Algebraic Array Theories

Rodrigo Raya

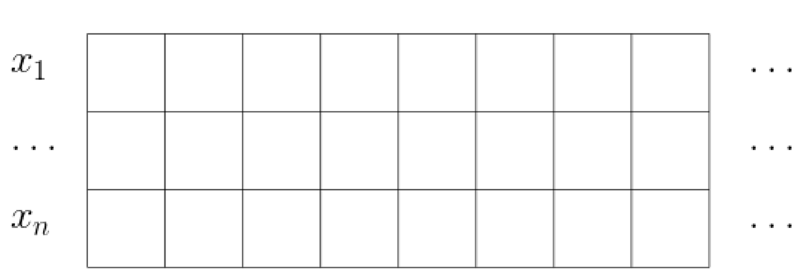
rodrigo.raya@epfl.ch
PhD Advisor: Viktor Kunčak

Introduction

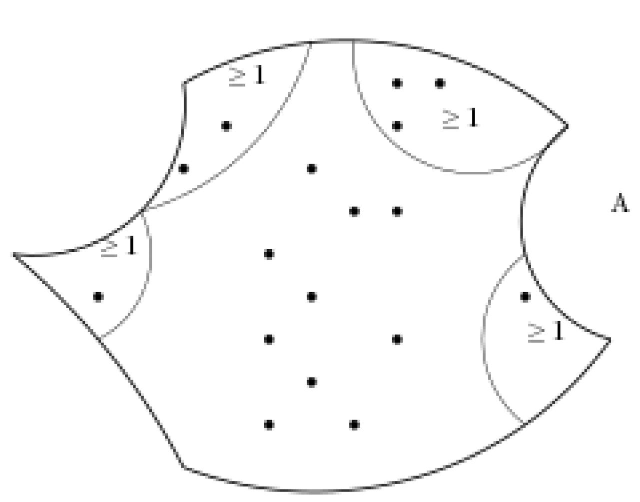
- **Problem:** memory-manipulating programs are hard to get right. Existing methodologies like software model checking struggle to automatically verify these programs.
- **Goal:** provide a mathematical proof that programs meet their specified intended behaviour. Verification ensures the absence of errors.
- **Abstract:** we design efficient decision procedures for theories encoding the behaviour of these programs. As a byproduct, we obtain theoretical results on the logical and computational properties of these theories.

Memory Model

As a model of computer memory we choose arrays stored by rows.



- Combinatory array logic [1] allows to use reads, writes, pointwise functions and relations and its decision problem is NP-complete.
- Example: $a = b + c$ means array a is the component-wise sum of array b and array c. $a > 0$ means that all elements of a are greater than zero.
- In [2], we show that this language imposes qualitative and cardinality restrictions on sets of indices where formulae from an NP-decidable theory hold.



Main Results

❶ Satisfiability of the existential fragment of the first-order theory of a power structure $Th_{\exists^*}(\mathcal{M}^I)$ reduces to satisfiability of the existential fragment of the first-order theory of the component theory $Th_{\exists^*}(\mathcal{M})$ and the existential fragment of the monadic second-order theory of the indices $Th^{mon}_{\exists^*}(\langle I, \text{Fin}, <, |\cdot|\rangle)$.

❷ Furthermore, $Th_{\exists^*}(\mathcal{M})$ and $Th^{mon}_{\exists^*}(\langle I, \text{Fin}, <, |\cdot|\rangle)$ are NP-complete iff $Th_{\exists^*}(\mathcal{M}^I)$ is NP-complete.

❸ The resulting logics are closed under propositional and weakest precondition operators.

General cardinalities

To generalise the result we use sets of indices $\{r \in I \mid \varphi_i(x_1(r), \dots, x_n(r), c_1, \dots, c_m)\}$ and cardinalities. We use linear arithmetic constraints on these cardinalities.

Ordering on the Index Set

We use the connection between regular expressions and the weak monadic theory of order found by Büchi to express ordering relations on the index set. For example, the one model of the regular expression $\left(\begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}\right)^*$ is the table

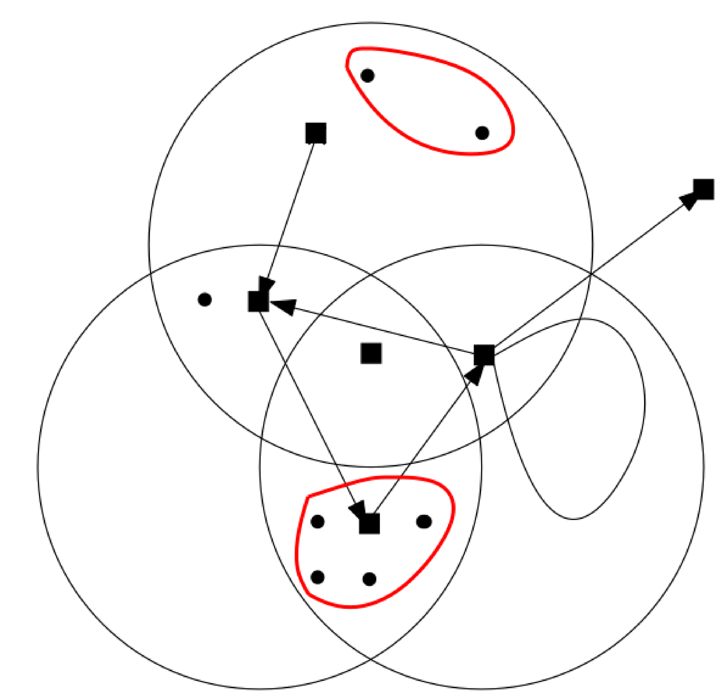
A	1	0	1	0	1	0	1	0	0	0	0	0	0	0	0	…
B	0	1	0	1	0	1	0	1	0	0	0	0	0	0	0	…

These gives sets of odd and even indices $A = \{1, 3, 5, 7\}$ and $B = \{2, 4, 6, 8\}$ in which we can specify that certain property holds.

Summation constraints

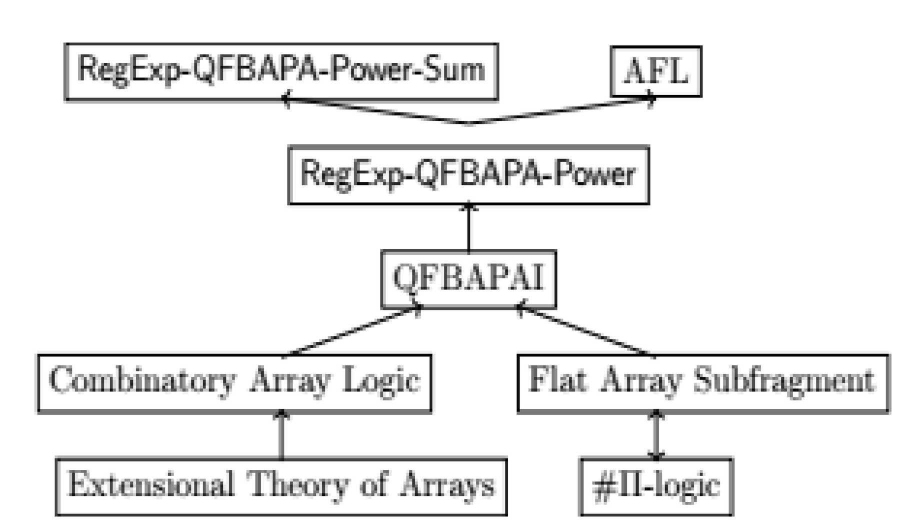
- We can also impose the constraint that σ is the sum of certain number of elements satisfying a formula φ, which we write $\sigma \in \{k; \varphi(k)\}^*$.
- The proof needs special care selecting the elements that will participate in the sum (circled dots in the image).

Proof methods



- Analysis of the disjunctive and Stone normal forms of the formulas in the investigated fragments.
- Existence of sparse solutions of exponential-sized systems of linear equations.
- Combination of theories through sets and cardinalities.

Classification of theories



- According to the definable relations.

Future Directions

- Implement some of the decision procedures on top of SMT solver routines (both Z3 and the CVC family implement combinatory array logic).
- Systematic classification of existing decision procedures for array theories in terms of definability and computational complexity properties.
- Devise new combination schemes for theories extending Nelson-Oppen [3] and combination through sets and cardinalities [4].

References

[1] Leonardo de Moura and Nikolaj Bjorner. Generalized, efficient array decision procedures. In *2009 Formal Methods in Computer-Aided Design*, pages 45–52, Austin, TX, November 2009.

[2] Rodrigo Raya and Viktor Kunčak. NP Satisfiability for Arrays as Powers. In *Verification, Model Checking, and Abstract Interpretation*, pages 301–318, Cham, 2022.

[3] Greg Nelson and Derek C. Oppen. Simplification by Cooperating Decision Procedures. *ACM Transactions on Programming Languages and Systems*, 1(2):245–257, October 1979.

[4] Thomas Wies, Ruzica Piskac, and Viktor Kuncak. Combining Theories with Shared Set Operations. In *Frontiers of Combining Systems*, pages 366–382, Berlin, Heidelberg, 2009.

[5] Georg Stefan Schmid and Viktor Kunčak. Generalized Arrays for Stainless Frames. In *Verification, Model Checking, and Abstract Interpretation*, pages 332–354, Cham, 2022.

EPFL
Automated
Reasoning
Group