

by  
Aaron Bradley  
Zohar Manna

Springer 2007

(2) Array Property Fragment of  $T_A$

Decidable fragment of  $T_A$  that includes  $\forall$  quantifiers

Array property

$\Sigma_A$ -formula of form

$$\forall \vec{i}. F[\vec{i}] \rightarrow G[\vec{i}],$$

where  $\vec{i}$  is a list of variables.

► index guard  $F[\vec{i}]$ :

$$\begin{aligned} \text{iguard} &\rightarrow \text{iguard} \wedge \text{iguard} \mid \text{iguard} \vee \text{iguard} \mid \text{atom} \\ \text{atom} &\rightarrow \text{var} = \text{var} \mid \text{evar} \neq \text{var} \mid \text{var} \neq \text{evar} \mid \top \\ \text{var} &\rightarrow \text{evar} \mid \text{uvar} \end{aligned}$$

where *uvar* is any universally quantified index variable,  
and *evar* is any constant or unquantified variable.

► value constraint  $G[\vec{i}]$ : a universally quantified index can occur  
in a value constraint  $G[\vec{i}]$  only in a read  $a[i]$ , where  $a$  is an  
array term. The read cannot be nested; for example,  $a[b[i]]$  is  
not allowed.

Array Property Fragment of  $T_A$

Boolean combinations of quantifier-free  $T_A$ -formulae and array  
properties

Example:  $\Sigma_A$ -formulae

$$F : \forall i. i \neq a[k] \rightarrow a[i] = a[k]$$

The antecedent is not a legal index guard since  $a[k]$  is not a  
variable (neither a *uvar* nor an *evar*); however, by simple  
manipulation

$$F' : v = a[k] \wedge \forall i. i \neq v \rightarrow a[i] = a[k]$$

Here,  $i \neq v$  is a legal index guard, and  $a[i] = a[k]$  is a legal value  
constraint.  $F$  and  $F'$  are equisatisfiable.

However, no manipulation works for:

$$G : \forall i. i \neq a[i] \rightarrow a[i] = a[k].$$

Thus,  $G$  is not in the array property fragment.

Remark: Array property fragment allows expressing equality between arrays (extensionality): two arrays are equal precisely when their corresponding elements are equal.

For given formula

$$F : \dots \wedge a = b \wedge \dots$$

with array terms  $a$  and  $b$ , rewrite  $F$  as

$$F' : \dots \wedge (\forall i. \top \rightarrow a[i] = b[i]) \wedge \dots$$

$F$  and  $F'$  are equisatisfiable.

### The Algorithm

Given array property formula  $F$ , decide its  $T_A$ -satisfiability by the following steps:

#### Step 1

Put  $F$  in NNF.

#### Step 2

Apply the following rule exhaustively to remove writes:

$$\frac{F[a\langle i \triangleleft v \rangle]}{F[a'] \wedge a'[i] = v \wedge (\forall j. j \neq i \rightarrow a[j] = a'[j])} \text{ for fresh } a' \text{ (write)}$$

After an application of the rule, the resulting formula contains at least one fewer write terms than the given formula.

#### Step 3

Apply the following rule exhaustively to remove existential quantification:

$$\frac{F[\exists \bar{i}. G[\bar{i}]]}{F[G[\bar{j}]]} \text{ for fresh } \bar{j} \text{ (exists)}$$

Existential quantification can arise during Step 1 if the given formula has a negated array property.

### Decision Procedure for Array Property Fragment

The idea of the decision procedure for the array property fragment is to reduce universal quantification to finite conjunction. That is, it constructs a finite set of index terms s.t. examining only these positions of the arrays is sufficient.

Example: Consider

$$F : a\langle i \triangleleft v \rangle = a \wedge a[i] \neq v ,$$

which expands to

$$F' : \forall j. a\langle i \triangleleft v \rangle[j] = a[j] \wedge a[i] \neq v .$$

Intuitively, to determine that  $F'$  is  $T_A$ -unsatisfiable requires merely examining index  $i$ :

$$F'' : \left( \bigwedge_{j \in \{i\}} a\langle i \triangleleft v \rangle[j] = a[j] \right) \wedge a[i] \neq v ,$$

or simply

$$a\langle i \triangleleft v \rangle[i] = a[i] \wedge a[i] \neq v .$$

Simplifying,

$$v = a[i] \wedge a[i] \neq v ,$$

it is clear that this formula, and thus  $F$ , is  $T_A$ -unsatisfiable.

Steps 4-6 accomplish the reduction of universal quantification to finite conjunction.

Main idea: select a set of symbolic index terms on which to instantiate all universal quantifiers. The set is sufficient for correctness.

#### Step 4

From the output  $F_3$  of Step 3, construct the **index set**  $\mathcal{I}$ :

$$\mathcal{I} = \cup \{ \lambda \} \cup \{ t : \cdot[t] \in F_3 \text{ such that } t \text{ is not a universally quantified variable} \} \cup \{ t : t \text{ occurs as an } \textit{evar} \text{ in the parsing of index guards} \}$$

This index set is the finite set of indices that need to be examined. It includes

- ▶ all terms  $t$  that occur in some read  $a[t]$  anywhere in  $F$  (unless it is a universally quantified variable)
- ▶ all terms  $t$  (constant or unquantified variable) that are compared to a universally quantified variable in some index guard.
- ▶  $\lambda$  is a fresh constant that represents all other index positions that are not explicitly in  $\mathcal{I}$ .

### Step 5 (Key step)

Apply the following rule exhaustively to remove universal quantification:

$$\frac{H[\forall \vec{i}. F[\vec{i}] \rightarrow G[\vec{i}]]}{H \left[ \bigwedge_{\vec{i} \in \mathcal{I}^n} (F[\vec{i}] \rightarrow G[\vec{i}]) \right]} \quad (\text{forall})$$

where  $n$  is the size of the list of quantified variables  $\vec{i}$ .

### Step 6

From the output  $F_5$  of Step 5, construct

$$F_6 : F_5 \wedge \bigwedge_{i \in \mathcal{I} \setminus \{\lambda\}} \lambda \neq i.$$

The new conjuncts assert that the variable  $\lambda$  introduced in Step 4 is indeed unique.

### Step 7

Decide the  $T_A$ -satisfiability of  $F_6$  using the decision procedure for the quantifier-free fragment.

Example: Consider array property formula

$$F : a[\ell < \nu][k] = b[k] \wedge b[k] \neq \nu \wedge a[k] = \nu \wedge \underbrace{(\forall i. i \neq \ell \rightarrow a[i] = b[i])}_{\text{array property}}$$

Index guard is  $i \neq \ell$  and the value constraint is  $a[i] = b[i]$ . It is already in NNF. By Step 2, rewrite  $F$  as

$$F_2 : a'[k] = b[k] \wedge b[k] \neq \nu \wedge a[k] = \nu \wedge (\forall i. i \neq \ell \rightarrow a[i] = b[i]) \wedge a'[\ell] = \nu \wedge (\forall j. j \neq \ell \rightarrow a[j] = a'[j])$$

$F_2$  does not contain any existential quantifiers. Its index set is

$$\begin{aligned} \mathcal{I} &= \{\lambda\} \cup \{k\} \cup \{\ell\} \\ &= \{\lambda, k, \ell\}. \end{aligned}$$

Thus, by Step 5, replace universal quantification:

$$F_5 : a'[k] = b[k] \wedge b[k] \neq \nu \wedge a[k] = \nu \wedge \bigwedge_{i \in \mathcal{I}} (i \neq \ell \rightarrow a[i] = b[i]) \wedge a'[\ell] = \nu \wedge \bigwedge_{j \in \mathcal{I}} (j \neq \ell \rightarrow a[j] = a'[j])$$

Step 6 distinguishes  $\lambda$  from other members of  $\mathcal{I}$ :

$$\begin{aligned} F_6 : & a'[k] = b[k] \wedge b[k] \neq \nu \wedge a[k] = \nu \wedge (\lambda \neq \ell \rightarrow a[\lambda] = b[\lambda]) \\ & \wedge (k \neq \ell \rightarrow a[k] = b[k]) \\ & \wedge a'[\ell] = \nu \wedge (\lambda \neq \ell \rightarrow a[\lambda] = a'[\lambda]) \\ & \wedge (k \neq \ell \rightarrow a[k] = a'[k]) \\ & \wedge \lambda \neq k \wedge \lambda \neq \ell \end{aligned}$$

Simplifying,

$$F_6' : a'[k] = b[k] \wedge b[k] \neq \nu \wedge a[k] = \nu \wedge a[\lambda] = b[\lambda] \wedge (k \neq \ell \rightarrow a[k] = b[k]) \wedge a'[\ell] = \nu \wedge a[\lambda] = a'[\lambda] \wedge (k \neq \ell \rightarrow a[k] = a'[k]) \wedge \lambda \neq k \wedge \lambda \neq \ell$$

There are two cases to consider.

- ▶ If  $k = \ell$ , then  $a'[\ell] = \nu$  and  $a'[k] = b[k]$  imply  $b[k] = \nu$ , yet  $b[k] \neq \nu$ .
- ▶ If  $k \neq \ell$ , then  $a[k] = \nu$  and  $a[k] = b[k]$  imply  $b[k] = \nu$ , but again  $b[k] \neq \nu$ .

Hence,  $F_6'$  is  $T_A$ -unsatisfiable, indicating that  $F$  is  $T_A$ -unsatisfiable.

$$F_5 : a'[k] = b[k] \wedge b[k] \neq \nu \wedge a[k] = \nu \wedge \bigwedge_{i \in \mathcal{I}} (i \neq \ell \rightarrow a[i] = b[i]) \wedge a'[\ell] = \nu \wedge \bigwedge_{j \in \mathcal{I}} (j \neq \ell \rightarrow a[j] = a'[j])$$

Expanding produces

$$F_5' : a'[k] = b[k] \wedge b[k] \neq \nu \wedge a[k] = \nu \wedge (\lambda \neq \ell \rightarrow a[\lambda] = b[\lambda]) \wedge (k \neq \ell \rightarrow a[k] = b[k]) \wedge (l \neq \ell \rightarrow a[l] = b[l]) \wedge a'[\ell] = \nu \wedge (\lambda \neq \ell \rightarrow a[\lambda] = a'[\lambda]) \wedge (k \neq \ell \rightarrow a[k] = a'[k]) \wedge (l \neq \ell \rightarrow a[l] = a'[l])$$

Simplifying produces

$$F_5'' : a'[k] = b[k] \wedge b[k] \neq \nu \wedge a[k] = \nu \wedge (\lambda \neq \ell \rightarrow a[\lambda] = b[\lambda]) \wedge (k \neq \ell \rightarrow a[k] = b[k]) \wedge a'[\ell] = \nu \wedge (\lambda \neq \ell \rightarrow a[\lambda] = a'[\lambda]) \wedge (k \neq \ell \rightarrow a[k] = a'[k])$$

### (3) Theory of Integer-Indexed Arrays $T_A^{\mathbb{Z}}$

$\leq$  enables reasoning about subarrays and properties such as subarray is sorted or partitioned.

signature of  $T_A^{\mathbb{Z}}$ :  $\Sigma_A^{\mathbb{Z}} = \Sigma_A \cup \Sigma_{\mathbb{Z}}$

axioms of  $T_A^{\mathbb{Z}}$ : both axioms of  $T_A$  and  $T_{\mathbb{Z}}$

#### A Decision Procedure

The idea again is to reduce universal quantification to finite conjunction.

Given  $F$  from the array property fragment of  $T_A^{\mathbb{Z}}$ , decide its  $T_A^{\mathbb{Z}}$ -satisfiability as follows:

##### Step 1

Put  $F$  in NNF.

##### Step 2

Apply the following rule exhaustively to remove writes:

$$\frac{F[a(i \triangleleft e)]}{F[a'] \wedge a'[i] = e \wedge (\forall j. j \neq i \rightarrow a[j] = a'[j])} \text{ for fresh } a' \text{ (write)}$$

To meet the syntactic requirements on an index guard, rewrite the third conjunct as

$$\forall j. j \leq i - 1 \vee i + 1 \leq j \rightarrow a[j] = a'[j].$$

Array property:  $\Sigma_A^{\mathbb{Z}}$ -formula of the form

$$\forall \vec{i}. F[\vec{i}] \rightarrow G[\vec{i}],$$

where  $\vec{i}$  is a list of integer variables.

►  $F[\vec{i}]$  index guard:

$$\text{iguard} \rightarrow \text{iguard} \wedge \text{iguard} \mid \text{iguard} \vee \text{iguard} \mid \text{atom}$$

$$\text{atom} \rightarrow \text{expr} \leq \text{expr} \mid \text{expr} = \text{expr}$$

$$\text{expr} \rightarrow \text{uvar} \mid \text{pexpr}$$

$$\text{pexpr} \rightarrow \text{pexpr}'$$

$$\text{pexpr}' \rightarrow \mathbb{Z} \mid \mathbb{Z} \cdot \text{evar} \mid \text{pexpr}' + \text{pexpr}'$$

where  $\text{uvar}$  is any universally quantified integer variable, and  $\text{evar}$  is any existentially quantified or free integer variable.

►  $G[\vec{i}]$  value constraint:

Any occurrence of a quantified index variable  $i$  must be as a read into an array,  $a[i]$ , for array term  $a$ . Array reads may not be nested; e.g.,  $a[b[i]]$  is not allowed.

Array property fragment of  $T_A^{\mathbb{Z}}$  consists of formulae that are Boolean combinations of quantifier-free  $\Sigma_A^{\mathbb{Z}}$ -formulae and array properties.

#### Step 3

Apply the following rule exhaustively to remove existential quantification:

$$\frac{F[\exists \vec{j}. G[\vec{j}]]}{F[G[\vec{j}]]} \text{ for fresh } \vec{j} \text{ (exists)}$$

Existential quantification can arise during Step 1 if the given formula has a negated array property.

#### Step 4

From the output of Step 3,  $F_3$ , construct the index set  $\mathcal{I}$ :

$$\mathcal{I} = \begin{aligned} & \{t : \cdot[t] \in F_3 \text{ such that } t \text{ is not a universally quantified variable}\} \\ & \cup \{t : t \text{ occurs as a pexpr in the parsing of index guards}\} \end{aligned}$$

If  $\mathcal{I} = \emptyset$ , then let  $\mathcal{I} = \{0\}$ . The index set contains all relevant symbolic indices that occur in  $F_3$ .

### Step 5

Apply the following rule exhaustively to remove universal quantification:

$$\frac{H[\forall \vec{i}. F[\vec{i}] \rightarrow G[\vec{i}]]}{H \left[ \bigwedge_{\vec{i} \in \mathcal{I}^n} (F[\vec{i}] \rightarrow G[\vec{i}]) \right]} \quad (\text{forall})$$

$n$  is the size of the block of universal quantifiers over  $\vec{i}$ .

### Step 6

$F_5$  is quantifier-free in the combination theory  $T_A \cup T_{\mathbb{Z}}$ . Decide the  $(T_A \cup T_{\mathbb{Z}})$ -satisfiability of the resulting formula.

Example:  $\Sigma_A^{\mathbb{Z}}$ -formula:

$$F : \begin{aligned} & (\forall i. \ell \leq i \leq u \rightarrow a[i] = b[i]) \\ & \wedge \neg(\forall i. \ell \leq i \leq u+1 \rightarrow a[u+1] < b[u+1])[i] = b[i]) \end{aligned}$$

In NNF, we have

$$F_1 : \begin{aligned} & (\forall i. \ell \leq i \leq u \rightarrow a[i] = b[i]) \\ & \wedge (\exists i. \ell \leq i \leq u+1 \wedge a[u+1] < b[u+1])[i] \neq b[i]) \end{aligned}$$

Step 2 produces

$$F_2 : \begin{aligned} & (\forall i. \ell \leq i \leq u \rightarrow a[i] = b[i]) \\ & \wedge (\exists i. \ell \leq i \leq u+1 \wedge a'[i] \neq b[i]) \\ & \wedge a'[u+1] = b[u+1] \\ & \wedge (\forall j. j \leq u+1-1 \vee u+1+1 \leq j \rightarrow a[j] = a'[j]) \end{aligned}$$

Step 3 removes the existential quantifier by introducing a fresh constant  $k$ :

$$F_3 : \begin{aligned} & (\forall i. \ell \leq i \leq u \rightarrow a[i] = b[i]) \\ & \wedge \ell \leq k \leq u+1 \wedge a'[k] \neq b[k] \\ & \wedge a'[u+1] = b[u+1] \\ & \wedge (\forall j. j \leq u+1-1 \vee u+1+1 \leq j \rightarrow a[j] = a'[j]) \end{aligned}$$

Simplifying,

$$F'_3 : \begin{aligned} & (\forall i. \ell \leq i \leq u \rightarrow a[i] = b[i]) \\ & \wedge \ell \leq k \leq u+1 \wedge a'[k] \neq b[k] \\ & \wedge a'[u+1] = b[u+1] \\ & \wedge (\forall j. j \leq u \vee u+2 \leq j \rightarrow a[j] = a'[j]) \end{aligned}$$

The index set is

$$\mathcal{I} = \{k, u+1\} \cup \{\ell, u, u+2\},$$

which includes the read terms  $k$  and  $u+1$  and the terms  $\ell$ ,  $u$ , and  $u+2$  that occur as pexprs in the index guards.

Step 5 rewrites universal quantification to finite conjunction over this set:

$$F_5 : \begin{aligned} & \bigwedge_{i \in \mathcal{I}} (\ell \leq i \leq u \rightarrow a[i] = b[i]) \\ & \wedge \ell \leq k \leq u+1 \wedge a'[k] \neq b[k] \\ & \wedge a'[u+1] = b[u+1] \\ & \wedge \bigwedge_{j \in \mathcal{I}} (j \leq u \vee u+2 \leq j \rightarrow a[j] = a'[j]) \end{aligned}$$

Expanding the conjunctions according to the index set  $\mathcal{I}$  and simplifying according to trivially true or false antecedents (e.g.,  $\ell \leq u+1 \leq u$  simplifies to  $\perp$ , while  $u \leq u \vee u+2 \leq u$  simplifies to  $\top$ ) produces:

$$\begin{aligned}
& (\ell \leq k \leq u \rightarrow a[k] = b[k]) & (1) \\
& \wedge (\ell \leq u \rightarrow a[\ell] = b[\ell] \wedge a[u] = b[u]) & (2) \\
& \wedge \ell \leq k \leq u + 1 & (3) \\
F'_5 : & \wedge a'[k] \neq b[k] & (4) \\
& \wedge a'[u + 1] = b[u + 1] & (5) \\
& \wedge (k \leq u \vee u + 2 \leq k \rightarrow a[k] = a'[k]) & (6) \\
& \wedge (\ell \leq u \vee u + 2 \leq \ell \rightarrow a[\ell] = a'[\ell]) & (7) \\
& \wedge a[u] = a'[u] \wedge a[u + 2] = a'[u + 2] & (8)
\end{aligned}$$

$(T_A \cup T_{\mathbb{Z}})$ -unsatisfiability of this quantifier-free  $(\Sigma_A \cup \Sigma_{\mathbb{Z}})$ -formula can be decided using the techniques of Combination of Theories.

Informally,  $\ell \leq k \leq u + 1$  (3)

- ▶ If  $k \in [\ell, u]$  then  $a[k] = b[k]$  (1). Since  $k \leq u$  then  $a[k] = a'[k]$  (6), contradicting  $a'[k] \neq b[k]$  (4).
- ▶ if  $k = u + 1$ ,  $a'[k] \neq b[k] = b[u + 1] = a'[u + 1] = a'[k]$  by (4) and (5), a contradiction.

Hence,  $F$  is  $T_A^{\mathbb{Z}}$ -unsatisfiable.

Application: array property fragments

- ▶ Array equality  $a = b$  in  $T_A$ :

$$\forall i. a[i] = b[i]$$

- ▶ Bounded array equality  $\text{beq}(a, b, \ell, u)$  in  $T_A^{\mathbb{Z}}$ :

$$\forall i. \ell \leq i \leq u \rightarrow a[i] = b[i]$$

- ▶ Universal properties  $F[x]$  in  $T_A$ :

$$\forall i. F[a[i]]$$

- ▶ Bounded universal properties  $F[x]$  in  $T_A^{\mathbb{Z}}$ :

$$\forall i. \ell \leq i \leq u \rightarrow F[a[i]]$$

- ▶ Bounded and unbounded sorted arrays  $\text{sorted}(a, \ell, u)$  in  $T_A^{\mathbb{Z}} \cup T_{\mathbb{Z}}$  or  $T_A^{\mathbb{Z}} \cup T_{\mathbb{Q}}$ :

$$\forall i, j. \ell \leq i \leq j \leq u \rightarrow a[i] \leq a[j]$$

- ▶ Partitioned arrays  $\text{partitioned}(a, \ell_1, u_1, \ell_2, u_2)$  in  $T_A^{\mathbb{Z}} \cup T_{\mathbb{Z}}$  or  $T_A^{\mathbb{Z}} \cup T_{\mathbb{Q}}$ :

$$\forall i, j. \ell_1 \leq i \leq u_1 < \ell_2 \leq j \leq u_2 \rightarrow a[i] \leq a[j]$$