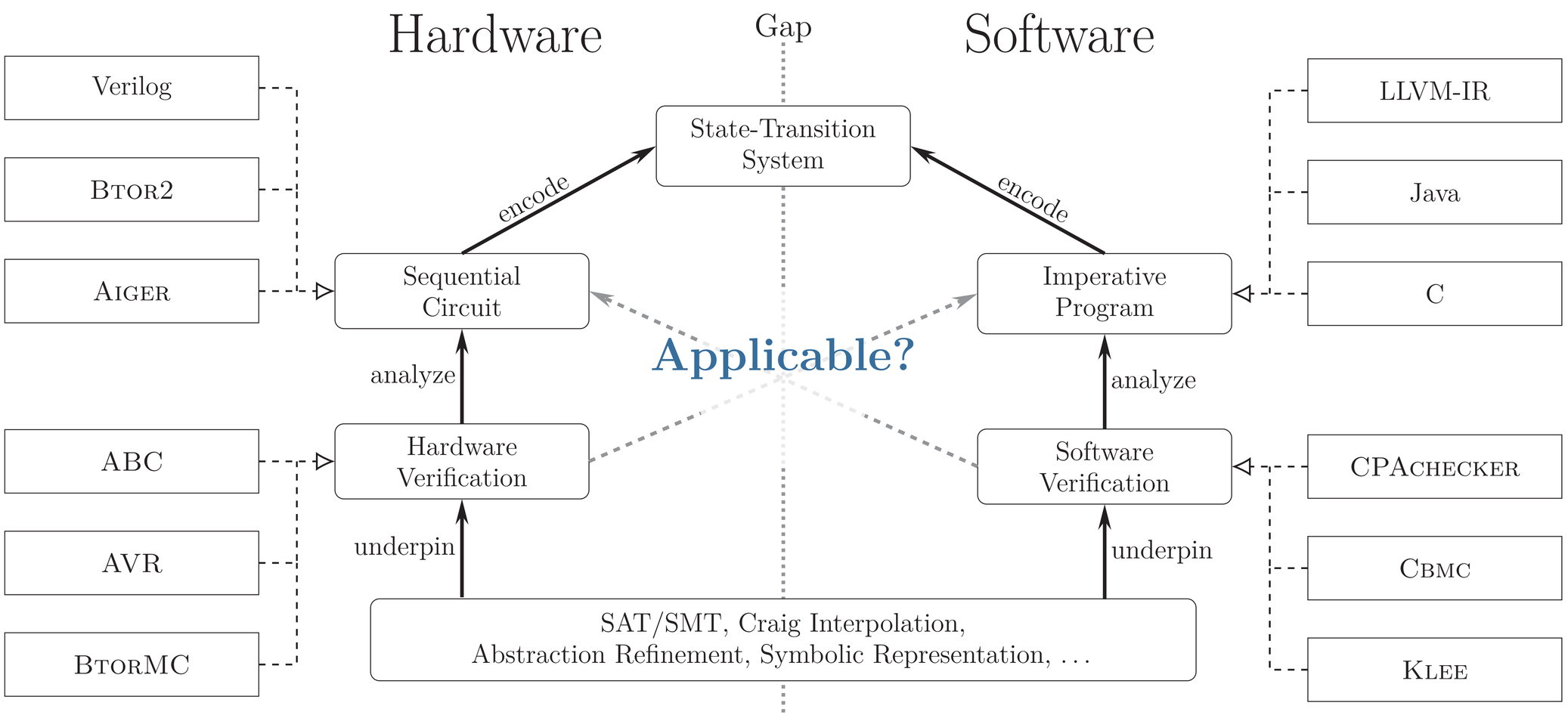
Bridging Hardware and Software Formal Verification

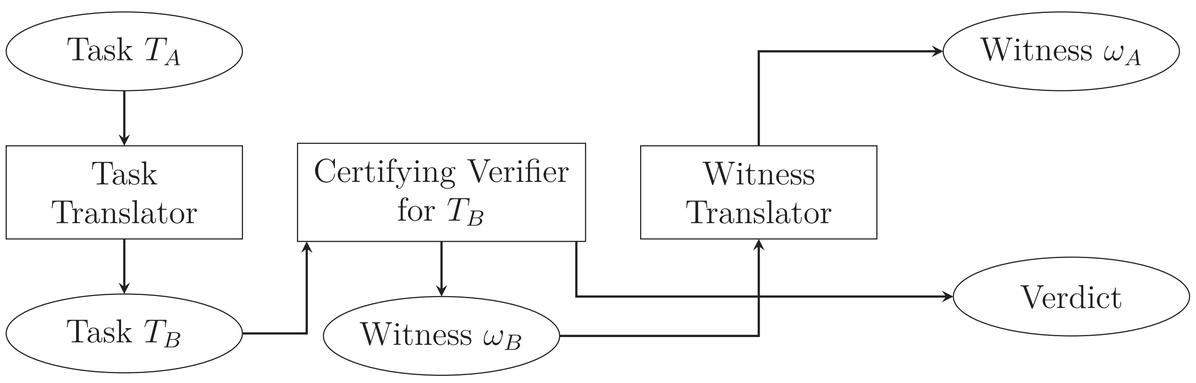
Po-Chun Chien
po-chun.chien@sosy.ifi.lmu.de

Motivation: Cross-Apply Verification Tools and Techniques



Verification Task Translation

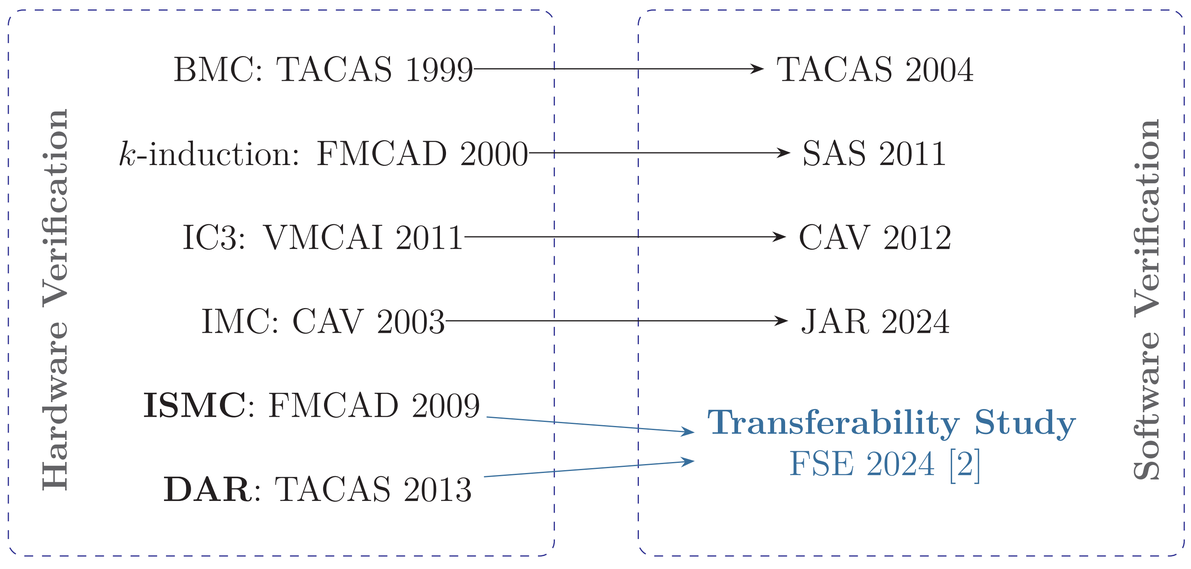
- Btor2-Cert [1]
  - Btor2-to-C translation by Btor2C [3]
  - Certifying software analysis
  - Witness/certification translation
- CPV [6]
  - C-to-Btor2 translation by Kratos2 [7]
  - Certifying hardware model checking
  - Witness/certification translation



Data Availability

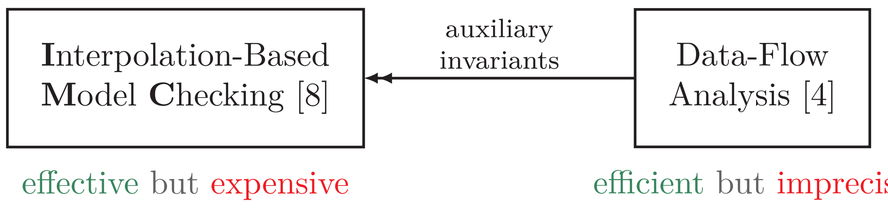
- Open-source tools at `https://gitlab.com/sosy-lab/software/`
  - `btor2-cert` [1, 3]
  - `cpv` [6]
  - `cpachecker` [2, 4, 5]
- Papers are accompanied with reproduction artifacts (available on Zenodo)

Verification Algorithm Adoption



Joining Forces of HW & SW Verification

- Cooperative verification via invariant injection [5]



  - Aux. invariants refine interpolants by pruning unreachable states
  - IMC reaches fixed-points in fewer iterations
- Adaptive algorithm selection using reinforcement learning (WIP)
  - Task translation makes more tools applicable
  - Extract features from graph representations of verification tasks

Summary

- Bridge HW and SW verification by
  - Cross-applying analysis tools through translating tasks
  - Transferring and adopting verification algorithms across domains
- Tackle tasks unsolvable by existing methods
- Consolidate knowledge from both domains and pave a pathway for comprehensive system-level verification

References

[1] Ádám, Z., Beyer, D., Chien, P.C., Lee, N.Z., Sirrenberg, N.: Btor2-Cert: A certifying hardware-verification framework using software analyzers. In: Proc. TACAS (3). pp. 129–149. LNCS 14572 (2024)
[2] Beyer, D., Chien, P.C., Jankola, M., Lee, N.Z.: A transferability study of interpolation-based hardware model checking for software verification. Proc. ACM Softw. Eng. **1**(FSE) (2024)
[3] Beyer, D., Chien, P.C., Lee, N.Z.: Bridging hardware and software analysis with Btor2C: A word-level-circuit-to-C translator. In: Proc. TACAS (2). pp. 152–172. LNCS 13994 (2023)
[4] 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 (2023)
[5] Beyer, D., Chien, P.C., Lee, N.Z.: Augmenting interpolation-based model checking with auxiliary invariants. In: Proc. SPIN (2024)
[6] Chien, P.C., Lee, N.Z.: CPV: A circuit-based program verifier (competition contribution). In: Proc. TACAS (3). pp. 365–370. LNCS 14572 (2024)
[7] Griggio, A., Jonáš, M.: Kratos2: An SMT-based model checker for imperative programs. In: Proc. CAV. pp. 423–436 (2023)
[8] McMillan, K.L.: Interpolation and SAT-based model checking. In: Proc. CAV. pp. 1–13. LNCS 2725 (2003)