Formal Methods in Computer Science

Block 2: Satisfiability problems

From Uninterpreted Functions to Equality Logic

WS 2013

Ackermann's Reduction

(on page 67 in D.Kroening, O. Strichman. Decision Procedures, Springer, 2008)

Algorithm: ACKERMANN'S-REDUCTION

Input: An EUF-formula φ^{EUF} with k uninterpreted functions $F^{(1)}, \ldots, F^{(k)}$ of arity > 0. For each $F^{(l)}$ $(1 \leq l \leq k)$, m_l instances occur in φ^{EUF}.

Output: An equality logic formula φ^E such that φ^E is valid if and only if φ^{EUF} is valid.

1. Assign indices to the uninterpreted function instances from subexpressions outwards (separately for each function symbol). Denote by $F_i^{(l)}$ the instance $F^{(l)}$ that is given the index i. Denote by $arg(F_i^{(l)})$ the argument(s) of $F_i^{(l)}$.
2. Let $\mathit{flat}^E(\varphi^{EUF}) := \mathcal{T}(\varphi^{EUF})$, where $\mathcal{T}$ is a function that takes an EUF-formula (or term) as input and transforms it to an equality formula (or term respectively) by replacing each uninterpreted function instance $F_i^{(l)}$ with a new term variable $f_i^{(l)}$. In the case of nested functions, only the variable corresponding to the most external instance remains. Constants and variables remain unchanged under $\mathcal{T}$.
3. Let $FC^E_{F^{(l)}}(\varphi^{EUF})$ denote the following conjunction of functional consistency constraints for a function symbol $F^{(l)}$:

   $$FC^E_{F^{(l)}}(\varphi^{EUF}) := \bigwedge_{i=1}^{m_l-1} \bigwedge_{j=i+1}^{m_l} (\mathcal{T}(arg(F_i^{(l)})) \doteq \mathcal{T}(arg(F_j^{(l)}))) \rightarrow f_i^{(l)} \doteq f_j^{(l)}.$$

   If the arity of $F^{(l)}$ is > 1, then read $(s_1, \ldots, s_n) \doteq (t_1, \ldots, t_n)$ as $\bigwedge_{p=1}^{n}(s_p \doteq t_p)$.
4. Let $FC^E(\varphi^{EUF})$ be $\bigwedge_{l=1}^{k} FC^E_{F^{(l)}}(\varphi^{EUF})$. Moreover, let

   $$\varphi^E := FC^E(\varphi^{EUF}) \rightarrow \mathit{flat}^E(\varphi^{EUF}).$$

   Return φ^E.

Bryant's Reduction

(on page 70 in D.Kroening, O. Strichman. Decision Procedures, Springer, 2008)

Algorithm: BRYANT'S-REDUCTION

Input: An EUF-formula φ^{EUF} with m instances of an uninterpreted function F.

Output: An equality logic formula φ^{E} such that φ^{E} is valid if and only if φ^{EUF} is valid.

1. Assign indices to the uninterpreted function instances from subexpressions outwards. Denote by F_i the instance F that is given the index i, and by $arg(F_i)$ its argument(s).
2. Let $\mathit{flat}^E(\varphi^{EUF}) := \mathcal{T}^*(\varphi^{EUF})$, where $\mathcal{T}^*$ is a function that takes an EUF-formula (or term) as input and transforms it to an equality formula (or term respectively) by replacing each uninterpreted function instance F_i with a new term variable F_i^* (in the case of nested functions, only the variable corresponding to the most external instance remains). Constants and variables remain unchanged under $\mathcal{T}^*$.
3. For $i \in \{1, ..., m\}$, let f_i be a new variable. Let
$$F_i^* \doteq \left(\begin{array}{lllcl} \mathit{case} & \mathcal{T}^*(arg(F_1)) & \doteq & \mathcal{T}^*(arg(F_i)) & : & f_1 \\ & \vdots & & \vdots & & \vdots \\ & \mathcal{T}^*(arg(F_{i-1})) & \doteq & \mathcal{T}^*(arg(F_i)) & : & f_{i-1} \\ & TRUE & & & : & f_i \end{array} \right)$$
be a case statement (as defined in the lecture slides) and let
$$C(F_i^*) := \bigvee_{j=1}^{i} \left(F_i^* \doteq f_j \wedge \mathcal{T}^*(arg(F_j)) \doteq \mathcal{T}^*(arg(F_i)) \wedge \bigwedge_{k=1}^{j-1} \mathcal{T}^*(arg(F_k)) \not\doteq \mathcal{T}^*(arg(F_i))\right)$$
be the associated formula.
Finally, let
$$FC^E(\varphi^{EUF}) := \bigwedge_{i=1}^{m} C(F_i^*).$$
4. Let
$$\varphi^E := FC^E(\varphi^{EUF}) \rightarrow \mathit{flat}^E(\varphi^{EUF}).$$
Return φ^E.

Remarks:

- The generalization to more function symbols and to function symbols with arity > 1 works as in Ackermann's reduction.
- In the aforementioned book, there are two small errors, which we corrected:
    1. In the case statement we replaced the wrong statements of the form $arg(F_j^*)$ by the correct ones of the form $arg(F_j)$.
    2. In the definition of $FC^E(\varphi^{EUF})$ we replaced the wrong statement of the form F_i^* by the correct one of the form $C(F_i^*)$.