Solving Relational Constraints with Extensions to a Theory of Finite Sets in SMT

Baoluo Meng, Andrew Reynolds, Cesare Tinelli

The University of Iowa

Our Research

- **Goal:** Solving Relational Constraints with Extensions to a Theory of Finite Sets in SMT
- Propose relational extensions to a theory of finite sets with cardinality
- Design and implement a calculus for the relational extensions in CVC4 SMT solver
- Develop a natural translator from Alloy to SMT

Related Work

- Alloy [1] is a declarative language for modeling and analyzing structurally-rich problems based on relational logic with built-in transitive closure and cardinality
  - The analysis of Alloy specification is performed automatically by the Alloy Analyzer – a SAT-based finite model finder

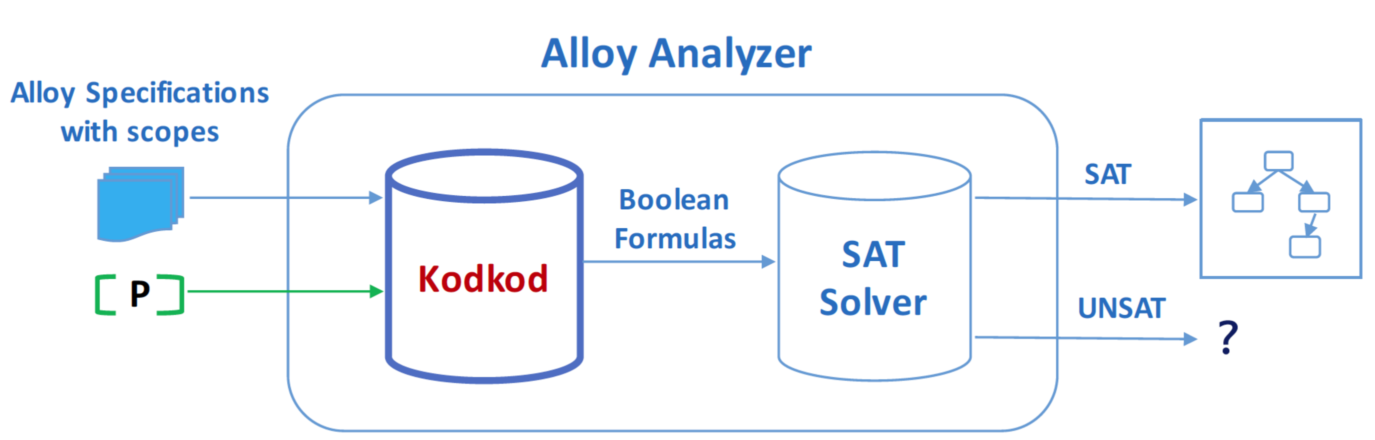

Figure 1: The Alloy Analyzer

  - **Limitation:** Can only automatically disprove properties, but not prove them
  - **Limitation:** Limited support for numerical reasoning
- To overcome the limitations of Alloy Analyzer, El Ghazi et al. translated Alloy kernel language to SMT-LIB language [3] and leveraged SMT solvers to solve resulting SMT formulas [6]
  - **Limitation**: Heavy usage of quantifiers to axiomatize relational constructs

Motivation

- Support relational constructs and operators natively in SMT solvers
- Build a natural translator from Alloy to SMT-LIB
- Leverage SMT solvers to solve the resulting SMT formulas
  - Take advantage of other supported theories in SMT
  - Translation require much less quantifiers
  - Can prove and disprove properties of Alloy specifications

Our Approach – Relational Extensions to a Theory of Finite Sets in SMT

- Kshitj Bansal et al. introduced a theory $\mathcal{T}_S$ of finite sets in SMT [5]
  - **A parametric sort**: Set(α) with sort α for set elements
  - **Constant and function symbols**:

    EMPTYSET : Set(α)
    SINGLETON : $\alpha \to$ Set(α)
    UNION, INTERSECTION, DIFFERENCE : Set(α) × Set(α) → Set(α)
  - **Predicate symbols**:

    IS_IN : α × Set(α)   SUBSET : Set(α) × Set(α)
- A decision procedure for $\mathcal{T}_S$ was implemented in CVC4 [4]
  - Also extended to support cardinality CARD: Set(α) → Int

Relational Extensions

- We propose extensions to $\mathcal{T}_S$ with relational operators
  - **Relational signature extensions**:

    TCLOSURE : Set(Tuple) → Set(Tuple)
    TRANSPOSE : Set(Tuple) → Set(Tuple)
    JOIN : Set(Tuple) × Set(Tuple) → Set(Tuple)
    PRODUCT : Set(Tuple) × Set(Tuple) → Set(Tuple)
    Tuple = $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ of arity n where α_i is a sort $\forall i \in [1, \ldots, n]$
- Developed a calculus for the relational extensions

A Relational Solver in CVC4

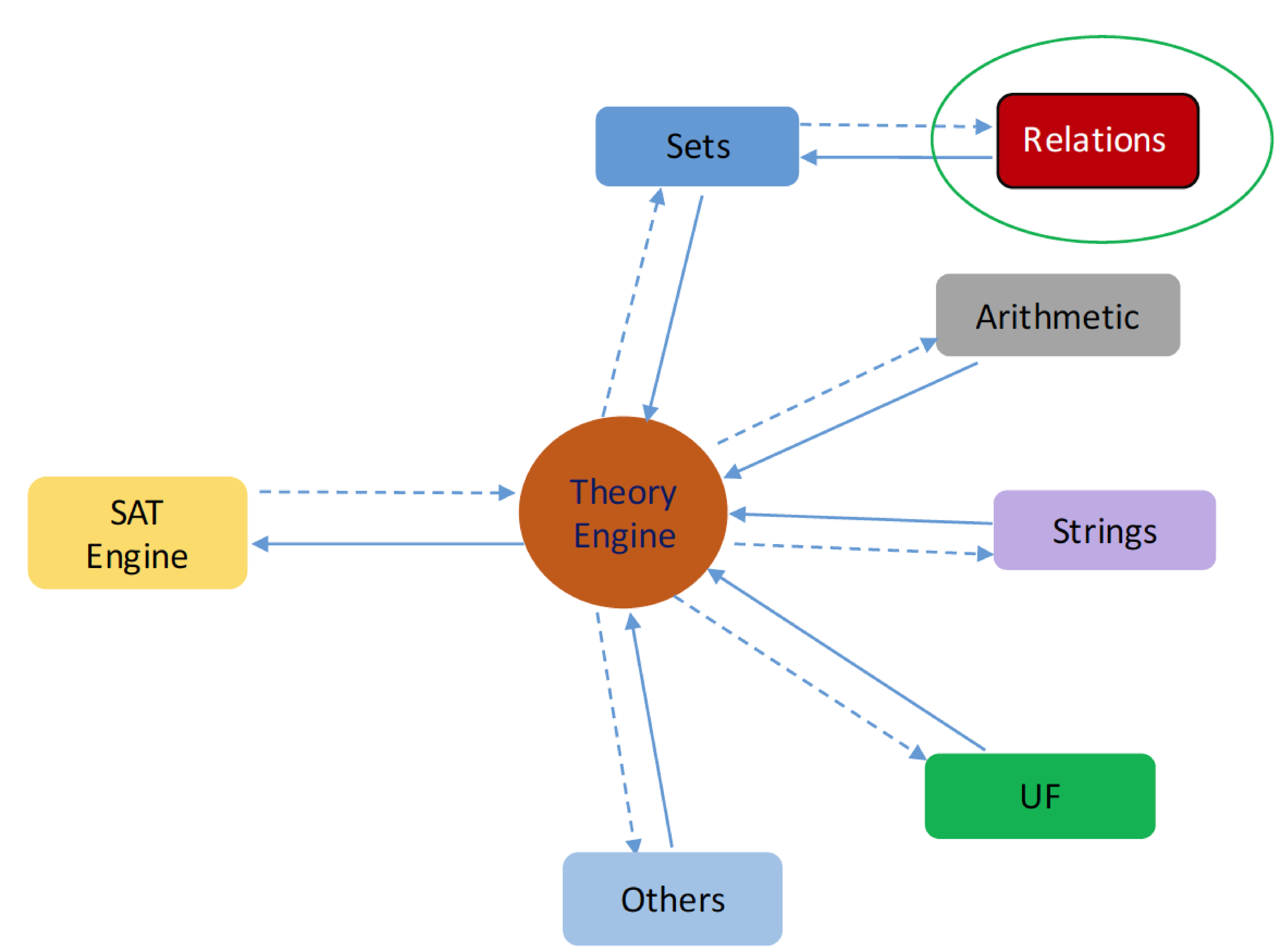

Figure 2: A relational solver in CVC4

Conclusion

- Fully support Alloy kernel language in SMT natively
- The initial version of the calculus for the extensions has been implemented in CVC4
- Extended the CVC4 native language to accept relational operators
- Modular, can solve constraints in combination with all other theories supported by CVC4

Future Work

- Identify decidable fragments of relational logic, for which our calculus is sound, complete and terminating
- Fully support relational reasoning with cardinality
  - E.g. CARD(TCLOSURE(S)) = 2 + CARD(S)
- Complete the implementation of translator from Alloy to SMT

References

[1] Daniel Jackson. Software Abstractions: logic, language, and analysis. MIT press, 2012.

[2] Barrett, Clark W., Roberto Sebastiani, Sanjit A. Seshia, and Cesare Tinelli. Satisfiability Modulo Theories. Handbook of satisfiability 185 (2009): 825-885.

[3] Clark Barrett, Pascal Fontaine, and Cesare Tinelli. The SMT-LIB Standard Version 2.6. 2010.

[4] Clark Barrett, Christopher L. Conway, Morgan Deters, Liana Hadarean, Dejan Jovanovic, Tim King, Andrew Reynolds, and Cesare Tinelli. Cvc4. In International Conference on Computer Aided Verification, pp. 171-177. Springer Berlin Heidelberg, 2011.

[5] Bansal, K., Reynolds, A., Barrett, C., Tinelli, C. A New Decision Procedure for Finite Sets and Cardinality Constraints in SMT.

[6] El Ghazi, Aboubakr Achraf, and Mana Taghdiri. Relational reasoning via SMT solving. International Symposium on Formal Methods. Springer Berlin Heidelberg, 2011.