The Complexity of Model Checking Multi-Stack Systems

Benedikt Bollig[1] Dietrich Kuske[2] Roy Mennicke[2]

[1]LSV, CNRS and ENS de Cachan, France

[2]Technische Universität Ilmenau, Germany

November 16, 2012

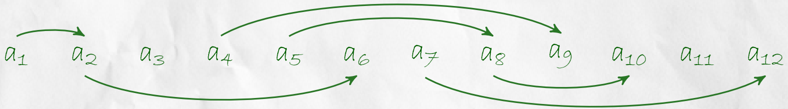
Multiply Nested Words

Concurrent programs with recursive procedure calls can be modelled by pushdown automata with multiple stacks.

An execution of a multi-stack system can be considered as a word with multiple nesting relations.

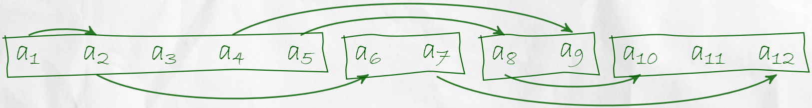
Each edge of a nesting relation relates a push (procedure call) with its matching pop (return).

For example, consider the following 2-nested word:



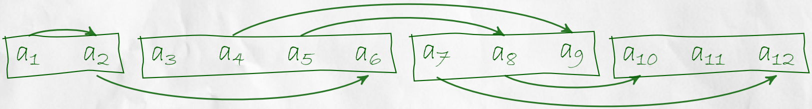
The first (second) nesting relation is represented by the upper (lower) edges.

Phase-Boundedness (La Torre, Madhusudan, Parlato '07)



A phase is an interval within a nested word in which all returns refer to the same nesting relation.

A nested word is a τ-phase nested word if it can be divided into τ many phases.



Hence, the above example nested word is a 4-phase NW.
However, it is no 3-phase nested word since no two of the positions 2, 6, 8, and 10 can belong to a phase.

MSO Formulas

The class of MSO(Γ,σ)-formulas is given by the following grammar

$$\begin{aligned}\varphi ::= P_a(x) \mid x \lessdot y \mid x \prec_s y \mid x = y \mid x \in Z \\ \mid \mathrm{call}_s(x) \mid \mathrm{return}_s(x) \mid \min(x) \mid \max(x) \\ \mid \neg\varphi \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \exists x : \varphi \mid \forall x : \varphi \mid \exists Z : \varphi \mid \forall Z : \varphi\end{aligned}$$

where a ranges over Γ and s ranges over $\{1, \ldots, \sigma\}$.

We define the monadic quantifier alternation hierarchy:

$\mathrm{M}\Sigma_n(\Gamma,\sigma)$ is the set of all formulas $\exists \overline{Z}_1 \forall \overline{Z}_2 \ldots \exists/\forall \overline{Z}_n : \psi$ where $\overline{Z}_i$ are tuples of individual and set variables and ψ is a first-order formula.

MSO-definable Temporal Logics

The existential until construct $(\varphi \, \mathsf{EU} \, \psi)$ is $\mathrm{M}\Sigma_1(\Gamma,\sigma)$-definable. It claims the existence of a path $x_0, x_1, \ldots, x_n$ starting at the current position x_0 s.t. x_n satisfies ψ and φ holds at x_i for all $1 \leq i < n$.

$$[\![\mathsf{EU}]\!](Z_1, Z_2, x) = \exists P\colon \left[\begin{array}{l} P \cap Z_2 \neq \emptyset \wedge P \subseteq Z_1 \cup Z_2 \wedge x \in P \\ \wedge \forall y \in P\colon (x = y \vee \exists z\colon (z \in P \wedge z \lessdot y)) \end{array} \right]$$

An MSO(Γ,σ)-definable temporal logic is a temporal logic whose modalities are MSO(Γ,σ)-definable.

Let TL be an MSO(Γ,σ)-definable temporal logic.

Bounded Satisfiability Problem of TL

Input: formula F from TL and phase bound $\tau \in \mathbb{N}$

Question: Is there a τ-phase σ-nested word satisfying F?

If τ is fixed, then it is decidable in EXPTIME (Bollig, Cyriac, Gastin, Zeitoun '11).

Lower Bound: Labelled Grids

Let $TL^{\mathcal{G}}$ be an $MSO^{\mathcal{G}}(\Gamma)$-definable temporal logic over grids.

Bounded Satisfiability Problem of $TL^{\mathcal{G}}$

Input: formula F from $TL^{\mathcal{G}}$ and $m \in \mathbb{N}$

Question: Is there a labelled grid with m columns satisfying F?

Theorem

For every $n > 0$ and alphabet Γ with $|\Gamma| \geq 2$, there exists an $\mathrm{M}\Sigma_n^{\mathcal{G}}(\Gamma)$-definable temporal logic $TL^{\mathcal{G}}$ over labelled grids whose bounded satisfiability problem is n-EXPSPACE-hard.

Idea: Let M be a Turing machine solving an n-EXPSPACE-hard problem. We reduce the word problem of M to the bounded satisfiability problem of some $\mathrm{M}\Sigma_n^{\mathcal{G}}(\Gamma)$-definable temporal logic over labelled grids.

Core of the proof: Encoding of large counters using formulas of low monadic quantifier alternation depth (cf. Kuske and Gastin '10).

Lower Bound: Representing Grids by NWs

Labelled grid G over alphabet Γ:

a_1	a_2	a_3
a_4	a_5	a_6
a_7	a_8	a_9

Representation of G as 2-nested word over $\Gamma \uplus \{\perp\}$:

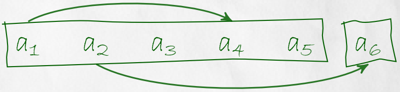
$$a_1 \; a_4 \; a_7 \; \perp \; \perp \; \perp \; a_2 \; a_5 \; a_8 \; \perp \; \perp \; \perp \; a_3 \; a_6 \; a_9$$

Theorem

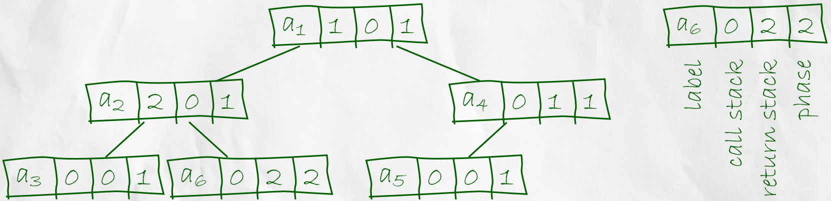
For all $n > 0$, alphabets Γ with $|\Gamma| \geq 3$, and $\sigma > 1$, there is an $\mathrm{M}\Sigma_n(\Gamma, \sigma)$-definable temporal logic whose bounded satisfiability problem is n-EXPSPACE-hard.

Upper Bound: Representing NWs by Trees

2-phase 2-nested word ν:

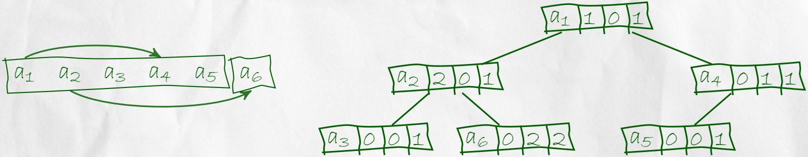


The tree t_ν representing ν:



Theorem (La Torre, Madhusudan, and Parlato '07)
From $\tau \in \mathbb{N}$, one can construct in time $\text{tower}_2(\text{poly}(\tau))$ a tree automaton recognizing the set of all tree representations of τ-phase σ-nested words.

Upper Bound: From Formulas to Tree Automata



Let $\varphi(x_1,\ldots,x_k,Z_1,\ldots,Z_\ell)$ be an MSO(Γ,σ)-formula and $\tau \in \mathbb{N}$.
We want to construct a "small" tree automaton $\mathcal{A}$ such that
$(t_\nu,x_1,\ldots,x_k,Z_1,\ldots,Z_\ell) \in L(\mathcal{A})$ iff $\nu,x_1,\ldots,x_k,Z_1,\ldots,Z_\ell \models \varphi$
for all τ-phase σ-nested words ν.

For this, we construct tree automata for all (negated) atomic formulas in space polynomial in τ.

This is quite easy for the following atomic formulas:

- $\mathrm{call}_s(x)$
- $\mathrm{return}_s(x)$
- $x \prec_s y$
- $\min(x)$
- $P_a(x)$
- $x \in Z$
- $x = y$

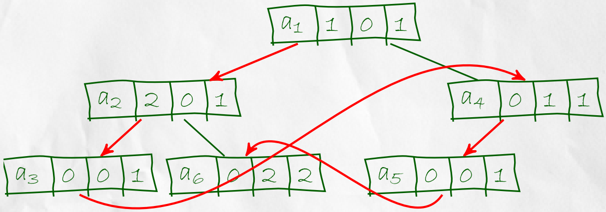
It is also easy to transform the negations of the above formulas.

Upper Bound: Recovering the Relation $\lessdot$

La Torre, Madhusudan, Parlato '07: $\neg(x \lessdot y)$ and $\neg\max(x)$

Remaining: $x \lessdot y$ and $\max(x)$

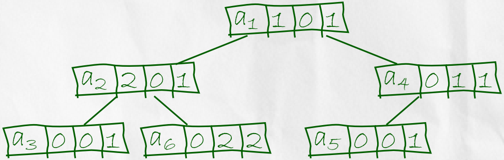
Recovering the direct successor relation is quite difficult.



Upper Bound: Characterizing $\leq$

We define a new characterisation of the order relation $\leq = (\lessdot)^*$ of a nested word ν in the tree t_ν.

Let v be a node of t_ν. The phase word pw(v) of v is the sequence of the phases on the path from the root of t_ν to v where repetitions are deleted.



We define a strict partial order on phase words: $(s_1, \ldots, s_m) \sqsubset (t_1, \ldots, t_n)$ iff

- $s_m < t_n$
- $s_m = t_n$ and $(s_1, \ldots, s_{m-1}) \sqsupset (t_1, \ldots, t_{n-1})$

For instance, $(1, 2, 4) \sqsubset (1, 5)$ and therefore $(1, 2, 4, 6) \sqsupset (1, 5, 6)$.

If x and y are positions and $pw(x) \sqsubset pw(y)$, then $x < y$ (because nesting edges may not intersect each other).

Upper Bound: Characterizing $\leq$

Lemma

Let ν be a τ-phase σ-nested word, x, y be positions. Then $x < y$ iff

(1) $pw(x) \sqsubset pw(y)$

(2) $pw(x) = pw(y)$ and x is a predecessor of y in t_ν

(3) $pw(x) = pw(y)$ and there exist positions z, x', y' such that $x' \neq y'$, x' and y' are children of z, x' is a predecessor of x and y' one of y, and x' is left child of z $\iff$

$(|pw(x)| - |pw(z)|$ even iff x' and y' belong to the same phase$)$

This allows us to construct tree automata for $x < y$ and $\max(x)$ in polynomial space.

We save one exponent timewise compared to La Torre, Madhusudan, Parlato.

Upper Bound

Theorem

Let TL be an $\mathsf{M\Sigma}_n(\Gamma, \sigma)$-definable temporal logic. A formula F from TL can be transformed in polynomial time into an equivalent formula (over nested words)

$$\psi = \exists Z(\neg\psi_1(Z) \wedge \forall x\, \psi_2(x, Z))$$

such that, for all $i \in \{1, 2\}$, ψ_i is of the form $\exists Z_1 \forall Z_2 \ldots \exists/\forall Z_n : \varphi$ where φ is quantifier-free.

Proof uses Hanf's locality principle and exploits the fact that every position has at most one preceding (resp. succeeding, matching return, and matching call) position.

Theorem

Let $n \geq 0$ and TL be some $\mathsf{M\Sigma}_n(\Gamma, \sigma)$-definable temporal logic. The bounded satisfiability problem of TL is in $(n+2)$-EXPTIME (where τ is encoded in unary).

Conclusion

We showed that the bounded satisfiability problem of every $M\Sigma_n(\Gamma, \sigma)$-definable temporal logic is solvable in $(n+2)$-EXPTIME.

We provided, for each level n, a temporal logic whose bounded satisfiability problem is n-EXPSPACE-hard.

Future Work:

- close the gap between the lower and upper bounds
- consider other under-approximation concepts for nested words (like bounded split-width recently introduced by Cyriac, Gastin, and Narayan Kumar)
- investigate the complexity of model checking message-passing automata using MSO-definable temporal logics