Array Fold Logic Proof

October 20, 2020

Overview

- Overview of the proof.
- Proof of Complexity.

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* $\mathcal{M}_i = (\boldsymbol{\eta}_i, X_i, Q_i, \delta_i, q_i^{\mathrm{init}})$*, is an SCM* $\mathcal{M} = (\boldsymbol{\eta}, X, Q, \delta, q^{\mathrm{init}})$ *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*,*
- $q^{\mathrm{init}} = (q_1^{\mathrm{init}}, q_2^{\mathrm{init}})$.

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 problem in **PSPACE**.
- Hardness: Reduce the emptiness problem of intersection of DFAs which is **PSPACE**-complete 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 accepting? Why this work?

Proof of Small Model Property

Given a array a and a assignment σ, assume σ satisfiy ϕ.
Let $s = |\psi| \leq 3|\phi|$.

$$\mathcal{R} = \{[0, c_1], [c_1, c_1], [c_1 + 1, c_2 - 1], [c_2, c_2], \ldots, [c_l, +\infty]\}$$

Size of $\mathcal{R}$: $2dim(\mathbf{c}) + 1 \leq 3s$.
A *mode*: is a tuple in $\mathcal{R}^k$ that describes the region of each counter.
Reversal-bounded: $\mathcal{M}$ is reversal-bounded, then any run can traverse at most $max = r \cdot k \cdot |\mathcal{R}| \leq \mathcal{O}(s^3)$ different modes.
Take an accepting run $Tr = Tr_1 \cdots Tr_{max}$ of $\mathcal{M}$.
The property of $Tr_i = \delta_m, \cdots, \delta_n$. How to modify Tr_i to get $\bar{T}r_i, Tr_i^*$.

Proof of Small Model Property

The satisfiability of ϕ then can be translated into a LP problem $\mathbf{LP} = \bigwedge_{i=1}^{5} \mathbf{LP}_i$, where
$\mathbf{LP}_1$:

$$z_{i,j} = w_{i,j} + \bar{b}_{i,j} + \sum_{m=1}^{|S_i^=|} b_{i,j,m}\ y_{i,m},$$

$$w_{i+1,j} = z_{i,j} + b_{i,j}^{+}$$

$\mathbf{LP}_2$: not fold(copy of variables).
$\mathbf{LP}_3$: link fold and not fold.
$\mathbf{LP}_4$: bound of counters.
$\mathbf{LP}_5$: all input constraint in Tr are satisfiable.
Then we get an LP problem, which by [1] the model is bounded.
[1]C. H. Papadimitriou. On the complexity of integer programming.