Dist-AI in TLA^{+*}

Xiaosong Gu
State Key Laboratory for Novel Software Technology
Nanjing University
Nanjing, China
xxx@smail.nju.edu.cn

Jiacheng Zhao
State Key Laboratory for Novel Software Technology
Nanjing University
Nanjing, China

Wenjun Cai
State Key Laboratory for Novel Software Technology
Nanjing University
Nanjing, China
xxx@smail.nju.edu.cn

Hengfeng Wei*
State Key Laboratory for Novel Software Technology
Nanjing University
Nanjing, China
hfwei@nju.edu.cn

Yu Huang
State Key Laboratory for Novel Software Technology
Nanjing University
Nanjing, China
yuhuang@nju.edu.cn

...

...

ABSTRACT

PVLDB Reference Format:
Xiaosong Gu, Jiacheng Zhao, Wenjun Cai, Hengfeng Wei*, Yu Huang, . . . , and . . . . Dist-AI in TLA$^+$. PVLDB, 14(1): XXX-XXX, 2020.
doi:XX.XX/XXX.XX

PVLDB Artifact Availability:
The source code, data, and/or other artifacts have been made available at URL_TO_YOUR_ARTIFACTS.

1 INTRODUCTION

TLA$^+$, TLC, and TLAPS.

Automatic invariant inference.

Overview.

- **TLA$^+$traces sampling**
  - **Counter-example Guided**
  - **Coverage (e.g., minimal spanning)**
- **invariants space enumeration (exploration)**
  - **using Apalache: VARIABLES to relations (in Ivy), which are used as items in invariants**
- **Validation (utilizing Apalache)**
  - **on finite models; for any steps**
- **Refinement**
  - **Counter-example Guided**
- **Generalization to any models (for any steps)**
  - **How to validate it? (find some SMT???)**

Our Contributions.

-

*Corresponding author. Hengfeng Wei is also with Software Institute at Nanjing University.

Proceedings of the VLDB Endowment, Vol. 14, No. 1 ISSN 2150-8097.
doi:XX.XX/XXX.XX

-
-

2 OVERVIEW

2.1 Sampling TLA$^+$ Traces

2.2 Enumerating Invariants

- **directed by syntax of TLA$^+$**
- **restricting terms, operations,** . . .

2.3 Validating Inductive Invariants

- **using Apalache (modified for validating fols with quantifiers)**
- **using [?]**

3 CASE STUDY

3.1 Lock Server

3.2 Two-phase Commit

3.3 Paxos

4 RELATED WORK

DistAI

SWISS

Ivy

I4: inductive invariants for finite models (utilizing Averroes), and then generalize them to general models

Apalache

5 CONCLUSION

@inproceedingsProofAutomation:PhDThesis2014, title=Proof automation and type synthesis for set theory in the context of TLA+. (Automatisation de preuves et synthèse de types pour la théorie des ensembles dans le contexte de TLA+), author=Hernán Vanzetto, year=2014