Polite Combination in Parametric Array Theories

Rodrigo Raya and Christophe Ringeissen

EPFL and Inria & Loria Nancy

October 1, 2025

Work supported by the SNSF Postdoctoral Mobility Programme

Motivation

- First-order reasoning techniques have difficulty in dealing with array-like verification conditions.
- Instead, abstract away certain quantification patterns.
- Example:
  $b = \text{write}(a, i, e) \leftrightarrow (b[i] = e \wedge \forall j \neq i . a[j] = b[j])$.
- Develop specific theorem proving procedures to deal with these abstractions.
- Here: focus in *parametric* array theories.

Arrays as Functions

- Power structures
  - $\langle M^I, R \rangle$
  - $R(a_1, \ldots, a_n) \leftrightarrow \forall i. R(a_1(i), \ldots, a_n(i))$
- Does not have quantifier elimination.
- Generalised power structures
  - Enrich the language.
  - $S = \{i \in I \mid \varphi(a_1(i), \ldots, a_n(i))\}$
  - Boolean algebra on sets, cardinalities of sets, automata (through the logic automata connection), aggregation.
  - ...
- How do we automatically reason about these?
- Today: how to combine data structure decision procedures with decision procedures for different element and index theories.

Combination Methods

- What happens if we restrict to specific domains?

$$
\begin{aligned}
e \in B &:= B[e] = 1 \\
B_1 \subseteq B_2 &:= \mathit{map}_{\rightarrow}(B_1, B_2) \\
B_1 \cup B_2 &:= \mathit{map}_{\vee}(B_1, B_2) \\
B_1 \cap B_2 &:= \mathit{map}_{\wedge}(B_1, B_2) \\
B_1 \setminus B_2 &:= \mathit{map}_{\cdot \wedge (\neg \cdot)}(B_1, B_2) \\
\emptyset &:= K(0) \\
\{e\} &:= \mathit{write}(K(0), e, 1)
\end{aligned}
$$

- Can we derive a decision procedure for sets from a decision procedure for combinatory array logic?
- Not with Nelson-Oppen, which requires stably infinite element theory.

- Idea: use polite theory combination.
- Caveat: disjointness condition does not allow element theories with symbols that occur in map terms.
- Still there are interesting questions:
  1. Politeness of sets with cardinalities open in Bansal et alii's work.
  2. How far can we push the method in the disjoint case?
- Alternative: rewrite into polite theory (not in paper).

Politeness

If T_1 and T_2 are two signature-disjoint theories such that T_1 is **strongly polite** w.r.t the set of sorts shared by T_1 and T_2, then the existence of a T_i-satisfiability procedure for $i = 1, 2$ implies the existence of a $T_1 \cup T_2$-satisfiability procedure.

Sufficient condition:

Smoothness: possibility to increase arbitrarily the cardinality of the model with respect to given sorts.

Finite witnessability: existence of a model over the variables of an equivalent formula $w(\phi)$.

Additivity: w preserves models and variables when the input is already a witness plus some "arrangement".

Sets with Cardinalities (I)

Sets with a bridging function returning their cardinality.

$T_{\mathbf{Z}}$**'s syntax**:

$$
\begin{aligned}
F &::= A \,|\, F_1 \wedge F_2 \,|\, F_1 \vee F_2 \,|\, \neg F \\
A &::= i_1 = i_2 \,|\, i \in B \,|\, B_1 = B_2 \,|\, B_1 \subseteq B_2 \,|\, T_1 = T_2 \,|\, T_1 < T_2 \\
B &::= x \,|\, \emptyset \,|\, B_1 \cup B_2 \,|\, B_1 \cap B_2 \,|\, B_1 \setminus B_2 \\
T &::= k \,|\, K \,|\, T_1 + T_2 \,|\, K \cdot T \,|\, |B| \\
K &::= \ldots \,|\, -2 \,|\, -1 \,|\, 0 \,|\, 1 \,|\, 2 \,|\, \ldots
\end{aligned}
$$

Example:

Post-condition after insertion of an element in a data structure

$$
\begin{aligned}
& a' = a \cup E \wedge |E| = 1 \wedge \\
& (E \subseteq a \rightarrow |a'| = |a|) \wedge \\
& (E \cap a = \emptyset \rightarrow |a'| = |a| + 1)
\end{aligned}
$$

Sets with Cardinalities: Smoothness

Smoothness: easy to prove

Proposition: let $\mathcal{A}$ be a T_Z-interpretation satisfying a conjunction Γ of flat Σ_Z-literals. Then there exists a T_Z-interpretation $\mathcal{B}$ satisfying Γ such that $|B_{\mathsf{index}}| = \kappa$, for each $\kappa > |A_{\mathsf{index}}|$.

Proof: define $\mathcal{B}$ as $\mathcal{A}$. Add new indices to the complement of the union of sets, which is unconstrained.

Sets with Cardinalities: Finite Witnessability

$\mathrm{witness}_Z(\Gamma)$:

- introduction of Venn regions
- set up a linear integer programming problem, to get the cardinalities of Venn regions minimizing the cardinality of the whole set
- inhabit Venn regions according the computed cardinalities (yields a set of possible configurations)
- output conjunction of input and disjunction over all configurations

Sets with Cardinalities: Additivity

$f(\phi)$:

1. if ϕ not arranged then output $\bigvee_{arr \in \chi} f(arr \wedge \phi)$
   (χ is set of arrangements of index variables in ϕ)
2. if $\phi = \phi' \wedge \varphi$ is T_Z-satisfiable, where
   - ϕ' is a witness of some arranged input and
   - φ a conjunction of literals between *index* variables in ϕ',

   then $f(\phi) := \phi$;
3. if $\phi = \phi' \wedge \varphi'$ is T_Z-satisfiable, where
   - φ' a conjunction of literals between *index* variables i, j such that i or j does not occur in ϕ',

   then $f(\phi) := f(\phi') \wedge \varphi'$;
4. otherwise, $f(\phi) := \text{witness}_Z(\phi)$.

Sets with Cardinalities: Politeness

Theorem: T_{Z} is additively finitely witnessable with respect to the sort index.

Theorem: T_{Z} is strongly polite with respect to the sort index.

Combinatory Array Logic (II)

Theory of arrays + map function to define arrays by extension

$T_{\mathbf{CAL}}$'s **syntax**:

$$F ::= F_1 \wedge F_2 \mid F_1 \vee F_2 \mid \neg F \mid \mathrm{map}_R(\overline{A}) \mid A[i] = e$$
$$A ::= a \mid \mathrm{write}(A, i, E) \mid K(e) \mid \mathrm{map}_f(\overline{A})$$
$$E ::= A[i] \mid e$$

Example:
$a[0] = s_0 \wedge \mathrm{map}_{\mathrm{valid}}(a) \rightarrow a[l] = s_f$

Satisfying assignments describe systems with a given start/end state and consisting only of valid components.

With theory combination we can support element theory specifications constraining the valid states.

Combinatory Array Logic: Smoothness

Show that given a model $\mathcal{A}$ one can find a model $\mathcal{B}$ with larger cardinality for <u>both index and element sorts</u>.

Index's cardinality: $|B_{\text{elem}}| = |A_{\text{elem}}|$, $\kappa = |B_{\text{index}}| > |A_{\text{index}}|$.

Let $i_0 \in A_{\text{index}}$, define $\mathcal{B}$ over the array-variables as

$$a^{\mathcal{B}}(i) = \begin{cases} a^{\mathcal{A}}(i), & \text{if } i \in A_{\text{index}} \\ a^{\mathcal{A}}(i_0), & \text{otherwise} \end{cases}$$

Increasing element sort's cardinality is trivial.

Combinatory Array Logic: Finite Witnessability

$\text{witness}_{\text{CAL}}(\Gamma)$:

1. Replace each literal of the form $\neg R(a_1, \ldots, a_n)$ in Γ with a literal of the form $\neg R(a_1[i], \ldots, a_n[i])$, where i is a fresh index-variable.
2. For each array index i and each array variable a used in the formula, add formulas $a[i] = e_i$ where e_i is a fresh element variable.
3. Substitute other occurrences of the terms $a[i]$ by the element variable e_i introduced in Step 2 (to simplify the proof of finite witnessability).

Combinatory Array Logic: Additivity and Politeness

Additivity is simple: we do not include any index or element theory specifications in the signature of the theory.

Additivity condition $\rightarrow$ witness function behaves as **idempotence** for equivalence and variable preservation.

Theorem:
T_{CAL} is strongly polite with respect to $\{elem, index\}$.

Theories with Set Interpretations (III)

Set membership constrained by formula over array elements.

$T_{\mathbf{F}}$**'s syntax**:

$$
\begin{aligned}
F &::= A \,|\, F_1 \wedge F_2 \,|\, F_1 \vee F_2 \,|\, \neg F \\
A &::= a[i] = e \,|\, i_1 = i_2 \,|\, i \in B \,|\, B_1 = B_2 \,|\, B_1 \subseteq B_2 \,|\, T_1 = T_2 \,|\, T_1 < T_2 \\
B &::= x \,|\, \emptyset \,|\, B_1 \cup B_2 \,|\, B_1 \cap B_2 \,|\, B_1 \setminus B_2 \,|\, \{i \mid \varphi(\overline{a}[i], \overline{e})\} \\
T &::= k \,|\, K \,|\, T_1 + T_2 \,|\, K \cdot T \,|\, |B| \\
K &::= \ldots \,|\, -2 \,|\, -1 \,|\, 0 \,|\, 1 \,|\, 2 \,|\, \ldots
\end{aligned}
$$

Example: invariants in consensus protocols, e.g.

$$
\forall i.\ \neg decided(i)\ \vee\ \exists v.\ |\{\, i \mid x(i) = v \,\}| > \tfrac{2n}{3} \wedge \\
\forall i.\ decided(i) \rightarrow decision(i) = v
$$

Theories with Set Interpretations: Smoothness

Technical condition for smoothness w.r.t the *index* sort:

Let $\varphi_1, \ldots, \varphi_n$ be the formulas under set interpretations in the T_F-formula φ, $cl(\varphi_1, \ldots, \varphi_n)$ is the sentence $\exists \overline{v}. \bigwedge_{i=1}^{n} \neg \varphi_i(\overline{v})$.

Assume that $cl(\varphi_1, \ldots, \varphi_n)$ is T_F-satisfiable.

The theory $T_F(\varphi_1, \ldots, \varphi_n)$ is the set of Σ_F-sentences φ such that $T_F \cup \{cl(\varphi_1, \ldots, \varphi_n)\} \models \varphi$.

Corollary:

- T_F is smooth w.r.t. *elem*.
- $T_F(\varphi_1, \ldots, \varphi_n)$ is smooth w.r.t. $\{elem, index\}$.

Theories with Set Interpretations: Finite Witnessability

Proposition:
T_{F} is finitely witnessable w.r.t. $\{$elem, index$\}$.

- introduction of Venn regions
- associate a formula to each Venn region
- set up a linear integer programming problem **removing those regions that are empty because their corresponding formulas are unsatisfiable**
- use the formula associated to each Venn region to build an appropriate witness

Theories with Set Interpretations: Additivity and Politeness

Additivity as in sets with cardinalities.

Theorem:

- T_F is strongly polite with respect to elem.
- $T_F(\varphi_1, \ldots, \varphi_n)$ is strongly polite w.r.t. $\{elem, index\}$.

Contributions

- We showed how to modularly derive decision procedures for expressive parametric array theories using the polite theory combination method.
- We extended the method used in the original paper by Ranise, Ringeissen and Zarba incorporating recent techniques such as the **additivity** of witnesses.
- Our results enable the use of combination algorithms for addressing rich classes of constraints over arrays including properties that hold componentwise and which are formulated over arbitrary datatypes.