ALGEBRAIC ARRAY THEORIES

Rodrigo Raya

rodri.go.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 memory-manipulating programs meet their specified intended computational properties of these theories.
- 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.

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 $\{1, 3\}^*$ is the table:

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>

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 $\tau$ is the sum of certain number of elements satisfying a formula $\varphi$, which we write $\tau \in \langle \varphi \rangle$.
- The proof needs special care selecting the elements that will participate in the sum (circled dots in the image).

GENERAL CARDINALITIES

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

PROOF METHODS

- Analysis of the disjunctive and Stone normal forms of the formulas in the investigated fragments.
- Combination of theories through sets and cardinalities.

CLASSIFICATION OF THEORIES

- Systematic classification of existing decision procedures for array theories in terms of definability and computational complexity properties.

REFERENCES