Array Fold Logic Proof

October 20, 2020

Overview

- Overview of the proof.
- Proof of Complexity.
- Decision Procedure.

Definitions

Definition (SMC)

A symolic k-counter machine is a tuple $\mathcal{M} = (\eta, X, Q, \delta, q^{init})$, where $\delta \subseteq Q \times \mathrm{CC}_k(X) \times \mathtt{IC}(X) \times Q \times \mathbb{Z}^k$.

Definition (Translation)

We define a translation of a functional constant f of $\mathtt{FSort}^m$ as an SCM $\mathcal{M}(f) = (\eta, X, Q, \delta, q^{init})$. Let $G = \langle S, E, \gamma \rangle$ be the edge-labeled graph of f, then the translation...

Definitions

Definition 3. *The parallel composition (product) of two SCMs* $\mathcal{M}_1$ *and* $\mathcal{M}_2$*, where* $\mathcal{M}_i = (\boldsymbol{\eta}_i, X_i, Q_i, \delta_i, q_i^{\text{init}})$*, is an SCM* $\mathcal{M} = (\boldsymbol{\eta}, X, Q, \delta, q^{\text{init}})$ *such that:*

- $\boldsymbol{\eta} = \boldsymbol{\eta}_1 \boldsymbol{\eta}_2$,
- $X = X_1 \cup X_2$,
- $Q = Q_1 \times Q_2$,
- *for each pair of transitions* $(q_i, \alpha_i, \beta_i, p_i, \boldsymbol{w}_i) \in \delta_i$*, where* $i = 1..2$*, there is the transition* $\big((q_1, q_2), \alpha_1 \wedge \alpha_2, \beta_1 \wedge \beta_2, (p_1, p_2), \boldsymbol{w}_1 \boldsymbol{w}_2\big) \in \delta$*, which are the only transitions in* δ*,*
- $q^{\text{init}} = (q_1^{\text{init}}, q_2^{\text{init}})$.

Small model property

Lemma

There exists a constant $c \in \mathbb{N}$*, such that an AFL formula* Φ *is satisfiable iff there exists a model* σ *it maps each variable in* X *to integer that* $\leq 2^{|\Phi|^c}$ *and array to sequence of* $\leq 2^{|\phi|^c}$ *where each integer of the array also lies in the bound.*

Complexity

Theorem

The satisfiability problem of AFL is **PSPACE***-complete.*

- Membership: If the small model property holds, an NTM can
  - nondeterministically guess variable use space of $|\Phi|^c$ bits.
  - guess one-by-one the value of $2^{|\Phi|^c}$ array cells and use $|\Phi|^c$ bits to count the current index.
  - due to the bound of the variable and the bound of length, the counter value of fold is also bounded in poly.

  Then a NTM can simulate the SAT problen in PSPACE.
- Hardness: Reduce the emptiness problem of intersection of DFAs to this problem.

$$\bigcap_{i=1}^{n} \mathcal{L}(A_i) \neq \emptyset$$

A_i can be simulated by $fold_a^i$ with a single counter: What is the alphabet? What is accept? Why this work?
Intersection of folds.

Proof of Small Model Lemma